CORA Cork Open Research Archive
Cartlann Taighde Oscailte Chorcaí

Title	Smartphone and mobile technology for the communication of patient data
Authors	John, Bernadette
Publication date	2024
Original Citation	John, B. 2024. Smartphone and mobile technology for the communication of patient data. PhD Thesis, University College Cork.
Type of publication	Doctoral thesis
Rights	© 2024, Bernadette John. - https://creativecommons.org/licenses/by-nc-nd/4.0/
Download date	2026-11-01 16:32:11
Item downloaded from	https://hdl.handle.net/10468/17557



UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

Ollscoil na hÉireann, Corcaigh
National University of Ireland, Cork



Smartphone and mobile technology for the communication of patient data

Thesis presented by

Bernadette John
BSc (Hons), PG Dip, RGN, RH, PHN

ORCID: 0000-0002-7610-7731

A Thesis Submitted to the College of Medicine and Health of University College Cork for the Degree of
Doctor of Philosophy

School of Dentistry
University College Cork
November 2024

Head of School: Professor Paul Brady

Supervisors: Professor Anthony Roberts, Dr Christine McCreary and Professor Ciara Heavin

DECLARATION

This is to certify that the work submitted herein is my own and has not been submitted for another degree, either at University College Cork or elsewhere. All external references and sources are clearly acknowledged and identified within the contents. I have read and understood the regulations of University College Cork concerning plagiarism and intellectual property.



Bernadette A. John

ABSTRACT

The widespread use of Bring Your Own Device (BYOD) personal smartphones, Instant Messaging (IM) and third-party apps has made these technologies compelling and ubiquitous for efficient communication among clinicians facilitating patient care. However, the sensitivity of patient information necessitates secure, General Data Protection Regulation (GDPR) compliant digital channels that prevent unauthorised access and ensure confidentiality. This is a series of studies forming a thesis addressing the research question: *How do / should clinicians use smartphone technologies to communicate patient data?*

Objectives

There are four objectives for this thesis:

1. To evaluate the available literature on the use of personal smartphone technology for communication between clinicians.
2. To determine the current usage of smartphones and mobile technology among clinicians in Ireland (and UK).
3. To evaluate the current guidelines that are available to inform practice-based communication between clinicians using personal BYOD smartphones, IM and third-party Apps in Ireland and the UK.
4. To develop & evaluate a toolkit to assist clinicians in their assessment of the available guidelines regarding communication using smartphone technologies.

METHODS

A range of methods were employed to achieve these objectives, including two scoping literature reviews, an online quantitative survey, two focus group sessions, as well as user testing and statistical analysis.

Objective 1

A scoping review was conducted to assess the literature regarding the use of smartphone technology for communications between clinicians with a focus on data privacy, security and regulatory compliance. Two separate systematic searches were conducted across selected academic databases, targeting publications from 2016 onwards, reflecting the GDPR implementation period, in June and October of 2020. The review included studies, editorials, and grey literature, all focusing on clinician-to-clinician communication using smartphone applications within the EU, but also included relevant international research. The Joanna Briggs Institute (JBI) framework was followed, with search results reported as per the PRISMA ScR for scoping reviews guidelines.

Objective 2

An online quantitative survey was conducted via weblink between May 2020 and March 2021, to determine the current use of personal smartphone technology for communications in healthcare in Ireland and the UK amongst dental professionals and the wider dental profession. The questionnaire was a blend of 38 open and closed style questions to determine the perception and knowledge of potential pitfalls, risks and limitations of these technologies among dental professionals.

Objective 3

A scoping literature review was conducted to identify and explore existing guidance informing clinical communications using personal BYOD, IM and third-party apps in Ireland and the UK in Spring 2024. Academic databases were searched, searches of professional entities' websites, including trade unions, regulators, two national health systems, and several employers were conducted, and direct inquiries were made to 69 professional entities.

Objective 4

The artefact was developed using an Action Design Research (ADR) approach, following iterative cycles of Diagnosis, Design, Implementation, and Evolution. The methodology involved gathering insights from IS literature, including Data Quality Dimensions (DQDs), to create a framework that addresses data security, confidentiality, and regulatory compliance in digital communications. Experienced clinicians and senior clinical students were actively involved in cycles to refine the DDA, ensuring it aligned with real-world clinical needs.

RESULTS

Objective 1

The scoping review revealed that clinicians widely use apps such as WhatsApp, Zoom, and Facebook Messenger for sensitive communications between each other. However, these channels are frequently non-compliant with GDPR, raising significant concerns regarding patient privacy and data security. The review highlighted a lack of sufficient governance, technical safeguards, and awareness among clinicians regarding secure use in the literature, pointing to essential knowledge gaps in implementing compliant communication practices in healthcare.

Objective 2

A total of 123 responses were received from dental professionals in the Republic of Ireland (RoI) and 77 responses from dental professionals in the UK. The majority of dental professionals confirmed that they were aware of the risks associated with smartphone use for communicating clinical data and perceived that they were adequately skilled in digital professionalism. However, concerning practices regarding the communication of sensitive patient data were identified, with the potential for patient data to be stored on insecure devices and cloud servers. Many ROI and UK dental professionals confirmed that they would need support to remove patient-identifying data when ‘trading in’ their device.

Objective 3

The review identified 18 guideline papers that generally acknowledge the importance of secure communication among clinicians. However, a lack of information on the appropriate selection or configuration of the popular technologies was evident.

Objective 4

The artefact was refined through repeated testing and feedback cycles, involving experienced clinicians and senior students in evaluating its usability and relevance. The tool highlighted areas where existing guidelines lacked clarity on secure communication practices, helping clinicians identify gaps in guidance and improve their understanding of secure data handling. Cohen's Kappa coefficient scores from user testing revealed a wide variation in the level of accuracy by reviewers across papers and also between reviewers, with scores ranging between >0.2 (fair) and >0.6 (substantial).

CONCLUSIONS

Objective 1

The findings signpost a requirement for advice, policy, regulation and training to ensure safe and secure use of digital communication tools for communication in clinical practice. The lack of acknowledgement of compliance and security measures in the literature suggests a requirement for dedicated resources to address these gaps, support clinician awareness, and align practice with legal requirements.

Objective 2

App and BYOD smartphone ownership among dental professionals for clinical communications is widespread in the RoI (and UK), with respondents using their devices to send images (photos and radiographs) to one another. However, the risks of such activities are only partly acknowledged, with many having a lack of insight into data security and data privacy.

Objective 3

Most guidelines emphasise general security and data protection standards rather than providing clear actionable recommendations for technology use, thereby leaving a significant gap in technical guidance for clinicians.

Objective 4

Findings indicate that while the artefact proved valuable for assessing the quality of guidance on the use of digital tools for clinical communication has the potential to aid decision-making, it is dependent on the quality of input data. This input can vary significantly between users, potentially affecting its consistency and accuracy. The iterative design process ensured that the tool is both clinically applicable and accessible, to effectively promote better decision-making around secure patient communication. The study highlights the role of precise, high quality actionable data in clinical guideline development and the need for continuous education and decision support for clinicians using BYOD digital technologies.

PEER REVIEWED PUBLICATIONS FROM THIS THESIS

- **John B., McCreary C., Roberts, A.,** (2022) Smartphone Technology for Clinical Communication in the COVID-19 Era: A Commentary on the Concerning Trends in Data Compliance. Frontiers in Digital Health. 2022 Mar 22:4:816604. DOI: 10.3389/fdgth.2022.816604. eCollection 2022. **Publication 1. Chapter 1. (Appendix 1)**
- **John, B., McCreary, C. and Roberts, A. (In press)** 'Digital Communication'. In Jenkinson, J. and Woolward, J. (eds.) *A Clinician's Brief Guide to Communication Skills in 21st Century Psychiatry*. Cambridge: Cambridge University Press. **Publication 2. Chapter 1. (Appendix 2)**
- **John B., McCreary C., Roberts, A.,** (2022) Smartphone Technology for Communications between clinicians – A Scoping Review. Journal of Dentistry, Vol. 1222, pp. 1-13, July 2022, DOI: https://doi.org/10.1016/j.jdent.2022.104112 **Publication 3, Chapter 3. (Appendix 3)**
- **B. John, McCreary C., Roberts A.,** (2023) Smartphone and mobile technology use among the dental profession. Journal of the Irish Dental Association. January 2023. (PP 2 – 6) DOI: 10.58541/001c.67927 **Publication 4, Chapter 4.** (**Appendix 4)**
- **John, B., McCreary, C., Wilcox, A., Roberts, A**. (2021) Smartphone clinical communication amongst Irish Dental Professionals**.** Conference Presentation**,** IADR - Irish Division. Online. 5th February 2021. **Publication 5, Conference presentation. Chapter 4. (Appendix 5)**
- **John, B., Heavin, C., Roberts, A.** (2025) Navigating the Wild West: A Review of Guidance on Clinical Communications using personal BYOD, IM and Third-Party Apps in the UK and Ireland. Frontiers in Digital Health, 2024, 6, DOI: https://doi.org/10.3389/fdgth.2024.1457848 **Publication 6, Chapter 5.**

PAPER SUBMITTED TO JOURNAL FOR PEER REVIEW & PUBLICATION

- **John, B., Heavin, C., Roberts, A.** (Submitted 9th October, 2024) Designing a Data Dimensions Artefact for the use of BYOD, IM and third-party app-based technology by clinicians: An Action Design Research Approach. **Submitted to:** Journal of Decision Systems. **Publication 7. Chapter 6.**

ACKNOWLEDGEMENTS

I would like to express my gratitude to everyone who supported me throughout my PhD journey. This thesis would not have been possible without their guidance, patience and encouragement.

First and foremost, I am profoundly grateful to my three supervisors, Dr Christine McCreary, Prof Anthony Roberts and Prof Ciara Heavin. Your support, expert guidance and constructive feedback have been invaluable.

I would like to thank Prof Declan Millet for his patience and encouragement.

I would also like to extend my heartfelt thanks to my husband, Simon. His constant support, understanding and patience during the highs and lows of this have been invaluable. Thank you for always believing in me and for your unconditional love and encouragement.

A special thank you goes to Anita Wilcox, a retired librarian from University College Cork, whose encouragement and insightful advice have been a great source of motivation. Her passion for knowledge and her kindness have inspired me throughout this process.

Finally, I am grateful to all my friends, colleagues, and the staff members including Mary Keelan, Neil Nash and the students at UCC who have offered their support and time to contribute to the research. Your encouragement and friendship have made this journey more manageable and fulfilling.

Thank you all for your contributions to my academic and personal growth.

THE IMPACT OF THE COVID-19 PANDEMIC ON THIS THESIS

The COVID-19 pandemic had a significant impact on my experience as a remote doctoral student and on the progression and scope of this thesis. Prior to the onset of the pandemic, I had been actively engaged in presenting and teaching at professional gatherings such as The British Dental Association, The British Association of Oral Surgeons and the Royal College of Surgeons of Edinburgh, where I was regularly invited to speak on issues regarding digital professionalism, information governance, and the risks to professionalism and data security posed by the use of personal technology by clinicians for communication between each other concerning patient care. I had anticipated leveraging these in-person engagements to circulate the survey tool with large, audiences of multidisciplinary clinicians, with a view to generating a wider dataset suitable for statistical analysis and hypothesis testing across Ireland and the UK. However, lockdown measures and the subsequent cancellation of in-person teaching and presentations disrupted these plans, sharply curtailing my opportunities to both gather data and collate early feedback from clinical stakeholders.

Additionally, access to research subjects became increasingly restricted as healthcare professionals faced unprecedented pressures, redeployments, and, in some cases, temporary cessation of their clinical practice. These constraints directly affected my ability to recruit participants for aspects of my study that sought to examine real-world use of personal digital technologies (e.g., BYOD and IM) for clinical communication. While I was able to adapt elements of the study design to accommodate these limitations, the impact on potential data richness and the generalisability of findings was unavoidable.

On a personal level, studying remotely as a mature student was already a challenging undertaking, and the isolating effects of the pandemic further exacerbated this. I was unable to establish or access a supportive peer network at the university, which meant that informal opportunities for collaboration, exchange of ideas, and reassurance were largely absent. This isolation presented both emotional and academic challenges over the course of the research.

The pandemic had a wider impact on the scholarly publishing environment. As the academic and clinical communities responded to COVID-19, it was widely reported that many journals were inundated with submissions as some doctoral students who were now unable to access research subjects instead focused their attention on library projects and literature reviews towards producing PhDs by publication. This

created increased competition for space in relevant publications and delays affecting the timeline for dissemination of the work.

The pandemic also created considerable barriers to engaging with patients and the public. While the importance of incorporating the patient voice into digital health tool development is widely recognised, the challenges of remote research and restricted contact with healthcare services meant that the inclusion of patient focus groups or other participatory activities was not feasible during the first phase of this study. I acknowledge that, as clinicians engage with sensitive patient data, patients themselves must have an active voice in the development of decision-support tools such as the toolkit. In future iterations of the toolkit, patient involvement will be prioritised in both design and evaluation phases, in alignment with principles of co-production and transparency in digital health innovation.

TABLE OF CONTENTS

LIST OF TABLES **1**
LIST OF FIGURES **1**
CHAPTER 1 SMARTPHONE TECHNOLOGY FOR CLINICAL COMMUNICATION IN THE COVID-19 ERA: A COMMENTARY ON THE CONCERNING TRENDS IN DATA COMPLIANCE **5**
1.1 INTRODUCTION **6**
1.2 CLINICAL COMMUNICATIONS, SMARTPHONE TECHNOLOGY AND APPS **7**
1.3 DIGITAL PROFESSIONALISM **7**
1.4 RECORD KEEPING AND CLINICAL IMAGES **8**
1.5 DATA SECURITY **9**
1.6 CYBERCRIME **9**
1.7 DATA AS A COMMODITY **10**
1.8 INFORMATION GOVERNANCE **10**
1.9 GDPR AND HUMAN RIGHTS **11**
1.10 CONCLUSION **12**
1.11 DIGITAL COMMUNICATION **13**
1.11.1 CLINICAL COMMUNICATIONS, SMARTPHONE TECHNOLOGY AND APPS 13
1.11.2 DIGITAL PROFESSIONALISM 18
1.11.3 DATA SECURITY AND CYBERCRIME CONCERNS 19
1.11.4 GDPR 20
1.11.5 TRAINING AND GUIDELINES 22
1.12 RESEARCH QUESTION **25**
1.12.1 OBJECTIVES FOR THIS STUDY 25
1.12.2 STRUCTURE OF THE THESIS 25
1.12.3 TERMINOLOGY 27
1.12.4 CANDIDATE'S CONTRIBUTION TO THE PUBLICATIONS 28
CHAPTER 2 METHODOLOGY **29**
2.1 OVERVIEW OF RESEARCH METHODS **29**
2.2 PHASE ONE: SCOPING REVIEWS AND SURVEY **31**
2.3 PHASE TWO: TOOLKIT DEVELOPMENT, TESTING AND EVALUATION **32**
2.4 INTEGRATION AND ANALYSIS **33**
2.4.1 ETHICAL CONSIDERATIONS 34
CHAPTER 3 SMARTPHONE TECHNOLOGY FOR COMMUNICATION BETWEEN CLINICIANS – A SCOPING REVIEW **35**
3.1 ABSTRACT **36**
3.1.1 OBJECTIVES 36
3.1.2 DATA 36
3.1.3 SOURCES 36
3.1.4 STUDY SELECTION 36
3.1.5 CONCLUSIONS 37
3.1.6 CLINICAL SIGNIFICANCE 37
3.2 INTRODUCTION **37**
3.3 METHODS **39**
3.3.1 OVERVIEW 39
3.3.2 OBJECTIVES AND RESEARCH QUESTIONS 39

3.3.3 Identifying relevant studies and eligibility criteria 39
3.3.4 Eligibility criteria 39
3.3.5 Evidence searches 40
3.3.6 Selecting the evidence 43
3.3.7 Data extraction 43
3.3.8 Synthesis of results 44
3.3.9 Risk of bias (quality) assessment 44
3.4 Results 45
3.4.1 Study selection 45
3.4.2 Themes 47
3.5 Discussion 51
3.5.1 Summary of evidence 51
3.5.2 Popular consumer apps for clinical communications 52
3.5.3 GDPR 52
3.5.4 Consent for processing 53
3.6 Conclusion 55
CHAPTER 4 SMARTPHONE AND MOBILE TECHNOLOGY USAGE AMONGST THE DENTAL PROFESSION 57
4.1 Precis 58
4.2 Abstract 58
4.2.1 Statement of the problem 58
4.2.2 Purpose of the study 58
4.2.3 Materials and methods 58
4.2.4 Results 58
4.2.5 Conclusions 59
4.3 Introduction 59
4.4 Materials and methods 60
4.5 Results 61
4.5.1 Respondent Demographics: 62
4.5.2 Current use of smartphones and mobile technology for communicating patient data: 63
4.5.3 Level of perceived risk associated with Smartphone and mobile technology use: 65
4.6 Discussion 66
4.7 Conclusions 69
CHAPTER 5 NAVIGATING THE WILD WEST: A REVIEW OF GUIDANCE ON CLINICAL COMMUNICATIONS USING PERSONAL BYOD, IM AND THIRD-PARTY APPS IN IRELAND AND THE UK 70
***5.1* Abstract 71**
5.1.1 Introduction 71
5.1.2 Methods 71
5.1.3 Results 71
5.1.4 Discussion 72
5.2 INTRODUCTION 72
5.3 METHODS 74
5.3.1 Review Question 75
5.3.2 Eligibility criteria 75
5.3.3 Sources 76
5.3.4 Search Strategy 77

5.3.5 Study/Source of Evidence Selection....77
5.3.6 Data Extraction....77
5.4 Data Analysis and Presentation....79
5.5 RESULTS....80
5.5.1 Communication Best Practice....80
5.5.2 Data Protection, GDPR and Laws....83
5.5.3 Policy Adherence and Training....84
5.5.4 Device Guidance....87
5.5.5 IM and App Use....88
5.6 DISCUSSION....89
5.6.1 Ambiguity and Inconsistency:....89
5.6.2 Adherence to Policies and Training:....91
5.6.3 Technical Guidance for Secure Communication:....91
5.6.4 Limitations....92
5.6.5 Conclusions....93
CHAPTER 6 DESIGNING A DATA DIMENSIONS ARTEFACT FOR THE USE OF BYOD, IM AND THIRD-PARTY APP-BASED TECHNOLOGY BY CLINICIANS: AN ACTION DESIGN RESEARCH APPROACH....94
6.1 Abstract....95
6.2 Introduction....96
6.3 Theoretical Background....97
6.4 Research Approach....101
6.4.1 DDA v1.0: Diagnosis, Design, Implement and Evolution....104
6.4.2 DDA v2.0: Diagnosis, Design, Implement and Evolution....108
6.4.3 DDA v3.0 Diagnosis, Design, Implement, and Evolution....120
6.5 Discussion....121
6.6 Conclusion....128
CHAPTER 7 DISCUSSION....130
7.1 Objective 1: To evaluate the available literature on the use of personal smartphone technology for communication between clinicians....130
7.2 Objective 2: To determine the current use of smartphones and mobile technology among clinicians in Ireland and the UK....133
7.3 Objective 3: To evaluate the current guidelines that are available to inform practice-based communication between clinicians using personal BYOD smartphones, IM and third-party Apps in Ireland and the UK....136
7.4 Objective 4: To develop and evaluate an artefact to assist clinicians in their assessment of the available guidelines regarding communication using smartphone technologies....137
7.5 Cultural Shift and Interdisciplinary Collaboration....139
7.6 Implications for Practice....140
7.6.1 Limitations and Challenges....141
7.7 Synthesis of Findings Across Objectives....142
7.8 Future Research and Recommendations....145
7.9 Key Findings and Contributions....147
CHAPTER 8 CONCLUSION....150
Final Thoughts....151
CHAPTER 9 BIBLIOGRAPHY....155
CHAPTER 10 APPENDICES....169

APPENDIX 1 PAPER 1 169
APPENDIX 2 BOOK CHAPTER 173
APPENDIX 3 PAPER 2 226
APPENDIX 4 PUBLICATION 4, PAPER 3. 237
APPENDIX 5 PUBLICATION 5. PRESENTATION. 242
APPENDIX 6 ABSTRACT, IADR PRESENTATION 251
APPENDIX 7 LETTER OF ACCEPTANCE FROM PUBLISHER FOR BOOK CHAPTER 253
APPENDIX 8 DATA EXTRACTION MICROSOFT SPREADSHEET (CHAPTER 3.) 254
APPENDIX 9 SURVEY TOOL REPUBLIC OF IRELAND 259
APPENDIX 10 SURVEY TOOL UK 276
APPENDIX 11 ENTITIES CONTACTED (PUBLICATION 6, PAPER 4.) 293
APPENDIX 12 DATA DIMENSION ARTEFACT VERSION 1.0 (DDA V1.0) 297
APPENDIX 13 GLOSSARY OF TERMS FOR DATA DIMENSION ARTEFACT 300
APPENDIX 14 DATA DIMENSION ARTEFACT V1.0 (DDA V1.0) INFORMATION SHEET 301
APPENDIX 15 DATA DIMENSION ARTEFACT V2.0 (DDA V 2.0) 310
APPENDIX 16 DATA DIMENSION ARTEFACT V2.0 (DDA V2.0) INSTRUCTION SHEET 313
APPENDIX 17 FOCUS GROUP SCRIPT 322
APPENDIX 18 STUDY SPECIFIC TRAINING 324
APPENDIX 19 ETHICAL APPROVAL (SOCIAL RESEARCH ETHICS APPROVAL FROM UCC) 325

LIST OF TABLES

Table 1: Privacy Decision Making Aid: Video Call Apps (Dutch Supervisory Authority [22]) 16
Table 2: PRISMA ScR Review Checklist 42
Table 3: Age & Gender Demographics of Respondents 61
Table 4: Dental Professional and Employment Demographics 62
Table 5: Current Use of Smartphones & Mobile Technology for Communicating Patient Data .. 64
Table 6: Level of Perceived Risk Associated with Smartphone and Mobile Technology Use 66
Table 7: Snapshot of Data Extraction Form (DEF) 82
Table 8: Results - Publications Coded to Superordinate Themes and Subthemes 85
Table 9: Summary of Revisions to DDA v1.0 108
Table 10: Summary of Qualitative Data Collection regarding DDA v2.0 109
Table 11: Accuracy of Reviewers' Responses 111
Table 12: Summary of Revisions to DDA v2.0 119
Table 13: Data Dimension Artefact (DDA) v3.0 123
Table 14 Next Steps 152

LIST OF FIGURES

Figure 1: Structure of Thesis 26
Figure 2: Mixed Methods Embedded Design 30
Figure 3: PRISMA ScR Flow Diagram, RESULTS (June - October 2020) 46
Figure 4: Illustration of number of papers by positive and negative by year 49
Figure 5: Illustration of number of papers by year and document type 50
Figure 6: Supporting data for number of papers by positive and negative 51
Figure 7: Illustration of data streaming between networked devices via the cloud 68
Figure 8: Study Search Strategy 76
Figure 9: PRISMA ScR Flow Diagram RESULTS (January - March 2024) 78
Figure 10: Publications Mapped to Superordinate Themes 79
Figure 11: Elaborated ADR process (Adapted from Mullarkey & Hevner 2018) 103
Figure 12: Accuracy Score and Strength of Agreement (Landis and Koch 1977) 113
Figure 13: Objectives, Methods, Outputs from this Thesis 153
Figure 14: Key Legislation and PhD study Timeline 154

ABBREVIATIONS AND GLOSSARY OF TERMS

AI Act	Artificial Intelligence Act is a European Union regulation concerning artificial intelligence. It establishes a common regulatory and legal framework for AI within the European Union. It came into force on 1 August 2024, with provisions that shall come into operation gradually over the following 6 to 36 months.
App	Application. Downloadable by a user to a smartphone or computer device
ADR	Action Design Research
Artefact	In this context an artefact is a construct, model or instantiation developed within the field of Information Systems. It is designed to solve specific problems, support decision-making processes, or improve practices through the application of technology and data management principles. Examples of IS artefacts include software applications, data frameworks, and methodologies. The development of IS artefacts often involves iterative cycles of testing and refinement to ensure they effectively meet the needs of users.
Bluetooth	Is a standard for the short-range wireless interconnection of mobile phones, computers and other electronic devices
BYOD	Bring Your Own Device (BYOD) bring your own personally owned technology - phone, laptop, tablet rather than an officially provided device
DDA	Data Dimension Artefact
DQD	Data Quality Dimension
DPC	Data Protection Commission (Ireland)
DSA	The Digital Services Act is an EU regulation adopted in 2022 that addresses illegal content, transparent advertising and disinformation.
EXIF	Exchangeable Image File Format
FOI	Freedom of Information (Act)
GDPR	General Data Protection Regulation (2018) as stipulated for use across the European Union, and currently also being adhered to by the UK
HIPAA	Health Insurance Portability and Accountability Act of 1996 is a United States Act of Congress, stipulating the guidelines by which personally identifiable healthcare information is maintained by the healthcare and healthcare insurance industries and protected from fraud and theft

HSE	Health Service Executive (Ireland)
ICO	Information Commissioner's Office (UK)
IS	Information Systems
IM	Instant Messaging
MDM	Mobile Device Management (MDM) is a software solution that allows IT teams to control, secure and manage mobile devices, including smartphones, tablets and laptops
MFA	Multi Factor Authentication (MFA) is an electronic method of authentication which grants the user access to a digital resource such as an app only after successfully presenting two or more pieces of evidence to an authentication mechanism
NHS	National Health Service (UK)
PDF	Portable Document Format (PDF) is a file format for capturing and sending electronic documents in exactly the intended format
RoI	Republic of Ireland
SAR	Systems Access Request (SAR) is a formal request made to a data controller by an individual for a copy of their personal data (as opposed to original documents) which that data controller holds on that individual. Under Article 15 of the General Data Protection Regulation, you have a right to obtain a copy of any information relating to you which is kept on a computer or on a structured manual filing system or intended for such a system, by any entity or organisation. Making a SAR allows an individual to see what information an entity or company holds on them
Shadow IT	Information technology systems deployed by departments other than the central IT department to bypass the limitations and restrictions that have been imposed by central IT systems. While it can promote innovation and productivity, it can introduce security risks and compliance concerns
Sovereignty of data	Data sovereignty is the idea that data are subject to the laws and governance structures of the nation where they are collected. The concept of data sovereignty is closely linked with data security, cloud computing, network sovereignty and technological sovereignty

Suspicious App	A suspicious or malicious App is an App that potentially acts as malware, that may steal data or harm the device on which it is hosted
Third Party App	An App that was not created by the same party that created the device on which it is hosted. When downloading such Apps it is usually a condition of use that you allow the App to access some functionality as well as access to your data. Generally, this data is used to generate income by allowing targeted advertising, but it can also be used for more harmful purposes if it falls into the wrong hands
Toolkit	The term *toolkit* is used in this thesis to refer to a structured set of resources or guidance designed to support clinical decision-making, data quality assessment, and regulatory compliance in the use of personal digital technologies. The term is used interchangeably with *artefact*, particularly in clinical contexts where *toolkit* is more commonly understood. While *artefact* is the preferred term in the field of Information Systems, where it denotes a construct developed through design science research, the terms are used synonymously throughout this work to reflect both the theoretical and practical applications of the development of the *Data Dimensions Artefact* (DDA)
UK	United Kingdom
Wi-Fi	A facility allowing computers, smartphones, tablets, laptops and other devices to connect to the internet or to communicate with one another wirelessly within a particular area
VPN	A Virtual Private Network establishes a digital connection between your computer and a remote server owned by a VPN provider, creating a point-to-point tunnel that encrypts your personal data, masks your IP address and lets you sidestep website blocks and firewalls on the internet

CHAPTER 1 SMARTPHONE TECHNOLOGY FOR CLINICAL COMMUNICATION IN THE COVID-19 ERA: A COMMENTARY ON THE CONCERNING TRENDS IN DATA COMPLIANCE

A peer reviewed opinion paper publication serves as the foundation for the introduction to this thesis, to provide context, explain why this topic is important, establishing a gap in the knowledge which this study seeks to address (Publication 1, Paper 1 [1]).

This is followed by abridged (to avoid repetition) extracts from book chapter, to enrich and expand on the details presented, adding depth and enhancing the content conveyed in Paper 1. The peer reviewed book chapter (Publication 2) jointly commissioned by the Royal College of Psychiatrists and Cambridge University press, concerns the importance of the security and privacy of sensitive information for professional development, essential considerations fundamental for the effective use of digital channels of communication by clinicians.

- **Copy of the peer reviewed publication: Appendix 1**
- **Copy of the original content (unabridged draft) of book chapter: Appendix 2**
- **Letter of acceptance (received 8th September 2022) from the publisher for the draft book chapter: Appendix 7**

REFERENCES:

John, B., McCreary, C., Roberts, A. (2022) Smartphone Technology for Clinical Communication in the COVID-19 Era: A Commentary on the Concerning Trends in Data Compliance. Front. Digit. Health, 22 March, 2022. Volume 4. https://doi.org.10.3389/fdgth. 2022.816604

John, B., McCreary, C. and Roberts, A. (In press) 'Digital Communication'. In Jenkinson, J. and Woolward, J. (eds.) *A Clinician's Brief Guide to Communication Skills in 21st Century Psychiatry*. Cambridge: Cambridge University Press.

1.1 INTRODUCTION

The COVID-19 global pandemic has rightly been the focus of attention for the healthcare workforce and has accelerated the global proliferation and adoption of smartphone and digital technologies for clinical communication and remote consultation [2, 3]. This is an understandable development as functionality that enables dialogue between clinicians *via* IM applications or apps (e.g., such as WhatsApp and iMessage), and between clinicians and patients through videoconferencing apps (e.g., such as Zoom and Skype), has never been more important. Clinicians have drawn on the familiar and simple to use smartphone technology to overcome the communication barriers required for social distancing, reducing the risks associated with face-to-face contact and optimising efficiencies in healthcare [2], often without adequate training as to potential clinical safety risks or data security incidents. These interventions have often had efficiency of communication at their core but may leave legacy issues that will become apparent as the health emergency passes. These channels have permanently and positively transformed communications, although they also raise professional, ethical, security and legal concerns that are associated with these technologies [4, 5]. Clinicians (and their patients) may be in danger of becoming "*ensnared"* in a web of hidden data harvesting. Busy clinicians using smartphones to communicate effectively within their own healthcare teams or directly with patients, could face negative ramifications of these technologies unless the Information Commissioners Office (ICO; UK) or Data Protection Commission (DPC; Ireland) actively regulate to ensure data compliance within the National Health Service (NHS: UK) or Health Service Executive (HSE; Ireland). This paper explores the contemporary clinical context and regulatory ramifications within which practicing clinicians are operating. It highlights the need for appropriate guidelines, tools, and education in digital health to enable clinicians to practice in an environment where sensitive patient data can be processed and communicated securely with clarity for patients as to how their data might be used.

1.2 CLINICAL COMMUNICATIONS, SMARTPHONE TECHNOLOGY AND APPS

Effective communication is an essential element of good clinical care. However, the traditional methods of communications (e.g., landline telephones, pagers and fax machines) are restrictive. Smartphone technology and communications apps (including IM) have become ubiquitous in society facilitating cost effective and efficient communication on a "one-to-one" or "one-to-many" basis. For clinicians, the functionality facilitates conversations and consultations between colleagues and enables the sharing of (potentially sensitive) supplementary voice recordings, images and video at the "*touch of a button"* with WhatsApp being the most cited IM application in healthcare [4].

Presumably as a consequence of the magnitude of the COVID-19 pandemic combined with inadequate investment in communications infrastructure, clinicians have been encouraged to draw on their BYOD smartphones and apps [6] (e.g., Skype, iMessage, Zoom) for telemedicine activities. Such functionality has positively enabled online / remote consultations, reviews and test result discussions, patient monitoring and clinical photography, including the use of diagnosis apps from smartphone images. The patient journey and the working life of clinicians have improved whilst pragmatically bypassing the need for time-consuming additional training or purchase of costly new technology at a time of crisis. Regrettably, the perceived advantage of familiarity of these technologies, contrasts with usage of BYODs potentially introducing data security risks for clinicians which they may not be aware of due to a lack of education and training. Of course, not all patients have an awareness of such technologies, or own a compatible device generating inequality in availability to digital services.

1.3 DIGITAL PROFESSIONALISM

Digital Professionalism may be defined as "*the competence or values expected of a professional when engaged in social, digital communication and mobile technology"* (amended from Oxford English dictionary definition of professionalism [7]).

There are clear challenges for how health professionals conduct themselves in a rapidly evolving digital landscape. It has been suggested that Digital Professionalism education and learning should begin in undergraduate training, "given its relevance at all levels" [8].

This issue has recently been acknowledged in the latest Curriculum for Graduating European Dentists [9] which has an Intended Learning Outcome:

"*Graduating dentists must demonstrate digital professionalism by protecting patient data and the appropriate use of social media and digital communication, mindful of how these activities may force them into ethically challenging situations and / or damage the reputation of the wider profession."*

This healthcare exemplar challenges education providers to best equip its graduates for the challenges of modern digital society. Our anecdotal experience indicates that clinicians have a broad range of attitude with risky behaviour by busy clinicians on the frontline being a concern.

1.4 RECORD KEEPING AND CLINICAL IMAGES

Record keeping of clinical images and "chat messages" stored on BYOD smartphones shared *via* IM and apps pose a range of serious safety concerns [10]. The clinician initiating a dialogue has responsibilities to ensure that any messages / data and responses are recorded in the patient's notes; IM conversations may be subject to Freedom of Information (FOI) requests or Subject Access Requests (SARs) [11]. However, downloading of the dialogue and any clinical images to store it in the patient notes or digital healthcare record may not be technically possible and even if so, are these data being promptly deleted from the smartphones by all members of the app group? Clinicians may not be aware that smartphones store deleted images in the "*deleted images"* album for 28 days [3]. Further, smartphones must be password protected with image streaming to insecure cloud servers and between networked devices turned "OFF" [3, 11]. The storage of clinical images using insecure cloud servers associated with a BYOD is concerning [4, 11]. Digital images contain additional Exchangeable Image File Format (EXIF) data from geographical co-ordinates to

date, time and device details, so anonymising digital clinical images requires a level of digital literacy that many clinicians do not possess or are unaware of.

1.5 DATA SECURITY

The "minimalisation" of sensitive patient identifiable data is essential when engaged in clinical communications *via* smartphone apps due to concerns regarding data security [11]. Conversely, clear identification of the patient being discussed is necessary for patient safety as communication failure could result in poor clinical outcomes and avoidable errors [12]. The conflict between communication accuracy and patient data security arose pre-COVID-19 with patient care prioritised over the security of patient data [13]. The potential for a security breach of patient data is heightened when IM apps use unregulated servers outside the European economic area (EEA). Lack of compliance with data protection requirements regarding data mining, fair processing, records management, and the technical challenges posed by BYOD, are well documented [4, 11].

1.6 CYBERCRIME

Healthcare is one of the most targeted sectors for cybercrime globally due to its rich data source and perception as a "soft target" [13]. Data vulnerability in healthcare is attributable to limited budgetary resources, fragmented governance, cultural behaviours and through the use of obsolete systems unable to support the latest software / updates [14]. Regrettably, high risk and critical vulnerabilities in healthcare systems are increasingly targeted by ransomware and the COVID-19 pandemic anecdotally resulted in an increase in malicious cybercrime activity. An example was the successful access and exploitation of personal and health data from a major ransomware attack on the HSE on 14th May 2021 [15]. This was a highly significant attack and the largest known against a health service computer system, with massive negative impact on healthcare delivery. Reports that more was paid to ransomware criminals during the first half of 2021 than for the whole of 2020, statistics that could serve as inspiration to other criminals [15] intent on exploiting health systems. A post incident review commissioned by the HSE provided

key learning points for healthcare professions in relation to regular cybersecurity awareness and training for all staff grades [15].

1.7 DATA AS A COMMODITY

The business model for many smartphone and app-based communications channels involves actively commodifying user data from the device, any networked devices (e.g., fitness trackers) and associated cloud storage. The consequences of "data harvesting" by companies such as Meta (owners of WhatsApp and Instagram) and Alphabet (owners of Google, Fitbit, YouTube, Nest) and the "profiling" of individuals by exploiting personal data by companies (e.g., Cambridge Analytica) cannot be underestimated or ignored [16]. Smartphones have the potential to threaten the security of sensitive patient data and yet, "*the opaque nature of online (including mobile app) tracking, along with the use of data held by mobile operators, is beyond the awareness and understanding of many individuals*" [17]. This is acknowledged widely outside of healthcare settings (e.g., auto-manufacturing) where employees are forbidden from using WhatsApp, Snapchat etc. on company issued devices due to data breach concerns [18]. Surveillance by smartphone apps that harvest the sensitive data, is a genuine concern spanning national, EU and international Data Protection, Information Privacy and Human Rights Laws. Clinicians may be inadvertently enabling the long-term exploitation of patients and their data by third parties (e.g., health insurance companies) or through malicious spyware (e.g., Pegasus).

1.8 INFORMATION GOVERNANCE

UK Guidance to clinicians has evolved significantly over recent years. Advice from the National Health Service (NHSX; with a remit for technology, digital and data sharing and transparency and now part of the NHS Transformation Directorate) in October 2020 [6] stated that "*in the current circumstances it could be more harmful not to share health and care information than to share it*". Further, they report that "*The Information Commissioner has assured NHSX that she cannot envisage a situation where she would take action against a health and care professional clearly trying to deliver care*". This assertion is limited to the regulatory action that could be taken by the

ICO itself and related specifically to the context of COVID-19. Worryingly, the advice also explicitly endorses the use of "*commercial, off-the-shelf applications such as WhatsApp and Telegram where there is no practical alternative, and the benefits outweigh the risk*".

NHS Clinicians are currently advised to adopt personal BYOD's for video conferencing consultations, home working and mobile messaging [6] (advice current as of December 2020, and remained online as of publication of this paper - March 2022). Reassurances have been provided for off-the-shelf tools (Skype / WhatsApp) to be used, with implied consent obtained by patient acceptance of the invitation and entering into the consultation [6]. However, intentional in inadvertent sharing of patient data could be unlawful as patients only consent to the video consultation and not for their (sensitive) data to be shared further. A clinician (data controller), cannot simply contract their way out of their obligations to the patient (data subject) under the General Data Protection Regulation (GDPR) [19]. Helpfully, the European Commission has provided guidance to EU Member States and app developers on how to comply with GDPR and the ePrivacy Directive [20].

1.9 GDPR AND HUMAN RIGHTS

The implementation of GDPR in May 2018, created a single legal framework across EU member states on "*the protection of natural persons with regard to the processing of personal data and on the free movement of such data*" [19]. This increased the safeguarding of privacy obligations on organisations that process personal data to undertake significant technical and organizational measures to demonstrate compliance.

The protection of personal information is arguably the most pressing concern in defending fundamental freedoms and human rights [21]. If a patient feels that their privacy rights have been violated by a clinician using an inappropriate technology, the ICO or DPC could find their assertion that clinicians are free to use such channels challenged. It is noteworthy that since the UK has left the EU, their data protection regulations are likely to diverge, so clinicians trained outside the UK will need training supports to raise awareness of any differences.

It is also important to note that not all patients have equal benefit from or access to these technologies and the relationship with discrimination for underserved and marginalised groups, and health inequality must be acknowledged and explored.

1.10 CONCLUSION

Smartphone technologies afford clinicians (and their patients) a broad range of highly positive advantages observed acutely during COVID-19. Clinicians have always had the best interests of their patients as a key driver however, the legacy of the well-intended measures undertaken during COVID-19 in relation to patient data and privacy could be felt long after the current emergency ends. Concerns highlighted in this article should be addressed by unambiguous healthcare sector and institutional guidelines with supportive training and education opportunities. Clinicians should be able to access training to optimise appropriate smartphone technologies within regulatory frameworks to overcome data security concerns. Embedding this training into undergraduate curricula, professional CPD requirements and mandatory institutional clinical training would positively encourage digital professionalism.

1.11 DIGITAL COMMUNICATION

Abridged (to avoid repetition) extracts from book chapter (Publication 2) are offered to enrich and expand on the details presented in the above Publication 1., adding depth and enhancing the content conveyed in the publication. By further elaborating on key topics from the published paper, under the following headings, this additional material provides greater depth and context to the original work:

Clinical Communications, Smartphone Technology and Apps

Digital Professionalism

Data Security and Cybercrime Concerns

GDPR

Training and Guidelines

Since the date of submission, the landscape of this area has further evolved, and I am currently in discussions with the Editor as to the possibility of producing a revised / updated version for publication. For the purposes of this thesis, the accepted version is presented here, and the updated elements are expanded upon in subsequent chapters of the thesis.

1.11.1 Clinical Communications, Smartphone Technology and Apps

Secure email remains an important and established method of clinical communication, particularly for formal correspondence, documentation exchange, and communication that does not require an immediate response. Its role is complemented by traditional methods such as hard copy letters, landline telephone and pagers which continue to be used in certain clinical contexts. However, there is a demand for modern, synchronous, and media-rich communication modalities that better reflect the realities of contemporary clinical practice. Clinicians frequently require the

ability to engage in rapid, media rich, dynamic exchanges, both one-to-one and one to many, within multidisciplinary teams, using current features such as real-time messaging, image and video sharing, and read receipts. These functionalities, typically absent in email systems, are essential for timely decision-making, collaborative diagnosis, clinical supervision and prioritising of care. While secure email supports information governance principles, it does not meet the immediacy and interactivity required in current clinical. Therefore, there is a growing reliance on personal technologies, IM, and third-party apps to fulfil these communication requirements.

Data governance in relation to smartphones and mobile technology is no longer something that clinicians in general and health systems across the EU can afford to ignore. Security and data protection must be a central concern for clinicians who understand that confidential patient data is no trivial issue. Patients disclose intimate personal information with the understanding that it will be stored and communicated in a way that protects their privacy and confidentiality.

Clinical data is arguably the most valuable and sensitive data of all. Typically, communications apps such as iMessage, WhatsApp, Facebook Messenger app etc. require access to a range of confidential information on the users' smartphone, including contact lists (which may be uploaded to servers in the cloud), contact information (physical address, email address, name, phone number etc.), calendars (to read and amend entries) Email, SMS, iMessage etc. (to read and send communications to those in the contact lists without notifying the owner), microphone and camera (to enable and support recording of communications), image gallery to enable access to, and downloading of, images between users.

Selecting an app for clinical communication involves numerous important considerations, as outlined in Table 1, which presents key factors for evaluating video call apps by way of an example. Frequent updates to app functionalities and terms and conditions further complicate this process, making it challenging for clinicians to remain fully informed of the changes that may impact the ongoing security and appropriateness of a particular app for clinical use. Anecdotal evidence suggests that users seldom review or understand revised terms and conditions associated with these updates, which may unintentionally expose private information to the

public domain. This highlights the importance of ongoing, specialised guidance and insights from dedicated or specialist Information Technology (IT), Legal, and Information Governance professionals to help clinicians select and remain abreast of secure communication channels that comply with evolving requirements.

Table 1: Privacy Decision Making Aid: Video Call Apps (Dutch Supervisory Authority [22])

Privacy Decision-making aid: Video Call Apps

As of 15 April 2020 UNOFFICIAL TRANSLATION by Christopher Schmidt, CIPP/E CIPM CIPT CBSA

	Discord	FaceTime	Hangouts Google	Hangouts Meets Google	Houseparty	Jitsi	Messenger Facebook	Signal	Skype	Talk Nextcloud	Teams Microsoft	Whatsapp	Zoom*
What does the app offer?													
(group) chat (text)	■	■	■	■		■	■	■	■	■	■	■	■
1-to-1 calls (audio and/or video)	■	■	■	■	1	■	■	■	■	■	■	■	■
group calls (audio and/or video)	■	■	■	■	■	■	■		■	■	■	■	■
set up and manage yourself (self-hosted)						■				■			
participation in conversation w/o creating an account			■	■		■			2	2	2		2
use in browser	■		■	■	3	■	■		4	■	■	5	■
use on different platforms (cross-platform)	■		■	■	6	■	■	■	■	■	■	■	■
What data does the app collect?													
address book		■	■	■	■		■		■		7	■	
location data		■	■	■	■		■		■		■	■	■
call data	■		■	■	■		■		■		■		■
metadata	■	■	■	■	■		■		■		■	■	■
linking data with data from other products or profiles			■	■			■		■		■	8	
For what purposes does the app process data?													
For using the app	■	■	■	■	■	■	■	■	■	■	■	■	■
For improving the app	■	■	■	■	■		■		■		■	■	■
Show (personalised) advertisements					■		■						9
How does the information flow look like?													
Data Processing Agreement possible				■		10				10	■	11	12
Data transfer to 3rd parties (if so, what data and to whom)	13	14	15	15	16		17		18		19	20	21
Location of data controller	US	US	IRL	IRL	US	10	IRL	US	IRL	10	IRL	IRL	US
data remain in the Netherlands						■		■		■			
data remain in the EU				■		■		■		■	■		
Is the communication secure?													
end-to-end encryption (even the provider of the app cannot access the content of the communication)		■				■	22	■	23	■		■	
encryption of traffic during transfer, so that third parties cannot access it (note: the provider of the app may be able to access it, but this does not mean it will happen).	■	■	■	■		24	■	■	■	■	■	■	■
minimisation of metadata use		■				■		■		■			
encryption by default	■	■	■	■		■		■	■	■	■	■	■
anyone can check source code (open source)						■		■		■			
How does the app make money?													
paid subscription or paid version	25	26		■					27	28	■		29
(personalised) advertisements			■		■		■		■			■	30
donations								■					
otherwise						31						32	
Where can you find information?													
privacy statement (refer to the Dutch original for clickable links)	🔗	🔗	🔗	🔗	🔗	🔗	🔗	🔗	🔗	33	🔗	🔗	🔗
privacy statement in Dutch	■	■	■	■			■		■	33	■	■	

1 Video only
2 After invitation
3 Google Chrome
4 Skype for Web in Microsoft Edge or Google Chrome
5 But not for video or audio
6 Android, iOS, Google Chrome
7 Mobile/exchange
8 With other Facebook products
9 Please note: when calling via website
10 N/A (self-hosted)
11 Standard agreement
12 For some sectors
13 Metadata and IP data for business purposes, but no sale of data
14 To Apple Subsidiaries and Agents
15 Within Google
16 To public authorities when they so request and to related companies
17 Within Facebook and to external partners
18 To public authorities when they so request
19 Within Microsoft
20 To Facebook and to third parties, but not (yet) for advertising purposes within Facebook
21 To supporting partners, but no sale of data
22 Not for (video) calling; for chatting you have to start this separately in Secret Mode
23 Only in private conversations (see: website)
24 In group discussions
25 Discord Nitro
26 Supplied as standard for new Apple products
27 Skype for businesses
28 The enterprise edition has been paid for
29 There are several subscriptions, but also a free version
30 Please note: when calling via website
31 Project is fully supported by the company 8x8
32 Part of Facebook
33 This depends on the person offering a Nextcloud service

* Be careful when using Zoom. This app is still in development.
** Note: For group calls, there is either no end-to-end encryption, or only with a limited number of participants.
Please note that the AP has not been able to do extensive technical research on the apps. The AP relies on what companies say about how video call apps process your data, for example in their privacy statement.

Operating system vendors such as Apple (iOS) and Google (Android), plus other, non-communication-based apps on any smartphone home screen may additionally access financial information, track purchase history, user's browsing data, search terms, user created content, and location, health, and fitness information (including weight, steps taken, heart rate etc.). Paying for access to the functionality on offer from these apps by providing ready access to the contents of a clinician's data and potentially that of patients is inappropriate and poses concerning information governance risks.

Clinicians are probably using their own personal Apple or Google accounts where data is analysed for Apple's and Google's own ad-related practices etc. and may themselves be compromised by how they personally manage access to their devices and cloud-based accounts. It is important to also be aware that each time a website or even a single newspaper article is accessed online via a smartphone, over a thousand private surveillance mechanisms can be granted access to data on the device. The browsing history, location data, lists of installed apps on the device, content within each app, contact lists, purchase information, details of offline activities, and any data on devices connected to the same IP address, including those belonging to cohabitants or family members, are all utilised to generate advertising revenue for the newspaper group publishing the article online. This is why institutions from tyre manufacturers to banks and insurance companies, install Mobile Device Management (MDM) software on any device from smartphones to laptops including BYOD, before allowing them to access work related data. Such security software helps to govern business related communications, data, and systems accessed via these devices and can remotely wipe a smartphone or laptop of all its contents in the event that it is lost or stollen or if an employee leaves the company.

In the USA, where clinicians are obliged to adhere to the requirements of the Health Insurance Portability And Accountability Act (HIPAA) of 1996 [23], the security and privacy of patient's medical data and communications is protected by the provision of a myriad of institutional digital solutions such as Voalte, Trillion, Tigerflow and Microsoft Teams. Hospitals in the USA, less concerned by budgetary restraints and arguably more risk averse regarding litigation, use expensive institutional solutions, commonly provide specifically configured hardware and

software including smartphones and digital communications channels for clinicians to use, thus ensuring that patient data is securely stored and communicated. HIPAA [23] is not as comprehensive a standard as GDPR and most of the established solutions being used in the USA are not yet GDPR compliant. It is possible that these solutions will be adapted and become available in the EU in the future.

A list of expertly risk assessed NHS and HSE approved apps, or the provision of institutional or enterprise solutions such as Hospify, Near Me, Microsoft Teams or Voalte for use by clinicians are well overdue in the UK and Ireland. Most popular free-of-charge apps, such as WhatsApp, are not compliant with the requirements of GDPR and are not secure or appropriate for clinical communications. Preventing all clinicians within the national health systems of the UK and Ireland from using their personal devices and technologies for work would likely have adverse effects on operational efficiency and may prove impractical. To promote both secure and efficient communication, it would be useful to establish a comprehensive list of core functionalities required by clinicians. Existing popular third-party apps could usefully undergo thorough risk assessments to identify those that meet the highest standards of security and GDPR compliance. Such assessments would inform the active promotion of secure, compliant applications, which are essential for contemporary clinical practice. Examples of indispensable tools include secure online image repositories, cloud-based document sharing platforms, online scheduling systems, video conferencing solutions, instant messaging applications, PDF creation software, voice dictation tools, and reference management software.

1.11.2 Digital Professionalism

The informal and instantaneous nature of communication via social, digital media and mobile technology can pose a serious challenge for all healthcare professionals, who must remain vigilant to the fact that their status in society and the public eye, requires them to always maintain a high standard of conduct.

Employers have become aware of the activities of its employees in relation to digital professionalism. In 2017, a report was published outlining disciplinary action against in excess of

1200 NHS staff, including 65 individuals who lost their jobs, for their use of social media and messaging apps [24]. This staff cohort, who ranged from porters to consultant surgeons, engaged in a range of inappropriate practices. These behaviours included the sharing of confidential patient information online, posting derogatory messages about patients and colleagues, and evidence of distractions caused by various platforms while at work. Much of the material that was published threatened professional reputations and patient confidentiality.

It has become evident that staff members have, in some cases, faced investigations years after messages were initially shared. For this reason, it is important for new entrants to the professions to carefully curate any past shared content, as it remains accessible and may be republished long into the future. Clinical practice can be highly stressful, and individuals must remain vigilant against a false sense of security provided by privacy settings on various accounts and networks, refraining from using social channels to 'vent' or release stress.

In the online world, private and professional lives cannot always be neatly compartmentalised. Consequently, it is prudent for individuals to invest time in curating and maintaining a positive online presence. Limiting the amount of personal information available across platforms can help mitigate potential risks, making it more challenging for various parties, from patients with casual curiosity to malicious actors, to gather personal details.

1.11.3 Data Security and Cybercrime Concerns

The increased reliance on smartphone technology and mobile communication channels during the COVID-19 pandemic has raised significant concerns around data security and cybercrime in healthcare. As healthcare systems adapted to the urgent need for remote communication, vulnerabilities in data protection became more apparent, making healthcare a prime target for cyberattacks with the potential for cybercriminals to significantly disrupt healthcare operations and compromise patient confidentiality and undermine trust in healthcare systems and the clinical professions.

Although BYOD enhances flexibility and efficiency in clinical communications, they simultaneously elevate the risk of data breaches, as personal devices may lack the comprehensive security measures typical of institutional devices. Careful consideration must be given to what data is accessed, processed and stored and protected on BYOD devices. Particular attention must be paid to ensuring that software is regularly updated, security patches are applied, secure and trusted networks are used (avoiding free or unsecured Wi-Fi use by any device which processes or stores confidential data), and strong authentication measures are in place. If a personal device is compromised, both professional and personal data may become accessible, further complicating the security landscape.

Another growing concern is the rise of phishing attacks, where fraudulent communications are sent to clinicians, attempting to trick them into revealing sensitive information or clicking on malicious links. These phishing emails often contain links that, once clicked, install malware or ransomware on the device, leading to further data breaches. Clinicians and healthcare workers must remain vigilant and be aware of the potential risks posed by such attacks, particularly as cybercriminals continue to target the healthcare sector.

To mitigate these risks, it is essential for all healthcare providers and systems to adopt comprehensive cybersecurity strategies, including regular training for all staff on identifying potential threats and following best practices for data security. In particular, the use of MDM software should be enforced for any BYODs used for professional purposes. Regular backups of clinical data and adherence to institutional policies regarding data streaming, cloud-storage and encryption are essential for maintaining the security of patient information.

As the landscape of cybercrime evolves, so too must the safeguards in place to protect healthcare data, particularly as mobile technology continues to be an integral tool in clinical communication.

1.11.4 GDPR

If clinicians are using BYOD and personal technology to discuss patients and share clinical images etc., the devices, apps and social media platforms they are using for communication and

processing of data must be compliant with GDPR [19]. Indeed, clinicians need to be sure that none of the apps hosted on their smart devices from smartwatches to fitness trackers, to smart speakers and smartphones threaten the security and confidentiality of the sensitive patient data.

GDPR [19] was enacted across the EU in May 2018, following four years of discussion and a two year transition period. Aimed at overhauling how organisations (including health services) process data, GDPR provides greater protection and rights for data subjects (including patients) and stipulates specific technical standards and requirements for the appropriate storage, encryption, and transmission of sensitive data, with violations set to generate financial penalties of up to four percent of annual turnover or twenty million euro [25]. In the context of digital communication for clinicians, the introduction of GDPR has major implications for how individuals and organisations operate.

In particular, GDPR stipulates that personal data shall be:

- Held securely and encrypted to specific requirements (256 bits, Official accreditation ISO 27001/27002 for the cloud provider (audited and confirmed at that).
- Not transferred to a country or territory outside the EEA for storage unless it complies with specific requirements.

Both of these points are of specific practical importance to healthcare provision as the channels that are used for clinical communications must host the data within the EU and also, despite the fact that some of the apps may indeed encrypt the content of the messages that are shared to the stipulated level, the default permissions within the apps (for example with WhatsApp) may be such that images are downloaded to a photo album and streamed between all of the networked devices via the USA hosted Apple iCloud.

A small number of special categories of sensitive data exist, and are afforded greater protections under GDPR, health information being one of them, and here again this is relevant to clinicians. Among a raft of new rights for ‘data subjects’, patients have the right protection against unauthorised or unlawful processing of their data, to be informed if their data is lost or destroyed

or damaged.

Healthcare providers are obliged to allow patients to access the data held on them (through System Access Requests or 'SARs'), patients have the right to portability of their data to another provider if they so wish, and they have the right to amend their data if it is inaccurate, and explicit consent of the data subject is required for data processing. Health systems, such as the NHS, and the clinicians who work within them need a good understanding of current data protection regulations and to work within the terms of GDPR. However, as the UK has left the EU, it is reasonable to assume that the regulations concerning data protection are likely to change and potentially diverge from the GDPR, so it is essential for clinicians to stay in touch with any emerging changes and consider their potential impact on the practicalities for clinical practice.

1.11.5 Training and Guidelines

While the convenience and efficiency of BYOD smartphone mobile communications have been widely acknowledged, the associated requirement for relevant training and guidelines to ensure that clinicians are adequately equipped for contemporary clinical practice must be addressed. The speed and ubiquity of internet access, and technological developments along with the rapid adoption of personal BYOD technology in clinical practice have resulted in a raft of new challenges around data protection, and professional standards. These are seldom acknowledged in the literature despite the information governance risks, threats to personal privacy and patient confidentiality, and ultimately trust in the clinical professions [26]. Clinicians and students can operate under misconceptions regarding the use of online content, assuming that digital materials can be freely used for teaching and scholarly work if they do not generate income. This misunderstanding poses risks of intellectual property infringement, resulting in potential legal and professional consequences, ethical issues and financial penalties.

Intellectual property (IP) includes all forms of creative and knowledge-based content, from literary and artistic works to photographs, images, and proprietary symbols. Given that IP is legally protected through licences, patents, trademarks, and copyrights, clinicians and students must be educated on these laws, especially as instant access to digital materials has increased

the ease of downloading, copying, and reworking online content. There is a requirement for structured training on these topics, covering plagiarism, permissions, and appropriate attributions. Such guidance is essential for clinicians to navigate the complexities of contemporary digital communication in healthcare, upholding both regulatory compliance and ethical standards.

Healthcare professionals must respect the fact that search engines are not free repositories for images, music, journal articles, or other resources. Guidelines regarding IP, permissions and ownership are especially critical in clinical contexts, where patient information must be handled with the utmost care. Clinicians require specific guidance regarding the use of clinical images in academic presentations, educational materials, professional websites and digital communications with a focus on permissions, consent and data security.

In most cases, clinical images are considered part of patient records and are subject to secure storage requirements. Sharing them for academic purposes or consultations mandates strict adherence to IP and data protection regulations to avoid unintentional breaches. Institutions should provide explicit guidance on these IP standards and promote resources, such as free-to-use stock images on intranet platforms, to prevent misuse of clinical images. Ensuring access to these resources would support clinicians in selecting legally compliant content for academic and professional presentations, while safeguarding patient privacy and data integrity.

Another important yet often overlooked area is the ability to effectively remove or delete sensitive data from the various digital modalities clinicians use for communication. Whether images, documents, or messages are shared through IM, apps, cloud-based platforms, or stored locally on BYOD devices, the persistence of such data poses considerable risks to patient confidentiality and data protection. Unlike traditional healthcare communication systems that are designed with audit trails and centralised controls, many third-party apps and smartphone functions do not allow for reliable deletion, secure archiving, or full traceability of shared content. This can lead to situations where patient data remains accessible on personal devices long after they have been abandoned or upgraded or considered obsolete. As such, clinicians require

targeted guidance and technical support to ensure that data shared via personal devices can be appropriately retracted, deleted, or protected post-communication. Training and organisational policies must address not only the safe sharing of information but also its lifecycle, highlighting strategies and technologies for ensuring that digital patient data does not persist beyond its legitimate use.

There is a requirement for clear, accessible guidelines on the ethical use of digital content. Given the risks associated with BYOD, including the potential for data privacy breaches, guidance regarding securing permissions and using IP-protected content is now essential. Training should address the complexities of consent, particularly in using patient images. Clinicians must navigate issues around obtaining comprehensive consent, as standard processes may not account for metadata (e.g., location, time) embedded in images or the possibility of unintended patient identification via facial recognition technologies.

For instance, while patients may consent to the creation of clinical images for anonymised educational purposes, using these images in a public domain or professional gallery without explicit permissions could violate data protection laws. Under GDPR, patients cannot waive fundamental rights, making it critical for clinicians to avoid even unintended infringements. To address these challenges, specialist tools and frameworks could be useful to provide structured insights and guidance regarding compliant digital communication practices.

Ongoing professional development (CPD) on IP, consent standards, and ethical management of patient data is essential to ensure that clinicians remain informed and compliant with evolving technology and legal regulations. With the support of structured guidance, clinicians can confidently navigate BYOD complexities while upholding professional and regulatory standards.

The widespread adoption of BYOD smartphones, IM and third-party apps for communication between clinicians has introduced a range of complex considerations, including digital professionalism, data security, GDPR compliance, and the ethical management of patient information. Addressing these areas requires clear guidelines, specialised training, and specialist

resources to empower clinicians to use personal technology effectively while upholding professional and regulatory standards.

1.12 RESEARCH QUESTION

This thesis addresses the overarching research question: *How do / should clinicians use smartphone technologies to communicate patient data?*

1.12.1 Objectives for this study

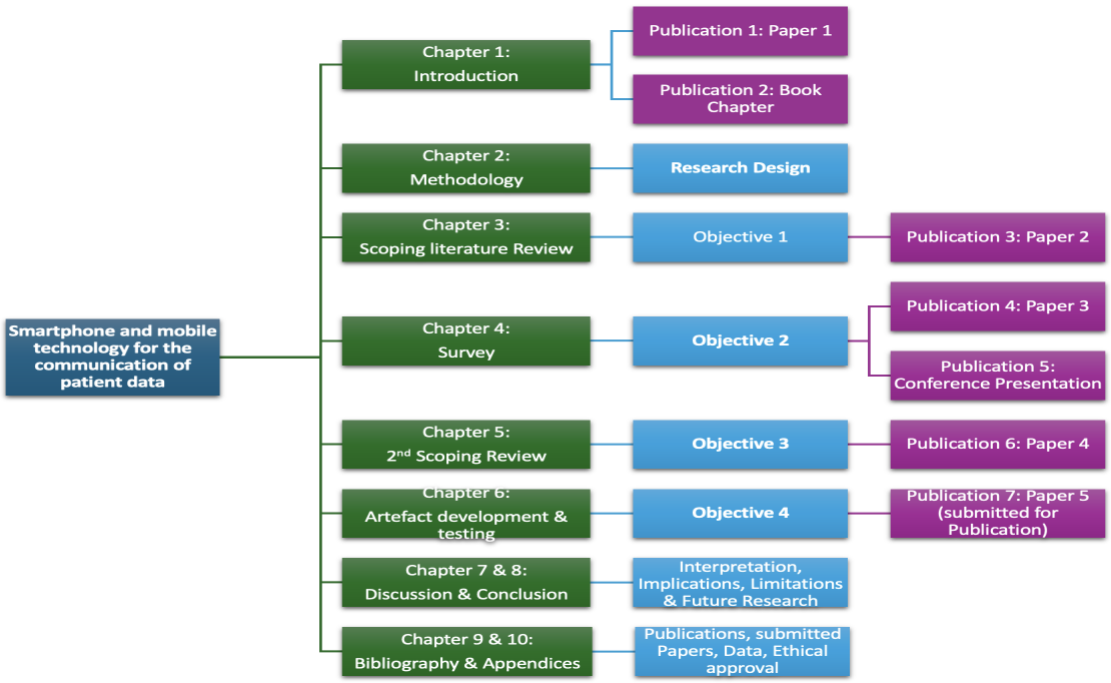
There are four objectives for this thesis:

1. To evaluate the available literature on the use of personal smartphone technology for communication between clinicians.
2. To determine the current usage of smartphones and mobile technology among clinicians in Ireland (and UK).
3. To evaluate the current guidelines available to inform practice-based communications between clinicians using their personal smartphones, IM and third-party apps in the UK and Ireland.
4. To develop & evaluate a toolkit to assist clinicians in their assessment of the available guidelines regarding communication using smartphone technologies.

1.12.2 Structure of the thesis

This thesis is structured in accordance with the University College Cork (UCC) guidelines for Publication-Based Thesis. The research is organised as a series of peer reviewed, published manuscripts, each serving as the foundation for a chapter of the thesis (see Figure 1). All work was conducted by the candidate during their PhD registration. Minor edits have been made to the text of all publications (such as the numbering of tables or figures and alteration of spellings to UK English) in order to fit the thesis format, and to minimise areas of duplication.

Figure 1: Structure of Thesis



Chapter one outlines the aims and objectives of the study, describes the structure of the thesis and provides an overview of the works that have been produced, including those published, presented at a conference, and submitted for peer review and publication. This chapter introduces the issues raised for clinical communication through the use of BYOD Smartphones, IM and apps and integrates a published paper, entitled "**Smartphone Technology for Clinical Communication in the COVID-19 Era: A Commentary on the Concerning Trends in Data Compliance**" to serve as background to the study. Several of the issues raised in the published paper are expanded upon in additional abridged text from a further publication, a book chapter entitled **"Digital Communication"** that was commissioned and accepted by the Royal College of Psychiatrists and Cambridge University Press.

Chapter two addresses the first research objective, incorporating a published scoping review paper entitled "**Scoping Literature Review of the current usage of smartphone technology for clinical communications between clinicians in the Republic of Ireland and UK**".

Chapter three, provides an overview of the research design, including the rationale for the selection of a mixed-methods approach. Details regarding the research process and rationale behind each methodological choice are provided.

Chapter four addresses the second research objective. It integrates a peer reviewed publication regarding a survey entitled "**Smartphone and Mobile Technology Usage amongst the Dental Profession**", and a conference presentation of the same data - **"Smartphone clinical communication amongst Irish Dental Professionals."**

Chapter five meets the third research objective and features a second scoping review paper which has been peer reviewed and published **"Navigating the Wild West: A Review of Guidance on Clinical Communications using personal BYOD, IM and Third-Party Apps in the UK and Ireland"**.

Chapter six addresses the fourth objective, comprised of another paper that has been submitted [27] to a journal for peer review and publication on 9th October 2024 entitled **"Designing a Data Dimensions Artefact for the use of BYOD, IM and third-party app-based technology by clinicians: An Action Design Research Approach".**

Chapter seven provides a comprehensive discussion of the study, summarising the findings of each paper and synthesising the overall findings to answer the overarching research question.

Chapter eight provides the conclusion for the study, explaining the significance of the research and its contribution to the knowledge in this area. Limitations of the research are acknowledged and areas for further research based on the findings discussed.

1.12.3 Terminology

In the context of this research, the terms *Clinician toolkit* and *artefact* and also *Data Dimension Artefact (DDA),* are used to describe the same concept, but their use varies depending on the audience. For clinicians, the term '*toolkit'* is more familiar, as it aligns with their practical, hands-on approach to problem-solving in clinical practice. However, within the IS discipline, the concept

of an IS artefact is defined as a system composed of three interconnected subsystems [28]: a technology artefact, an information artefact, and a social artefact. Together, these subsystems interact to form an IS artefact that is greater than the sum of its parts [28]. Unlike IT artefacts, which may or may not play a dominant role in design considerations, the IS artefact emphasises the holistic creation of systems by people, even in the absence of IT designers. This distinction highlights the broader context and complexity of IS artefacts compared to IT artefacts [28]. In this thesis, the term toolkit and artefact are used interchangeably, with the appropriate term selected based on the intended audience and the specific focus of the publication. Additionally, the Data Dimension Artefact is also referred to as the DDA. Due to the format of this PhD by publication, where several chapters are comprised of already published peer-reviewed journal articles, terminology has been preserved to maintain fidelity to each paper's disciplinary audience. However, for clarity and accessibility to a broader readership, particularly clinicians and healthcare professionals, the term *toolkit* is introduced and used where appropriate (in the introduction, methodology, discussion and conclusion) to reflect the practical application of the artefact in real-world clinical settings.

1.12.4 Candidate's contribution to the publications

The candidate is the first author of all manuscripts included in this thesis, whether published or under review. The candidate's contributions encompassed study design, quantitative and qualitative data collection, including library searches for literature reviews, survey design, distribution, statistical analysis and thematic data analysis using NVIVO software, and manuscript preparation. Dr Christine McCreary, Professor Anthony Roberts, and Professor Ciara Heavin aided with the concept, study design, research subject recruitment, and data collection. Anita Wilcox and the Library at UCC supported the literature searches. All authors reviewed and provided feedback on the manuscripts before submission and after receiving reviewer comments. Permissions have been obtained from publishers for the inclusion of accepted papers in this thesis.

CHAPTER 2 METHODOLOGY

2.1 OVERVIEW OF RESEARCH METHODS

This study employed a mixed methods [29] embedded design to comprehensively address the four research objectives and provide a deeper understanding of the use of personal digital technology for secure communication between clinicians. The embedded design integrates both quantitative and qualitative data collection and analysis, with one type of data serving as the primary method and the other offering supplementary insights. In this case, qualitative and quantitative data were collected concurrently across multiple phases of the research, each contributing uniquely to the overall findings (see Figure 2).

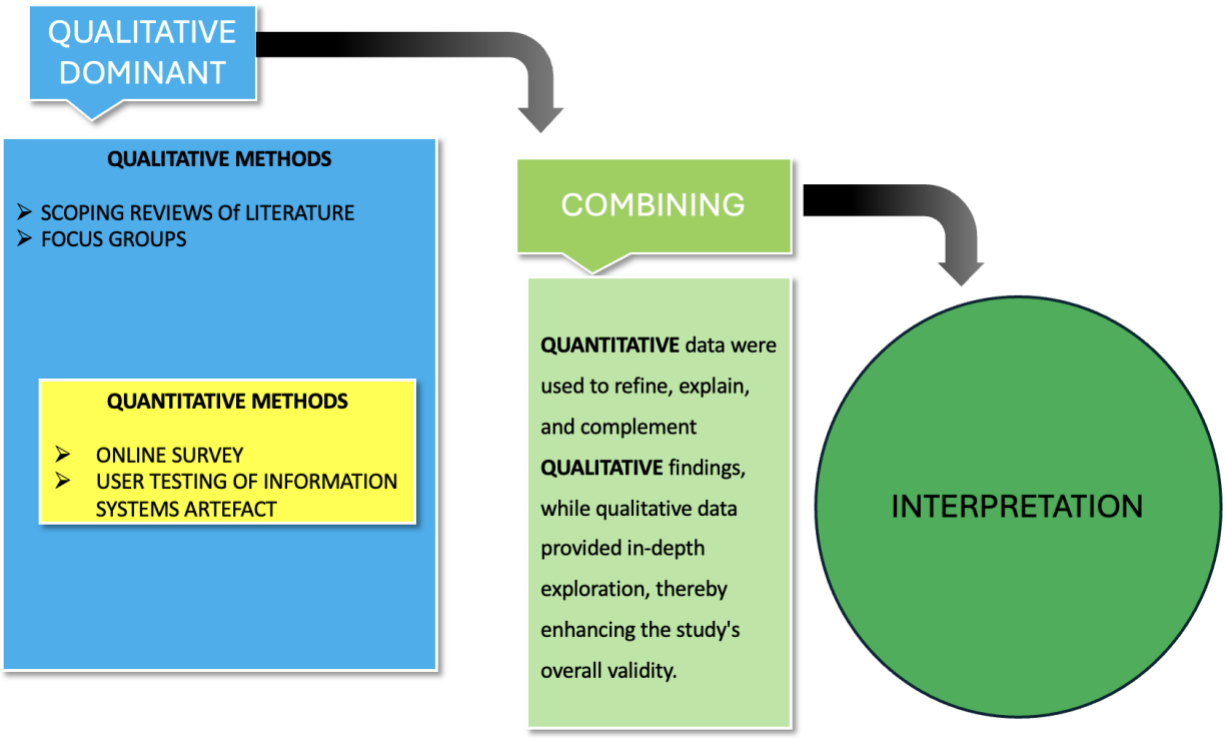
The combination of qualitative methods (scoping reviews and focus groups) with quantitative methods (online survey and user testing of the toolkit, followed by statistical analysis) facilitated a richer understanding of the topic. This approach minimises the limitations of each method [29] and effectively addressed the four objectives.

This design allowed for a comprehensive exploration of the topic, with qualitative data taking a dominant role and quantitative data offering supplementary insights. The approach facilitated an understanding not only of the prevalence and types of personal technology used but also of the underlying reasons, attitudes, and challenges associated with their use in clinical practice. Data were analysed separately and then integrated to form overarching conclusions. This design was particularly suited to the study's objectives and allowed flexibility and adaptability in response to the external constraints imposed by the COVID-19 pandemic, which necessitated adjustments to planned data collection and fieldwork.

Given the constantly evolving nature of BYOD smartphone, IM, and app technology, multiple publications were generated as the study progressed. This ensured that timely and relevant evidence was shared with the clinical community, further justifying the choice of a PhD by publication. Detailed descriptions of each method are provided in the respective chapters, which

outline specific techniques, data collection procedures, analytical tools, and software used, as well as ethical considerations.

Figure 2: Mixed Methods Embedded Design



Within the qualitative-dominant mixed methods embedded design, elaborated ADR [30] was integral to the development of the toolkit. Elaborated ADR's iterative process, spanning Diagnosis, Design, Implementation, and Evolution, enabled continuous refinement of the toolkit in close collaboration with clinicians. This methodological approach [30] aligned well with the study's embedded design, facilitating the integration of qualitative and quantitative insights in real time. Detailed descriptions of each ADR cycle and intervention are provided in Chapter 6, where elaborated ADR [30] is discussed as a foundational approach to ensure the toolkit's clinical relevance and practical application.

2.2 PHASE ONE: SCOPING REVIEWS AND SURVEY

The first phase of the study comprised two scoping literature reviews and an online quantitative survey, providing foundational insights into the current landscape:

- First Scoping Review: This review scoped and mapped the available literature on the use of BYOD smartphone technology among clinicians. It focused on identifying specific apps and channels used for clinical communication, with an emphasis on data security and data privacy practices. The JBI [31] framework was followed, and search results were reported according to the PRISMA ScR guidelines. A systematic search strategy was implemented using EBSCO and OneSearch databases, with two identical searches conducted in June and October 2020. These searches were limited to English-language articles published between 2016 and 2020. NVIVO software was employed to conduct thematic analysis, allowing for key concepts and knowledge gaps to be identified. The qualitative data generated from this review provided important context for subsequent survey findings and highlighted critical gaps in the literature. A narrative synthesis was used to integrate and report the findings, helping to guide the focus of later research stages.
- Second Scoping Review: This review explored existing guidelines and policies related to personal BYOD smartphones, IM, and third-party apps for clinical communication. It was important to map the current regulatory landscape in order to understand and contextualise the extent to which existing guidelines provided actionable recommendations for clinicians. Following the JBI updated Framework [32] for Scoping Reviews and PRISMA ScR guidelines, a systematic search was conducted across multiple academic databases, including OneSearch, Embase, EBSCO, PubMed, Medline, and CINAHL. Additional hand searches were performed on professional entities' websites, including those of trade unions, regulators, two national health systems, and several private and public hospital employers. Direct inquiries were made to sixty-nine professional entities via telephone, email, websites, and X (formerly known as Twitter). NVIVO software was used to conduct thematic analysis, allowing key themes and gaps in

the guidelines to be identified. The qualitative data from this review informed the development of the toolkit in Phase Two.

- Online Quantitative Survey: Distributed to dental professionals in Ireland and the UK, the survey (Appendices 9 & 10) assessed the current use and understanding of the risks and limitations associated with smartphones and mobile technology for sensitive communications among anonymous clinicians. The survey was distributed across multiple platforms, including Cork University Dental School and Hospital, the Dental Council of Ireland newsletter, and several dental organisations' events between May 2020 and March 2021. Due to the COVID-19 pandemic, planned face-to-face dissemination was curtailed. Adapted from relevant published studies, the survey tool was disseminated via a Google Form weblink to a convenient sample of dental care professionals, including dentists, dental specialists, hygienists, and nurses. Both quantitative data (e.g., frequency and types of technology use) and qualitative data (using open-ended responses regarding perceived risks and challenges) were collected. Quantitative data offered a broad understanding of technology use patterns, while qualitative responses provided deeper insights into clinicians' knowledge and attitudes towards digital professionalism and data security.

2.3 PHASE TWO: TOOLKIT DEVELOPMENT, TESTING AND EVALUATION

The second phase of the study focused on the development and evaluation of a toolkit (IS artefact) designed to help clinicians assess the quality of information in guidelines, particularly concerning digital communication tools and data security. The development followed an elaborated Action Design Research (ADR) [30] approach, incorporating iterative cycles of Diagnosis, Design, Implementation, and Evolution. Early engagement with practitioners is a particular strength of design research and clinicians were actively involved at every stage of development to ensure that the solution met user requirements.

- **Toolkit Design:** The toolkit was conceptualised using established Data Quality Dimensions [33] (DQDs) from IS literature, incorporating dimensions such as accuracy, completeness,

timeliness, relevance, clarity, and credibility. These dimensions were refined through review of relevant literature and publications from authoritative sources, including the National Cyber Security Centre (NCSC), National Institute of Standards and Technology (NIST), and the Information Commissioner's Office (ICO). The toolkit was designed to assess the quality and security of guidelines, ensuring they meet data protection and regulatory compliance requirements, such as GDPR [19].

- **Toolkit Development and Evaluation:** Iterative cycles of elaborated ADR [30], which took place between January and July 2024, involved in-depth internal / author reviews, pilot testing, dental clinician reviewer testing and feedback (including senior clinical dental students and experienced clinicians), and two focus group discussions. These steps provided quantitative data, statistical analysis (including accuracy and inter-rater reliability measures using Cohen's kappa), and qualitative data (concerning usability and effectiveness via thematic analysis using NVIVO software of focus group data). The iterative process highlighted areas for improvement, guiding successive refinements to enhance precision and applicability, informing the further generation of the toolkit.

Within the qualitative-dominant mixed methods embedded design, elaborated ADR [30] was integral to the development of the toolkit. Elaborated ADR's iterative process [30], spanning diagnosis, design, implementation, and evolution, enabled continuous refinement of the toolkit in close collaboration with clinicians. This methodological approach aligned well with the study's mixed methods embedded design, facilitating the integration of qualitative and quantitative insights in real time. Detailed descriptions of each ADR cycle and intervention are provided in Chapter 6, where ADR is discussed as a foundational approach to ensure the toolkit's clinical relevance and practical application.

2.4 INTEGRATION AND ANALYSIS

Throughout the study, quantitative data collected from the survey, literature reviews, and toolkit design, testing and evaluation were embedded within the broader qualitative framework

provided by the literature reviews and focus groups. This integration allowed for a comprehensive understanding of the research objectives:

- Qualitative Data offered deep insights into clinicians' attitudes, perceptions, and challenges regarding digital communication tools, complementing and contextualising the quantitative findings. It also signposted areas for further research and development.
- Quantitative Data provided a broad overview of the current use of smartphone and mobile technology among clinicians and assessed the effectiveness of the toolkit in guiding decision-making.

The ADR cycles were informed by both quantitative and qualitative data gathered through the interplay between the research team and clinicians, ensuring the toolkit evolved in response to real-world needs. This collaborative approach, inherent to ADR, was essential in refining the toolkit, deepening the understanding of practical challenges, and enhancing the applicability and relevance of the DDA for practical use by clinicians.

2.4.1 Ethical Considerations

All research activities adhered to the ethical principles outlined in the Declaration of Helsinki [34]. Participants provided informed consent, and all data were anonymised to protect confidentiality. Ethical approval was granted by the Social Research Ethics Committee at UCC (Approval No. 2018-131 – Appendix 19), with no amendments made without prior approval. A final report summarising the study's findings will be submitted to the committee upon its conclusion.

All data are securely stored on encrypted devices in compliance with the UCC guidelines. Data will be retained for ten years, accessible only by the researcher in compliance with UCC Code of Conduct.

CHAPTER 3 SMARTPHONE TECHNOLOGY FOR COMMUNICATION BETWEEN CLINICIANS – A SCOPING REVIEW

A peer-reviewed, published Scoping Literature Review was conducted to meet objective 1, to evaluate the available literature on the use of personal smartphone technology for communication between clinicians. Publication 3, Paper 2 [35]

- **Copy of the peer reviewed publication: Appendix 3**

REFERENCE:

John B., McCreary C., Roberts, A., (2022) Smartphone Technology for Communications between clinicians – A Scoping Review. Journal of Dentistry, Vol. 1222, pp. 1-13, July 2022, DOI: https://doi.org/10.1016/j.jdent.2022.104112

3.1 ABSTRACT

3.1.1 Objectives

This scoping review aims to review explore, assess, and map the literature to inform clinical practice regarding communication between clinicians. Specific apps / channels used were identified and assessed with a focus on data security with key concepts and knowledge gaps identified.

3.1.2 Data

The JBI [31] framework is followed, with search results reported as per the *PRISMA ScR for scoping reviews* guidelines.

3.1.3 Sources

A systematic search strategy encompassing EBSCO and OneSearch databases was conducted - two identical searches, (June and October 2020) limited to English language articles published 2016–2020. A narrative synthesis was used to integrate and report the findings.

3.1.4 Study selection

Sixty-six publications were selected. Twelve from EBSCO, thirty-five from OneSearch, nineteen were hand searched. Sixteen of the publications were research studies, nine were literature reviews, twenty-six were editorial, one was a newspaper article and fourteen were grey literature. Instant Messaging (40%, n = 23), image sharing (41%, n = 24), and video conferencing (19%, n = 11) were functions most popular with clinicians. WhatsApp, generic IM, Facebook messenger, ZOOM, and Skype are evidenced as channels for communication between clinicians within the EU. A sizeable proportion of the publications (38%; n = 25) failed to identify or adequately address technical security concerns and requirements around privacy and data protection.

3.1.5 Conclusions

Clinicians use personal BYOD smartphones / apps to communicate clinical information with each other. The security and privacy issues arising from their communication of sensitive data is absent or only superficially acknowledged within the literature.

3.1.6 Clinical significance

Clinicians need clearer guidance on the use of smartphone technology for clinical communications.

3.2 INTRODUCTION

There is growing international concern around the use of digital modalities for clinical communication [3-5, 10, 11, 25, 36-52]. A systematic review of the utilisation of Social Networking Sites for communication amongst health professionals in frontline clinical practice by Chan and Leung [36] is one example of such concern. Conducted prior to the strict stipulations required for GDPR [19], this international study clearly identifies limitations around technical insight, risks to the protection of sensitive data, professionalism and liability posed by the use of popular consumer digital communications channels. The education and training of health professionals and the necessity for policy were identified as areas of importance for future research.

GDPR came into force across the EU on the 25th of May 2018, following a two year 'run-in' preparation period, to safeguard data privacy. This regulation increased obligations for organisations that process personal data within member states. Health Information is considered to be the most confidential of all types of personal information [53] and organisations that process personal data are required to adopt significant new technical and organisational measures to demonstrate their GDPR compliance. Data subjects (all individuals within the EU) gained a raft of new legal rights regarding the processing of their data including the right of access, the right of rectification, the right to erasure, the right to restrict processing and the right to object to their data being processed [54].

The COVID-19 pandemic has heightened the urgency for digital solutions to aid remote consultation and communication [55] for the benefit of patient care and evidently has expedited the adoption of smartphone technology [2]. Concerns are intensifying, that current clinical communications practice has the potential to compromise data privacy and data protection with smartphones, popular apps and social media - technology that commodifies patient data [5, 14, 25, 45, 56]. The acquisition of patient data is possible through a variety of current advertising technologies including tracking and data profiling, analytics, location data, third party sharing of data, data brokers, surveillance technology and networked devices. These have the potential to violate privacy regulations and legislation including GDPR and the European Convention of Human Rights [57]. De Benedictis et al. [38] speculated that the use of WhatsApp in healthcare may represent an extreme version of 'backdoor adoption' which occurs when easy and familiar technology is embraced to meet a requirement. Unfortunately, this adoption is often without the appropriate formal approval or assessment from senior healthcare or IT management regarding the opportunities and risks that these innovations might bring along with them. The requirements for appropriate policy, technical evaluation and risk assessment should not be ignored.

In order to map existing literature and emerging evidence in this broad area and to clarify key concepts, identify gaps in the knowledge and guide future research and policy, a scoping review was identified as the 'next logical step' [31] and is the focus of this study.

It was anticipated that for this scoping review to be effective, it would be necessary to draw upon the full range of published literature, from quantitative research (surveys to establish the prevalence of smartphone and app use), qualitative studies (used to discover any problems with the specific technologies), to policies, editorial and press articles, including a range of outlets, from academic literature to Health Service policy and general press outlets, across the full range of clinical practice, in order to generate evidence that is relevant to the current practice of dentistry.

3.3 METHODS

3.3.1 Overview

A scoping review protocol was developed guided by the JBI [31]. Thus, an overview of the literature was mapped to address the broad research questions. A data extraction (selection and coding) protocol was developed around PICO (Population / Intervention or exposure / Comparator / Outcome).

3.3.2 Objectives and research questions

For the purpose and objectives of this review the questions asked were: What are the common smartphone functionalities being used by clinicians in Europe to communicate sensitive patient data at present? What specific consumer apps / channels are used most by clinicians for clinical communications? Are security issues acknowledged, explored, and appropriately mitigated for in relation to the consumer channels being used, with a specific focus on GDPR compliance?

3.3.3 Identifying relevant studies and eligibility criteria

Publications in the English language since 2016 were reviewed as most trade publications and grey literature on technology uses the English Language. Translating publications through Google translate was deemed not to be satisfactory as it translates literally and can miss nuances. Research studies, literature reviews, press releases, newspaper articles, editorial in journals and grey literature including government and health service policy papers were all included.

3.3.4 Eligibility criteria

Articles were included if they had content on clinical communication, clinical consultation or general clinical communications via consumer apps, or social media. Papers were included if they raised issues relevant for patient privacy, patient data, GDPR, data protection and data compliance using consumer digital channels. The focus of this study was communication between clinicians and as such, papers were excluded if they were concerned with communication be-

tween clinicians and patients. No effort was made to include only papers that concerned communications between dental clinicians, as it was felt that this would be too restrictive and was unlikely to generate enough evidence.

Although the purpose of this study is focussed on the use of consumer social media and apps within the EU, their functionality is identical worldwide and the issues around their implementation by clinicians are global. For this reason, it was planned *a priori* to include international papers.

As 2016 was the year when the two-year run-in period for the implementation of GDPR commenced, only papers published from 2016 were included in the search. Searching older publications would not have provided the appropriate currency for this study. Platforms, functionality, and the digital landscape is evolving so quickly that a recent and focussed time interval was important to achieve relevance. A very small number of policy documents could be included outside this date range if nothing more recent, that still appears to be informing current clinical practice could not be identified.

3.3.5 Evidence searches

Search results are reported as per the *Preferred Reporting Items for Systematic Reviews and Meta-Analyses extension (PRISMA ScR) for scoping reviews* guidelines (see Table 2). Comprehensive literature searches were conducted following consultation with Anita Wilcox, an expert information specialist.

The OneSearch discovery system (a search of approximately 200 databases including ProQuest databases, EBSCO databases including Business Source Complete, CINAHL, Science Direct, JStor, IEEE, BMJ, Nature, Royal Society of Chemistry, and many more, simultaneously for information which eliminates the need to hand search all of them individually). EBSCO was additionally hand searched specifically because OneSearch includes articles from peer reviewed journals, not trade/commercial publications, or grey literature in EBSCO. A systematic search strategy within these two system/databases was conducted and individual journal titles were included if they

were deemed relevant to the project (e.g., the Journal of Dentistry). Hand searches were also conducted to identify substantive or scholarly information that has not been formally peer-reviewed or published. The full search was performed twice (once on 24th June 2020, and once again on 20th October 2020); thus, ensuring all possible new publications and current content on this fast-moving topic were included.

Databases were searched with subsequent search terms:

OneSearch - Zoom OR WhatsApp OR patient data OR patient privacy keywords used in a basic search. OneSearch (2nd search); use of smartphone OR Zoom OR WhatsApp AND patient privacy OR health data at risk. Limiters selected were Medicine, Public Health, Nursing, Computer Science and Law.

As OneSearch Discovery system or search engine also searches EBSCO databases, a different search string was utilised in searching the database separately to establish if it were possible to capture anything new. For example, if COVID-19 was used with OneSearch it could have eliminated the articles without that word, and some very good, relevant articles would have been missed.

No limiter was used in the initial basic search of OneSearch. The abstracts of 1000 results were read, and articles were selected according to our inclusion criteria. Subsequently limiters used included Conference Proceedings, Trade Publication Articles, Data Sets, Journal Articles, Magazine Articles and Newspaper Articles. Date limitations were applied as described above.

For the first EBSCO search - Zoom, video communications, impact, COVID-19 OR clinical consultation OR (patient, data security and privacy) were used. Expanders - equivalent subjects Search modes were applied – Boolean / Phrase For EBSCO. For the second EBSCO search - Zoom OR Skype OR social network* OR WhatsApp OR clinical communication OR communication apps OR patient privacy OR GDPR or general data protection regulation OR patient data. Limiter used: Published Date: 2016–2021.

For both EBSCO and OneSearch the results were displayed by relevance. Hence, it was accepted that these are the most relevant to the topic. The OneSearch Discovery system displays only 1000 items per search. Also, although EBSCO saves all the searches, it does not indicate which search yielded the most articles. It is therefore assumed that if the system ranked the results by relevance, one would find the appropriate articles within the displayed results.

Table 2: PRISMA ScR Review Checklist

IDENTIFY THE REPORT AS A SCOPING REVIEW			
TITLE	**1.**	**Title**	**Yes**
ABSTRACT	**2.**	**Structured summary**	**Yes**
INTRODUCTION	**3.**	**Rationale**	**Yes**
	4.	**Objectives**	**Yes**
METHODS	**5.**	**Protocol and registration**	**N/A**
	6.	**Eligibility criteria**	**Yes**
	7.	**Information sources**	**Yes**
	8.	**Search**	**Yes**
	9.	**Selection of sources of evidence**	**Yes**
	10.	**Data charting process**	**Yes**
	11.	**Data items**	**Yes**
	12.	**Critical appraisal of individual sources of evidence**	**N/A**
	13.	**Synthesis of results**	
RESULTS	**14.**	**Selection of sources of evidence**	**Yes**
	15.	**Characteristics of sources of evidence**	**Yes**
	16.	**Critical appraisal within sources of evidence**	**N/A**
	17.	**Results of individual sources of evidence**	**Yes**
	18.	**Synthesis of results**	**Yes**
DISCUSSION	**19.**	**Summary of evidence**	**Yes**
	20.	**Limitations**	**Yes**
	21.	**Conclusions**	**Yes**
FUNDING	**22.**	**Funding**	**Yes N/A**

3.3.6 Selecting the evidence

All references identified on the databases listed in the search strategy were uploaded to reference management software (EndNote X9). Any duplicates were identified and removed.

Eligibility and relevance of the papers were assessed and confirmed in two phases:

1. In the first phase, titles and abstracts were examined by one reviewer, before the full texts of the articles were downloaded and identified as being potentially eligible using the pre-set inclusion and exclusion criteria. These articles were then screened to confirm their eligibility.
2. In the second phase, any doubts surrounding inclusion of a paper were discussed and agreed with the second reviewer.

3.3.7 Data extraction

All articles selected had data extracted on their characteristics by a single reviewer, charted on a Microsoft Excel spreadsheet (See Appendix 8) standardised for final inclusion in the Scoping review. Articles were coded by the following characteristics: Subject concerning clinical communications, author, year, book title, journal title, classification of publication (study, literature review, press release, newspaper article, general information article in journal, grey literature including government papers), title of article, main concept of article, which functionality the article concerns, the specific consumer smartphone channel being discussed, and if the article concerns EU or Non-EU communications. The evaluation of the literature was further coded and grouped into those publications that were mitigated for technical security concerns accurately, including the requirements of data protection and GDPR, and those that did not.

One characteristic of scoping reviews of note is that a formal assessment of research methodological quality of the included studies is generally not performed. This is because a

scoping review is designed to provide an overview of the existing evidence base regardless of quality [31].

3.3.8 Synthesis of results

The broad nature of this scoping review and the heterogeneity of the included publications made meta-analysis impossible. Full-text PDF articles were downloaded, individually uploaded into Endnote, and then imported into NVIVO qualitative data analysis software with the full text available for qualitative syntheses. NVIVO enabled the visualisation of data, the processing, analysis, and summarisation of text in relation to (I) the functionality being used for current clinical communications practice, (II) the specific consumer smartphone channels being used, (III) whether security concerns had been mitigated for, and (IV) the technical compliance with GDPR. The articles were evaluated for the quality of the content they contained and were grouped into categories as follows:

Positive content: An indication of a high level of technical understanding concerning the modality being described and / or fluency with the legal issues posed by such channels.

Negative content: Content that gives rise to debate or disagreement or controversy. Further, content that indicated superficial or outdated understanding of technical issues posed for data privacy regarding current smartphone and app technology and regulations, such as GDPR.

A narrative qualitative synthesis of the findings was then conducted from the selected publications.

3.3.9 Risk of bias (quality) assessment

The relevance and eligibility of the articles included in this review were assessed and critically appraised by one reviewer before being scrutinised and confirmed by a second reviewer, risk of bias was not applicable as this is a scoping review.

3.4 RESULTS

3.4.1 Study selection

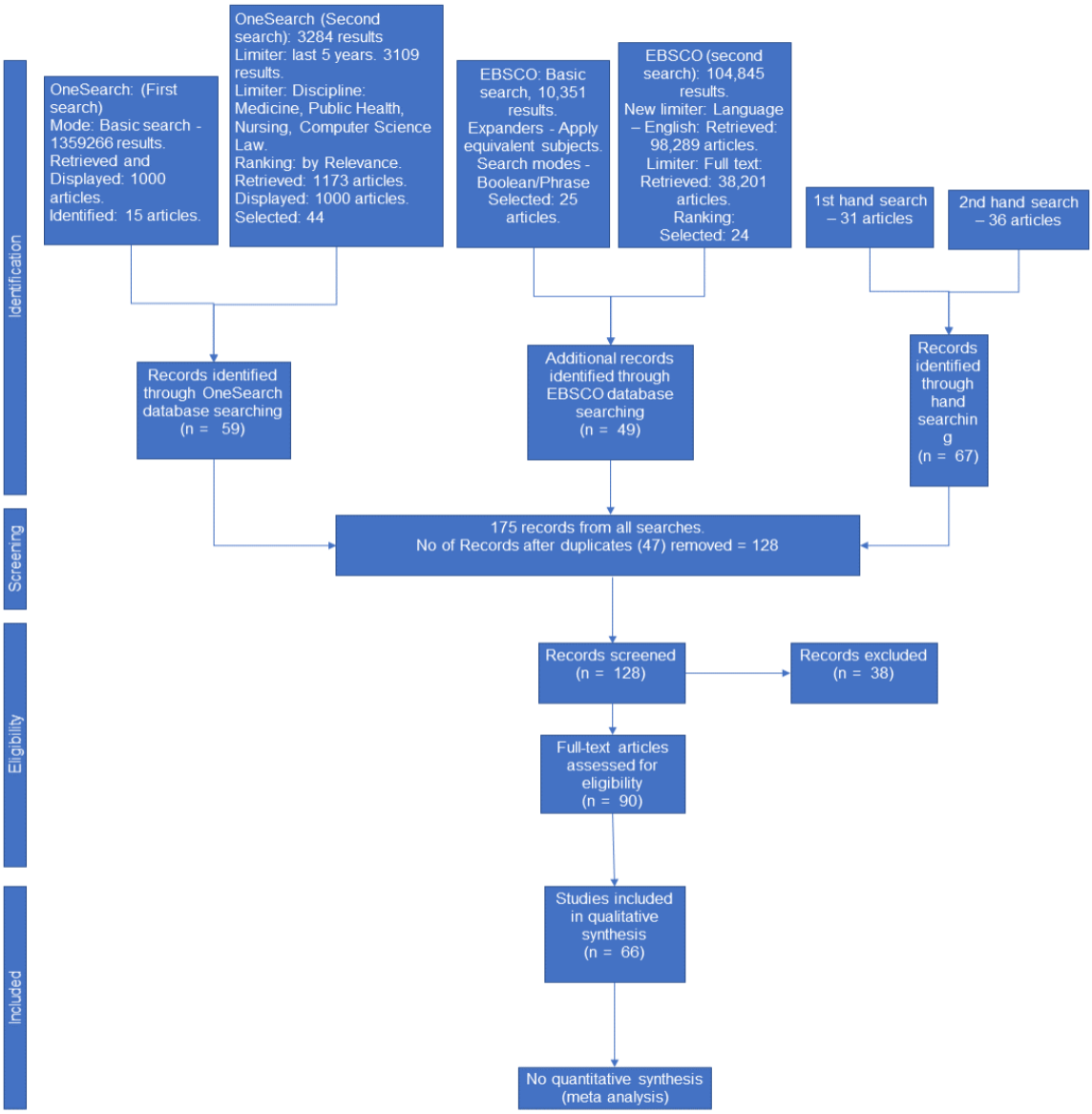
The first search of the OneSearch database search yielded 15 papers, the second search of OneSearch yielded 44 papers, a total of 59 papers combined. A first search of EBSCO resulted in 25 papers and a second yielded 24, 49 in total from EBSCO. The first-hand search yielded 31 papers and the second 36, 67 papers in total. 175 papers from all searches identified by OneSearch, EBSCO database and hand searching, respectively (Figure 3). After removal of 47 duplicates, 128 records were screened, and 38 records excluded based on not meeting the eligibility criteria. A total of 90 full text articles were assessed for eligibility.

Discussions with a second reviewer were undertaken when there was ambiguity whether to include (or exclude) papers with a final yield of 66 records included for the final qualitative synthesis. The 24 articles that were excluded at this point were found to be focused on a range of interesting but irrelevant areas, from the use of public social media platforms by clinicians for professional networking or medical education purposes, to the utilisation of consumer apps for patient peer support, the information governance risks posed by hacked medical devices, the evolving risks within apps and current statistics to be aware of regarding the use of specific consumer apps such as WhatsApp.

Sixteen of the publications were studies, 9 were literature reviews, 26 were editorials, 1 was a newspaper article and 14 were grey literature. Seventeen publications were from the UK, ten were from Ireland, eight were from the USA and 7 were international collaborations. Four were from Italy, two were from Portugal, two were from Spain, three were collaborations within the EU and one was from Holland. The rest were from a variety of countries outside the EU, including Switzerland, Canada, Hong Kong, Australia, South Africa, Turkey, Israel, India, Morocco, and Turkey. Publications covered a range of clinical specialities, from primary care to paediatrics, radiology, oncology, orthopaedics, dermatology, obstetrics and gynaecology to cardiology, pathology, and emergency medicine. The disciplines of clinicians described as using smartphone

technology and apps for clinical communications were mainly doctors but also included dentists and nurses. Several papers included the generic term *clinicians.*

Figure 3: PRISMA ScR Flow Diagram, RESULTS (June - October 2020)



3.4.2 Themes

Three themes and two sub-themes were identified, based on the objectives and research questions.

3.4.2.1 Theme 1: smartphone functionality used by clinicians in Europe to communicate sensitive patient data

The most popular functionality for clinicians in the literature was evidenced as image sharing as described in 41% (*n* = 24) of the articles, closely followed by IM at 40% (*n* = 23) and video conferencing with 19% (*n* = 11).

3.4.2.2 Theme 2: specific apps / channels are used most and are they compliant with the current GDPR policy and legislation

WhatsApp (owned by Facebook) was the consumer app most reported as popular with clinicians with 42% (*n* = 33) papers that named a specific channel, evidencing its use. WhatsApp is not compliant with current GDPR policy and legislation, and its use raises a raft of privacy and technical data security concerns as evidenced in the literature [4, 5, 10, 18, 25, 38, 45, 46, 52]. Generic IM (such as iMessage) was also extremely popular with 28% (*n* = 22) of the mentions of its use by clinicians, again, this functionality is not compliant with GDPR and raises concerns for data security [11, 49, 58]. Facebook Messenger was specifically named as used by 17% (*n* = 13) clinicians. This app, which is owned by Facebook, hosts its data in the USA and for that reason and various others, it is not deemed secure enough to be GDPR compliant. Video conferencing app Zoom was evidenced as popular in 8% (*n* = 6) of the papers that named a specific channel. The use of Zoom raises a range of security concerns and is not GDPR compliant [59, 60]. Skype was described as used in 5% of papers (*n* = 4). Skype also has been associated with a range of security issues and is not compliant with GDPR requirements or other current legislation [52].

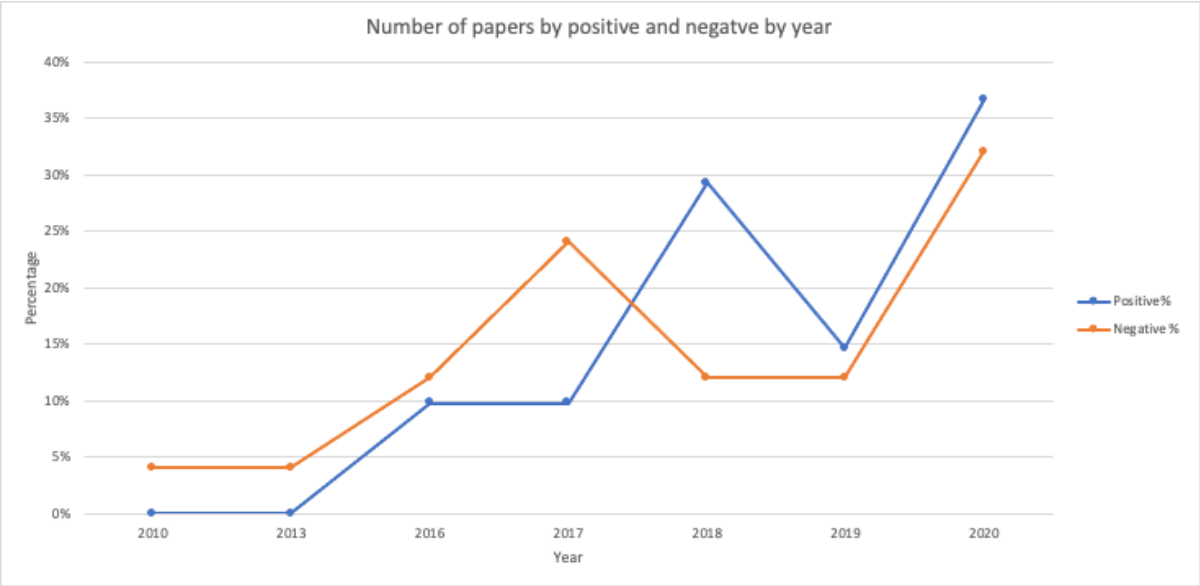
3.4.2.3 Theme 3: acknowledgement, exploration, and mitigation of security issues

A sizeable proportion of the publications around smartphone and app use for clinical communications (37.87% (*n* = 25/66)) [2, 6, 37, 39, 55, 61-79] either fail to appropriately acknowledge, totally ignore, or mitigate for technical security concerns, including issues concerning data protection, from HIPAA (in the case of USA publications) to GDPR.

Each publication was categorised as either a 'Positive Publication' or a 'Negative Publication'. Content that was identified as Positive, including content that evidenced a high level of technical fluency, made up sixty two percent of the publications [3-5, 10, 11, 14, 18, 25, 36, 38, 40, 42-46, 48-52, 54, 56, 58-60, 80-91], with general information articles or editorial from journals making up most of these publications. Studies made up 19% (*n* = 8) of these well-informed papers published. 15% (*n* = 6) were literature reviews. 2% or 1 paper was a newspaper article. 49% (*n* = 20) were general information articles such as editorials in clinical journals. 15% (*n* = 6) of the positive publications around the use of these modalities were grey literature.

The timeline of material being published that was defined as Negative and did not mitigate for technical security concerns and / or the requirements of GDPR or contained controversial content from 2016 to 2020 is insightful (see Figure 4). One paper was included from 2010 [79], and another from 2013 [78] as they were the only policies that could be found from the HSE that were intended to inform clinicians on their use of 'mobile phone' and information technology. These documents are currently available online and although they may have been well informed when published, some of the technology described and the content concerning it is obsolete and could be responsible for misleading current clinical practice. These documents contained information that were deemed both negative and positive but must currently be classified as Negative as it was published prior to the era of smartphones and the prolific popularity of apps on BYOD smartphones for clinical communications.

Figure 4: Illustration of number of papers by positive and negative by year



During 2016 and 2017 the predominance was for Negative content to be published, material that evidenced superficial understanding of the data protection or technical issues to be published, while well informed or Positive publications were largely silent. From 2018 this trend reversed, particularly in 2018 where there was a predominance of Positive, well-informed content, and content that demonstrated technical insight but nevertheless 12% (*n* = 3) of all poor advice recorded was also published in 2018. This is probably due to the heightened awareness of issues around data protection and data security due to the implementation of GDPR. Positive publications become sparse again in 2019 but in 2020, pandemic year, both types of publication proliferate again. Fifty-six percent (*n* = 14) of all the Negative quality material has been published since the implementation of GDPR. This is hugely significant, because when clinicians are under most pressure to use smartphone channels to facilitate efficiency and social distancing, the literature is providing conflicting information regarding the safety of the use of consumer apps and smartphone functionality for clinical communications.

The following graph (Figure 5) illustrates the same information by year, content type and type of publication. In 2016 and 2017, poorly informed Negative content dominated, emanating exclusively from research Studies. In 2018, the year of Positive content, demonstrating technical insight, most emanates from general information articles in journals and grey literature. In 2019,

and particularly 2020, Negative content once again emerges from general information articles, grey literature, literature reviews and studies, but these sources also published Positive content which all came once again from general information articles (editorials) in clinical journals in the main (Figure 6).

Figure 5: Illustration of number of papers by year and document type

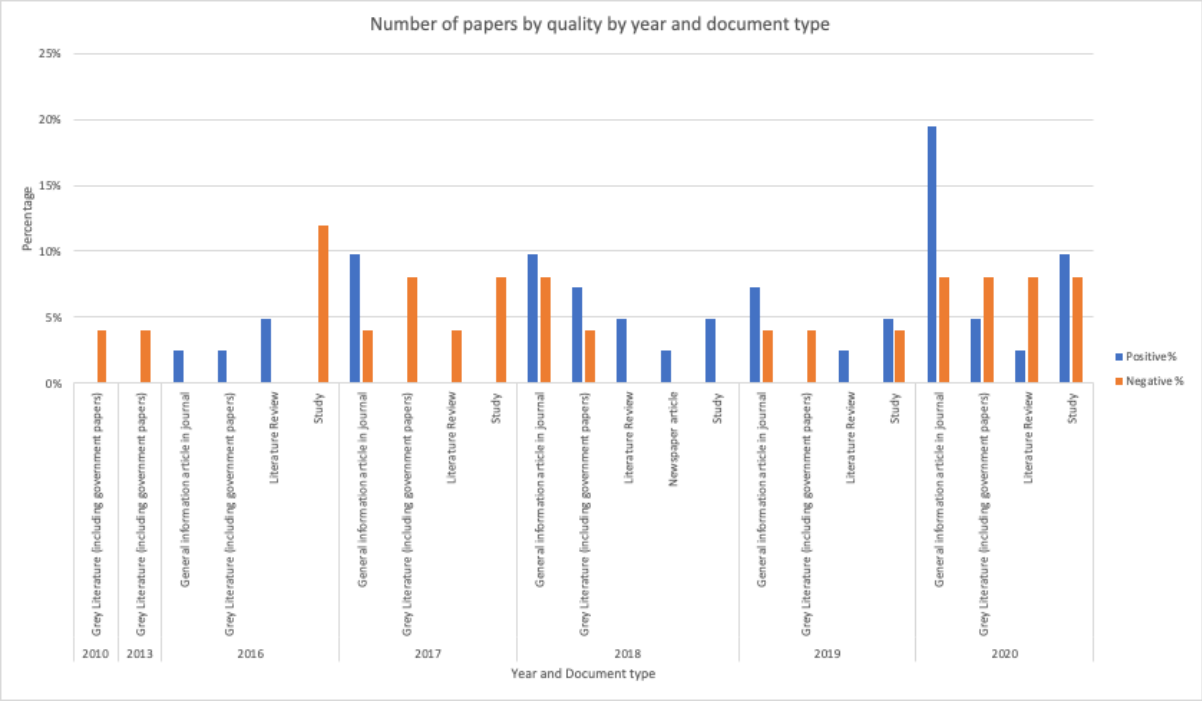


Figure 6: Supporting data for number of papers by positive and negative

Year	Sum of Positive	Sum of Negative	Positive%	Negative %
2010				
Grey Literature (including government papers)	0	1	0%	4%
2013				
Grey Literature (including government papers)	0	1	0%	4%
2016				
General information article in journal	1	0	2%	0%
Grey Literature (including government papers)	1	0	2%	0%
Literature Review	2	0	5%	0%
Study	0	3	0%	12%
2017				
General information article in journal	4	1	10%	4%
Grey Literature (including government papers)	0	2	0%	8%
Literature Review	0	1	0%	4%
Study	0	2	0%	8%
2018				
General information article in journal	4	2	10%	8%
Grey Literature (including government papers)	3	1	7%	4%
Literature Review	2	0	5%	0%
Newspaper article	1	0	2%	0%
Study	2	0	5%	0%
2019				
General information article in journal	3	1	7%	4%
Grey Literature (including government papers)	0	1	0%	4%
Literature Review	1	0	2%	0%
Study	2	1	5%	4%
2020				
General information article in journal	8	2	20%	8%
Grey Literature (including government papers)	2	2	5%	8%
Literature Review	1	2	2%	8%
Study	4	2	10%	8%
Grand Total	**41**	**25**	**100%**	**100%**

3.5 DISCUSSION

3.5.1 Summary of evidence

Image sharing [3, 4, 10, 25, 39, 44, 46-48, 50, 58, 64, 65, 67, 68, 70, 72, 81, 92, 93] IM [4, 6, 10, 11, 36, 37, 39, 44, 48-50, 58, 63-65, 68, 70, 75, 85, 90, 93, 94] and video conferencing [4, 6, 10, 11, 36, 37, 39, 44, 48-50, 58, 63-65, 68, 70, 75, 85, 90, 93, 94] are functions that are evidenced as popular and necessary for current clinical practice in general but may therefore be assumed to be of relevance to current dental practice specifically. Of significance here is the fact that if a BYOD smartphone is used to create a clinical image, it contains EXIF data by default, from date and time to geographical co-ordinates of where the image was taken. Any image created on a smartphone is also streamed by default to all of the networked devices

associated with the smartphone (for example a smart- watch, tablet, laptop, and PC) via the cloud – in the case of the iCloud – this is located outside the EU and is not GDPR compliant. The processes required to anonymise and store a digital image securely requires a level of digital literacy that is not evident in many of the articles that describe the use of this functionality. If digital images are shared between clinicians via an IM service such as WhatsApp, it is potentially downloaded by default into the image album on all the devices that receive it, and streamed to their networked devices, ultimately stored in their insecure clouds also.

3.5.2 Popular consumer apps for clinical communications

It is evident that WhatsApp, generic IM, iMessage, Facebook Messenger, Zoom and Skype are extremely popular, perhaps even endemic consumer apps, amongst healthcare professionals, despite concerns that the use of such modalities raise. The functionality offered by consumer apps are paid for by allowing the developers to access and exploit the data on a device, and if these modalities are being used by clinicians for sensitive communications, they are being paid for by enabling the app owners to access sensitive patient data.

3.5.3 GDPR

The GDPR does not allow sensitive data of EU citizens to be stored on cloud located outside the EU. This regulation applies to all EU member states without the intervention of national parliaments. If a hospital or health system is faced with a request for access to personal data (Subject Access Request or SAR) they are obliged to produce the information so that data subject or patient can correct or delete it and it is mandatory therefor that health systems, such as the HSE or NHS know where and how data is stored. This requirement is currently impossible to comply with when clinicians use WhatsApp. Issues such as this are clearly described and articulated by some authors including Masoni & Guelfi [5] illustrating their well-informed insight.

The installation of most consumer apps from WhatsApp, online calendars, Dropbox, to Google drive on any smartphone, allows the uploading of contact lists, images and messages to servers outside the EU [95] meaning that it is virtually impossible to comply with GDPR requirement for

entities such as the HSE and NHS to be able to locate all of the data being processed on a patient if requested. The business model for consumer apps is to collect, process and monetise data from their users. Masoni & Guelfi [5] state that WhatsApp is not GDPR compliant or indeed compliant with HIPAA in the USA. Some authors clearly articulate the mechanisms of consumer apps, how companies data mine devices, monetise the data they contain, and the security issues apps pose. Chen [59] describes a black box of company secrecy in his evaluation of Zoom and lists several steps that can be taken to improve privacy if no other channel is available.

A number of publications included in the review contain information that is open to dispute, could be termed as controversial and were therefor classified as Negative. NHSX [6] published advice online for clinicians around their use of messaging apps such as WhatsApp, Facetime (owned by Apple) and Skype in November 2020, and this serves as a good example of this type of content. This publication stated that clinicians in the UK are free to adopt their BYOD to facilitate the use of video conferencing for consultations, home working and mobile messaging.

3.5.4 Consent for processing

Reassurances are provided regarding off the shelf tools from Skype to WhatsApp as acceptable to use, with the patient or service user *implying consent* by accepting an invitation and commencing the consultation [6]. However, it can be argued that assuming consent from a patient to their data being shared by apps like Zoom or WhatsApp, could be perceived as unlawful, if what we are asking patients to do is to allow the clinician to contract out of GDPR data protection obligations; in effect, asking patients to agree that they are not going to be subject to the law. Where this advice refers to consent, it is specifically consent to the nature of the consultation i.e., video rather than face-to-face, rather than (GDPR) consent for any aspect of the data processing. A data controller cannot evade their legal obligations by seeking to get the patient's consent. If the patient 'consented' to opting out of the GDPR, that could not preclude the regulator from acting for a breach of the regulations as the requirements which must be met to achieve GDPR compatible consent are exacting.

Consent to engage in a remote consultation, even if it were GDPR compatible, is not the same as consent to the sharing of related data within the platform's insecure ecosystem. A patient's remedy for a breach would be under the GDPR, on the basis that the Controller cannot contract their way out of the obligations to the Data Subject. This advice was published, two years after the implementation of GDPR and four years after the two-year run-in period prior to the implementation of GDPR, to inform clinicians of the communications channels they could use during the COVID-19 Pandemic emergency. It states that the Information Commissioner has assured NHSX that she cannot envisage a situation where she would act against a health care professional trying to deliver care.

Two specific issues are troubling regarding the articulation of the ICO's position is in this document.

- The advice is limited to regulatory action being taken by the ICO itself.
- A context specific risk-based approach is taken i.e., the COVID-19 pandemic.

These are not clearly explained to the busy clinicians who may be drawing on this advice. Many medical and indeed dental consultations may relate to matters which have a significant impact on health and well-being and may involve life or limb threatening conditions where the absence of a consultation may result in genuine harm. This advice document specifically endorses consumer channels only *"where there is no practical alternative, and the benefits outweigh the risks"*. The advice contained in this document is relevant only for the duration of the current health emergency and is not a carte blanche to use these modalities for clinical communications.

Twenty-five papers are concerned more with the usefulness of the functionality available from smartphone apps and BYOD and fail to acknowledge or consider the risks associated with them. They may superficially endorse the importance of obtaining and recording consent, and of minimising patient identifiable information, but they ignore the fact that EXIF data is embedded in digital photographs by default, or that images may be streamed by default between networked devices and hosted in an inappropriately secured cloud that is not GDPR compliant. There is no

mention of the dangers posed by facial recognition software in any of the papers reviewed and several of the papers draw quite concerning conclusions:

"We can conclude that WhatsApp instant messaging system is a useful and rapid tool to share information between healthcare professionals in the real world" [66].

It is our view that WhatsApp may indeed be useful and rapid as a modality, but it is not an appropriate communications solution for clinical communications as it is not GDPR or even HIPAA compliant.

The number of papers achieving publication despite the fact that they contain poor quality content (technical and / or legal) on the use of apps for clinical communication is noteworthy. The fact that the numbers of poorly informed articles reduced the year that GDPR was implemented (2018) was encouraging. However, as the COVID-19 Pandemic struck in 2020, when the requirement for remote consultation and efficient digital communications became essential, the number of poorly informed papers achieving publication increased again and that is most concerning. These publications are misleading and will cause issues in clinical practice as busy clinicians need to be able to access well informed content to inform their clinical practice.

3.6 CONCLUSION

There is a dearth of evidence of genuinely secure channels being used to communicate sensitive patient data between clinicians within the EU, and a sizeable proportion of publications in the clinical journals fail to explore or even acknowledge the technical security considerations necessary to ensure the security of confidential patient data to meet the requirements of GDPR.

There are gaps in the knowledge around what constitutes an appropriately secure digital communications channel and the process for risk assessing and approval of such channels for secure communication of sensitive clinical data. Research studies trialling, comparing, and evaluating the use of the various secure enterprise solutions would be extremely valuable (such as Hospify or Near Me). It is also important to establish why clinicians are using insecure

consumer channels as opposed to selecting free or cheap to use secure consumer channels (such as Signal or Siilo) for clinical communications. It can be speculated that busy clinicians are simply poorly informed, potentially due to the complete absence of leadership, relevant sign posting and current policy via health systems such as the NHS or the HSE, and lack of training. This of course coupled with the ready availability of insecure technology with which clinicians are already fluent, via their BYOD mobile phones.

GDPR within the EU sign posts specific technical and security requirements for the processing of sensitive data, including health data, and the European Convention of Human Rights (article 8 and convention 108) cannot be ignored.

Clear, well-informed advice, policy, regulation, and training is evidently required to mitigate for security concerns, constraints and technical requirements around privacy and data protection regulation and legislation, in relation to the modalities being used.

CHAPTER 4 SMARTPHONE AND MOBILE TECHNOLOGY USAGE AMONGST THE DENTAL PROFESSION

A peer reviewed publication describing the conduct of an online survey to establish the extent of BYOD smartphone use among dental professionals in Ireland and the UK to meet objective 2, to determine the current use of smartphones and mobile technology among clinicians in Ireland (and UK). Publication 4, Paper 3 [96] & Publication 5, Conference Presentation [97].

- **Copy of the peer reviewed Publication: Appendix 4**
- **Copy of IADR PowerPoint Presentation: Appendix 5**
- **Copy of IADR Abstract: Appendix 6**

REFERENCES:

B. John, McCreary C., Roberts A., (2023) Smartphone and mobile technologoy use among the dental profession. Journal of the Irish Dental Association. January 2023. (PP 2 – 6) DOI: 10.58541/001c.67927

John, B., McCreary, C., Wilcox, A., Roberts, A. (2021) Smartphone clinical communication amongst Irish Dental Professionals. Conference Presentation, IADR - Irish Division. Online. 5th February 2021.

4.1 PRECIS

Technical support and digital professionalism training are required to facilitate the appropriate use of smartphone technology for dental clinicians practising in the Republic of Ireland.

4.2 ABSTRACT

4.2.1 Statement of the problem

Smartphone technologies have changed the landscape of digital communication across society. The COVID-19 pandemic has accelerated the adoption of and requirement for technical solutions to facilitate remote clinical communications. Despite the benefits of smartphones in a clinical communication context, there are risks associated with their use.

4.2.2 Purpose of the study

The primary purpose of this study was to determine the extent of smartphone use among dental professionals in the Republic of Ireland (RoI). In addition, we sought to determine the perception and knowledge of potential pitfalls, risks, and limitations of these technologies among the same population. A smaller cohort of UK dental professionals was surveyed for comparison.

4.2.3 Materials and methods

An online quantitative survey was distributed to evaluate dental professionals' knowledge and understanding of the risks and limitations of smartphone and mobile technology, providing general understanding of the current use of smartphone technology in healthcare in the RoI and the UK.

4.2.4 Results

A total of 123 responses were received from dental professionals in the RoI (UK: n=77). The majority of dental professionals confirmed that they were aware of the risks associated with

smartphone use and perceived that they were adequately skilled in digital professionalism. However, concerning practice regarding the communication of sensitive patient data was identified, with the potential for these data to be stored on insecure devices and cloud servers. Many RoI and UK dental professionals confirmed that they would need support to remove patient-identifying data when trading in their devices.

4.2.5 Conclusions

App, smartphone and mobile device ownership among dental professionals for clinical communications is widespread in the RoI (and UK), with respondents using their devices to send images (photos and radiographs) to one another. However, the risks of such activities are only partly acknowledged, with many having a lack of insight into data security.

4.3 INTRODUCTION

There is an ever-increasing accessibility and availability of smartphone and mobile technology across society. The functionality of these 'bring your own devices' (BYODs) is vast, enabling a range of current media-rich communications between users [3]. From simple text messaging or image sharing (clinical photos and / or radiographs) to video conferencing, the intention of clinical digital communications is to improve patient care [1]. These technologies were widely adopted across healthcare during the COVID-19 pandemic, when minimising in-person meetings led to the heightened use of BYODs and digital solutions to aid remote and efficient communication between clinicians and their patients [35]. Clinical communications using BYODs have been the subject of a recent scoping review, which demonstrated knowledge gaps around digital security and risk assessment for the security of clinical data [35]. Health professionals must demonstrate the appropriate competence or skill when using digital media (digital professionalism), and yet security and privacy issues are often absent from or only superficially acknowledged in the published literature. Despite the clear advantages of improved clinical communication for all, the implementation of the European Union (EU) GDPR [19] resulted in increased regulatory requirements around the technology for hosting and processing sensitive data. This, along with

the catastrophic cyberattack on the Health Service Executive (HSE) in 2021, resulted in growing concern around the use of digital modalities for clinical communication for everyone involved in current healthcare / dental practice in Ireland [1]. Given their ubiquitous nature and for sensitive patient data to become compromised, it is timely to determine the culture of smartphone use among the dental profession.

4.4 MATERIALS AND METHODS

An online questionnaire was adapted (with the permission of the authors) from relevant published studies in the Republic of Ireland (RoI) and the United Kingdom (UK) [98, 99] to explore BYOD smartphone and mobile technology use among dental professionals. Ethical approval was granted (UCC Ref: 018-131) for dissemination of a Google Form weblink to dentists and the wider dental profession (dental specialists, dental hygienists, dental nurses, etc.). The invitation to complete the questionnaire provided a convenient sample open to any dental care professional in the RoI (and UK). The questionnaire included the anonymous demographic characteristics of each individual, current use of BYOD smartphones and mobile technology for communicating patient data, and the level of perceived risk associated with their use. The questionnaire was a blend of closed and open-style questions to allow free text / elaboration. The RoI questionnaire was distributed as a weblink across a number of organisations: Cork University Dental School and Hospital (May 2020); a Dental Council of Ireland newsletter to all registrants (August 2020); an Irish Dental Association webinar (October 2020); online attendees to the Irish Division of the International Association of Dental Research (February 2021); and the Orthodontic Society of Ireland (March 2021). Plans for wider dissemination at face-to-face conferences that had been planned were curtailed due to the COVID-19 pandemic. UK dissemination of the questionnaire was undertaken through the British Dental Association and the British Association of Oral Surgeons. The resulting data are presented descriptively with no statistical analysis undertaken.

The following text has been added to the text of the published article for the purpose of further explanation. It did not serve as part of the published paper due to the restricted word limit. *The survey tool (Appendix 10) was developed specifically for the purpose of exploring the use of personal smartphone*

and mobile technologies for communication among dental clinicians in the UK and Ireland. Its design was informed by two previously published and validated surveys as mentioned above: O'Connor et al. (2014)[98], which surveyed junior doctors in Limerick, Ireland, and Mobashieri et al. (2015)[99], which was a multi centred study of use by doctors and nurses in the UK. The authors of both studies were consulted and gave permission to draw on and amend their survey tools. These provided a valuable foundation from which to customise and develop a bespoke version tailored to the dental context. The original questions were adapted and expanded upon, adding items to capture more granular detail regarding respondents' qualifications, years of clinical experience, current employer, and geographic location. These additions were designed to enable more detailed statistical analysis and to ensure the survey's relevance to the dental workforce in the two jurisdictions of the UK and Ireland but also in both public and private practice. The revised questionnaire was piloted prior to full circulation to confirm clarity, relevance, and usability. However, due to the constraints of the COVID-19 pandemic, including limited opportunities for dissemination and reduced participation rates, the final dataset did not support advanced statistical testing. As a result, only descriptive analysis was possible. The decision to limit the depth of methodological detail in the published article from which this chapter is drawn was due to strict word count limitations; however, this thesis offers the opportunity to provide fuller context and transparency regarding the survey development process.

4.5 RESULTS

Table 3: Age & Gender Demographics of Respondents

	Republic of Ireland			United Kingdom		
Age (years)	**Female**	**Male**	**Total**	**Female**	**Male**	**Total**
20-29	5 (6%)	1 (2%)	6 (5%)	6 (13%)	-	6 (8%)
30-39	20 (26%)	3 (7%)	23 (19%)	17 (36%)	5 (17%)	22 (29%)
40-49	16 (21%)	9 (20%)	25 (20%)	14 (30%)	7 (23%)	21 (27%)
50-59	21 (27%)	15 (33%)	36 (29%)	8 (17%)	11 (37%)	19 (25%)
60-69	15 (19%)	14 (30%)	29 (24%)	2 (4%)	6 (20%)	8 (10%)
≥70	-	4 (9%)	4 (3%)	-	1 (3%)	1 (1%)
TOTAL	77 (63%)	46 (37%)	123 (100%)	47 (61%)	30 (39%)	77 (100%)

4.5.1 Respondent Demographics:

A total of 123 dental professionals from the RoI and 77 dental professionals from the UK completed the online survey. A similar gender balance was observed between the RoI (females n=77; 63%) and UK (females n=47; 61%) (Table 3). A wide age range for respondents was observed, with respondents in the 20-29 and >70-year categories in both jurisdictions. The majority of RoI respondents were in the 50- to 59-year age category (n=36; 29%), and for the UK the largest number of responses were seen in the 30- to 39-year age category (n=22; 29%).

The vast majority of RoI respondents were dentists in general practice (n=92; 75%), or dentists in specialist practice (n=22; 18%), with smaller numbers of dental hygienists, dental technicians and dental nurses (Table 4). A similar distribution pattern was observed for respondents from the UK.

Table 4: Dental Professional and Employment Demographics

	Republic of Ireland	**United Kingdom**
Dental Role	**Total**	**Total**
Dentist	92 (75%)	55 (71%)
Dental Specialist	22 (18%)	18 (24%)
Dental Hygienist	1 (1%)	0 (0%)
Clinical Dental Technician	0 (0%)	1 (1%)
Dental Nurse	8 (6%)	3 (4%)
Main Employment		
Public Sector	45 (37%)	55 (71%)
Private Sector	78 (63%)	22 (29%)

The demographic relating to employment type differed between the RoI and the UK – a much higher percentage of respondents work in the private sector in the RoI (n=78; 63%) than in the UK (n=22; 29%).

4.5.2 Current use of smartphones and mobile technology for communicating patient data:

High levels of smartphone use were observed among respondents (RoI 98%; UK 100%), with the Apple iPhone the most popular device (RoI n=78; 63%, and UK n=58; 75%). Android devices were less popular in the RoI (n=41; 33%) and UK (n=18; 23%), with the remainder using "other devices". Respondents were asked to answer questions in the following domains (Table 5):

- Technological skills: A majority of respondents from both jurisdictions (RoI n=105; 85%; UK n=71; 92%) perceived that they had an "appropriate level of technological skill to use a smartphone", although this belief was not evenly distributed across employment type in the RoI. The majority of those RoI respondents who perceived that they did not possess an appropriate level of technological skill to use a smartphone were in the private sector. Only six UK respondents felt that they did not have the technological skills to use a smartphone, with one of these being in the private sector.
- Usefulness: The majority of RoI respondents (n=95; 77%) confirmed that they found their smartphones useful for the meaningful exchange of clinical information (UK n=70; 91%) and this occurred in both public and private sectors.
- Sending images by messaging: Of the RoI respondents, the majority (n=78; 63%) confirmed that they use or have used their smartphones to communicate images, via WhatsApp or standard picture messaging, with a similar pattern observed in the UK (n=48; 62%). Of the RoI respondents who confirmed sending images, the majority were from the private sector.
- Patient / clinical information stored on their smartphone: Half of RoI respondents confirmed that they had or might have clinical information currently stored on their BYOD smartphones and, of these, the majority worked in the private sector. UK respondents who had patient / clinical information stored on their smartphone were mostly public sector.
- Multiple streaming devices: The majority of RoI respondents (n=90; 73%) confirmed that they own multiple smart devices and, of these, almost one-third (n=36; 29%) confirmed

that data does (or has the potential to) stream between these devices, with respondents in both the public and private sectors, a finding also seen in the UK.

- Streaming to the cloud: Half of RoI respondents confirmed that their devices did (or had the potential to) stream sensitive patient data to the cloud, an activity that was observed in both the public and private sectors, with similar results seen among UK responses.

Table 5: Current Use of Smartphones & Mobile Technology for Communicating Patient Data

			Republic of Ireland			United Kingdom		
			Total	**Public**	**Private**	**Total**	**Public**	**Private**
1	**Technological skills**	**Yes**	105 (85%)	42 (34%)	63 (51%)	71 (92%)	50 (65%)	21 (27%)
		No	18 (15%)	3 (2%)	15 (12%)	6 (8%)	5 (6%)	1 (1%)
2	**Usefulness**	**Yes**	95 (77%)	34 (28%)	61 (50%)	70 (91%)	49 (64%)	21 (27%)
		No	28 (23%)	11 (9%)	17 (14%)	7 (9%)	6 (8%)	1 (1%)
3	**Sending images by instant messaging and/or app**	**Yes**	78 (63%)	21 (17%)	57 (46%)	48 (62%)	35 (46%)	13 (17%)
		No	45 (37%)	24 (20%)	21 (17%)	29 (38%)	20 (26%)	9 (12%)
4	**Currently have patient/clinical information on smartphone**	**Yes**	62 (50%)	13 (10%)	49 (40%)	29 (38%)	22 (29%)	7 (9%)
		No	61 (50%)	32 (26%)	29 (24%)	48 (62%)	33 (43%)	15 (19%)
5	**Multiple devices streaming between each other**	**Yes**	36 (29%)	12 (10%)	24 (20%)	22 (29%)	15 (19%)	7 (9%)
		No	87 (71%)	33 (27%)	54 (44%)	55 (71%)	40 (52%)	15 (19%)
6	**Devices streaming to the cloud**	**Yes**	61 (50%)	21 (17%)	40 (33%)	30 (39%)	21 (27%)	9 (12%)
		No	62 (50%)	24 (20%)	38 (31%)	47 (61%)	34 (44%)	13 (17%)

4.5.3 Level of perceived risk associated with Smartphone and mobile technology use:

Respondents were asked to answer questions in the following domains (Table 6):

- Risk awareness: The majority of the respondents from the RoI (n=94; 76%) considered themselves aware of the risks associated with the use of smartphones and smart devices for the communication of work-related data; respondents were in both the public and private sector, with a similar UK trend (n=67; 87%).
- Skilled in digital professionalism: Approximately half of RoI dental professionals believed themselves to be skilled in digital professionalism (n=66; 54%); respondents were in both public and private sector, with a similar UK trend (n=50; 65%).
- Awareness of need for IT support: The majority of RoI respondents (n=98; 80%) were unaware of any IT supports for wiping or 'cleaning' BYODs at the point of trading in, trading up or abandoning devices. A similarly high percentage of UK respondents reported a lack of awareness of such IT support (n=54; 70%).
- Value of IT support: Respondents in the RoI (n=114; 92.6%) agreed that IT support when trading in devices would be useful (UK, n=74; 96%). The highest levels of value for such IT support were observed in the RoI private and UK public sectors.

Table 6: Level of Perceived Risk Associated with Smartphone and Mobile Technology Use

			Republic of Ireland			United Kingdom		
			Total	**Public**	**Private**	**Total**	**Public**	**Private**
1	**Risk Awareness**	**Yes**	94 (76%)	38 (31%)	56 (46%)	67 (87%)	47 (61%)	20 (26%)
		No	29 (24%)	7 (6%)	22 (18%)	10 (13%)	8 (10%)	2 (3%)
2	**Skilled in Digital Professionalism**	**Yes**	66 (54%)	25 (20%)	41 (33%)	50 (65%)	34 (44%)	16 (21%)
		No	57 (46%)	20 (16%)	37 (30%	27 (35%)	21 (27%)	6 (8%)
3	**Awareness of IT Support Available**	**Yes**	25 (20%)	7 (6%)	18 (15%)	23 (30%)	13 (17%)	10 (13%)
		No	98 (80%)	38 (31%)	60 (49%)	54 (70%)	42 (55%)	12 (16%)
4	**Would Value IT Support**	**Yes**	114 (93%)	42 (34%)	72 (59%)	74 (96%)	53 (69%)	21 (27%)
		No	9 (7%)	3 (2%)	6 (5%)	3 (4%)	2 (3%)	1 (1%)

4.6 DISCUSSION

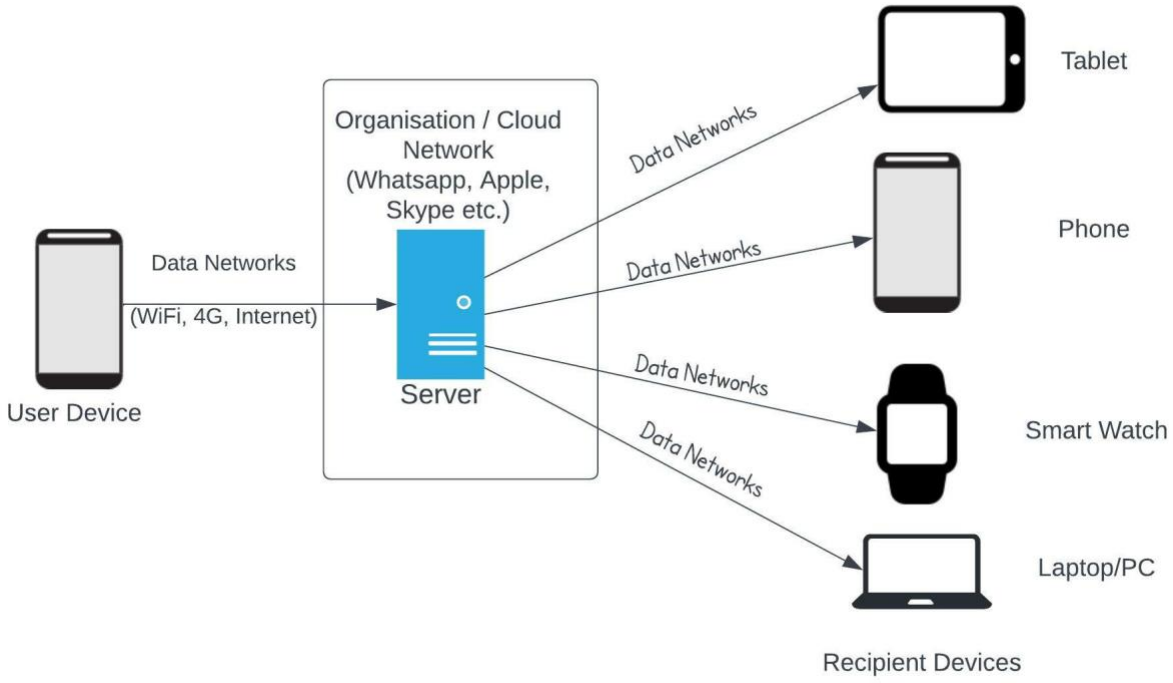
This study used an online questionnaire distributed to a convenient sample of dental care professionals in the RoI and UK and demonstrates that smartphone and mobile technology use is widespread. No attempt was made to match the demographics of RoI respondents with those of the UK; rather, the data was collated for trend comparison. Respondents confirmed that their smart devices are useful for the meaningful exchange of clinical information to assist patient management. However, while dental professionals may allow the exchange with a positive intention, the results confirm the use of inappropriate and insecure messaging apps [5] and video conferencing channels (e.g., WhatsApp and Zoom) [59] for the communication of sensitive patient data. Dental professionals currently practising within the EU (and UK) are obliged to work within the requirements of the GDPR. A minority of clinicians use SMS to communicate patient clinical

information, contravening their GDPR obligations [5]. Accepting the limitations of the study, clinicians are mainly unaware of the potential for sensitive data to be obtained and exploited [1], and yet clinicians ignoring GDPR may threaten patient confidentiality and bring the profession into disrepute. For the avoidance of doubt, the use of instant messaging and commercial apps such as WhatsApp for clinical communications is insecure and not GDPR compliant [5].

With regard to level of perceived risk, a large majority of dental professionals in the RoI confirmed that they had the appropriate level of technological skill to use a smartphone. Given the number of respondents confirming the streaming and storage of confidential patient data to additional networked devices (laptops, smartwatches, iPads, etc.), this confidence seems misplaced. This study raises information governance concerns regarding the potential for numerous insecure locations where sensitive patient data is being stored and points to an unmet need for further clinician training in this area.

A larger proportion of RoI dental professionals who practise privately responded to the questionnaire than in the UK sample, and report sending clinical images insecurely and storing patient information on insecure devices in concerning numbers. This may be a consequence of a lack of access to enterprise/institutional technology supports that might be available in the public sector (e.g., the HSE) and also suggests a requirement for private sector training. Only half of the RoI cohort were confident to confirm that their BYODs were not streaming work-related data to their associated non-institutional clouds, further highlighting the potential for sensitive patient data breaches. It appears to be poorly understood that the likes of the Apple iCloud are hosted in unregulated servers outside the European Economic Area (EEA) and therefore are not GDPR compliant. Figure 7 illustrates the potential for smart devices to stream data between networked devices via potentially non-GDPR-compliant and insecure cloud servers, an issue that is poorly acknowledged in the literature [35].

Figure 7: Illustration of data streaming between networked devices via the cloud



The professional, ethical, security and legal concerns posed by popular messaging apps are established [1, 4, 5]. However, the wider functionalities associated with these modalities, including the selection of secure channels to communicate patient data, the data security issues posed by information streaming between networked devices, the streaming of sensitive patient data to insecure cloud servers, and the cleaning of devices before they are abandoned, traded in, or traded up, provide further areas for concern. Poor awareness regarding phone stewardship (protecting and being responsible for the data held on a mobile phone) [47] also evidences a requirement for digital professionalism and technical training for even the most experienced dental professionals. Despite lack of insight with regard to data security, there is a high level of recognition among professionals that supports the requirement for tasks such as wiping devices of patient-identifying data in the public and private sectors.

4.7 CONCLUSIONS

App, smartphone, and mobile device ownership among dental professionals for clinical communications is widespread in the RoI (and UK), with this study demonstrating that dental professionals are using their devices to send images (photos and radiographs) to one another. The risks associated with these activities are only partly acknowledged, with many dental professionals evidencing a lack of insight into data security. Dental professionals may benefit from mobile device management software to remove data when required, online portals to securely store and manage clinical images, and digital professionalism training. Some of these solutions are emerging in the UK's National Health Service (NHS) and could be included as part of professionalism and ethics training provided to clinicians through their indemnity organisation, which has flagged concerns in professional publications [100].

We conclude that there is an unmet need for technical solutions, technical support, and digital professionalism training to facilitate the appropriate use of smartphone technology for dental clinicians practising in the RoI. Until these supports are in place, it is essential for dental professionals to engage in the use of smartphone and mobile technology for the dissemination of clinical data with caution as they try to best serve their patients.

CHAPTER 5 NAVIGATING THE WILD WEST: A REVIEW OF GUIDANCE ON CLINICAL COMMUNICATIONS USING PERSONAL BYOD, IM AND THIRD-PARTY APPS IN IRELAND AND THE UK

A second peer reviewed scoping review was conducted to meet objective 3, to evaluate the current guidelines that are available to inform practice-based communication between clinicians using personal BYOD smartphones, IM and third-party Apps in Ireland and the UK. Publication 6, Paper 4 [27].

REFERENCE:

John, B., Heavin, C., Roberts, A. (2025) Navigating the Wild West: A Review of Guidance on Clinical Communications using personal BYOD, IM and Third-Party Apps in the UK and Ireland. Frontiers in Digital Health, 2024, 6, DOI: https://doi.org/10.3389/fdgth.2024.1457848

5.1 ABSTRACT

5.1.1 Introduction

The ubiquity of Bring Your Own Device (BYOD) personal smartphones, Instant Messaging (IM), and third-party apps, has made these technologies compelling for efficient communications between clinicians regarding patient care. However, the sensitivity of patient-related information necessitates secure, GDPR compliant modalities that prevent unauthorised access and ensure confidentiality. This scoping review explores existing guidelines, policies, and regulations that advise clinicians in the UK and Ireland on the secure use of these digital communication tools.

5.1.2 Methods

Following the Joanna Briggs Institute (JBI) updated Framework for Scoping Reviews and the PRISMA ScR guidelines, this review examines the literature to identify relevant guidelines, policies, and regulations informing current clinical practice on the use of this technology. Academic databases including OneSearch, Embase, EBSCO, PubMed, Medline, and CINAHL were searched, in addition to hand searches of professional entities' websites, including trade unions, regulators, two national health systems, and several employers. Direct inquiries were made to 69 professional entities via telephone, email, websites, and X (formerly known as Twitter).

5.1.3 Results

The review identified 18 papers that broadly recognise the importance of secure communication. However, a lack of information on the appropriate selection or configuration of these popular technologies was evident. Most guidelines emphasise general security and data protection standards rather than providing clear actionable recommendations for technology use, thereby leaving a significant gap in technical guidance for clinicians.

5.1.4 Discussion

There is a distinct lack of detailed, specific, consistent technical guidance available to clinicians. This review evidences an urgent requirement for enhanced guidelines that specify the most secure platforms, appropriate features, and configuration to maximise the security and confidentiality of clinical communications. Further research is recommended to develop comprehensive, actionable advice for clinicians.

5.2 INTRODUCTION

The widespread adoption of smartphone technology has transformed global communication practices, with a significant uptake in the use of digital tools such as personal smartphones Instant Messaging (IM) and third-party apps (e.g. WhatsApp) for private communications between clinicians regarding patient care. These communications are well intended by clinicians as they strive for timely and optimal patient management, amidst stringent data processing requirements under the GDPR within the EU [19]. In their publication on developing a core competency framework for clinical informatics professionals, Davies et al. [101] emphasise the critical need to enhance digital skills across the entire healthcare workforce to prepare for a digitally driven future where IT significantly influences clinical practice. This backdrop poses an essential question: *How do clinicians determine the most appropriate methods for communicating with each other using their personal devices?* Professional bodies—including trade unions, Royal Colleges, regulators, health systems (e.g. UK National Health Service (NHS) and Irish Health Service Executive (HSE)), and large and small private healthcare providers, provide clinical guidelines. These guidelines aim to inform clinicians on the full range of their professional duties, from clinical procedures to record keeping, confidentiality, consent, and communications.

A scoping review by John (2022) [35] evidenced growing international concern regarding the use of non-enterprise digital channels for confidential clinical communications among healthcare professionals noting that while practitioner reports revealed widespread adoption of apps and

smartphones, they often lacked critical insights into the technical security measures required to safeguard patient data in compliance with GDPR [19]. A recent survey revealed the widespread adoption of apps and smartphones for clinical communication between dental professionals in the Republic of Ireland and the UK, signifying a reliance on personal smartphone modalities for sharing clinical information, including images, often without fully understanding the data security implications of this practice [96].

In the USA, large financial institutions like Wells Fargo and BNP Paribas faced substantial fines in 2023 (114 million and 35 million euros, respectively) for their employees' unofficial use of messaging services such as WhatsApp for business purposes, thus avoiding regulatory oversight [102]. Reflecting this trend, the UK's Information Commissioner's Office (ICO) reprimanded NHS Lanarkshire in 2023 when their staff were found to be improperly sharing patient data via WhatsApp, a method that violates existing policies [103]. In a statement regarding the case, the Information Commissioner stressed the importance of securely handling sensitive patient data to maintain public trust in healthcare data management [103]. The ICO emphasised that data protection standards must not be compromised. Although NHS Lanarkshire was not fined on this occasion, the incident highlighted the potential for significant penalties under the GDPR. Recent policy from the HSE [104, Page 4] explicitly classifies WhatsApp and IM as social media platforms and states; *"Data protection laws protect an employer where the employees' use of social networking sites causes damage to that organisation's reputation or leads to the release of confidential information.*" This is a clear indication that the HSE interprets the liability for any breach lying with the employee, thereby highlighting the importance of clinicians adhering to policy and guidance on this issue.

In August 2022, an initial exploratory search of academic databases, to identify relevant guidelines available to clinicians across all 26 EU health systems yielded no results. Despite extensive efforts, including a thorough hand search of national health system websites and direct communication, the absence of publicly accessible policies was noted. The complexity of navigating these health systems websites, many of which were available in the English language but segmented by region or specialty, further hampered access to existing publications or

policies. Prior searches, including inquiries to The European Observatory on Health Systems and Policies, the WHO's library, and the Wellcome Library, also proved fruitless.

This scoping review aims to identify and evaluate the existing guidelines, regulations, and policies available to clinicians in Ireland and the UK for managing sensitive communications between each other via personal BYOD smartphones, IM, and third-party apps. For the purposes of this study, 'clinicians' refers broadly to healthcare professionals across various disciplines, including but not limited to doctors, nurses, dentists, and allied health professionals, who use personal digital devices to communicate with each other regarding patient care. The focus is specifically on scenarios where patient data is exchanged between professionals and the guidelines that inform these interactions.

5.3 METHODS

The methodology for this scoping review was informed by the Joanna Briggs Institute (JBI) Methodology [32] and adhered to the Preferred Reporting Items for Systematic Reviews and Meta-analysis guidelines for scoping reviews (PRISMA ScR). The updated JBI framework for scoping reviews was chosen due to its established rigour and suitability for mapping broad and complex evidence landscapes, particularly in areas lacking highly specific guidance, as is the case for clinicians' use of personal digital devices for secure communications. A scoping review approach was selected over a systematic review because it allows for a more comprehensive exploration of the types and scope of guidance available, rather than focusing solely on evaluating outcomes. Alternative frameworks, such as systematic review methodologies (e.g., PRISMA), were considered; however, these approaches did not align with the study's objective to map and synthesise a broad range of policy, guideline, and regulatory documents without evaluating specific intervention outcomes.

5.3.1 Review Question

What resources (regulations, guidelines and or policies), are available to inform practice-based communications between clinicians using personal BYOD smartphones, IM and third-party Apps in the UK and Ireland?

5.3.2 Eligibility criteria

5.3.2.1 Inclusion Criteria:

- Position statements, Regulatory documents, Guidelines or Policies issued by healthcare employers, health systems, regulators, or professional organisations including trade unions in the UK and Ireland.
- Targeted at clinicians, including but not limited to nurses, doctors, dentists, and health and social care professionals.
- Focused on secure, clinical communications between clinicians.
- Pertaining to the use of BYOD personal smartphones and or IM, third-party apps (such as WhatsApp, Signal or Siilo) platforms.
- Published in the English language post-May 2018, aligning with the implementation of General Data Protection Regulation (GDPR).

5.3.2.2 Exclusion Criteria:

- Publications not specifically concerning practice-based communication between clinicians using personal BYOD smartphones, IM, or third-party apps.
- Journal articles, including literature reviews, editorial or research papers.
- Publications that only concern social media sites for public engagement.
- Publications specific to the pandemic emergency period only.

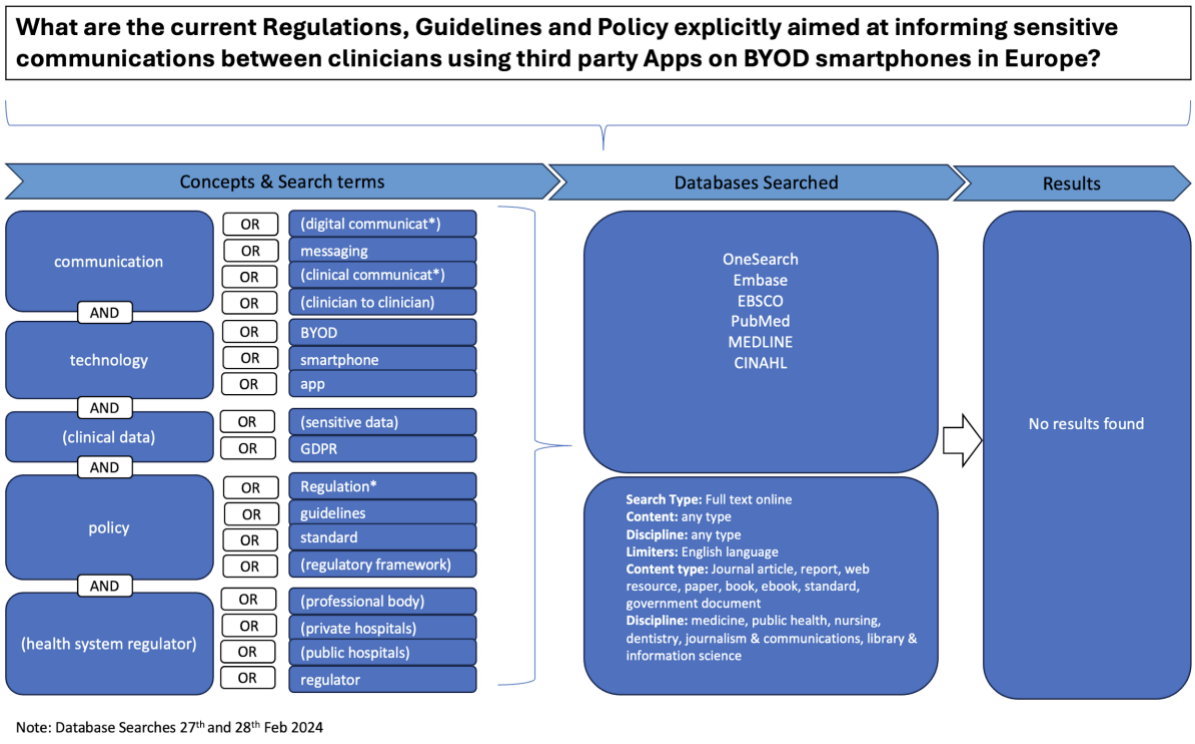
Several significant publications by regulators such as the General Medical Council [105] the Medical Council of Ireland [106] and the Health and Care Professions Council [107] were excluded due to their

lack of specific guidance regarding current technology, security considerations and obligations under the law.

5.3.3 Sources

Given the challenges in identifying relevant publications during the preliminary searches, the focus was expanded to access policies and guidelines within the UK and Ireland via academic databases, hand searches of websites and by contacting relevant organisations directly via telephone and social media. The search was limited to guidelines, regulations, policy, and position statements by health systems, a broad range of regulators, professional bodies, public and private hospitals, and trade unions (such as the Dental Defence Union (DDU), Medical Defence Union (MDU), Irish Nurses and Midwives Organisation (INMO)) allowing for a comprehensive exploration of the guidance available.

Figure 8: Study Search Strategy



Note: Database Searches 27th and 28th Feb 2024

5.3.4 Search Strategy

A comprehensive search was conducted using keywords related to secure clinical communications via personal BYOD smartphones, IM, and third-party apps across databases including OneSearch, Embase, EBSCO, PubMed, Medline, and CINAHL (Figure 8). Additionally, general online searches and direct inquiries via telephone, email, and social media were made to 69 professional entities in the UK and Ireland (Appendix 11).

5.3.5 Study/Source of Evidence Selection

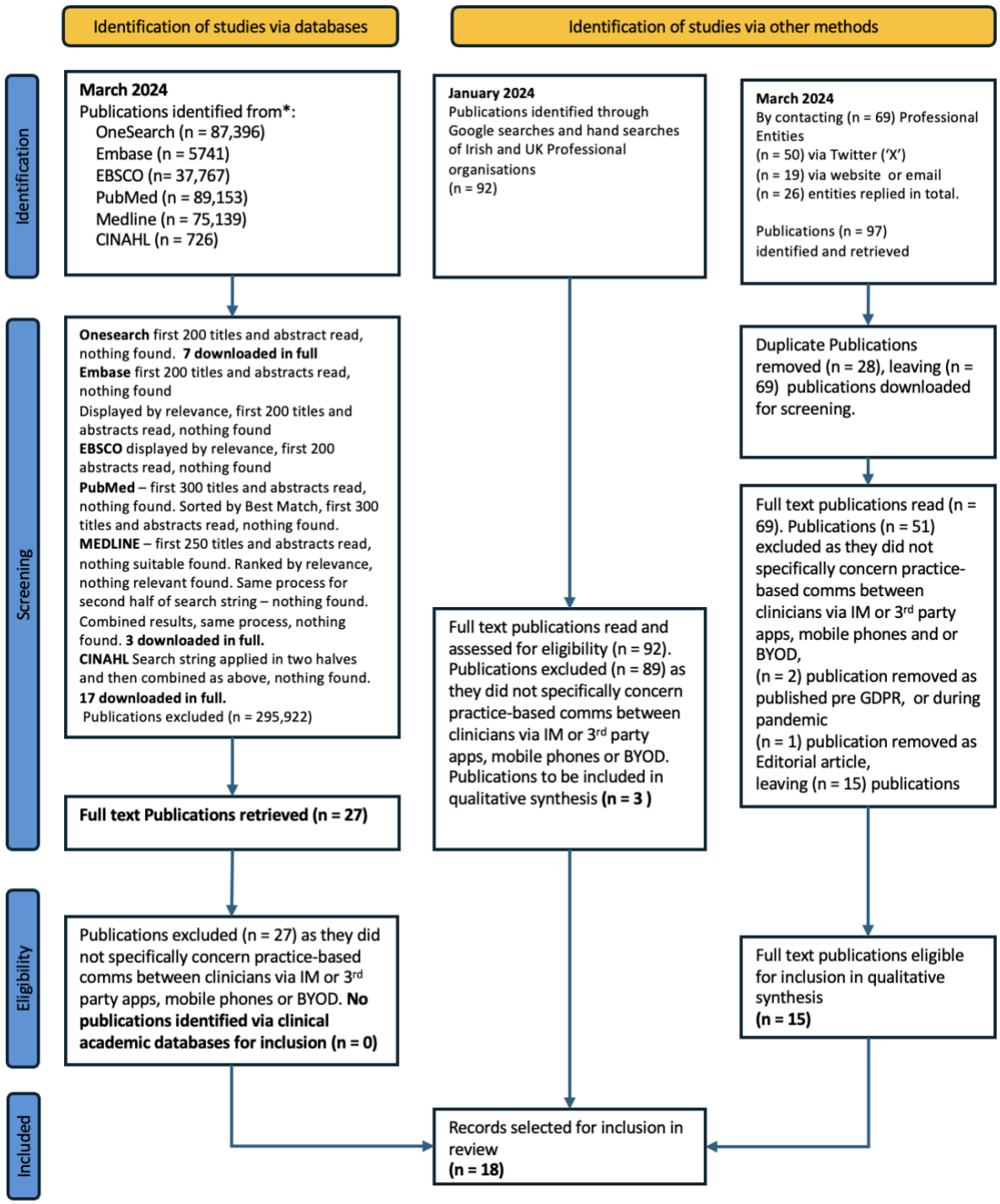
Initial screening involved reviewing titles and abstracts against eligibility criteria, followed by full-text evaluation of potentially relevant publications. Data extraction was performed using a Data Extraction Form (DEF) to capture publication details, type of publication, geographical focus, and practical guidance on secure communications (Table 7). The draft data extraction tool was piloted, refined, and revised prior to the process.

5.3.6 Data Extraction

The initial screening of titles and abstracts was conducted by one reviewer assessing each against eligibility criteria. Potentially relevant publications were then retrieved for evaluation. The data extraction was systematically performed using the DEF, where citation details and all relevant key variables were recorded.

Discrepancies that arose during the screening and selection processes were resolved through discussion and consensus, involving all three reviewers. If necessary, authors were contacted to request additional data or clarify ambiguities. The inclusion and exclusion of publications, along with reasons for exclusion at the full-text stage, were meticulously documented following the PRISMA-ScR Guidelines to ensure transparency and reproducibility and are documented in the PRISMA-ScR flow diagram (Figure 9).

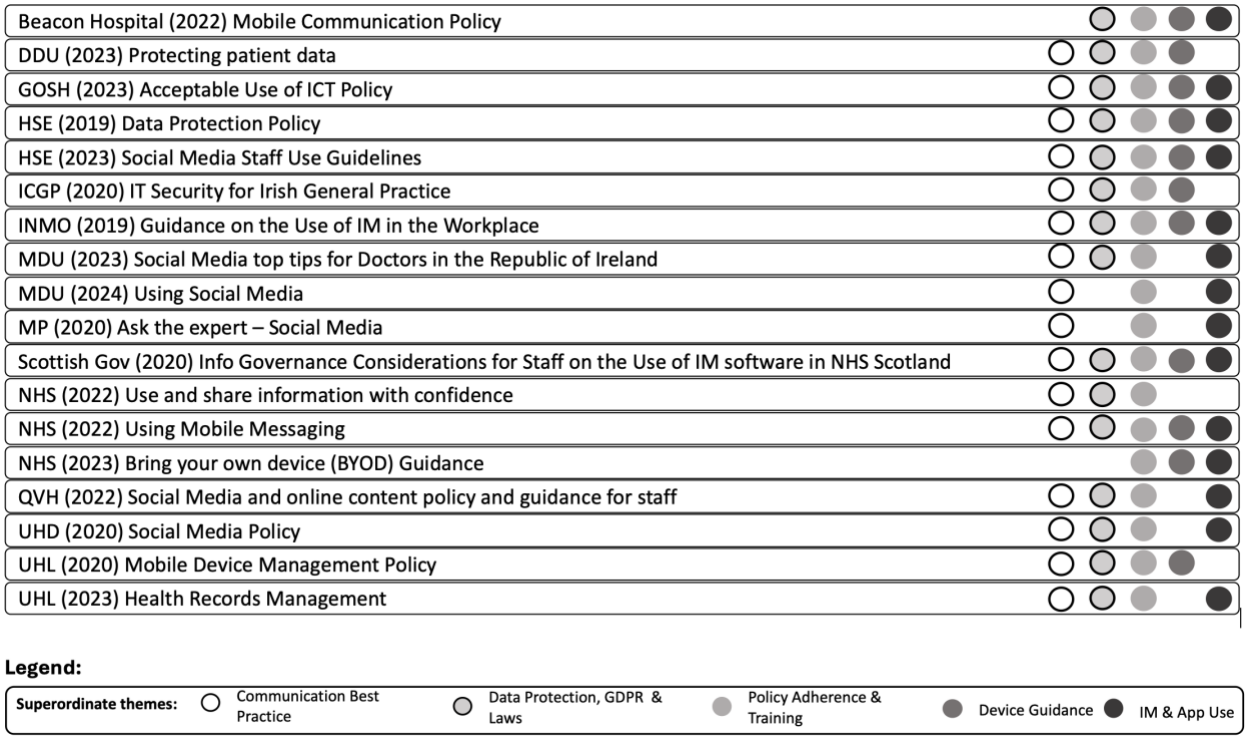
Figure 9: PRISMA ScR Flow Diagram RESULTS (January - March 2024)



5.4 DATA ANALYSIS AND PRESENTATION

Data from the included studies were uploaded into EndNote citation management software and NVIVO a qualitative data analysis software to facilitate narrative synthesis and thematic analysis. In NVIVO, documents were systematically coded according to thematic categories based on Braun and Clarke's [108] six-step thematic analysis method. This method involved familiarisation with the data, generating initial codes, and reviewing these codes to identify recurring themes and common concepts across the publications (Figure 10). NVIVO's features, such as code categorisation, query functions, and visualisation tools, supported an organised approach to analysing patterns and consolidating insights.

Figure 10: Publications Mapped to Superordinate Themes



5.5 RESULTS

The search strategy identified eighteen publications and Table 8 presents a visual overview of these publications alongside the five superordinate themes and eighteen subthemes developed from our analysis.

5.5.1 Communication Best Practice

A superordinate theme that emerged from the review in 16 of the publications is the provision of broad guidance regarding digital communications best practices, addressing the significance of confidentiality, consent, and record-keeping. This content was frequently relevant and coded to additional superordinate themes such as Data Protection, GDPR and Laws, Device Usage, IM, and Third-Party app Use, though they are present in varying degrees of detail.

5.5.1.1 Confidentiality

This subtheme was identified in 16 of the publications and broadly refers to key principles but offered little technical detail or practical guidance. Examples of such broad statements include "*individual dental professionals have an ethical duty of patient confidentiality, and must keep patient data from being mislaid or accidentally disclosed*" [109].

5.5.1.2 Consent

Issues concerning consent were identified in seven publications. Gaining informed consent from patients for data sharing via IM or third-party apps is notably absent, with the focusing on staff adherence to BYOD policies and the broader implications of consent for public data sharing.

5.5.1.3 Record Keeping

Record keeping issues were raised in nine of the publications, with guidance most often discussed in terms of principles, and scant acknowledgement of the technical and legislative requirements, standards or features required to ensure that records are kept securely, in compliance with the requirements of GDPR [19]. For example, the DDU [109, Page 1] quotes directly from the GDC's standards [110, Principle 4.5] which states clinicians must "*keep patients' information secure at all times, whether your records are held on paper or electronically*".

Table 7: Snapshot of Data Extraction Form (DEF)

								INCLUSION CRITERIA							EXCLUSION CRITERIA			
Included	**Title**	**Author**	**Year**	**Author is Health System (HSE/NHS)**	**Author is Regulator**	**Author is Professional Body**	**EU or Territory in which the paper is published**	**Position statement, regulation, guideline, or policy issued by employer, health system, governing body, or professional organisation**	**Targeted at clinicians, including but not limited to nurses, doctors, dentists, & AHPs**	**Focused on/relevant to the topic of sensitive clinical communications between clinicians**	**Pertaining to the use of third-party apps (such as WhatsApp or Siilo) and/or instant messaging platforms**	**Addressing the utilization of smartphones /mobile devices and/or BYOD**	**English Language**	**Post GDPR, NOT specific to Pandemic**	**Not specifically concerning practice based communication between clinicians using via IM/3rd party apps, and personal mobile phones as BYOD**	**Journal articles, literature reviews, editorial or research papers**	**Concerning only social media for broadcast & public engagement**	**Rationale for inclusion**
Yes	Using Social Media	MDU	2024	NO	NO	YES	UK	YES	YES	YES	YES	NO	YES	YES	NO	NO	NO	This advice is the opposite to that of Dr Ellie Man from the same organisation in 2022, 'Smartphone safety'. Both pieces still available online.
Yes	Social media in the Republic of Ireland, top tips for doctors	MDU Ireland	2023	NO	NO	YES	Republic of Ireland	YES	YES	YES	YES	NO	YES	YES	NO	NO	NO	One paragraph only
Yes	HSE Social Media Staff Use Guidelines	HSE	2023	YES	NO	NO	Republic of Ireland	YES	YES	YES	YES	YES	YES	YES	NO	NO	NO	HSE *"REMEMBER: Data protection laws protect an employer where the employees' use of social networking sites causes damage to that organisation's reputation, or leads to the release of confidential information."* Mostly things are forbidden but that is good advice! Mentions 'messaging apps", Whatsapp and private messaging superficially
Yes	Bring Your Own Device (BYOD) guidance	NHS Trans Directorate	2023	YES	NO	NO	UK	YES	YES	YES	YES	YES	YES	YES	NO	NO	NO	Minimal advice for clinicians, better advice and links for IG professionals. It literally says you should be able to use your own device for work where there is no alternative, and your employer should ask you to sign a policy and what that policy should say.
Yes	Protecting patient data	DDU	2023	NO	NO	YES	UK	YES	YES	YES	NO	NO	YES	YES	NO	NO	NO	Really useful ALTHOUGH appears to specifically avoid acknowleding communications and apps, the general advice it provides is useful. Concerns mobile phones and includes general advice on electronic data.
Yes	Health Records Management?	UHL NHS Trust	2023	YES	NO	NO	UK	YES	YES	YES	YES	YES	YES	YES	NO	NO	NO	This policy specifically includes text messages as health records.
Yes	Acceptable Use of ICT Policy	GOSH	2023	YES	NO	NO	UK	YES	YES	YES	YES	YES	YES	YES	NO	NO	NO	Relevant
Yes	Using Mobile Messaging	NHS Trans Directorate	2022	YES	NO	NO	UK	YES	YES	YES	YES	YES	YES	YES	NO	NO	NO	Some useful information for clinicians, but in a separate section for IG professionals, its says they should work with colleagues to manage any risks associated with using mobile messaging apps, to come up with a solution that will ensure that the benefits to care can be delivered. A data protection impact assessment (DPIA) can support you to do this. A DPIA must be carried out before implementing the use of an app, including due diligence on the provider, trackers and permissions embeded in the app.

Legend: This table provides the variables extracted from the relevant publications during the review process. Key variables include citation details, publication year, publisher classification (e.g., regulator, health system, professional organisation), type of publication (e.g., regulation, guidelines, policy), the geographical focus of the publication, and whether the publication provides practical guidance for secure interprofessional communication using personal BYOD smartphones, IM, or third-party apps. The extracted data were systematically recorded to assist with the analysis and synthesis of the finding

5.5.2 Data Protection, GDPR and Laws

This superordinate theme refers to guidance regarding data protection and compliance with laws and was raised in 15 of the papers. Few specific obligations were raised concerning how these laws apply to the use of personal BYOD, IM, or third-party apps for communications between clinicians.

5.5.2.1 Access to Data

Four papers refer to a legal requirement for access to data in respect to rights such as portability or correction by data subjects (patients), or for personal data not to be transferred to third parties outside the European Economic Area (EEA) or for the protection of the data from destruction or damage, a requirement for compliance with GDPR [19].

5.5.2.2 Data Transfer

Eight publications superficially acknowledged the security requirements for the transfer of health-related data to comply with GDPR.

5.5.2.3 Rules, Regulations and Acts etc.

The importance of laws in general, from mentioning laws in general to signposting the specific requirements for clinicians processing patient data using current 'digital technologies' under particular acts or laws was found in 14 papers. However, their specific relevance to the use of BYOD smartphones, IM and third-party apps for secure communication was sometimes ambiguous.

5.5.3 Policy Adherence and Training

This superordinate theme, found in all 18 papers, evidences where publications refer clinicians to additional resources such as professional codes of conduct, employer policies or dedicated cybersecurity sources, training, support, and awareness raising regarding the issues of concern.

Table 8: Results - Publications Coded to Superordinate Themes and Subthemes

SUPERORDINATE THEMES	Communication Best Practices			Data Protection, GDPR & Laws			Policy Adherence and Training;				Device Guidance					IM and App Use;			No of Codes	Total Occurances
SUBTHEMES	Confidentiality	Consent	Record Keeping	Access to data	Data Transfer	Rules and Regulations, Acts etc.	Cybersecurity Sources	Employer or Organisational Policies & Advice	Professional Guidelines, Codes, Policy etc.	Staff Training, Awareness & Support	BYOD Security	Smartphone Configuration	Legal / Regulatory Requirements	MDM Software	Network Security	Context Appropriate Use	Regulatory Scrutiny	App Selection		
Beacon Hospital (2022) Mobile Communication Policy	0	0	0	0	0	3	0	1	0	2	0	4	0	1	0	0	5	0	6	16
DDU (2023) Protecting patient data	3	0	1	0	0	4	0	4	4	0	2	2	2	0	0	0	0	0	8	22
GOSH (2023) Acceptable Use of ICT Policy	3	1	1	0	2	3	1	5	0	3	3	5	3	1	0	2	2	0	14	35
HSE (2019) Data Protection Policy	1	3	0	6	5	9	0	3	0	2	0	0	1	0	0	0	1	0	9	31
HSE (2023) Social Media Staff Use Guidelines	3	1	0	0	0	2	0	2	0	0	0	1	0	0	0	1	1	0	7	11
ICGP (2020) IT Security for Irish General Practice	1	1	1	0	1	0	0	0	2	0	0	6	1	0	1	0	0	0	8	14
INMO (2019) Guidance on the Use of IM in the Workplace	4	0	6	1	1	7	0	6	19	0	1	4	0	0	1	13	8	1	13	72
MDU (2023) Social Media top tips for Doctors in the Republic of Ireland	1	0	0	0	0	1	0	0	1	0	0	0	0	0	0	2	2	1	6	8
MDU (2024) Using Social Media	1	1	0	0	0	0	0	0	4	0	0	0	0	0	0	1	0	1	5	8
MP (2020) Ask the expert - Social Media	1	0	0	0	0	0	0	0	3	0	0	0	0	0	0	1	0	0	3	5
Scottish Gov (2020) Information Governance Considerations for Staff on the Use of IM software in the NHS Scotland	1	0	3	1	1	4	1	5	4	0	2	8	0	0	0	9	5	6	13	50
NHS (2022) Use and share information with confidence	1	0	0	0	1	1	0	2	0	0	0	0	0	0	0	0	0	0	4	5
NHS (2022) Using Mobile Messaging	2	0	1	0	0	1	0	10	1	0	2	7	0	0	0	22	1	4	10	51
NHS (2023) Bring your own device (BYOD) Guidance	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	2	0	3	4
QVH (2022) Social Media and online content policy and guidance for staff	1	2	1	0	0	1	0	1	1	0	0	0	0	0	0	19	5	0	8	31
UHD (2020) Social Media Policy	3	2	0	0	1	2	0	6	3	1	0	0	0	0	0	3	1	0	9	22
UHL (2020) Mobile Device Management Policy	2	0	2	0	0	1	1	10	0	6	13	16	1	7	3	0	0	0	11	62
UHL (2023) Health Records Management	1	0	11	3	1	8	0	12	4	2	0	0	0	0	0	1	0	0	9	43
Totals	16	7	9	4	8	14	3	14	11	6	7	9	5	3	3	11	11	5		

Key
Health Service Executive (HSE) Set:
HSE (2019) Data Protection Policy
HSE (2023) Social Media Staff Use Guidelines
NHS Transformation Directorate Set
NHS Transformation Directorate (2022) Use and share information with confidence
NHS Transformation Directorate (2022) Using Mobile Messaging
NHS Transformation Directorate (2023) BYOD Guidance
University Hospital Leicester (UHL) Set
UHL (2020) MDM
UHL (2023) Health Records Management

Legend: This table presents a visual summary of the findings from the review, illustrating the relationship between the publications and the identified themes. It highlights the recurring themes and common concepts that emerged from the dataset, organised into overarching superordinate themes with associated subordinate themes. The table provides a structured overview of how the publications addressed issues such as confidentiality, consent, record keeping, data protection, and the use of personal devices and third-party apps for clinical communication.

5.5.3.1 *Cybersecurity Sources*

Three publications signposted or asserted the value of specific, dedicated cybersecurity resources for further information. One publication referred clinicians usefully to the authoritative resources of the National Cyber Security Centre website (NCSC) [111] with two of the NHS Trusts referring to their own internal, dedicated *Cybersecurity* resources for any additional information [112, 113] specifically concerning the use of BYOD, IM and third-party apps for communications between clinicians.

5.5.3.2 *Employer or Organisational Policies*

The general importance of, or referral directly to specific additional relevant employer's or organisational policies is made in 14 of the publications for this subtheme.

5.5.3.3 *Professional Guidelines, Codes etc.*

The majority of publications (11) referenced additional professional guidelines , or codes of conduct. The resources referenced were often principle-based guidelines lacking specific detail on their integration into current personal communications technology with professional responsibilities described in general terms such as; "*the existence of IM platforms does not change the responsibility to maintain a comprehensive nursing/midwifery record*" [116].

5.5.3.4 *Staff Training, Awareness and Support*

This subtheme concerns not only training offered and the importance of awareness and understanding to ensure information governance compliance, but mandatory training stipulated as a requirement, and signposting to relevant references and dedicated specialist resources. This was evidenced in six publications, all provided by large employers.

5.5.4 Device Guidance

This superordinate theme spanned the range of guidance offered to inform the use of BYOD personal smartphones for interprofessional communication and was offered across 10 papers.

5.5.4.1 BYOD Security

Seven publications offer a range of guidance under this subtheme, from advising against the use of personal BYOD for clinical communications, to guidance for safer use, including non-technical but relevant 'common sense' advice such as the importance of not allowing anyone else to access a device if it is used for confidential clinical communication. Signposting to the expert external resources of the NCSC for more detailed information "*specific to different operating systems*" is included in one document [111, Page 3].

5.5.4.2 Smartphone Configuration

A range of advice regarding the configuration of personal smartphones was offered in this subtheme across nine publications. The Scottish Government [111] the INMO [116] and NHS [118] recommend disabling lock screen message notifications. Security suggestions vary, but include using secure passwords [109, 116] two-factor authentication (2FA) [114, 118], encryption, antivirus software [123], auto-lock and extra security settings. This subtheme also includes advice on the importance of remote wipe functionality and considerations for if a device is lost or stolen.

5.5.4.3 Legal/Regulatory Requirements

Five publications specifically address legal or regulatory requirements such as encryption as an important element of device security when transmitting or storing sensitive data. The security of any patient data (which is classified as 'special category' under GDPR [19]) streaming to a potentially insecure commercial cloud associated with a personal smartphone is mentioned in two publications [109, 123].

5.5.4.4 MDM software

Publications from three large employers [112-114] describe the value of the security features offered by Mobile Device Management (MDM) software.

5.5.4.5 Network Security

Three publications mention network "*vulnerabilities*" or "*insecure networks*" with minimal detail on any action required to maximise security.

5.5.5 IM and App Use

This superordinate theme concerned a range of issues specifically concerning the use of IM and third-party apps, direct messaging on social media platforms across 14 of the publications.

5.5.5.1 Context Appropriate use

A range of advice was offered across 11 of the publications regarding context appropriate use, from the importance of confirming that communications are sent to the correct person [111, 116, 118, 120] to the specific circumstances in which the use of such modalities would be acceptable, such as to alert a member of staff to a communication waiting for them on an approved enterprise channel [113], with a general emphasis on not sharing sensitive or confidential patient data via IM and third-party apps. Several publications condone the use of these tools to facilitate interprofessional communications where no sensitive personal data is shared [113, 120, 121, 126], in specific or emergency circumstances only [111], or where no alternative is available [118].

5.5.5.2 Regulatory Scrutiny

The issues raised under this subtheme were mentioned in eleven publications. The statutory requirement for the availability of data / messages and images sent via IM or third-party apps, for access by Data Subjects (patients) in compliance with GDPR [127] (for

correction and or portability and or deletion) and the availability of messages if requested for Subject Access Requests (SAR)s was described in five of the publications [111, 113, 114, 116, 118]. Several publications actively discourage [111, 116, 124] or completely forbid the use of IM and third party apps for the communication of patient information between clinicians [104, 113, 114, 120, 121] with assertions such as *"the current services on offer do not meet NHS information governance standards for the transmission of confidential information and their use for this purpose has been explicitly banned by NHS Digital"* [121].

The requirement for any channels utilised for the processing of sensitive clinical data to be encrypted was mentioned in four publications [111, 113, 116, 119]. One publication [114] points out that the conduct of a Data Protection Impact Assessment (DPIA) [128] is mandatory where any sensitive information is being processed, which is relevant to the selection of an IM or third-party App [114].

5.5.5.3 App Selection

Guidance in relation to app selection was provided in five publications. Information on how to evaluate an app's suitability for secure communication was provided in one publication [111], and information regarding specific configuration in order to maximise the security of sensitive data was provided in five publications [111, 116, 118, 124, 125].

5.6 DISCUSSION

5.6.1 Ambiguity and Inconsistency:

This scoping review reveals a lack of consistent, detailed, actionable guidance regarding the protection of patient data when healthcare professionals use personal BYOD, IM, and third-party apps for communication between each other, across the majority of the publications. This ambiguity risks undermining the professional reputation of clinicians, both individually and collectively, and may attract regulatory scrutiny, sanctions from employers and substantial financial penalties for violations of GDPR [19].

The literature is unclear on digital communication best practices, despite the fact that health related data is categorised as a special category, requiring enhanced protection under GDPR [19]. For example, few publications [111, 116, 120] advise clinicians to transcribe details and outcomes of clinical conversations conducted via personal BYOD, third-party app and IM into patient records and all leave the question of whether it might be more effective to directly download these exchanges as PDFs and integrate them into electronic health records (EHR) unresolved. This process would provide a reliable audit trail, save time, and meet the requirements of Freedom of Information or Subject Access Requests [111, 114-116]. Furthermore, if deletion of the data is necessary, the importance of removing it from both the sender's and all recipients' devices [118] should also be addressed consistently across publications. Clinical images constitute medical records and must be preserved [122] so this area of ambiguity must also be addressed, and any inconsistencies resolved.

Several publications describe a requirement for data minimisation of confidential communication information via personal smartphones, third-party apps or IM [111, 112, 118, 120, 126]. However, the INMO [116] alone acknowledges the risks of confusion regarding patient identity, a concern established by scholars in the literature [4, 129] and considered "*crucial for safe healthcare delivery*" [129].

As previously noted, the HSE [104] classifies WhatsApp and IM as social media, advising against sharing confidential information via such modalities, yet proactive policy communication is unclear. Several publications actively discourage [111, 116, 124] while others completely forbid the use of personal BYOD, IM and third-party apps for the communication of patient information between clinicians [104, 114, 120, 121], with assertions such as *"the current services on offer do not meet NHS information governance standards for the transmission of confidential information and their use for this purpose has been explicitly banned by NHS Digital" [121].* Significant variations in the guidance offered exist across all publications and this can cause confusion.

5.6.2 Adherence to Policies and Training:

There is a potential flaw in how existing policies are promoted and how the importance of regular training is emphasised. While some public health systems and large employers have dedicated cybersecurity resources, including specialist staff and technical support, there is a requirement for comprehensive, consistent policies and training programs addressing the specific concerns regarding the use of current BYOD personal smartphones IM, third-party apps for secure interprofessional communications in clinical settings. Coordination between employers, unions and regulators could enhance training for all clinicians, including those in specialist training (who can be mobile between employers nationally with differing policies) and those employed in small private practices, who may not even be aware of the availability of MDM software or their own statutory obligations under GDPR [19].

A raised awareness on the importance of regular compulsory training on the relevant areas (cybersecurity, the law etc.) could become part of annual Continuous Professional Development (CPD) enforced by the regulators. The fact that the Government of Scotland provided some of the most detailed, comprehensive, and specific guidelines we accessed [111], flags issues regarding how well this guidance is communicated, in order to have meaningful impact on clinical practice, as evidenced from the recent ICO sanction of NHS Lanarkshire in 2023 [103].

The comprehensive range of support and mandatory education and training around cybersecurity and information governance described in several of the large employer policies [112-115, 121, 122] would be valuable for all clinicians, especially for those who do not work for large employers, without dedicated support.

5.6.3 Technical Guidance for Secure Communication:

There is a gap in the provision of detailed considerations, technical requirements, and guidance regarding current popular communication modalities in healthcare. Few publications offer well informed, practical advice or signpost expert resources to inform the safer integration of these digital tools into clinical practice while maintaining data security. The literature focuses on

general principles rather than providing detailed statutory requirements or specific technical guidance. Most publications offer high level recommendations on data security practices without including concrete technical details, such as configuration for apps or devices [104, 109, 111-113, 115-118, 120-126]. This hampers clinicians' understanding of data protection obligations and requirements, particularly for GDPR compliance where even an IP address is considered personal data [121, Page 5]. Clinical images with EXIF data [45] (including geographical coordinates, date, time, and device details) are also personal data, yet this is not addressed in any of the reviewed publications. Only two publications highlight the requirement for DPIAs when processing sensitive information [114, 115], indicating a widespread lack of awareness of essential data protection procedures. The failure to reference specific security requirements for patient health data using BYOD, IM, or third-party apps suggests a lack of awareness among clinicians [125, 126].

This review highlights significant gaps in guidance provision in terms of actionable, specific recommendations. The existing literature and policy guidance vary widely, with some sources emphasising general principles and others offering more detailed but inconsistent advice. This disparity highlights the need for harmonisation of well-informed guidance to ensure clinicians have access to both practical advice and regulatory clarity. Comprehensive, technically detailed guidelines are needed, especially for clinicians in private practice without specialist IT or cybersecurity support. A unified approach, directing healthcare professionals to authoritative resources such as the NCSC [130-134], could enhance decision making and patient data security practices.

5.6.4 Limitations

The restricted access to documentation, available only to full members with paid memberships, hampered our ability to gather a comprehensive set of publications for analysis. This limitation may have affected the generalisability or accuracy of our findings but also highlights a significant gap in accessibility.

5.6.5 Conclusions

This scoping review highlights the complex landscape of guidelines and policies for personal BYODs, third-party apps, and IM for interprofessional clinical communication in the UK and Ireland. The absence of appropriate guidelines poses challenges for clinicians, particularly those outside large healthcare employers, who may lack access to specialised resources, dedicated technical support, policy, and training, exacerbating any disparities in information security and data protection practices. Existing guidance is often superficial, inconsistent, and does not appear to be informed by up-to-date expertise, threatening patient confidentiality and data security. There is an urgent requirement for harmonised, contemporary guidelines that can adapt to evolving technology.

The specialist discipline of health informatics has emerged to address the requirement for uniquely skilled professionals to design, develop, implement, and evaluate health information technology, which highlights the extensive body of evidence and tools existing in this field [135]. Drawing upon established work from Healthcare, Health Informatics, and areas such as Information Systems (IS) is essential to inform the research and development of a comprehensive, holistic model of data quality dimensions to assess the quality of data / information currently informing clinical practice in this area. Such a model is essential for identifying and addressing gaps in current guidance. A collaborative approach involving healthcare providers, regulatory bodies, trade unions, cybersecurity experts, legal advisors, IS and health informatics specialists is vital for developing and disseminating guidance that keeps pace with technological advances, ensuring the highest standards of data protection, patient confidentiality, and professionalism in clinical communications.

CHAPTER 6 DESIGNING A DATA DIMENSIONS ARTEFACT FOR THE USE OF BYOD, IM AND THIRD-PARTY APP-BASED TECHNOLOGY BY CLINICIANS: AN ACTION DESIGN RESEARCH APPROACH

This paper has been submitted to a journal for peer review and publication (Journal of Decision Systems on 9th October 2024) and the peer review process is currently in progress. This study was conducted to meet objective 4, to develop & evaluate an artefact to assist clinicians in their assessment of the available guidelines regarding communication using smartphone technologies. Publication 7. Submitted Paper 5.

The following text has been submitted to the *Journal of Decision Systems* for peer review and publication on 9th October 2024.

6.1 ABSTRACT

Digital technologies are transforming how clinicians communicate confidential work-related data between each other, with bring your own device (BYOD) smartphones, instant messaging (IM), and third-party apps widely used. These tools offer efficient and affordable functionality but present significant data security and compliance challenges for clinicians. Using an Action Design Research (ADR) approach in collaboration with clinicians, we address the knowledge gap regarding clinicians' use of these digital tools through the design and evaluation of the Data Dimensions Artefact (DDA) including continuous cycles of diagnosis, design, implementation, and evolution. Qualitative data underwent thematic analysis using NVIVO software to inform refinements concerning artefact usability and clarity. Statistical analysis of quantitative data, using Cohen's Kappa, was conducted to assess the reliability of the proposed DDA. Findings indicate that the artefact supports clinicians' decision making through a toolkit for assessing the quality of guidelines on secure clinical digital communication practices. The ADR approach revealed a tension between the precise technical terms used to communicate data and digital security requirements while maintaining the practical usability of the artefact. Ongoing education and current guidance are necessary to maximise the DDA's potential and maintain compliance with data protection regulations.

6.2 INTRODUCTION

Effective communication is a cornerstone of good clinical care, playing a critical role in ensuring positive patient outcomes [12]. As healthcare becomes increasingly complex, the need for clear, accurate, and efficient communication among clinicians is more important than ever. Digital technologies are revolutionising services and processes in organisations of all sizes [136], with BYOD smartphones, IM, and third-party apps becoming prevalent in healthcare [1, 35, 96]. It is unsurprising that clinicians are using smartphones and apps, to support the prompt and efficient sharing of patient details amongst their teams thereby enhancing the coordination and delivery of care to support better patient outcomes. However, the informal adoption of personal digital technology by clinicians introduces challenges, particularly in terms of the security and confidentiality of sensitive patient data. Key issues include the risk of unauthorised access to sensitive patient information, potential data breaches, and difficulties with record-keeping [129]. These challenges are exacerbated by the complexity of ensuring compliance with legal and regulatory requirements, e.g. GDPR in the UK and EU [19] and HIPAA in the USA [23]. The informal use of personal BYOD's often bypasses institutional IT policies [4] and increases the risk of non-compliance with legal regulations [1, 129]. In turn, this can jeopardise patient privacy and expose healthcare institutions to legal and financial penalties.

Guidelines and policies from regulators, health systems, employers, and professional bodies play a significant role in informing clinicians on all aspects of practice, including clinical communication. However, the absence of clear guidance on record keeping and data storage when using personal technology has led to problematic practices that heighten concerns regarding patient privacy and the safeguarding of sensitive health information [4, 129]. Despite the widespread use of digital communication technologies in healthcare, gaps remain in the availability of comprehensive, actionable guidelines for clinicians [1, 27] . In our recent scoping review, we identified that existing guidelines are often vague or non-specific, lacking the actionable detail necessary to guide clinicians [27]. Moreover, these guidelines frequently fail to keep pace with the rapid evolution of technology and the regulatory landscape, making them less relevant to current clinical practice over time. This poses the research question:

How can clinicians assess the quality and security of guidelines regarding the use of these digital technologies?

Therefore, the objective of this research, is to design an artefact that enables clinicians to self-assess the quality of guidelines and other published / accessible materials (current or future). Equipping clinicians with a decision support that empowers them to make informed decisions, ensuring that the technology is deployed in a manner that is both secure and compliant with relevant regulations. To best support clinicians who use personal digital technologies to enhance their clinical communications, a decision support guide would necessitate a strategic approach that comprehensively incorporates both the technological and the regulatory aspects of the environment. Heavin and Power [136] advocate for the development of conceptual decision support models to inform the decision-making processes in addressing the unique challenges introduced by digital technologies. This paper is structured as follows: first the theoretical background that focuses on data quality is provided highlighting the need to design meaningful guidance for clinicians, then the research methodology is outlined. This is followed by a detailed account of the ADR stages undertaken by the research team in close collaboration with clinicians, to generate, develop, and evaluate the DDA, ensuring that real-world challenges are addressed. Finally, the broader implications of the research findings are discussed and opportunities for future research are presented.

6.3 THEORETICAL BACKGROUND

In recent years, the need for guidelines, issues with data breaches, and regulatory compliance have become critical areas of concern for healthcare providers in the use of digital health tools [137], such as BYOD smartphones, IM, and third-party apps that facilitate sensitive patient data sharing between clinicians. Existing research highlights that while these digital tools have transformative potential for improving patient care coordination and outcomes, they also introduce risks related to data privacy, security, and accuracy [138]. Studies indicate that the healthcare industry sees the greatest number of data breaches among all major industries around the world [139-141]. Given the increased use of BYOD, smartphones, IM, and third-party apps in

healthcare, clinicians need clear guidance to ensure that the tools they use support safe and effective patient care [142]. Such guidance can help them evaluate whether these digital tools maintain the necessary standards for data integrity, security, and accuracy when sharing clinical information.

Ensuring high-quality data is critical, as it directly influences decision-making, efficiency, and trust [143]. Quality is the degree to which characteristics of an object meet requirements, and data quality is the degree to which dimensions of data fulfil requirements [144]. Poor data quality can compromise clinical decision-making, lead to misdiagnoses, and undermine patient trust [145]. The regulatory landscape surrounding data sharing is complex and often challenging for clinicians to navigate due to evolving regulations such as HIPAA in the United States and GDPR in the European Union, which mandate rigorous standards for handling sensitive health information [146]. As these regulations stipulate strict requirements, healthcare organisations face pressure to ensure clinicians can both understand and apply these in their daily practice while also maintaining quality care [147].

Data Quality Dimensions (DQDs) [144] were established for the classification and assessment of the quality of data [148, 149]. From a comprehensive list of sixty dimensions with standardised definitions meeting the ISO 704 standard, a shortlist can be used, that can not only assess traditional aspects of data quality but also capture security, confidentiality, and regulatory compliance, critical to clinical communication using BYOD technologies [144]. The importance of regulatory compliance is reinforced by the GDPR [19], which imposes specific requirements for safeguarding personal health information, classified as special category data. The DQDs serve as a foundation for the assessment of data quality that is readily adapted to meet the needs of this specific problem, providing measurable features or characteristics of a data concept for better informed decision making [144]. DQDs define essential dimensions for customisation (such as accuracy, completeness, confidentiality, and accessibility) that are required for assessing regulatory and technical aspects of data security when using BYOD, IM, and third-party apps for confidential communications [144].

Data protection and cybersecurity standards are informed by reputable, authoritative sources such as the National Cyber Security Centres (NCSC) in the UK and Ireland, the National Institute of Standards and Technology (NIST) in the USA, the Information Commissioner's Office (ICO) in the UK, and the Data Protection Commission (DPC) in Ireland. Synthesising insights from these sources and aligning them with established DQDs allows for the identification and adaptation of a set of dimensions specifically suited to this study's clinical focus. Existing research underscores significant concerns surrounding the use of digital technologies, such as smartphones and third-party apps in clinical communication [1, 4, 35, 96, 129]. According to John et al. [35] "*Clear, well-informed advice, policy, regulation, and training is evidently required to mitigate for security concerns, constraints and technical requirements around privacy and data protection regulation and legislation, in relation to the modalities being used*". In the absence of quality guidance, clinicians need a decision-support toolkit to aid them in evaluating the quality and security of these digital resources.

Research indicates that in the current environment clinicians are making their own decisions based on balancing the risks and benefits of using mobile devices in a clinical setting [150]. These findings underscore the need for a structured approach to help them effectively evaluate the quality and reliability of digital technologies, such as smartphones and third-party technical resources. Despite the pressing demand for digital resource evaluation, current guidance remains limited and fragmented [141]. Joint guidance from NHS England, NHS Digital, Public Health England and the Department of Health and Social Care, published in November 2018 [75] , concerning NHS Instant Messaging, attempted to address user privacy and security concerns, yet they fell short of offering comprehensive, user-friendly advice [151]. Moreover, many frameworks / guidelines do not fully incorporate critical aspects of cybersecurity, an essential factor in assessing any digital tool's safety. While clinicians recognise and appreciate the need to protect patient data privacy, if it prohibits the delivery of quality care for patients, they tend to prefer patient care [142]. As a result, clinicians can find themselves without a practical, streamlined means of evaluating resources, leading to potential risks associated with the use of BYOD, smartphones, IM, and third-party apps to share sensitive patient data.

A comprehensive decision-support toolkit, therefore, should integrate both quality and security evaluation criteria tailored to a healthcare context. Recent studies advocate for frameworks that emphasise user-centric design, adaptability to clinical workflows, and clear guidelines for data privacy and compliance standards [141, 142]. Such an approach can also promote trust and consistency, enabling clinicians to leverage technology confidently while safeguarding patient well-being. Research suggests that decision support tools can be effective in reducing cognitive load, increasing adherence to best practices, and mitigating errors when navigating regulatory standards [152]. However, the design of such tools must consider usability and accessibility to be effective in clinical settings, where time constraints, complex clinical workflows, and varying levels of digital literacy can limit adoption [142]. For instance, poor user experience and lack of integration with existing clinical workflows have been cited as barriers to the successful implementation of decision support tools, indicating the need for solutions tailored to the specific workflow requirements of clinicians [153]. Action Design Research (ADR) is widely used in Information Systems (IS) research, with a focus on changing practices through the creation of a problem solving environment in response to specific needs and facilitating the participation of key stakeholders towards an understanding of complex problems [154]. Elaborated ADR [30] emphasises continual improvement and ongoing refinement of an artefact as it is developed in cycles. Using an elaborated ADR approach, this study seeks to provide clinicians with a decision-making toolkit, the DDA, to evaluate the quality of the guidelines pertaining to digital technologies for clinical communications. In turn, the proposed artefact enables clinicians to identify gaps within these guidelines, helping them recognise where BYOD, third-party apps, and IM may fall short in meeting regulatory standards for patient data confidentiality. By alerting clinicians to previously unconsidered risks, the DDA supports informed decisions about the suitability of these technologies in compliance with data protection regulations. Next, we describe the ADR method in general before we report on the process and outcome of its application in the context of this study.

6.4 RESEARCH APPROACH

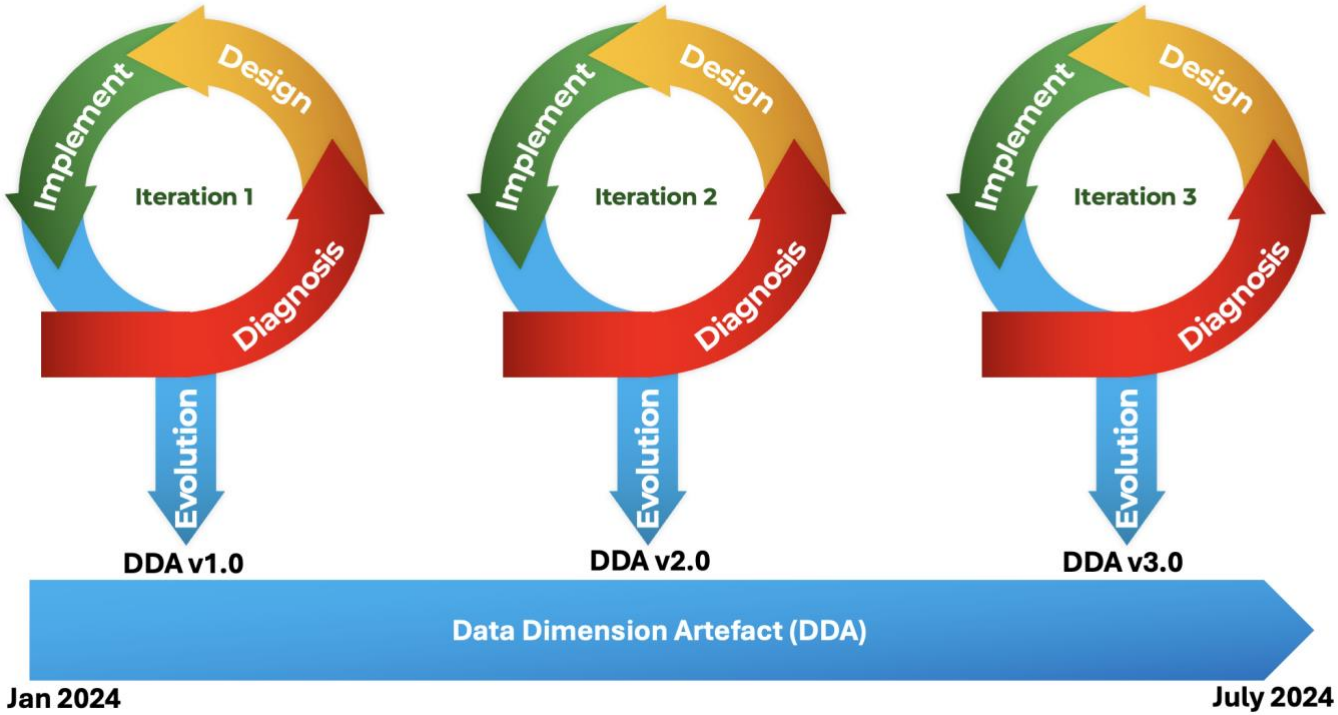
ADR is a methodology designed to address complex, real-world problems by developing and refining practical solutions, such as technological artefacts, through iterative cycles of design, evaluation, and reflection [155]. ADR integrates elements of both Action Research [156] and Design Science Research [157], which makes it well-suited to tackle problems that require both the development of an innovative solution and continuous interaction with its operational environment. The iterative nature of ADR means that a solution is constantly refined in real-time as it is tested, used, and evaluated in its intended context. This methodology bridges the gap between theory and practice linking thinking with doing [158], ensuring that the solution being developed is continuously adapted and evolved based on feedback from real-world use.

In conventional ADR [155], two main parties are typically involved: researchers and practitioners. These play important collaborative, mutually reliant roles, influencing not only the iterative design and development cycle but also shaping and affecting one another, concurrently throughout the research process [155]. Researchers provide the theoretical frameworks and structured methods to steer the design process, while practitioners offer practical insights and expertise, ensuring the solutions are relevant to real-world challenges [155, p.38]. This collaboration fosters the ongoing refinement of both the artefact and the underlying theory being evaluated or expanded. The motivation for ADR is to better serve the 'dual mission' of IS research, that is, to *"make theoretical contributions and assist in solving the current and anticipated problems of practitioners"* [155]. In this study, we follow an elaborated ADR approach (Figure 11) to support clinicians in assessing the quality and reliability of guidelines for secure communication practices. The reciprocal shaping process ensures that an intervention is guided by both practical needs and research goals, with each intervention cycle involving essential, co-dependent roles for both parties, which are crucial for the success of the research, enhancing the knowledge of both researchers and practitioners. This elaborated approach extends standard ADR by incorporating additional detail and steps within each stage of development, including distinct cycles of diagnosis, design, implementation, and evolution to ensure thorough evaluation, reflection, and learning with each cycle [30].

This approach is ideal for the healthcare context, where continual refinement is essential to ensure that the artefact aligns with both the evolving technological landscape and the regulatory requirements clinicians must navigate**.** It is particularly beneficial in a healthcare setting where clinicians' needs are dynamic, and regulatory compliance (for example with GDPR) is required. We used elaborated ADR to develop the DDA, an IS artefact, designed to inform clinicians in their assessment of the quality of the data in their guidelines, thus solving a real-world problem. By using iterative cycles (Figure 11) of diagnosis, design, implement, and evolution the DDA was refined based on user feedback, ensuring that it remains relevant and practical for real-world clinical settings, while also addressing the complex legal, technical, and ethical obligations related to data protection and patient confidentiality. The development process involved a dynamic, two-way engagement between researchers and clinicians, where each group influenced the evolution of the DDA. Each cycle allowed us to refine not only the design of the DDA but also our understanding of the broader problem context [159].

Our ADR process commenced with a diagnosis cycle. The entry point of the project is problem-centred, i.e., designing a novel artefact that enables clinicians to self-assess the quality of digital communication guidelines.

Figure 11: Elaborated ADR process (Adapted from Mullarkey & Hevner 2018)



6.4.1 DDA v1.0: Diagnosis, Design, Implement and Evolution

6.4.1.1 Diagnosis

In response to the absence of a decision toolkit tailored to support clinicians in assessing safe and compliant use of digital technologies, this study aimed to develop an artefact based on data quality dimensions. In the diagnosis phase, we identified two key tasks: understanding the problem domain and defining the requirements for an artefact that equips clinicians with a structured decision support model or toolkit to support the assessment of guidelines for digital communication. First, we conducted a thorough investigation of the literature. Two scoping reviews [27, 35] regarding their use of BYOD technology identified significant gaps in the existing guidelines for secure clinical communication using BYOD smartphones IM and third party apps. John et al.[35] found that despite clinicians using smartphones and apps to communicate clinical information, the security and privacy issues arising from their communication of sensitive data was either absent or only superficially acknowledged within the literature. Existing studies [4, 129] identify gaps in providing clear actionable guidance for clinicians regarding the secure configuration and use of personal digital technologies in healthcare settings. A study by John et al. [96] confirmed that personal smartphone use was widespread by dental professionals in the Republic of Ireland and the UK, with the risks only partly acknowledged and limited insight into data security.

Second, we specified the requirements to inform the design of the artefact. Here, we attempt to provide actionable guidance for practitioners to support their decision making regarding their use of digital tools for communicating clinical information. Drawing on existing standards available for broad application in data protection and cybersecurity, key resources were leveraged, including the NCSC [130-134] in the UK and Ireland, the NIST [160] in the USA and the DPC in Ireland and the ICO [161] in the UK. These frameworks provided the foundation to shape the tool's requirements. Our approach ensured that the artefact aligns with best practices in cybersecurity and compliance, offering clinicians a practical, standards-based resource to navigate complex regulatory demands. We sought to enhance the DDA's relevance and adaptability promoting data-sharing practices in alignment with regulatory expectations.

6.4.1.2 Design

Drawing on our understanding of existing data quality research and the requirements establish during diagnosis; we focused on the design of the Data Dimensions Artefact (DDA v1.0). Addressing the secure communication challenges, we extended the three core dimensions of Accuracy, Completeness, and Timeliness [162] to seven, through careful evaluation between the research team, with additional dimensions identified to cover the broader aspects of data quality relevant to this study [33, 163]. These dimensions included: Accuracy, Completeness (sub-dimensions: Confidentiality, Integrity, Availability), Timeliness, Relevance, Clarity, Credibility and Accessibility. Notably, the 'Completeness' dimension includes three subsections: Confidentiality, Integrity, and Availability, which are critical for assessing Information Security [164]. These dimensions were selected and customised through collaborative input by the research team to provide clinicians with measurable criteria that address both traditional data quality concerns and specific security needs related to BYOD use. The DDA's confidentiality and accessibility checks are adapted from DQDs to support GDPR compliance, which mandates specific protections for patient health data [19].

This theoretical foundation informs the initial DDA design, ensuring it facilitates accurate and comprehensive assessments in real-world clinical contexts. The DDA v1.0 was designed as a clinician-centred toolkit that meets data quality and confidentiality requirements, balancing ease of use and usability with compliance standards. This design incorporates practical guidance, empowering clinicians to make informed decisions regarding the secure use of BYOD technology in their clinical practice. Following a structured plan, the DDA's development progressed through iterative cycles of elaborated ADR [30] allowing the artefact to evolve based on user feedback, thus ensuring relevance to clinical practice and legal alignment. This approach allowed the artefact to evolve in response to user feedback, ensuring that it remained relevant to clinical practice while aligning with legal requirements.

6.4.1.3 Implement

Research ethics approval for the study was obtained from the Social Research Ethics Committee (no.2023-293A1) at University College Cork, confirming that the research adhered to institutional standards for ethical research conduct. Initial internal testing of DDA v1.0, was conducted within the research team including two clinicians (a nurse and a dentist whose expertise was key to providing real-world insights) and an IS academic. The DDA v1.0 was created using a Microsoft (MS) Excel spreadsheet and distributed by the lead investigator via email on 16th January 2024, accompanied by four selected PDF documents for evaluation. Each of the publications were drawn from a broad range of guidance publications from different clinical professions focused on the use of BYOD, smartphones, IM, and third-party apps. Team members were given one week to complete the assessment. During this period, the team used the DDA v1.0 to evaluate the guidance documents. The feedback was both qualitative and quantitative, ensuring a thorough assessment of the toolkit's effectiveness. Following the completion of the evaluations, an online meeting was convened to discuss the usability and clarity of the DDA, with feedback collected and analysed by the lead investigator.

While the DDA v1.0 proved useful in assessing security risks and identifying gaps in the documents reviewed, some of the technical language was identified as being overly complex. Specific terms such as 'Confidentiality' and 'Integrity' were flagged as potentially difficult for clinicians to understand and interpret in the context of data security and compliance. Though the MS Excel format was considered user-friendly for those familiar with spreadsheets, there were suggestions to further simplify the interface. The language used in the DDA v1.0 was revised, and a Glossary of Terms (Appendix 13) was created alongside a supplementary user 'Instructions Sheet' which provided detailed instructions and definitions for users less familiar with digital technology. These resources were tailored to accommodate younger clinicians, who were assumed to have more advanced digital skills, as well as those newer to data / digital security terminology.

6.4.1.4 Evolution

We aimed to further refine the artefact based on insights gained from both initial user engagement with the DDA and subsequent pilot reviews. Following feedback, the design was

adjusted to enhance user accessibility and relevance. This phase emphasises the balance between technical precision and clinician usability, ensuring the DDA meets practical requirements in a clinical setting. The continuous adjustments were made with the dual aim of maintaining technical rigour, fostering a clinician-friendly tool to support secure and compliant use of personal devices for clinical communication.

Three external pilot reviewers, recruited through the lead investigator's network, included an undergraduate student, an IT professional familiar with the importance of data quality, and a business consultant experienced in policy evaluation. The revised DDA v1.0, accompanied by the supplementary material (Glossary of Terms and Instructions Sheet), and the four selected PDF guideline documents was circulated on 24th January 2024. Feedback was requested and received by 1st February 2024. Reviewers provided feedback both verbally and via email regarding usability, language clarity, and overall practicality. As a result, the language used in several questions was revised to make them more clinician / user-friendly while maintaining their alignment with data protection standards and requirements. All three reviewers recommended reducing the number of selected PDF guideline documents for future evaluation cycles, as they felt these made the assessment task too arduous. The interplay between the research team and the pilot reviewers was central to the iterative refinement of DDA v1.0 (Table 9). Reflecting on these insights allowed us to incorporate learning from the pilot activity into the planning for the next cycle of the development and evaluation process. The refined DDA v1.0 was thus ready for the next testing phase with larger groups of clinicians.

Table 9: Summary of Revisions to DDA v1.0

Dimension	Issue Identified	Action Taken
Completeness / Confidentiality	Question allowed non-compliance to score 'YES' misleadingly	Revised question to ensure meaningful scoring
Completeness / Integrity	Sub-question was too broad, covering mutually exclusive issues	Divided into separate, focused questions
Credibility	First question caused confusion and misinterpretation	Reworded for clarity
Task Size	Four papers too large a task for reviewers	Reduced to three papers per testing round
Accessibility	Redundant as papers were provided	Removed this dimension for testing

6.4.2 DDA v2.0: Diagnosis, Design, Implement and Evolution

6.4.2.1 Diagnosis

During this phase, we focused on uncovering and addressing usability and technical challenges that were identified in DDA v1.0. The goal was to set clear objectives for the further improvement and validation of a more effective artefact. To achieve this, we generated 'Gold Standard' Test Scores for three selected guideline documents [109, 111, 116] using the DDA v2.0. These scores represented an ideal evaluation outcome, independently derived by the researchers. Each author applied the DDA v2.0 to the guidance documents, assessing each of these against the established data quality dimensions. In the small number of instances where a discrepancy in scoring arose, these were resolved by discussion to form consensus. This collaborative approach ensured that the Gold Standard Scores reflected a rigorous and unified consensus of how the artefact should function which served as a benchmark to evaluate the accuracy of the user scores. By comparing the reviewers' scores against this Gold Standard, we could determine whether the DDA was enabling clinicians to accurately apply the data quality dimensions, and to what extent the artefact facilitated consistent and reliable evaluations of the guidelines. This process was essential for validating the effectiveness and usability of DDA v2.0, ensuring it met the objectives set out in this phase.

Table 10: Summary of Qualitative Data Collection regarding DDA v2.0

Characteristic	Details
Focus Group 1	Five clinically active undergraduate student clinicians in their penultimate year of study
Focus Group 2	Five qualified clinicians with 5 - 20 years of post-qualification experience
Selection Process	Participants recruited by the supervision team through open email invitation of existing contacts
Email Sent	18th June 2024
Documents Circulated	1 X Study Information Sheet 1 X Consent Form DDA v2.0 of the Data Dimension Artefact (MS Excel spreadsheet with two tabs) 3 X PDF Guideline Documents
Assessment Requested	Review PDF Guidelines using the DDA v2.0 and return scores and signed consent forms by email within seven days
Focus Group Session Date	26th June 2024
Session Details	Pre-compiled script of open questions; discussions on user experience, usability, and effectiveness of DDA v2.0
Session Duration	Approximately one hour each, recorded and transcribed using MS Teams
Session Times	Morning for students (Focus Group 1) Afternoon for qualified clinicians (Focus Group 2)
Data Processing	Data anonymised and thematic analysis conducted using NVIVO software

6.4.2.2 Design

In June 2024, ten clinician reviewers (five qualified dentists and five clinically active undergraduate dental students) were recruited to participate in the testing of DDA v2.0 (Table 10). Each practitioner was provided with the three PDF guideline documents [109, 111, 116], along with DDA v2.0 (accompanied by supplementary documents). They were instructed to evaluate these independently. In preparation for the focus group sessions, a detailed script of questions was developed to guide the discussions, ensuring that feedback on the artefact's usability, clarity, and practicality would be collected systematically. In line with ethical standards, each participant was provided with a consent form for signing in advance of the

session. The goal of this phase was to test DDA v2.0 in a real-world clinical context and gather data to inform further refinements.

6.4.2.3 Implement

Following their independent evaluations of the guideline documents using DDA v2.0, the ten reviewers submitted their scores. Reviewers were subsequently invited to participate in one of two scheduled focus groups. The discussions were structured to capture the participants' perspectives on the toolkit's practicality in clinical settings, potential areas of confusion, and suggestions for further refinement. The process of evaluation involved analysing these data to assess the artefact's performance. Collecting diverse data not only enhanced the evolution of the DDA v2.0 but also allowed for a thorough evaluation of its practical usability and perceived effectiveness. This approach ensured that user feedback informed the design process, leading to improvements in the effectiveness and accuracy of the DDA v2.0.

Using the DDA v2.0, the scores for each paper received from each expert reviewer were anonymised using Python. Reviewer's scores for the DDA v2.0 across three papers were compared with the Gold Standard ratings. With ten clinician reviewers each evaluating three papers [109, 111, 116], a total of 30 scores were generated for each question in the DDA v2.0.

6.4.2.3.1 Quantitative data

Analysis revealed significant variation in the accuracy of the answers provided by each reviewer. While two questions achieved a perfect score of 30 correct assessments (regarding the year of publication, and clarity of terminology), others showed considerable discrepancies (Table 11). For some questions, only seven out of 30 answers were correct, while others had 12, 17, or 19 correct answers, indicating a range of accuracy across different questions and reviewers (Table 11). Feedback from previous iterations indicated the requirement for clearer language and more intuitive navigation to support clinicians unfamiliar with data security protocols.

Table 11: Accuracy of Reviewers' Responses

Data Dimensions		Questions answered	Correct answers
1.Accuracy		Does the publication cite and align with credible cyber security sources?	12
		Is a description of how to use IM or third-party Apps on a BYOD smartphone for secure and confidential communication provided?	27
2. Completeness	**2.1 General**	Is a clear rationale for the use of IM or third-party App on a personal BYOD smartphone for clinical communications described?	24
		Has the requirement for a formal risk assessment (e.g. a DPIA in the EU) been explained?	27
	2.2 Confidentiality	Are regulations (such as GDPR (EU) or HIPAA (US)) and their relevance to BYOD, IM, and third-party Apps discussed and obligations described?	22
		Is verifying that an App does not access sensitive metadata in exchange for functionality, or steps to limit such access, discussed?	22
		Is it specified that BYOD should never access free Wi-Fi if hosting or processing sensitive data?	23
		Is it stated that unauthorised users must be prevented from accessing any device on which sensitive data is hosted?	19
		Is the importance of avoiding the installation of any suspicious Apps on personal BYOD devices used for confidential professional communication explained?	24
	2.3 Integrity	Are requirements regarding server location, data encryption, data security in transit and at rest, and relevance to BYOD, IM and third-party App clearly described?	12
		Are requirements for configuring of any third-party App (e.g., disabling image and data streaming to networked devices and unsecured cloud servers) explicitly described?	20
		Are security settings, password protection and MFA of device and or Apps discussed?	26
		Is the requirement for regular training or briefings on security stipulated?	25

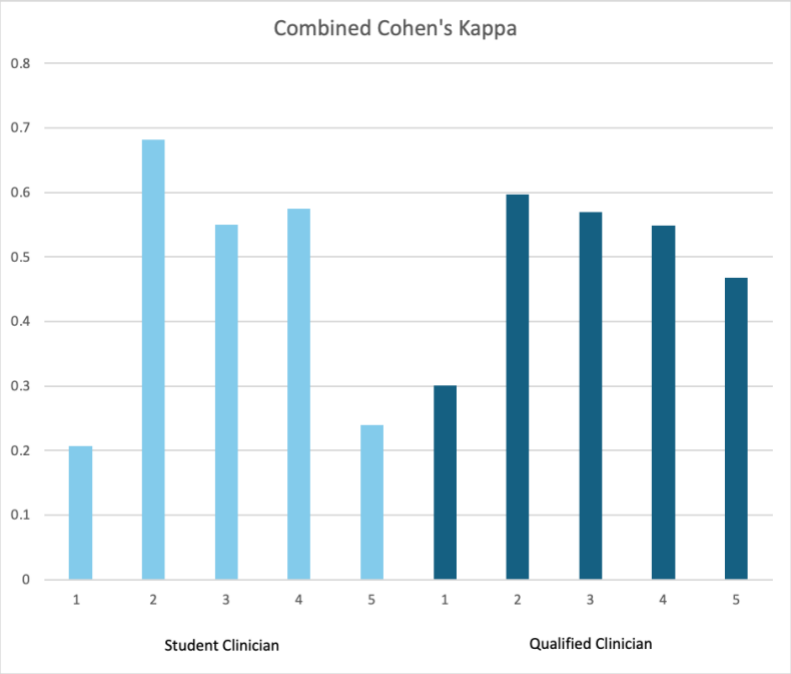
		Is the need for a regular, scheduled review of the App clearly communicated?	28
	2.4 Availability	Is evaluation of the network capacity, network coverage, power usage, and data accessibility discussed?	22
		Are there clear instructions for record-keeping of chat / images in patient records, inc. scheduled recording / downloading & deletion of confidential data from senders' & receivers' Apps & devices?	17
3. Timeliness		Is the publication date after May 2018?	30
		Are there scheduled updates, or is the content from a source that regularly provides updated information? Is this publication recent enough to be relevant?	7
4. Relevance		Does the guidance cover the use of relevant functionality for maximum security and compliance with data protection regulations?	20
		Are the legal and ethical issues of obtaining informed consent from patients discussed and explained in relation to the processing of their data on personal BYOD devices, IM, or third-party Apps?	20
5. Clarity		Is the terminology easily understood?	30
		Is the advice easy to interpret and apply in clinical practice?	28
6. Credibility		Is the content specific to a jurisdiction, such as specifying GDPR requirements (EU / UK) or HIPAA requirements (USA)?	23
		Is the source of this publication credible to clinicians?	27
		Publication contains declaration of no bias, or no evidence of sponsorship or bias present	17

6.4.2.3.1.1 Data analysis

Cohen's Kappa was chosen as the statistical test because it effectively measures the level of agreement between individual expert reviewers' scores and our predefined Gold Standard scores for each guideline article. A comparison of each set of scores was used to calculate a Cohen's Kappa coefficient value for each expert reviewer for each paper. The coefficients varied significantly, ranging from less than 0.05 (slight agreement) to as high as 0.9 (almost

perfect agreement), indicating substantial differences in rating accuracy between reviewers on certain questions [165].

Figure 12: Accuracy Score and Strength of Agreement (Landis and Koch 1977)



Kappa Statistic	Strength of Agreement
<0.00	Poor
0.00 – 0.20	Slight
0.21 – 0.40	Fair
0.41 – 0.60	Moderate
0.61 – 0.80	Substantial
0.81 – 1.00	Almost Perfect

The individual Cohen's Kappa scores were combined to create an overall Cohen's Kappa score for each reviewer. This served as an accuracy measure for each reviewer using DDA v2.0 (Figure 12). These results revealed considerable variation in accuracy across reviewers. The overall Cohen's Kappa scores ranged from 0.2 (slight agreement) to 0.68 (substantial agreement) [165]. These findings demonstrate the utility of DDA v2.0 in assessing the quality of data within guideline documents.

6.4.2.3.2 Qualitative data

The focus group dialogue was guided around the utility, comprehensiveness, and application of the DDA v2.0; five main themes emerged from our thematic analysis (informed by work of Braun and Clarke 2006) [108] . The themes included (1) appreciation for the utility of the DDA artefact, (2) awareness of improvements in personal insight and competency due to engagement with the artefact, (3) recommendations for improvements in clinician education, (4) issues concerning compliance with legal and regulatory frameworks, and (5) suggestions

for improvements of the artefact. This analysis informed our understanding of the DDA's utility and were used to guide further refinements.

6.4.2.3.2.1 Utility and Impact of the DDA v2.0

There was general appreciation that DDA v2.0 could be used to inform and refine user understanding of the reliability of clinical guidelines. Most participants acknowledged how effectively the artefact identified areas that were either omitted, insufficiently addressed, or overlooked in existing guidelines. This provided a structured approach to evaluating the completeness and quality of guideline documents, thereby supporting informed decision-making regarding communications technology.

> *"This is great, kind of shows you the holes in the paper. I had not seen those holes. You know, in the initial read? I had to go through these questions and then I was able to pick through the whole thing spotting this and that."* (Student Clinician 4)

Thus, it highlighted the effectiveness of the DDA v2.0 in identifying important omissions in guidelines that clinicians were previously unaware of.

> *"Even the confidentiality part, easily specified that BYOD should never access free Wi-Fi, so that's very clear and very relatable and understandable."* (Qualified Clinician 1)

Thus indicating that she had not previously considered that accessing free Wi-Fi may pose a security threat to the processing or hosting of confidential patient data on a personal mobile phone, demonstrating the potential of the DDA v2.0.

6.4.2.3.2.2 Awareness and competency development

Despite widespread publicity regarding the GDPR's implementation in May 2018 [19, 25], discussions revealed a significant gap in knowledge among both student and qualified clinicians, regarding professional responsibilities under the law when processing patient data using personal smartphones, IM, and third-party apps to process confidential data. Engagement with the DDA v2.0 served as a catalyst for transitioning clinicians from a state of *"unconscious incompetence"* (Qualified Clinician 2) to conscious incompetence, particularly in areas involving digital tools and legal obligations. This shift was marked by a growing

awareness and consciousness of the clinicians' knowledge gaps as they progressed through the materials (three test guideline papers [109, 111, 116]), with improvements in their understanding noted with each subsequent review.

> *"Using this tool, I suppose it brings you to a stage of what they call conscious incompetence, where you realise, oh, there's so much I don't know, but that is an awareness."* (Qualified Clinician 2)

This sentiment was widely supported by the qualified clinicians. Both groups described how their insights had improved from their reading of the first to the third guideline document while using the artefact.

6.4.2.3.2.3 Educational needs and recommendations

Engaging with the DDA raised awareness of a requirement for training and education on using digital communications technology, focusing on professional and legal obligations for handling sensitive patient data. It was suggested that this could be included as compulsory Continuing Professional Development (CPD) to ensure practitioners are well-prepared for contemporary clinical environments. Student reviewers voiced concern about how they could inform themselves post qualification if they did not have access to the university academic library for their professional development.

> *"We've got *CPR requirements, and you know, all various, like CPD requirements, and as you said"* (referring to a fellow Research Subject) *"radiological licenses and everything. Like we should be forced, it should be compulsory."* **(**Qualified Clinician 2).
> *CPR - Cardiopulmonary Resuscitation

> *"Our programme would really benefit from at least having like workshops or something about this kind of stuff."* (Student Clinician 2)

> *"Do you think we'll struggle more to get access to stuff when we're out of the university?"* (Student Clinician 3)

There was consensus among participants regarding the need to integrate this content into both undergraduate and postgraduate professional education.

6.4.2.3.2.4 Technology and compliance

Reviewers in both groups acknowledged their overreliance on, and implicit trust in encrypted well known and widely used commercial apps for communication between clinicians. There was agreement regarding a pervasive general assumption that these apps are inherently safe for the communication of sensitive patient data. The lack of explicit guidelines from authoritative bodies was highlighted as a critical issue, indicating an urgent need for clear, actionable guidance to navigate the complexities of technology use in clinical practice.

> *"And it's interesting because for all the other things we use, most of the things we need some knowledge to start using them? So, not for technology, so, everybody's using it, so nobody's waiting for guidelines or recommendations. So, it is very urgent really."* (Qualified Clinician 1)

> *"We need to be aware because we're going, maybe we're starting to get there in the hospital but we're going to be entering a world where it's completely driven by that, so if we're not aware of it. Yeah, we're going to have a hard time."* (Student Clinician 1)

Participants emphasised the requirement for well-informed guidance to assist busy professionals to navigate the complexities of digital technologies for processing confidential data and meeting legal requirements.

6.4.2.3.2.5 Areas for improvement

Suggestions for creating a clearer and more accessible DDA design were proposed by both groups of practitioners. These included adopting a vertical format to avoid horizontal scrolling and making questions more concise. There was frustration expressed by some student clinicians with the instructions sheet that required them to flip between the tabs of a MS Excel spreadsheet to access the additional information. They advised on the importance of digitising the artefact in the future. One reviewer suggested that an app would allow users to track their progress and estimate the time needed to complete the task, potentially generating a result or conclusion upon completion of the task.

To accommodate users unfamiliar with technical jargon, one qualified clinician reviewer suggested completely removing certain regulatory requirements from the DDA v2.0. Another clinician indicated that technical assessments might be more appropriately handled by certified specialists, reducing the burden on those who may find some technical details challenging. Conversely, student clinicians were enthusiastic about learning more, to better inform themselves.

> *"Yes, shorter, more of the shorter questions, or more focused questions. Because again, it was just frustrating. I said - do I say yes? Or do I not say no for this or do I say yes, yes, yes."* (Qualified Clinician 3)

> "*Because I feel like sometimes by the time you're flipping pages, you forgot already what that meant."* (Student Clinician 5)

> "…at the end you kind of get like a summary or like a result of based on what your input was." (Student Clinician 5)

> *"Do you really need to ask all those? Or, because I understand where you're coming from that you wanted to include everything that is important, but it's, say from a clinician's perspective. And in order for you to make a decision."* (Qualified Clinician 1)

> *"This is practical. These are things that we need to know, right?"* (Student Clinician 1).

6.4.2.3.3 Synthesis of quantitative and qualitative data

By integrating the results of the statistical analysis with the qualitative feedback from the focus groups, additional important insights emerged. During the drafting of the DDA v1.0 and DDA v2.0, the wording of questions was kept deliberately concise, with supplementary details provided on the additional Instructions Sheet as an additional tab of an Excel spread sheet. This approach aimed to avoid excessive description, particularly for younger and more IT-literate users. However, when examining the results for a specific question in the Accuracy dimension - "Does the publication cite and align with credible cybersecurity sources?" It became clear that further clarification was necessary. The original explanation on the separate Instructions Sheet stated: "*Draws upon and aligns with the latest guidance from*

reputable cybersecurity sources like the National Cyber Security Centre (NCSC) in Ireland and / or the UK, the National Institute of Standards and Technology (NIST) in the USA, or insights from a software assurance professional / security analyst who has conducted specific App vetting. The document must explicitly mention widely used third-party communication Apps (e.g., WhatsApp, Signal, Trello), IM, and or personal BYOD smartphones."

Despite this, only 12 out of 30 answers to this question were correct (Table 11). Comments from the focus groups indicated that reviewers only recognised what constituted a credible cybersecurity source after they had completed the scoring exercise and during the focus group discussions, such as: *"I'm going to just say cybersecurity resources from now on when I'm reading these things because it's true. Like it has to be from a credible source."* (Student Clinician 1)

It became apparent that some reviewers were unaware of what constituted a credible source until it was discussed, and they were unfamiliar with the content of the Instructions Sheet.

> *"But even since I come into the room now, I know I didn't fully understand some of the terms in the tool either."* (Qualified Clinician 4)

Due to the variation in scores and the inaccuracy of interpretation of the question, we revised the wording. Additionally, 'hints' were included beneath each question to assist those who might not read the additional information on a separate tab or sheet. The descriptors were further simplified in DDA v2.0 and questions were broken into focused sub-questions to ensure precision and clarity. This approach aimed to minimise subjectivity and ensure consistent application by raters (Table 12). During the focus groups, two expert reviewers showed a significant lack of familiarity with the Instructions Sheet, and another reviewer's engagement with it was uncertain due to minimal contribution during the focus group. These three reviewers recorded the lowest Cohen's Kappa scores.

Table 12: Summary of Revisions to DDA v2.0

Dimension	Initial Issue	Action Taken
Accuracy	Confusion regarding interpretation of the question as reviewers unsure as to what constituted a reputable source	Reworded to include more specific detail, less reliant on separate Instructions Sheet
Confidentiality / Integrity	Question concerned too many mutually exclusive issues.	Reworded to contain three sub-questions for clarity
Completeness / Integrity	Sub-question caused confusion and misinterpretation	Reworded for clarity
Completeness / Availability	Question concerned several associated issues	Reworded to contain four sub-questions for clarity
ALL	Layout in landscape meant it was difficult to print or read on computer monitor	Format changed from landscape to portrait, making it easier to print on one page and read on a computer monitor. Numeration added to some subdimension questions to aid clarity
ALL	Flipping between tabs to access the Instructions Sheet tab and the DDA questions was time consuming and caused confusion	Included user instructions / information as 'hints' underneath each question to make requirement for moving between sheets less likely

6.4.2.4 Evolution

This cycle focused on evaluating how well clinicians applied the toolkit in a real-world setting. Several design aspects were refined and revised to ensure that DDA v2.0 could be more accurate and effective for future use (Table 12). One of the defining features of the development of DDA v2.0 was the dynamic and iterative collaboration between the research team and the clinician reviewers. This two-way engagement was essential to ensure that the artefact remained grounded in practical clinical realities. The clinicians' feedback, informed by their hands-on experience in clinical settings, not only identified key usability issues, such as the universal lack of familiarity with complex security terminology, but also guided us in making refinements that would make the tool more accessible without compromising on technical accuracy.

Further, it was apparent that not all clinicians had familiarised themselves with or fully utilised the additional Instructions Sheet, affecting their ability to use the tool effectively. Pointing to

the need to further refine the DDA v2.0 to integrate key information. This two-way engagement ensured that the DDA v2.0 was co-designed with the practitioners it was intended to support. The collaborative nature of the process allowed for iterative improvements that bridged the gap between academic research and practical application.

6.4.3 DDA v3.0 Diagnosis, Design, Implement, and Evolution

6.4.3.1 Diagnosis

In this cycle, the focus was on further refining and improving DDA v3.0. Consistent with Mullarkey and Hevner's [30] elaborated ADR model, the interplay between the research team and clinicians was central to the co-creation process, where both parties engaged in iterative cycles of diagnosis, intervention, and reflection. Reflection in this ADR process is not a final step but is integrated into each cycle, helping to ensure that the research evolves dynamically in response to the context and outcomes observed during the study. Upon further conscious reflection on the problem, and after consideration of the results of testing, we concluded that some clinicians either chose not to use the Instructions Sheet or did not refer to it consistently, which in turn affected the accuracy of their assessments.

6.4.3.2 Design

The primary design change involved the removal of the Instructions Sheet in its standalone form. While 'hints' had been introduced during DDA v2.0, they were further enhanced. Essential details were incorporated directly into the DDA v3.0 in the form of expanded 'hints', making the toolkit more streamlined and user-friendly. These were strategically placed in sufficiently prominent positions, to ensure that clinicians would use them. The goal was to simplify the use of the DDA without sacrificing the depth of information needed to apply the toolkit accurately. Additionally, the interface was updated to improve its usability, including adjustments to the font size and the transition to a more user-friendly table format in MS Word.

6.4.3.3 Implement

Following these refinements, we reshared the DDA v3.0 with the ten focus group participants via email on 25th September 2024. Clinicians were asked to review the revised version and

provide feedback. True to the elaborated ADR model, the implementation phase was seen as an intervention that involved ongoing evaluation and learning, guided by feedback from clinicians. The reviewers were asked to focus specifically on the effectiveness of the 'hints' and the overall ease of use of the new format to inform the next phase of the DDA evolution.

6.4.3.4 Evolution

In this phase, the feedback received from the clinician reviewers confirmed that the removal of the Instructions Sheet had simplified the artefact, while still ensuring comprehensive coverage of all key issues. The only further amendment suggested was to ensure that the word 'hint' is highlighted in bold typeface. Reviewers expressed confidence in the artefact's practical application, with one reviewer stating that they would be happy to recommend it to colleagues. As emphasised by the principles of ADR, the close collaboration between researchers and practitioners allowed the artefact to evolve in response to both theoretical considerations and practical needs of users [155], ensuring that it effectively addresses the core problem of secure and compliant clinician communication. The co-creation process ensured that the DDA is not only a research artefact but a tool that is practical, user-friendly, and aligned with the day-to-day realities of clinical communication. The next step will involve assessing the wider deployment of DDA v3.0 in additional clinical settings and collecting further data to support ongoing improvements.

6.5 DISCUSSION

This study designed and evaluated a decision-support tool, the DDA, to support clinicians in assessing the quality and reliability of guidelines for secure communication practices using BYOD smartphone, IM, and third-party app technology, presented in Table 13. The DDA was developed to address the gap between existing guidelines and the steps required to ensure compliance with data protection regulations, such as GDPR. It addresses these challenges by combining technical accuracy with usability, making data compliance more accessible to non-IT specialists. The development and iterative evaluation of the DDA followed a systematic approach inspired by elaborated ADR [30], facilitating a collaborative process between clinicians and researchers, with both parties playing essential interdependent roles to ensure that the artefact addressed practical clinical needs while revealing new research insights.

The proposed artefact is valuable in raising awareness among clinicians of complexities they may not have previously considered. Working with practitioners, the ADR process revealed a widespread lack of awareness regarding their obligations under the GDPR and the challenges associated with using personal smartphones, IM, and third-party apps. These challenges include data streaming between devices and to potentially insecure cloud servers, record-keeping, and obtaining informed consent from patients, echoing recent literature [4, 96, 129]. This finding reinforces the importance of integrating this subject matter into undergraduate healthcare curricula and ongoing professional education to ensure compliance and effective use of digital technologies in clinical settings. While student participants recognised the need for this content, aligning with current thinking regarding requirements for undergraduate dental curricula in Europe [9], qualified clinicians stressed the role of regulatory bodies in mandating CPD to cover these legal responsibilities.

Table 13: Data Dimension Artefact (DDA) v3.0

DATA DIMENSION		GUIDANCE FOR SECURE COMMUNICATION	Yes	No
1. Accuracy		**Does the publication mention advice from trusted cybersecurity sources like the National Cyber Security Centre (NCSC) in the UK / Ireland or the National Institute for Standards and Technology (NIST) in the USA?** ***Hint****: Mentions of these organisations.*		
		Does the publication explain how to use messaging Apps (e.g. WhatsApp or Signal) & other third-party Apps on personal smartphones for secure communication? ***Hint****: Clear step-by-step instructions for maintaining private and secure communications.*		
2. Completeness	2.1 General	**(i) Does the publication clearly explain why a personal device, Instant Messaging, or third-party App is being used for clinical communications?** ***Hint:*** *Look for reasons like specific features and efficiency to enable understanding of the benefits and risks.*		
		(ii) Does the publication clearly state the need for a formal risk assessment (such as a Data Protection Impact Assessment (DPIA) in the EU) before using these technologies? ***Hint:*** *Ensure it emphasises the legal requirement to assess potential security issues and develop a best practice plan.*		
	2.2 Confidentiality	**(i) Does the publication explain and describe the obligations for clinicians when using personal smartphones, Instant Messaging, and third-party Apps to process patient information in terms of relevant laws like GDPR (EU) or HIPAA (US)?** ***Hint****: How these regulations apply and what needs to be done to comply – for example, patients have the right to request access to the data to correct it, or to have it deleted.*		
		(ii) Does the publication discuss verifying that an App does not access sensitive metadata (like location, date, and time) in exchange for functionality? Are steps to limit such access explained? ***Hint:*** *Check if it mentions ways to disable features like geolocation, camera, and microphone.*		
		(iii) Does the publication specify that personal smartphones should never use free Wi-Fi if they host or process sensitive data? ***Hint:*** *Ensure it advises against using free Wi-Fi to prevent data breaches.*		
		(iv) Is it stated that unauthorised users must be prevented from accessing any device that hosts sensitive data? ***Hint:*** *Look for guidance on keeping the device secure and not sharing it with others.*		

		(v) Does the publication explain the importance of avoiding the installation of suspicious Apps on personal smartphones used for confidential professional communication? *Hint**:*** *Advice against installing and / or co-hosting Apps (e.g. TikTok) that might pose security risks.*		
	2.3 Integrity	**(i) Are the requirements regarding the following aspects clearly described, including their relevance to personal smartphones, IM, and third-party Apps? *Hint:*** *Each aspect is specifically addressed in the context of personal smartphones, IM, and third-party Apps, detailing how these requirements impact secure usage.*		
		(a) **Server location**		
		(b) **Data encryption**		
		(c) Data security in transit and at rest		
		(ii) Does the publication explicitly describe how to configure any third-party App (e.g., disabling image and data streaming to networked devices and unsecured cloud servers) to minimise risk? *Hint:* *Clear instructions on adjusting App settings to enhance security.*		
		(iii) Is the importance of security settings, AND password protection, AND Multi-Factor Authentication (MFA) for devices and Apps thoroughly explained and emphasised? *Hint:* *Recommendations on using strong passwords, enabling MFA, and configuring security settings.*		
		(iv) Is the requirement for regular training or briefings on security clearly stated? *Hint:* *The need for ongoing education on security practices.*		
		(v) Is the need for regular, scheduled reviews of the App clearly communicated? *Hint:* *Advises regular evaluations and updates on security measures.*		
	2.4 Availability	**(i) Does the publication discuss the importance of evaluating the following elements? *Hint:*** *Explanations of how factors affect the availability and functionality of the App.*		
		a) **Network capacity**		
		b) **Network coverage**		
		c) **Power usage**		
		d) **Data accessibility**		

		(ii) Are there clear instructions for keeping records of chats and images in patient records, including regularly scheduling the recording / downloading and deletion of confidential data from both the sender's and receiver's Apps and devices? *Hint:* *Steps on how to save and delete data securely to ensure compliance with ethical, regulatory, and legal requirements.*		
3. Timeliness	**Is the information published after May 2018 (post-GDPR implementation)? *Hint:*** *Publication date should be no older than 2 years with older editions archived to avoid confusion.*			
	Does the source regularly update the content, or are there scheduled updates? Is this publication recent enough to be relevant? *Hint:* *look for information on how often the content is updated and if the publication is still current.*			
4. Relevance	**Does the guidance explain how to use personal smartphones, messaging Apps, or third-party Apps securely in compliance with data protection laws? *Hint:*** *Advice on avoiding insecure cloud backups, suggestions for securely storing chats and images and the specific requirements for legally processing patient data under the law (e.g. GDPR)*			
	Does the guidance discuss the legal and ethical issues of getting informed consent from patients for using these technologies? *Hint:* *Explains the need for clinicians to understand and communicate the risks and benefits and clarifies that patients cannot consent to illegal data processing.*			
5. Clarity	**Is the language used simple and easy to understand, with all necessary materials or links provided for further information? *Hint****: Check if you understand terms used without needing to look them up elsewhere, and if the document includes links or additional materials for more information.*			
	Is the advice clear and easy to apply in your clinical practice? *Hint:* *Can you apply the guidance to your daily work?*			
6. Credibility	**Does the content mention specific legal requirements, like GDPR (EU / UK) or HIPAA (USA)? *Hint:*** *Data protection laws and regulations in your region.*			
	Is the source of this publication a trusted and reputable authority for clinicians? *Hint:* *Trusted sources for example: clinical defence unions, HSE / NHS, Royal Colleges etc.*			
	Does the publication clearly state that there is no bias or sponsorship, or is there no evidence of bias or sponsorship? *Hint:* *Declaration of no bias or indication that the content might be influenced by sponsors.*			
7.Access	**Can you access the full publication without needing to pay, subscribe, or log-in? *Hint:*** *Document is freely available and not behind any paywalls or membership requirements*.			

The GDPR may place clinicians, particularly those in private practice, in the role of data controller, creating significant responsibilities they may not be prepared for. These include determining how personal data is processed and ensuring its protection by adhering to the GDPR principles, such as securing patient data and upholding patients' rights [19, 25] when using personal BYOD smartphones, IM, and third-party apps. The GDPR is designed to create a clear and consistent framework that helps organisations, including clinicians, understand their obligations and ensure compliance [166]. One experienced clinician's feedback suggested that in her opinion some dimensions of the DDA v2.0 were too complex and should be removed. This reflects a concerning perception that legal and regulatory mandates might be optional or even irrelevant to clinicians. This may reveal a disconnect between the legal requirements of clinicians and their understanding of them, despite the stringent security mandates under the GDPR for clinical data (classified as special category data). Further, findings indicate that many clinicians did not fully grasp their legal obligations when using personal digital tools to manage patient data. This lack of understanding extends to the practical and technical measures necessary for GDPR compliance.

The analysis of Cohen's Kappa scores revealed significant variation in the level of agreement between reviewers and the Gold Standard Scores when using the DDA v2.0 to assess the three selected published guidance articles [109, 111, 116]. The scores ranged from as low as 0.2 (slight agreement) to as high as 0.68 (substantial agreement) [165]. This highlights not only differing interpretations of the DDA v2.0 among practitioners but also underscores a critical issue: the overconfidence of some practitioner reviewers in their ability to complete the assessment without fully engaging with the accompanying Instruction Sheet. This overconfidence was evidenced in the focus group discussions, where it became apparent that some practitioners believed they understood the DDA questions better than their performance against the Gold Standard Test Scores. The lack of familiarity with the Instruction Sheet likely contributed to the lower Cohen's Kappa scores, suggesting that some reviewers had not recognised the complexities of the questions, or the nuances required for accurate assessment. This finding points to a potential "*unconscious incompetence*" [167] among clinicians, where they may not be aware of their own knowledge gaps. The observed variation in scores emphasises the importance of ensuring that all users are adequately prepared to use the DDA. While subsequent iterations of the DDA, including the DDA v3.0, incorporated improvements such

as additional ‘hints’ to eliminate the requirement for an additional instruction / information sheet, and a clearer format, these changes alone may not be sufficient. Overconfidence can significantly impair decision-making by fostering a false sense of competence and autonomy, leading individuals to overestimate their abilities and underutilise available resources [168, 169].

Practitioners noted the necessity for a significant cultural shift within clinical environments to support the safer use of personal digital communication technologies. By fostering a collaborative and informed culture, clinicians can better navigate the complexities of using digital technology, enhancing their understanding of data protection obligations, and ensuring patient data is managed responsibly. With the current absence of explicit guidelines from authoritative bodies [27], there is a broader need for a digital transformation strategy involving collaboration among regulatory bodies, health systems, IT and cybersecurity professionals, and patient groups. Following clinician feedback, it is likely that the next iteration DDA v4.0 will be a digitised version hosted by a health system or regulator to enhance usability and compliance support.

The psychological effects of perceived power, as detailed by See et al. [169], can lead to a diminished willingness to seek advice or adhere to guidelines, which directly impacts on the consistency and accuracy of evaluations. By understanding and mitigating the influence of overconfidence and the psychological effects of power on judgment, organisations can enhance the reliability and accuracy of assessments, ultimately improving decision-making processes in leadership and management contexts [168, 169]. Existing literature indicates that targeted training could significantly enhance the reliability and consistency of Cohen’s Kappa scores [170]. Such sessions could include practical exercises using real-world examples and calibration meetings where raters discuss and reconcile differences, thereby improving inter-rater reliability. Furthermore, practitioners perceived that the improvement in their ability to evaluate guideline papers was due to increased familiarity with the DDA questions through practice. However, without a predefined sequence for assessing the three papers [109, 111, 116], it was not possible to statistically verify this. This observation supports the need for structured training and calibration sessions to mitigate the risks associated with overconfidence and to enhance the accuracy and reliability of the DDA.

6.6 CONCLUSION

We adopted a holistic approach drawing on the areas of healthcare, IS, cybersecurity and legal / regulatory frameworks, to enhance the quality of decision-making regarding clinical communication using digital tools. This study emphasises a multi-stakeholder approach addressing the needs of both practitioners (i.e. Clinicians) and the larger organisational and regulatory ecosystem, aiming to support compliance and improve data quality in healthcare environments. Through an ADR approach, we developed the DDA for assessing and improving the data quality of guidelines concerning the use of BYOD, IM, and third-party apps for secure communication. This paves the way for more effective integration of digital technologies into clinical practice, setting the stage for future digital transformation in healthcare. Despite its strengths, our study has limitations. One primary constraint is the DDA's dependence on the quality of input data, which can vary between practitioners, potentially affecting its consistency and accuracy. Additionally, the artefact has been assessed in a controlled environment and its performance in 'real-world' clinical settings remains to be fully evaluated. Ongoing evaluation and iterative refinement are essential to ensure its reliability and effectiveness in practice. The DDA could evolve further, it has the potential to be tailored for specific clinical or healthcare areas to enhance its relevance and application in diverse settings.

This study advances theoretical development in the research-clinician design process in three important ways. Firstly, to the best of our knowledge, few studies have applied elaborated ADR [30] to design an artefact to guide clinicians use of BYOD, IM, and third-party apps. This theoretical lens provides a new perspective to explore a co-creation phenomenon in this context. The design of the initial DDA emerged from existing data dimensions [148], these ingrained elements were fundamental to informing the artefact's analytical capabilities. Thus ensuring adherence to rigorous data quality standards while aligning with evolving clinical requirements, thus manifesting the DDA *"in a socially recognisable form"* [171, p.19]. One key element of the artefact's evolution was the continual, close collaboration between researchers and clinicians, ensuring that the DDA remained relevant to clinical needs, and practical for real-world application. This interplay facilitated the iterative refinement of the artefact, allowing it to address real-world challenges more effectively while being shaped by

ongoing feedback from clinical practice. Secondly, this research reveals challenges encountered in contemporary clinical settings highlighting the tension between the need to ensure the precision of the technical terms used to communicate data and digital security guidance while maintaining the usefulness and usability of the DDA. This approach also serves to uncover the gaps in digital and data security literacy among clinicians. Thirdly, the value of researcher-clinician designed artefacts constitutes a research field of real importance as clinicians continue to rely on informal IT solutions to do their jobs. Building on the work of Twomey et al. (2020) [172], our approach enabled us to generate fresh insights into the phenomena, refining our understanding of the problem, and working towards a more holistic and inclusive perspective. Practical insights from clinicians contributed to the advancement of the design of the DDA.

This research primarily focuses on clinicians who need to navigate complex data quality standards and regulatory compliance when using digital tools to share sensitive patient information. These professionals often struggle with interpreting regulatory guidelines while managing time constraints and focusing on patient care. This study reveals an important opportunity to investigate the impact of decision confidence and perceived expertise on the use of the DDA [168] among clinicians. Overconfidence in one's judgment and expertise can lead to a biased interpretation of data and disregard for critical input, ultimately affecting the accuracy and reliability of assessments. Future studies could explore how these cognitive biases influence the effectiveness of the DDA in clinical settings and identify strategies to mitigate their effects. This could involve examining the relationship between decision confidence, information use, and decision outcomes, developing training interventions aimed at fostering a more balanced and reflective approach to decision-making among clinicians. While our proposed artefact supports decision-making by clinicians, there remains a need for specific, actionable, regularly updated guidance and education to keep pace with technological advancements and promote compliance among clinicians.

CHAPTER 7 DISCUSSION

This thesis addresses the overarching research question: *How do / should clinicians use smartphone technologies to communicate patient data?* To this end, four key objectives were pursued:

1. To evaluate the available literature on the use of personal smartphone technology for communication between clinicians.
2. To determine the current use of smartphones and mobile technology among clinicians in Ireland and the UK.
3. To evaluate the current guidelines that are available to inform practice-based communication between clinicians using personal BYOD smartphones, IM and third-party apps in Ireland and the UK.
4. To develop and evaluate a clinician toolkit (artefact) to assist clinicians in their assessment of the available guidelines regarding communication using smartphone technologies.

In this chapter, we examine how each of these objectives has been met, the findings are synthesised, and their significance critically evaluated in the context of enhancing secure communication practices in healthcare.

7.1 OBJECTIVE 1: TO EVALUATE THE AVAILABLE LITERATURE ON THE USE OF PERSONAL SMARTPHONE TECHNOLOGY FOR COMMUNICATION BETWEEN CLINICIANS

The initial scoping literature review [35] serves as a foundation for this study. It provides a comprehensive overview, map and assessment of the available published literature (as of early 2021) informing practice regarding the use of personal smartphones for secure communication between clinicians. Evidence was found of widespread, international adoption of BYOD smartphones, apps and functionality (from image sharing [3, 4, 10, 25, 39, 44, 46-48, 50, 58, 64, 65, 67, 68, 70, 72, 81, 92, 93] to IM [4, 6, 10, 11, 36, 37, 39, 44, 48-50, 58, 63-65, 68, 70, 75, 85, 90, 93, 94] and video

conferencing [4, 6, 10, 11, 36, 37, 39, 44, 48-50, 58, 63-65, 68, 70, 75, 85, 90, 93, 94] to communicate confidential information between clinicians.

Despite the efficiency and convenience these technologies offer, significant risks related to data security, patient privacy, and compliance with the legal and technical requirements of GDPR were found to be underexplored and inadequately addressed within the published literature. A key finding of this first scoping literature review was the significant lack of evidence describing the use of genuinely secure channels for communicating sensitive patient data between clinicians. Notably, almost 40% of publications failed to acknowledge or totally ignored the essential technical and security measures necessary for safeguarding confidential information [2, 6, 37, 39, 55, 61-79], which are necessary for ensuring compliance with GDPR [19] within the EU or HIPAA [23] in the USA. Given the strict technical and security requirements required by GDPR, underpinned by Article 8 of the European Convention on Human Rights [57], this gap in the literature is deeply concerning and raises significant questions regarding the adequacy of current digital communication practices. Significantly, data subjects (all individuals within the EU) gained a raft of new legal rights regarding the processing of their data including the right of access, the right of rectification, the right to erasure, the right to restrict processing and the right to object to their data being processed [54] with the implementation of GDPR in 2018. This oversight highlights gaps in knowledge regarding what constitutes an appropriate secure digital communication channel, as well as the processes for risk assessing and approving such channels for clinical use, not only for those who authored the papers but importantly, for those who peer reviewed and published them. The continued publication of material that lacks comprehensive acknowledgement or insight regarding these issues may contribute to the persistence of these gaps, potentially reinforcing misconceptions and perpetuating inadequate practices in clinical settings.

Adherence to data protection laws and regulations require actionable, well-informed advice, policy, and training to address the security and technical challenges posed by the current BYOD smartphone communication technology used in clinical practice. An appreciation of the complexities involved is essential, yet it is evident from the first scoping literature review that many authors / researchers and indeed peer reviewers lack sufficient insight into these issues, further exacerbating the problem.

While much of the published literature was found to acknowledge the availability, usefulness, and widespread use of these technologies, few studies provided detailed guidance on how to ensure data security and respect patients' rights under the law. This highlights a critical need for more targeted research that addresses the secure use of BYOD smartphone technology in clinical settings. It is essential that various associated subject matter experts (including cybersecurity, IT, information governance and legal specialists) with a deep understanding of the technical challenges posed by the technology, data protection laws and regulations or information governance, be drawn upon to inform policy, and peer review of any such material prior to publication. The simplicity of the use of this technology has evidently been taken at face value, and in doing so, the complex security challenges and the human rights of those involved have apparently been put at risk. Without specialist input from cybersecurity and data governance professionals familiar with the specific requirements for GDPR compliance, the published literature risks propagating a culture of inadequate and irresponsible communication practices.

These findings align with the research objective and emphasise the importance of understanding the landscape of BYOD smartphone technology use among clinicians. In light of the assessment of the literature for this scoping review in early 2021, it is notable that subsequent, recent work by Morris et al., of October 2024 [173] corroborates our observations. A simple PubMed search conducted as part of that study [173], highlights the continued informal, widespread reliance on WhatsApp, IM and other third-party apps for clinical communication in various settings globally, with almost 2000 citations and 16 literature reviews identified on the subject published over the last five years. Authors found the benefits and utility of IM and third-party apps such as WhatsApp widely reported, but noted the absence of guidelines, a lack of formalisation, or awareness of regulatory requirements in their review of publications. This aligns with the gaps observed in this thesis, particularly concerning when the technical and legal inadequacies of such platforms for secure communication are considered. These parallels underscore the urgent need for targeted guidelines and tools to ensure compliance with data protection standards like GDPR, a focus central to the development of the toolkit, presented in this thesis.

It is essential to understand why many clinicians continue to use insecure personal platforms rather than more secure alternatives, and apparently lack an appreciation of, or choose to ignore the risks this technology may pose. Clinicians' familiarity with easily accessible yet insecure technology via their BYOD smartphones may have escalated this issue of "*backdoor adoption*" [38] a challenge further intensified by the COVID-19 pandemic, which created an urgent need for efficient remote communication, further complicating efforts to ensure compliance with data protection regulations.

7.2 OBJECTIVE 2: TO DETERMINE THE CURRENT USE OF SMARTPHONES AND MOBILE TECHNOLOGY AMONG CLINICIANS IN IRELAND AND THE UK

The anonymous online survey [96] we conducted with dental professionals in Ireland and the UK revealed the widespread use of personal BYOD smartphones (98% of respondents from Ireland and 100% from the UK). Among the 123 respondents from Ireland and 77 from the UK, the majority confirmed regular use of BYOD smartphones to exchange clinical information with colleagues, including images (63% of respondents from Ireland and 62% from the UK) and messages related to patient care.

While most respondents expressed confidence in their technological skills (85% of respondents from Ireland and 92% from the UK), with the majority (77% of respondents from Ireland and 91% from the UK) believing they had the necessary proficiency to use smartphones for clinical purposes. The survey uncovered significant concerns and lack of awareness regarding gaps in their knowledge and practice in relation to the requirements of data security. Despite their stated confidence in their technical skills and insights, half of the participants admitted to storing or potentially storing sensitive patient data on their personal devices (50% of respondents from Ireland), a similar proportion confirmed streaming sensitive data to insecure, potentially non-GDPR compliant cloud storage. Furthermore, a number of respondents acknowledged that data were being streamed between networked devices, with 73% of respondents from Ireland confirming that they owned multiple devices, and 29% acknowledged that data was streaming (or could stream) between these devices, posing additional security risks. Such practices clearly illustrate a disconnect between

clinicians' perceptions of security and the actual risks posed by using BYOD smartphones to process confidential data. These results effectively signpost the gaps in knowledge among clinicians regarding secure communication practices and adherence to data protection regulations like GDPR, demonstrating the need for clear, actionable guidelines, practical tools and comprehensive training to support compliance with information governance requirements.

Despite a general, apparently superficial awareness of the risks associated with BYOD smartphone use, there was a notable lack of proactive measures being taken to mitigate these risks. Clinicians appeared unaware of their responsibilities under GDPR, particularly concerning data storage, transmission, and deletion. For example, many respondents confirmed that they would require technical support to remove patient-identifying data from their devices when upgrading or trading them in, highlighting a significant gap in their digital literacy. This highlights the need for practical support, resources or tools to assist clinicians in meeting data security requirements, as well as better signposting to help them select and navigate more secure BYOD smartphone communication effectively.

Although our survey had a relatively small sample size of dental clinicians, primarily attributed to difficulties in accessing respondents stemming from the restrictions imposed for the COVID-19 pandemic in 2020 and 2021, the demographic differences between employment types in Ireland and the UK are noteworthy. In our survey, a significantly higher percentage of respondents were employed primarily in the private sector in Ireland (n=78; 63%) compared to the UK (n=22; 29%). This distribution is generally reflective of broader dental workforce trends, where the private sector dominates in Ireland. However, there has been a rapid shift towards private practice in the UK in recent years [174] which has continued to escalate subsequently. This may have implications for access to specialist resources (such as the advice or support of various associated subject matter experts, from IT to Information Governance), which may only be available to those working for larger employers such as the NHS. Moving forward, regulators may need to play a more prominent role in providing clear, actionable guidance and mandating compulsory CPD or signposting the use of specialised services. Such measures would raise awareness, protect the human rights of data subjects (patients), and safeguard the reputation of the clinical professions.

These findings demonstrate that despite clinicians being increasingly reliant on BYOD smartphones for communication regarding patients between each other, they often lack a thorough understanding of the security measures required to protect sensitive patient data. This gap reveals the urgent need for more comprehensive education, specialist resources, clearer guidelines regarding secure communication practices, ensuring clinicians not only appreciate or understand the risks and complexities, but are equipped to navigate them effectively. These results align with the second research objective, revealing current practices and pointing to the critical need for specialist resources and tools, clear guidance and improved training to support compliance with data protection regulations.

Given the rapid evolution of technology, regulatory requirements, and privacy standards, clinicians must continuously adapt their practice to optimise security and maintain compliance. This reality makes guidelines and education a 'moving target', requiring ongoing updates and proactive training [175] to equip clinicians with the latest strategies for managing patient data responsibly. Without such adaptive support, the risk of non-compliance and security vulnerabilities remain high as technology and expectations advance. Following the assessment of clinicians' current use of BYOD smartphone technology for communication, it is important to evaluate the guidelines available to inform and guide these practices. Objective 3 addresses this need [96] by focusing on the evaluation of existing guidelines, as the previous findings highlight a gap between clinicians' awareness of secure communication practices and their actual compliance with data protection regulations. Without clear, actionable guidance, clinicians are left navigating this complex landscape with limited support, which increases the risk of data breaches and regulatory violations. Therefore, it is important to examine the adequacy of available guidelines to determine if they provide the necessary detailed, technical, actionable guidance clinicians need to ensure secure, GDPR compliant communication. This evaluation is essential to identify areas where additional support or tools may be required to enhance clinical practice.

7.3 OBJECTIVE 3: TO EVALUATE THE CURRENT GUIDELINES THAT ARE AVAILABLE TO INFORM PRACTICE-BASED COMMUNICATION BETWEEN CLINICIANS USING PERSONAL BYOD SMARTPHONES, IM AND THIRD-PARTY APPS IN IRELAND AND THE UK

The second scoping review [27] identified significant gaps in the current guidelines available to clinicians in Ireland and the UK regarding the secure use of BYOD smartphone technology, IM and third-party apps to exchange clinical information between colleagues. Despite the evidence of widespread informal adoption of this technology by clinicians, some of the entities contacted indicated that they offered no such guidance, as the practice is banned. While several publications emphasise the importance of adhering to GDPR requirements and confidentiality principles, few offer actionable guidance regarding tangible requirements of clinicians or secure communication, the selection, assessment, configuration, or optimisation of the security of contemporary BYOD digital communication tools. Moreover, any advice provided was principle based, overly simplistic, and lacked the depth needed to comprehensively address the complexities of secure digital communication required to comply with GDPR standards, neglecting the critical legal obligations of clinicians as data processors or data controllers to ensure the protection and lawful processing of special category health data [176].

This lack of specificity creates uncertainty for clinicians, many of whom are unaware of the full extent of their obligations regarding data protection and patients' rights under the law and further, unaware of the threats to confidentiality posed by their informal adoption of BYOD technology. GDPR clearly classifies health related information as *"special category data"* [176] which is subject to additional protection, and this leaves clinicians vulnerable to both unintentional data breaches and regulatory scrutiny. Other important findings of this second scoping review include the significant barriers to accessing guidelines (as many required paid membership credentials for access or were obscured behind automated systems), and the lack of coordination between employers, unions, professions and regulators, and inconsistency in the quality and depth of advice provided. This combination not only risks creating confusion among clinicians but also underscores the critical need for guidance that

is both easily accessible and uniformly applicable across all clinical professions and healthcare providers.

The absence of detailed guidance, coupled with the difficulty in accessing any such resources is particularly concerning given the use of these tools for clinical communication, as highlighted in the initial scoping literature review [35] and subsequent survey findings [96]. Clinicians regularly use BYOD devices to share patient data, often without fully understanding the risks or ensuring appropriate safeguards. The failure to provide clear guidelines on the secure use of these technologies not only compromises patient confidentiality but also undermines clinicians' ability to comply with data protection regulations, ensuring that patients' rights are respected.

This review [27] revealed a critical need for accessible, consistent, well-informed, detailed guidelines that go beyond broad principles and offer practical advice for clinicians on securely configuring and using BYOD smartphone technologies. Without such guidance, clinicians are left to navigate this "wild west" [27] of digital communication largely on their own, increasing the risk of data breaches and undermining compliance with GDPR.

In addressing this objective, this scoping review highlights the pressing need for a tool or resource that can provide clinicians with the support or framework they need to make informed decisions regarding secure communication practices. A tool could bridge the gap between existing broad guidelines and the practical, day-to-day realities of clinical smartphone communication, ensuring that clinicians are not only aware of their obligations but equipped to meet them effectively.

7.4 OBJECTIVE 4: TO DEVELOP AND EVALUATE AN ARTEFACT TO ASSIST CLINICIANS IN THEIR ASSESSMENT OF THE AVAILABLE GUIDELINES REGARDING COMMUNICATION USING SMARTPHONE TECHNOLOGIES

The development of a specialist clinician toolkit / artefact was driven by the need to support clinicians in evaluating the quality and adequacy of guidance concerning the security and

compliance of digital communication technologies. This toolkit was designed to fill a gap in the availability of clear, actionable guidance on secure clinical communication, as identified in the prior research. Drawing on expertise from IS, cybersecurity, and regulatory standards, the toolkit was generated to provide clinicians with a practical framework to inform their assessments of the quality of any guidelines they encounter, ensuring that their use of digital technologies aligns with the stringent data protection requirements of GDPR.

The toolkit was developed using a process inspired by elaborated ADR methodology [30], which integrates iterative cycles of diagnosis, design, implementation and evolution. The initial version (DDA v1.0) was created by customising key DQDs [148] and incorporating insights from authoritative sources such as the NCSC, NIST, the DPO and the DPC. These sources were essential for providing reliable expertise, informing the toolkit's focus on key elements of the data quality, including accuracy, completeness, timeliness, relevance, clarity, credibility and accessibility.

This four-stage elaborated ADR approach [30], followed through three iterations with clinician involvement at each stage, developed a toolkit that was tested through continuous cycles of structured evaluation to optimise the toolkit's evolution, usability and effectiveness.

Quantitative analysis involved comparing the clinician reviewers' evaluation scores of guideline documents using the toolkit with predefined gold standard scores. The results revealed a broad range of accuracy in responses, with some dimensions achieving high agreement and others showing significant variability, reflecting a gap in clinicians' understanding of data protection requirements. This discrepancy suggests an element of overconfidence, where some clinicians were unfamiliar with the additional documentation (Instruction Sheet) that had been provided, assuming a level of competence they have not fully attained, and potential "*unconscious incompetence*" [167]. This phenomenon was particularly evident in questions on credible cybersecurity sources, encryption, and scheduled updates, as clinicians' responses varied widely. Such overconfidence can impede clinicians' recognition of gaps in their understanding, highlighting a critical need for targeted training to bridge these gaps and enhance secure communication practices.

Qualitative feedback from the focus groups revealed several key themes:

- Utility of the toolkit: Clinician reviewers appreciated the structured approach that the toolkit provided for assessing guidelines. Many reported that using the toolkit improved their insight into areas of risk they had previously overlooked, such as the dangers of accessing unsecured WIFI with BYOD devices used for clinical communication.
- Awareness and Competency Development: Both student and experienced clinician reviewers acknowledged a significant improvement in their awareness of the legal and technical requirements for secure communication. One clinician noted that the toolkit prompted them to recognise previously unnoticed gaps in their knowledge, transitioning from *"unconscious incompetence"* [167] to a more informed understanding of secure communication practices.
- Educational Recommendations: The need for further training was strongly emphasised. Experienced clinician reviewers suggested that educational initiatives, including CPD, should incorporate training on data security and actionable guidance concerning digital communication to ensure practitioners are better equipped to meet GDPR requirements.

The iterative development of the toolkit revealed gaps in clinicians' digital literacy and underscored the challenges in maintaining compliance with data protection standards. A notable overconfidence among clinicians emerged, reflecting lack of awareness regarding their legal obligations and patient rights under the law, and an underestimation of the complexities associated with current BYOD, IM and third-party apps for processing this special category health data. These insights signpost the necessity for a cultural shift within healthcare, where digital transformation is supported not only by tools but also by a more comprehensive, interdisciplinary approach that prioritises secure communication practices.

7.5 CULTURAL SHIFT AND INTERDISCIPLINARY COLLABORATION

The evidence suggests that clinicians' knowledge of data protection standards often falls short. This research reflects a need for a cultural shift to fully support secure digital transformation in healthcare. Several clinicians admitted (during the focus group discussions) to their assumption of security for patient data when using well-known third-party apps and lacked awareness of specific GDPR obligations and actionable technical requirements. This gap illustrates a pressing need for interdisciplinary collaboration [10, 173, 177] among healthcare

providers, IT experts, and regulators, not only to enhance clinicians' digital literacy but to foster a proactive approach to managing secure communication technology in clinical settings. This shift involves evolving attitudes, behaviours, and practices at all levels of healthcare systems and across the range of clinical professions. Effective digital transformation requires not only technological advancement but also interdisciplinary collaboration [177] that draws on expertise from IT, cybersecurity, legal, information governance, and patient representatives. Together, these stakeholders can inform, develop and implement secure communication practices. The shift must also extend to professional attitudes and the cooperative culture that surrounds digital transformation, impacting everything, from the drafting of guidelines, to ensuring insightful current peer review processes of academic literature prior to publication, to the curriculum of undergraduate education and CPD, to impact contemporary communication practices in healthcare. This cultural change is necessary to ensure that technological solutions are seamlessly integrated into clinical workflows and sensitive patient data is effectively protected.

7.6 IMPLICATIONS FOR PRACTICE

The toolkit has significant potential as a catalyst for change, offering a means not only for clinicians to recognise the limitations in their guidelines, but also to help them to improve their appreciation and understanding of the complex considerations required to assess the security of BYOD smartphone, and third-party technologies. By highlighting these gaps, the toolkit could be used to motivate clinicians to seek collaboration with specialists from other fields, fostering interdisciplinary partnerships essential for comprehensive digital transformation. This shift not only raises awareness but also promotes a culture of shared expertise, ultimately advancing secure and informed digital communication practices in healthcare.

The elaborated ADR process [30], through its iterative cycles of continuous feedback and adaption of the toolkit to align it with clinicians' needs, was instrumental not only in informing the toolkit usability and effectiveness but also in providing real-time insights into the training, guidance, and resources clinicians require to navigate data security challenges in digital communication. Drawing on established knowledge from IS, including DQDs and elaborated

ADR methodology, this change of approach demonstrates the potential of interdisciplinary collaboration to enhance healthcare outcomes by fostering secure and efficient communication practices.

The findings highlight the urgent requirement for healthcare professionals to have access to more comprehensive and actionable, consistent and accessible guidelines, supported by practical tools such as the toolkit, which can be integrated into clinical practice to inform decision making and assist clinicians to achieve more secure communication practices. Furthermore, targeted education and training programmes, embedded in both undergraduate curricula and CPD, are necessary to equip clinicians with the knowledge and skills to prioritise and navigate the complexities required for data security and compliance with regulations such as GDPR. Immediate steps could include the implementation of thorough and actionable guidelines concerning the use of BYOD technology, the provision of tools to inform decision making, alongside ongoing training for clinicians on digital professionalism and data-security. An interdisciplinary approach to both research (through the use of collaborative methodologies such as elaborated ADR) and practice that integrates expertise from IS, IT, cybersecurity, data protection, along with healthcare policy and training will help drive the holistic cultural change necessary for meaningful digital transformation in healthcare. By leveraging these diverse areas of knowledge, healthcare systems can develop targeted training programs, adopt and implement secure communication technology, and clear practical guidelines that clinicians can readily action. Such collaboration ensures that technological solutions are not only compliant with data protection regulations and standards but also seamlessly integrate into clinical practice, ultimately enhancing patient safety and data security.

7.6.1 Limitations and Challenges

Several limitations emerged during the development and testing of the toolkit. A significant issue was the overconfidence of some clinicians, who initially believed they understood the security requirements better than they did, leading to inaccuracies in their assessment of the guideline documents provided. This echoes findings from the initial literature review [35] and survey [96] during prior research, and potentially highlights a requirement for targeted training to complement the toolkit, ensuring that clinicians apply it effectively.

The toolkit's reliance on the quality of input data was identified as a concern. It was successful in increasing clinicians' awareness of secure communication practices, there were clear challenges related to the variability in how it was used by clinicians. Cohen's Kappa scores indicated substantial variation in the accuracy of clinician responses, suggesting that further refinement of the toolkit was necessary. This variability in evaluation results, also underscores the importance of clinicians having access to high-quality, up-to-date guidance and training to ensure accurate toolkit assessments. The toolkit's effectiveness depends not only on its design but also on clinicians' understanding of each dimension it assesses. If clinicians lack a foundational understanding of data protection and security requirements, their interpretations may vary significantly, affecting the accuracy of their evaluations. Thus, comprehensive training and well-defined instructions are essential to support consistent use of the toolkit and ensure that clinicians can interpret its criteria reliably.

While the toolkit showed promise, further research is required to evaluate its effectiveness in real-world clinical settings with the broad range of healthcare professionals. Future iterations of the toolkit could include features such as digitisation to improve accessibility and usability, making it a more integrated tool for use in clinical practice.

The qualitative feedback during the ADR process, however, was positive, with practitioners acknowledging that the toolkit had improved their understanding of secure communication technologies. This outcome aligns with the objective of developing and evaluating a tool to enhance clinicians' decision-making around secure smartphone use.

7.7 SYNTHESIS OF FINDINGS ACROSS OBJECTIVES

The omnipresence of BYOD smartphones for sharing data between clinicians is undeniable, but it is equally clear that clinicians are not adequately equipped to mitigate the associated risks, particularly concerning data security but also with regard to their obligations in relation to patients' rights regarding their data. The findings across the four objectives converge on several key themes, including the requirement for comprehensive, actionable, accessible and consistent guidelines, the development of tools to support clinicians in secure communication practices and enhanced education to improve awareness of the complexities of this

technology as well as the rights of the data subjects (patients) and clinicians' obligations as data processors (or potentially data controllers) under the law.

A key finding from the development of the toolkit is the pressing need for a cultural shift within clinical environments to fully support secure digital communication practices. Given the current lack of compliance with GDPR in contemporary clinical communication practices, healthcare institutions face a critical choice: either invest significantly in secure, enterprise-level clinical communication systems or equip clinicians to use personal BYOD technologies as safely as possible. Effective enterprise systems would necessitate substantial and ongoing investment in infrastructure, software, and training to ensure all clinical communication remains secure and compliant. However, despite several entities asserting that BYOD, IM, and third-party app usage for clinical communication is prohibited, academic literature reveals prolific evidence of their continued use. Researchers in a recent study quote a range of perceived benefits of the use of WhatsApp specifically being widely reported in the literature, from efficiency, to ease of use, favourable response times, reduced referral rates and passive learning [173]. Studies consistently highlight how BYOD technology is widely adopted by clinicians to facilitate efficient communication [173], underscoring a significant gap between policy and actual practice in many healthcare settings globally. Alternatively, clinicians must be equipped with comprehensive education and robust tools to navigate the complexities of using BYOD smartphone technologies while adhering to GDPR and other regulatory requirements.

The recent study by Morris, Scott & Mars [173] confirmed the ongoing global adoption and breadth of utilisation of personal digital technology for clinical communication across the full range of clinical specialities internationally. Authors stated: "*No prior research has provided details of current practice in WhatsApp… nor offered evidence-based insight about how formalisation might be achieved*." These researchers (based in south Africa, where regulations such as GDPR or HIPAA don't apply) stated that formal policy, standards and guidelines are essential to ensure that practice is conducted appropriately. However, as previously stated, WhatsApp, IM and personal technology is not currently GDPR compliant or secure for the communication of sensitive patient data within the EU, and our evidence indicates that clinicians are unaware of the inherent dangers and inadequacies associated

with this practice. The toolkit has the potential to serve as an effective mechanism to enhance clinicians' awareness of gaps in their competence regarding secure communication practices, thereby motivating them to advocate for and adopt enterprise solutions and more robust, secure digital communication methods.

This lack of security in current digital communication practices risks undermining public trust in the healthcare professions and the health systems offering care. The present situation, which fails to ensure secure processing, is unsustainable and requires immediate attention to prevent future data breaches, regulatory non-compliance and reputational damage. This priority is underscored by a succession of recent data breech incidents, including the NHS cyber-attack of August 2024 [178], and the reports of exploitation of vast amounts of confidential financial data from government databases in Italy [179], which resulted in blackmail (October 2024), and the cyber-attack at South-East Technological University's Waterford Campus in November 2024 [180].

This research has addressed the overarching question of how do / should clinicians use BYOD smartphone technology to communicate patient data. By evaluating the literature, conducting a survey, reviewing existing guidelines, and developing and testing the toolkit, this thesis has provided a comprehensive response to the research question and four objectives. The lack of explicit guidelines from authoritative bodies highlights the necessity for a comprehensive, holistic digital transformation strategy that engages stakeholders across clinical professions, regulators, health systems, and patient representation. By fostering a collaborative and informed culture, clinicians will be better equipped to manage the complexities of BYOD smartphone communication technologies, ensuring that patient data is safeguarded, and that healthcare delivery is enhanced through secure, contemporary communication practices.

A significant challenge in healthcare is the influence of traditionally hierarchical structures that often dominate prestigious professions such as medicine and dentistry. These hierarchies could inhibit effective digital transformation. Individuals in positions of authority within these structures may be less inclined to seek or accept advice, believing their judgement to be superior. This overconfidence, as demonstrated by the work of See et. al. [169], may underlie a lack of understanding of their own limitations or an undervaluation of the specialist

knowledge of others, which is evident in both scoping literature reviews and worryingly, in many of the current principle-based guidelines in this area. Consequently, clinicians may lack awareness of their own knowledge limitations when contributing to guideline development or peer reviewing literature for publication in this area. As a result, such publications may inadvertently endorse practices that compromise data security, violate patient rights, and undermine the professional reputation of clinicians.

Throughout this study, there has been clear evidence that clinicians often lack awareness of the gaps in their understanding, operating with a concerning level of unconscious incompetence.

Such lack of awareness or reluctance to seek expert guidance can stifle innovation and impede the implementation of secure communication tools and policies. These dynamics underscore the necessity for interdisciplinary collaboration [10, 173, 177], where the expertise of various associated subject matter experts is integrated into policy, research, evaluation of ethics committee applications, peer reviewing of papers for publication, authoring of guidelines and ultimately, clinical practice. As Russo and Shoemaker [168] argue, organisations benefit from environments that encourage critical thinking and advice-seeking, which helps to mitigate the detrimental effects of overconfidence on decision-making. Addressing these entrenched power dynamics is essential for ensuring that clinicians can meet their data protection obligations, thereby safeguarding both patient rights and the reputation of the professions.

7.8 FUTURE RESEARCH AND RECOMMENDATIONS

Future research should broaden the scope of BYOD smartphone, IM and third-party app studies by incorporating insights from a diverse array of subject matter experts and multidisciplinary clinicians, such as those from radiology, obstetrics, and remote healthcare settings. Each clinical environment and specialty are likely to present unique requirements for functionality and technical capabilities, for instance, remote locations may face challenges with internet access, while obstetrics require the secure transmission of audio or high-resolution imaging, such as foetal heart rate or ultrasound data. Engaging multiple disciplines ensures that all specific requirements are considered, fostering a collaborative approach

where all stakeholders are active participants in developing and selecting secure, adaptable communication solutions that meet the varied demands of clinical practice. Longitudinal studies are essential to track the evolving use of BYOD smartphone communication technologies in clinical practice. Further refinement and rigorous testing of the toolkit is also critical to improve its usability and adaptability across various clinical environments. Importantly, the toolkit must support the full spectrum of clinical professionals involved in patient care to avoid fragmentation and confusion arising from different clinical professions working with disparate or inaccessible guidelines (those provided by professional bodies requiring membership credentials for online access). Unified, accessible guidance is essential for ensuring secure and effective communication practices, safeguarding patient rights while enabling clinicians to fulfil their legal and professional responsibilities. This could also be of increased significance in evolving environments such as the UK where dental practice may no longer be widely provided by a NHS, but devolved to smaller, private practices, who may not have access to the full infrastructure of support (from Information Governance to IT, compliance and training and development resources) that the NHS may have provided in the past.

The phenomenon of clinician overconfidence observed during toolkit testing suggests a need for targeted training interventions to address gaps in data security literacy and regulatory awareness. Future studies could investigate how cognitive biases, such as overconfidence and unconscious incompetence, influence the effective use of decision-support tools like the toolkit, with an emphasis on developing strategies to mitigate these biases. Moreover, digitising the toolkit and integrating it into existing clinical systems could improve accessibility and streamline its use in practice, making it a more practical resource for clinicians navigating the complexities of secure digital communication.

Recommendations for policymakers and healthcare institutions include the development of uniform, detailed, actionable guidelines regarding the secure use of BYOD smartphones for the exchange of data between clinical colleagues, as well as ongoing training programs for clinicians to stay informed regarding data security practices, and their obligations regarding data security and patient rights under GDPR. Moreover, active collaborations between healthcare providers, professional bodies, regulators, and various associated subject matter

experts could lead to raised awareness and implementation of tools such as MDM software and appropriate prioritisation of the provision of enterprise solutions for secure contemporary communication.

In summary, this discussion has outlined how the research objectives were addressed through a combination of literature reviews, a survey, and the development and testing of a practical toolkit for clinicians. The findings emphasise the critical importance of secure communication in healthcare [1] and the need for policy development [4, 129, 173], education, research involving interdisciplinary collaboration and inclusive transformation in this field.

The findings of this thesis can be theoretically positioned within the Theory of Workarounds [181], which provides an explanatory framework for understanding the persistent and creative ways in which clinicians respond to the systemic constraints of their working environments through their adoption of shadow IT. The widespread use of BYOD smartphones, IM, and third-party apps for sensitive communications around patient care by clinicians, as revealed in this research, reflects goal-oriented adaptations that bypass formal policies and systems, hallmarks of workaround behaviour. Applying Alter's [181] theory also reinforces the importance of developing solutions, such as the toolkit, that do not seek to suppress workaround behaviours outright, but instead acknowledge them as signals of innovation, necessity, or system failure. The integration of Alter's [181] theoretical perspective offers a pathway for future research that aims to understand, design for, and ethically manage the complex realities of personal technology use by clinicians. Subsequent studies could use the Theory of Workarounds to inform the co-design of adaptive, compliance-aware digital tools and to evaluate how systemic, behavioural, and cognitive factors intersect in the adoption and use of secure communication technologies.

7.9 KEY FINDINGS AND CONTRIBUTIONS

This research contributes to the growing body of literature regarding the use of BYOD smartphones for clinical communication in healthcare by not only identifying key gaps [4, 47, 129, 173] but also proposing a practical solution in the form of the toolkit. This toolkit provides clinicians with a structured approach to assess the quality of the guidelines they receive regarding the security of BYOD communication technologies, bridging the gap between broad, principle-based guidelines and real-world clinical practices, and in doing so, raising their awareness of critical considerations that clinicians may otherwise overlook. This study

also highlights the extensive use of insecure BYOD smartphone technologies by clinicians and the inadequacy of the guidance available to support secure communication.

In summary, the thesis makes the following contributions:

- The scoping review on BYOD smartphone usage revealed a wide range of published academic literature confirming usage of personal smartphones and associated third-party technologies for communication between clinicians albeit with a primary focus on the positive aspects.
- This scoping review also revealed a consistent lack of appreciation of the security and privacy issues associated with their usage.
- Our online survey of clinicians' usage of smartphones in Ireland (and UK) provides a previously unreported insight into the ownership and integration of BYOD smartphones for communication between clinicians. Clinicians reported using these devices to send clinical images and radiographs to one-another which has been widely suspected but not reported (to our knowledge). The survey results confirm the outcome of our scoping review in that the risks of BYOD smartphone usage were under-estimated by clinicians.
- Our second scoping review of guidance for clinicians on BYOD smartphone, IM and third-party app usage for communication between each other was the first study to identify the challenge for clinicians posed by the inaccessibility, inconsistence and absence of comprehensive and actionable guidance informing the use of these technologies.
- Finally, the development of the toolkit to support clinicians in evaluating guidelines for decision-making is entirely unique in its conceptual foundation and rigorous evaluation process. Drawing on established knowledge from IS, particularly by adapting DQDs through an elaborated ADR [30] process, this toolkit exemplifies interdisciplinary collaboration and integration. By synthesising IS theories with clinical needs and evolving the toolkit in close collaboration with clinicians, this work bridges a critical knowledge gap for those using BYOD smartphones, IM, and third-party apps for communication of confidential data. Such collaboration not only strengthens the toolkit's practical relevance but also advances theoretical understanding at the

intersection of IS and healthcare. Furthermore, the toolkit encourages clinicians to appreciate the value of expertise from other disciplines, particularly in addressing the legal and technical considerations vital for secure digital communication practices. This interdisciplinary approach has the potential to foster improved adherence to GDPR and bolster clinicians' capacity for well informed decision making. Further, this work sheds light on the nuanced challenge of balancing precise technical language with accessibility, a critical insight for designing tools that address security and regulatory requirements without compromising usability for clinicians with varied levels of digital literacy. The toolkit provides a robust example of a researcher-clinician designed toolkit, underscoring the growing importance of such tools as clinicians increasingly rely on informal IT solutions for communication. This interdisciplinary approach not only advances theoretical insights at the intersection of healthcare and IS but also empowers clinicians to evaluate and implement secure communication practices effectively, bridging crucial knowledge gaps in data security and regulatory compliance.

CHAPTER 8 CONCLUSION

This thesis addresses the critical question of how do / should clinicians use smartphone technologies to communicate patient data. Through comprehensive research and the development of a toolkit, this research identified persistent gaps in communication practices and knowledge, a reliance on insecure technologies, and a lack of actionable guidance in clinical settings. The toolkit demonstrates the potential to bridge this gap by offering clinicians a structured, accessible means to evaluate the adequacy of their guidelines to support secure communication practices.

Key findings underscore the widespread use of BYOD in clinical practice, the substantial risks it poses to data security and patient confidentiality and the considerable body of academic literature highlighting the advantages of this practice which may be inadvertently endorsing and perpetuating its use. Clinicians' widespread use of BYOD smartphone technology without well informed, current actionable guidance, leaves them vulnerable to data breaches and regulatory non-compliance. This thesis contributes to a growing body of knowledge in IS, health informatics and clinical communication, by identifying these gaps and providing a practical tool that could serve as a foundation for better-informed decision making and more secure clinical communication. This study's contribution to the literature is evidenced by a series of peer-reviewed publications generated throughout the research process (see Figure 13), each expanding the body of knowledge on the use of BYOD for communication regarding patients between clinicians.

These findings highlight an urgent requirement for clear, practical, expert informed and consistent guidance, resources and training that not only outlines regulatory compliance requirements but also provides clinicians with the tools and support necessary to integrate more secure practices into their daily communication workflows. Moving forward, this research underscores the critical role of insightful research methodologies, such as elaborated ADR [30], to actively engage stakeholders (including multidisciplinary clinicians and professionals from diverse fields such as IS, cybersecurity and information governance) through iterative cycles of collaboration. This collaborative approach is essential for ensuring effective digital transformation. This research emphasises the importance of interdisciplinary

collaboration in digital health transformation, with a call for policies that prioritise data security and respecting patient rights within healthcare communication practices.

FINAL THOUGHTS

This research underscores the critical importance of secure communication in healthcare, particularly as the use of BYOD smartphone technologies continues to rise. By providing clinicians with the tools and knowledge to recognise and navigate these complex challenges, this study lays a strong foundation for improved data security and patient confidentiality in contemporary clinical practice. The findings and proposed solutions serve as a call to action for healthcare institutions, policymakers, researchers and educators to prioritise secure communication practices, thus safeguarding patient rights and the integrity of the healthcare professions. Furthermore, the rapid advancement of Artificial Intelligence (AI) and generative AI introduces a new wave of data privacy and security concerns, highlighting the urgent need to address these emerging challenges alongside existing vulnerabilities. Table 14 outlines a series of recommended net steps arising from this research, offering practical guidance for future action and implementation. Figure 13 provides a visual overview of the thesis, illustrating the alignment between the research objectives, methodological approach, and key outputs generated across the course of the study.

In addition, Figure 14 presents the broad contextual backdrop for this research, highlighting significant legislative frameworks (for e.g. GDPR and HIPAA) as well as the global COVID-19 pandemic, which have collectively shaped the direction and relevance of this work. The timeline within figure 14 also incorporates the study timeline to situate the research chronologically within these developments.

Table 14 Next Steps

Next Steps
• **Actively Integrate Patient Involvement** Include patient voice in evolution and development of future iterations, ensuring the Toolkit evolves to reflect the rights and requirements of data subjects, ethical considerations and ensure appropriate clinical accountability. Further development of the Toolkit leveraging elaborated ADR in line with principles of co-production and person-centred care, engaging the range of multi-disciplinary clinicians drawn from a diverse array of clinical settings and patients.
• **Digitise the Toolkit** Transform the static, text version of the Toolkit into an interactive, user-friendly app capable of accommodating updates as the digital landscape evolves, integrating additional dynamic features and supporting clinicians in real-time.
• **Hosting by a Credible Authority** Seek endorsement, funding for ongoing and further development and hosting by a recognised authority to enhance legitimacy and adoption. Ideally the host would be a global body such as the World Health Organization (WHO), national health systems such as the HSE, NHS, health quality agencies in the UK or Ireland (such as HIQA) or the Welcome Trust in the UK could also play an important role. This could ensure that the Toolkit is viewed as a credible robust resource available across the range of clinical professions internationally.
• **Enable Regular Updates** Provide regular updates for the Toolkit in line with evolving regulatory frameworks and technological developments (depending on host, these could be offered specific to different global territories and legislation - for e.g. EU, UK and USA).
• **Adapt to Diversifying Technologies and Contexts** Customise the Toolkit to create additional iterations appropriate for the assessment of the full range of third-party apps in use by clinicians via their personal smart devices. This should include emerging AI technologies, in recognition of the increasing complexity of data confidentiality and privacy threats in a rapidly evolving global digital health landscape.
• **Support Digital Professionalism** Position the Toolkit within all recognised digital health governance frameworks internationally to reinforce its role in promoting ethical digital communication, data protection, and clinical accountability.

Figure 13: Objectives, Methods, Outputs from this Thesis

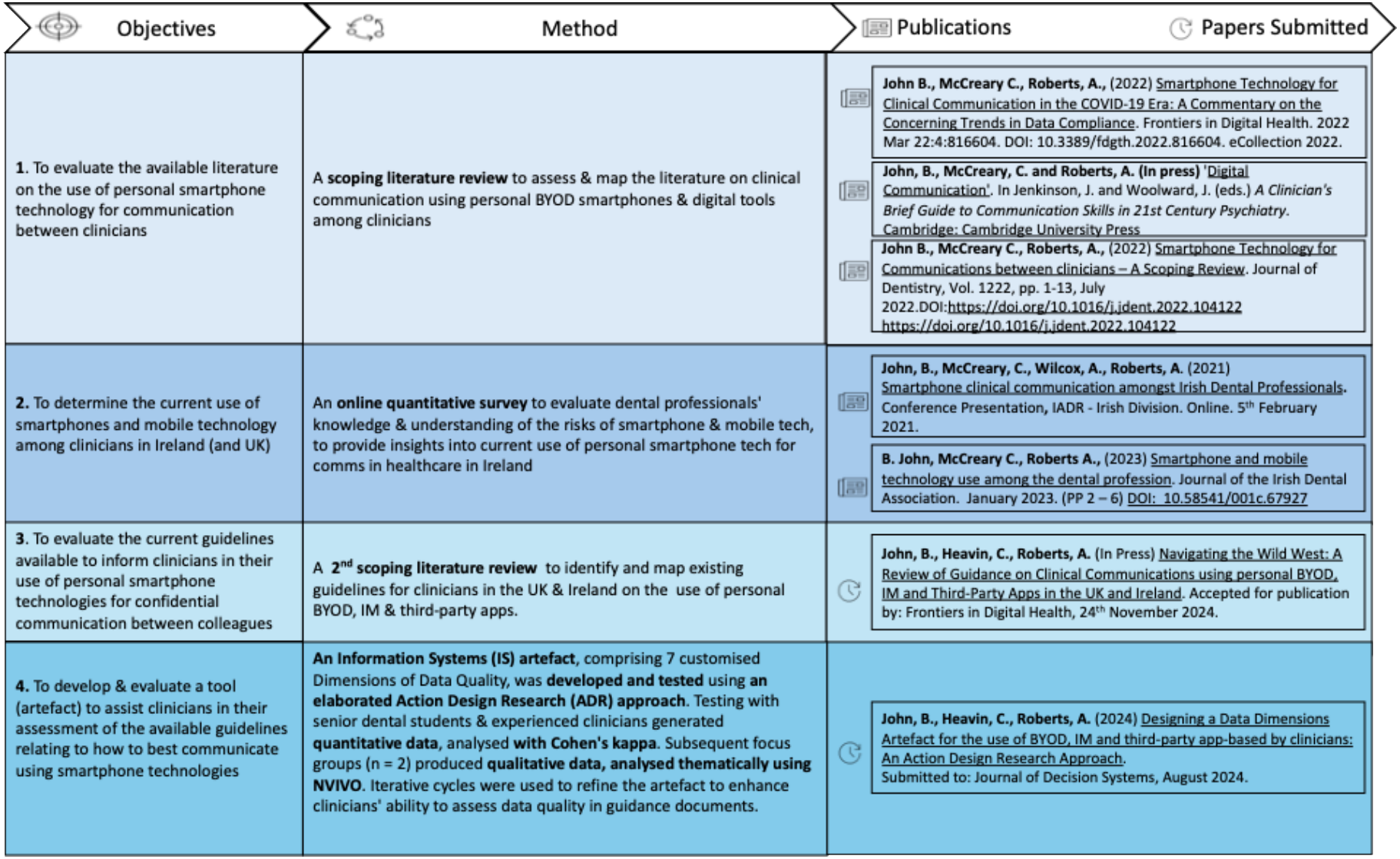
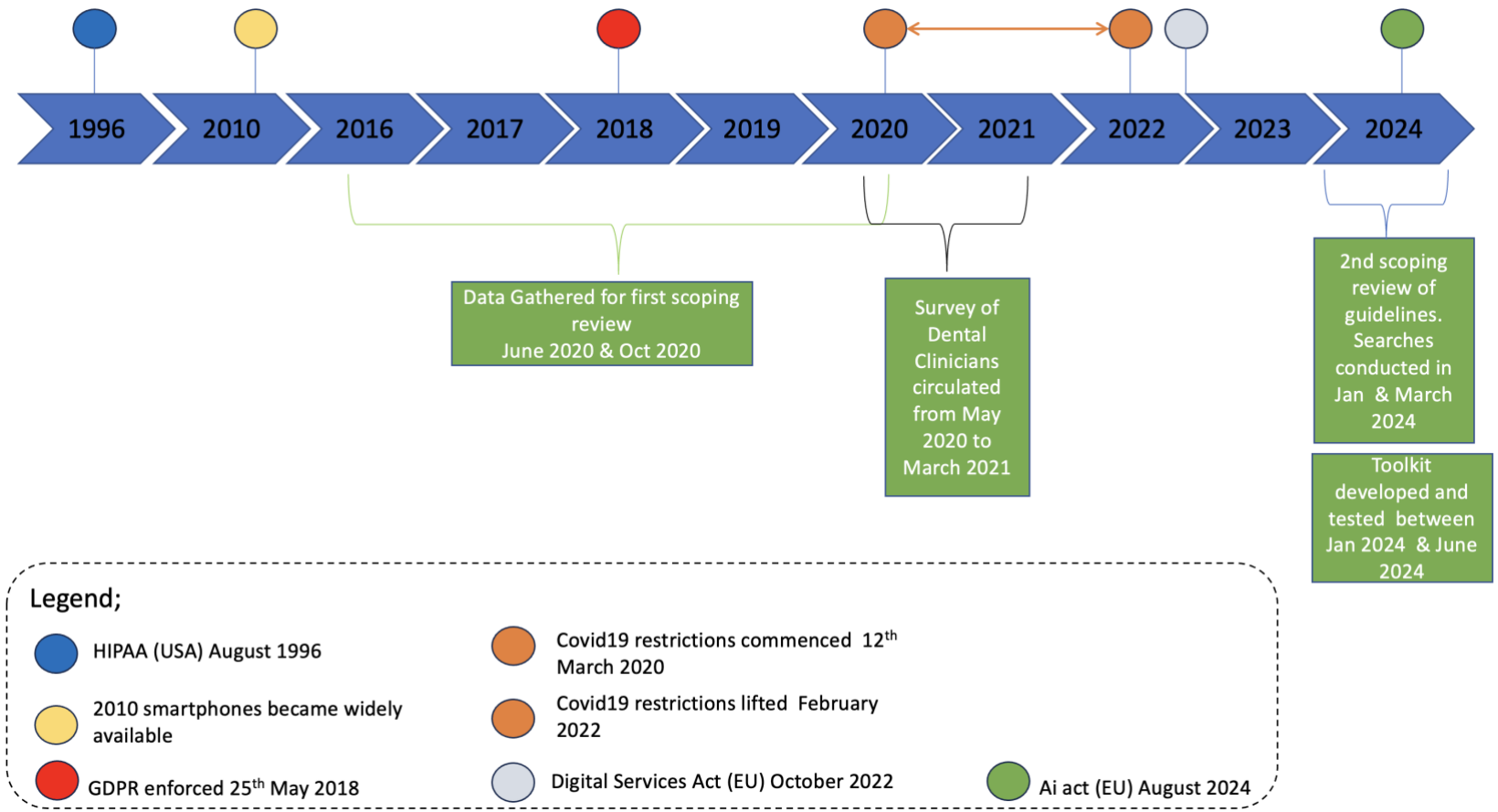


Figure 14: Key Legislation and PhD study Timeline



Legend: PhD study commenced April 2019; one year leave of absence from October 2022 for one year; thesis submitted November 2024.

CHAPTER 9 BIBLIOGRAPHY

1. John B, McCreary C and Roberts A. Smartphone Technology for Clinical Communication in the COVID-19 Era: A Commentary on the Concerning Trends in Data Compliance. *Frontiers In Digital Health* 2022; 4: 4. Opinion article. DOI: 10.3389/fdgth.2022.816604.

2. Barrios V, Cosín-Sales J, Bravo M, et al. Telemedicine consultation for the clinical cardiologists in the era of COVID-19: present and future. Consensus document of the Spanish Society of Cardiology. *Rev Esp Cardiol* 2020: 9. Study. DOI: doi.org/10.1016/j.rec.2020.06.032.

3. Rimmer A. Can I receive and store images sent from patients during remote consultations? *The BMJ* 2020; 370: 2. DOI: dx.doi.org/10.1136/bmj.m2675.

4. Mars M, Morris C and Scott R. WhatsApp guidelines – what guidelines? A literature review. *Journal of Telemedicine and Telecare* 2019; 25: 524-529. DOI: 10.1177/1357633X19873233.

5. Masoni M and Guelfi MR. WhatsApp and other messaging apps in medicine: opportunities and risks. *Internal and emergency Medicine* 2020; 15: 171-173. Review. DOI: https://doi.org/10.1007/s11739-020-02292-5.

6. NHSX. COVID-19 IG advice, https://www.nhsx.nhs.uk/information-governance/guidance/covid-19-ig-advice/ (2020, accessed 5th December, 2020 2020).

7. Stevenson A. *Oxford dictionary of English*. Oxford University Press, USA, 2010.

8. Gabbard GO. Digital Professionalism. *Acad Psychiatry* 2019; 43: 259-263. 2018/10/15. DOI: 10.1007/s40596-018-0994-3.

9. McLoughlin J, Zijlstra-Shaw S, Davies JR, et al. The graduating European dentist—Domain I: professionalism. *European Journal of Dental Education* 2017; 21: 11-13.

10. Mars M and Scott R. WhatsApp in Clinical Practice: A Literature Review. In: al. AJMe (ed) *The Promise of New Technologies in an Age of New Health Challenges*. IOS Press, 2016, pp.82-90.

11. Mistry K. *Information governance considerations for staff on the use of instant messaging software in acute clinical settings*. Official NHS England Policy. 09.11.18 2018. England: NHS England Publications Gateway.

12. Toussaint PJ and Coiera E. Supporting communication in health care. *International journal of medical informatics* 2005; 74: 779.

13. Martin G, Martin P, Hankin C, et al. Cybersecurity and healthcare: how safe are we? *British Medical Journal* 2017; 358. Review. DOI: 10.1136/bmj.j3179.

14. Ferreira A and Cruz-Correia R. COVID-19, Cybersecurity and the Human Right to Privacy. *JMIR Publications* 2020: 14. JMIR Preprints 04/06/2020:21069. DOI: https://doi.org/10.2196/preprints.21069.

15. PWC. *Conti cyber attack on the HSE, Independent Post Incident Review, Commissioned by the HSE Board in conjunction with the CEO and Executive Management Team*. 03 December, 2021 2021. Dublin, Republic of Ireland: The Board, HSE, Dr Steevens' Hospital, Dublin 8, Ireland.

16. Rabkin J. Revealed: Trump campaign strategy to deter millions of Black Americans from voting in 2016, https://www.channel4.com/news/revealed-trump-campaign-strategy-to-deter-millions-of-black-americans-from-voting-in-2016 (2020, accessed 28.12.20 2020).

17. Walsh P. Tweet. In: @PrivacyMatters, (ed.). *"IMHO the opaque nature of online (inc mobile App) tracking, inc the use of data held by mobile operators, is beyond the awareness and understanding of many individuals…"*. 13.27 PM ed. UK: X (formerly Twitter) 2020.

18. Bloomberg. WhatsApp, Snapchat Banned on Company Devices at Continental. *Windows IT Pro (Online) Chicago*. Informa, 2018.

19. EU Parliament. Regulation (EU) 2016/679 of the European Parliament and The Council of the European Union of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). In: EU TCot, (ed.). *L119/1*. Brussels: Official Journal of the European Union, for the European Parliament, The President M. Schulz, for the Council of the European Union, The President J.A. Hennis-Plasschaert, 2016, p. 88.

20. European Comission. Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection. Brussels: European Comission, 2020, p. 14.

21. Markopoulou V, Nieri A, Liaskos J, et al. Nursing Staff's Awareness of Processing Personal Data According to GDPR. In: al. JMe (ed) *The Importance of Health Informatics in Public Health during a Pandemic*. IOS Press, 2020, pp.237-240.

22. Dutch Supervisory Authority. Privacy Decision-making aid: Video Call Apps (Unofficial Translation of original work by The Dutch Supervisory Authority/Autoriteit Persoonsgegevens), https://www.clearycyberwatch.com/wp-content/uploads/sites/458/2020/04/Privacy-Decision-making-aid-Dutch-DPA-unofficial-transl..pdf (2020, 2020).

23. CDC (Centers for Disease Control and Prevention). Health Insurance Portability and Accountability Act of 1996 (HIPAA). USA: Centre for Disease Control (CDC.gov), 1996.

24. Rimmer A. Doctors' use of Facebook, Twitter, and WhatsApp is the focus of 28 GMC investigations. *The BMJ* 2017; 358. DOI: doi: https://doi.org/10.1136/bmj.j4099.

25. John B. Are you ready for General Data Protection Regulation? *The BMJ* 2018; 360: 2. DOI: 10.1136/bmj.k941.

26. Drake TM, Claireaux HA, Khatri C, et al. WhatsApp with patient data transmitted via instant messaging? *Am J Surg* 2016; 211: 300-301. 2015/05/28. DOI: 10.1016/j.amjsurg.2015.04.004.

27. John B, Heavin C and roberts A. Navigating the wild west: a review of guidance on clinical communications using personal BYOD, IM and third-party apps in the UK and Ireland. *Frontiers in Digital Health* 2025; 6: 13. Systematic Review 6th January, 2025. DOI: https://doi.org/10.3389/fdgth.2024.1457848.

28. Lee AS, Manoj T and Baskerville RL. Going back to basics in design science: from the information technology artifact to the information systms artifact. *Information Systems Journal* 2015; 25: 5-21. DOI: 10.1111/isj.12054.

29. Creswell JW and Creswell JD. *Research design: qualitative, quantitative, and mixed methods approaches*. Fifth ed. Thousand Oaks, California: SAGE Publications, 2018, p.275.

30. Mullarkey MT and Hevner AT. An elaborated action design research process model. *European Journal of Information Systems* 2018; 28: 6-20. 23rd April. DOI: DOI: 10.1080/0960085X.2018.1451811.

31. Peters MDJ, Godfrey CM, Khalil H, et al. Guidance for conducting systematic scoping reviews. *International Journal of Evidence-based healthcare* 2015; 12: 141-146. Methodology Paper.

32. Peters MDJ, Marnie C, Tricco AC, et al. Updated methodological guidance for the conduct of scoping reviews. *JBI Manual for Evidence Synthesis*. 2020 Version ed. Australia: Wolters Kluwer, 2020, pp.2119-2126.

33. Van Nederpelt P and Black A. *How to Select the Right Dimensions of Data Quality*. 5.11.2020 2020. The Netherlands: DAMA NL Foundation.

34. World Medical Association. Declaration of Helsinki - Ethical principles for medical research involving human subjects. Finland: The World Medical Association, Inc., 2008, p. 5.

35. John B, McCreary C and Roberts A. Smartphone Technology for Communications between Clinicians - A Scoping Review. *Journal of Dentistry* 2022; 122: 1-13. Scoping Review 10th April,. DOI: https://doi.org/10.1016/j.jdent.2022.104112.

36. Chan WSY and Leung AYM. Use of Social Network Sites for Communication Among Health Professionals: Systematic Review. *Journal of Medical Internet Research* 2018; 20: 12. Review. DOI: 10.2196/jmir.8382.

37. Crouch H. Information Governance Alliance drafts guidelines for instant messaging use, https://www.digitalhealth.net/2018/03/information-governance-alliance-guidelines-instant- messaging-use/ (2018, 2020).

38. De Benedictis A, Lettieri E, Masella C, et al. WhatsApp in hospital? An empirical investigation of individual and organizational determinants to use. *PLoS One* 2019; 14: 13. DOI: 10.1371/journal.pone.0209873.

39. El Hadidy TS, Alshafei AE, Mortell AE, et al. Smartphones in clinical practice: doctors' experience at two Dublin paediatric teaching hospitals. *Ir J Med Sci* 2017; 187: 9.

40. Ezra O, Toren A, Tadmor O, et al. Secure Instant Messaging Application in Prenatal Care. *Journal of Medical Systems* 2020; 44: 72-75. DOI: https://doi.org/10.1007/s10916-020-01552-3.

41. Fattore D, Delfino M and Fabbrocini G. Legal, medical, and ethical implications of instant messaging application use in dermatology. *International Journal of Dermatology* 2019; 58: 185-207. Letter to the Editor. DOI: 10.1111/ijd.14519.

42. Finn D and Dion KW. Security tips for using personal technology at your employer's site. *Reflections on Nursing Leadership* 2018; 43: 8. Security tips for nurses.

43. Hawkes N. Sixty seconds on . . . WhatsApp. *The BMJ* 2018; 360: 1. News. DOI: doi: 10.1136/bmj.k1041.

44. Jahn HK, Jahn IH, Roland D, et al. Mobile device and app use in paediatric emergency care: a survey of departmental practice in the UK and Ireland. *Archives of Disease in Childhood, 12/2019* 2019; 104: 1203-1207. 03.07.19. DOI: 10.1136/archdischild-2019-316872.

45. John B. Phones in Dentistry. *Bitesize - official newsletter of the Dental Council of Ireland*, July 2020 2020.

46. Kamel-Boulos MN, Guistini, D.M., Wheeler, S. Instagram and WhatsApp in Health and Healthcare: An Overview. *Future Internet* 2016; 8: 14. Review. DOI: 10.3390/fi8030037.

47. Mars M, Morris C and Scott R. Selfie Telemedicine - What are the Legal and Regulatory Issues? In: Ginige J.A. M, A.J. (ed) *Transforming Healthcare Through Innovation in Digital Health*. Amsterdam: IOS Press, 2018, pp.53-62.

48. Nikolic A, Wickramasinghe N, Claydon-Platt D, et al. The Use of Communication Apps by Medical Staff in the Australian Health Care System: Survey Study on Prevalence and Use. *JMIR MEDICAL INFORMATICS* 2018; 6: 7. DOI: 10.2196/medinform.9526.

49. Raths D. Messaging often fails HIPAA requirements. *Behavioral Healthcare Executive* 2017: 2. Technology.

50. R.C.N. Survey suggests widespread use of instant messaging apps to discuss patient care. *Nursing Standard* 2018; 32: 1. Misconduct.

51. Spencer A and Patel S. Applying the Data Protection Act 2018 and General Data Protection Regulation principles in healthcare settings. *Nursing Management* 2019; 26: 34-40. Evidence & practice/CPD/professional issues, peer reviewed.

52. Watson L, Pathiraja F, Depala A, et al. Ensuring safe communication in health care: A response to Johnston et al on their paper ‘‘Smartphones let surgeons know WhatsApp: an analysis of communication in emergency surgical teams’’. *The American Journal of Surgery* 2016; 211: 2. Letter to the Editor.

53. Mehraeen E, Ghazisaeedi, M., Farzi, J. Security challenges in healthcare cloud computing: a systematic review. *Global Journal of Health Science* 2016; 9: 12. Systematic Review. DOI: 10.5539/gjhs.v9n3p157.

54. European Society of Radiologists. The new EU General Data Protection Regulation: what the radiologist should know. *Insights Imaging* 2017; 8: 5. Statement 24th April, 2017.

55. Iyengar K, Upadhyaya GK, Vaishya R, et al. COVID-19 and applications of smartphone technology in the current pandemic. *Diabetes India - Diabetes & Metabolic Syndrome: Clinical Research & Reviews* 2020; 14: 733-737.

56. Wielawski IM. Are Patient Privacy and Health Data at Risk? *AJN* 2020; 120: 2.

57. Council of Europe. European Convention on Human Rights - Right to respect for private and family life. In: European Court of Human Rights, (ed.). *Article 8*. Strasbourg: European Court of Human Rights, 1994, p. 1-34.

58. Martinengo L, Spinazze P and Car J. Mobile messaging with patients. *British Medical Journal* 2020; 368: 884. 16th march 2020. DOI: 0/-0025.ali-l773

59. Chen B. Zoom is Easy to Use, and Easy to Bomb. *New York Times*, 9th April, 2020 2020.

60. Mehta I. Don’t believe Zoom: Its video calls are not encrypted end-to-end. *TheNextWebcom (Blog)*. 2020.

61. Marketwired. Zoom Launches Industry's First Scalable Cloud-Based Video Telehealth Solution. *Marketwired*, 20th April, 2017 2017.

62. Gould G and Nilforooshan R. WhatsApp Doc? *British Medical Journal* 2016; 2: 109-110. Commentary. DOI: doi:10.1136/bmjinnov-2016-000116.

63. Ellanti P, Moriarty A, Coughlan F, et al. The Use of WhatsApp Smartphone Messaging Improves Communication Efficiency within an Orthopaedic Surgery Team. *Cureus* 2017; 9. Study. DOI: 10.7759/cureus.1040.

64. Giordano V, Koch H, Godoy-Santos A, et al. WhatsApp Messenger as an Adjunctive Tool for Telemedicine: An Overview. *Interactive journal of medical research* 2017; 6. Literature review.

65. Gulacti U, Lok U, Hatipoglu S, et al. An Analysis of WhatsApp Usage for Communication Between Consulting and Emergency Physicians. *Journal of Medical Systems* 2016; 40. Article. DOI: 10.1007/s10916-016-0483-8.

66. Blasi L, Bordonaro, R., Borsellino, N., Butera, A., Caruso, M., Cordio, S., Di Cristina, l., Ferraù, F., Giuffrida, D., Soto Parra, H., Spada, M., Tralongo, P., Valenza, R., Verderame, F., Vitello, S., Zerilli, F., Dario, P. ; Firenze, A., Gebbia, V. Reactions and countermeasures of medical oncologists towards the incoming COVID-19 pandemic: a WhatsApp messenger-based report from the Italian College of Chief Medical Oncologists. *Ecancermedicalscience,* 2020; 14: 12. DOI: https://doi.org/10.3332/ecancer.2020.1046.

67. European Society of Radiologists. ESR paper on the proper use of mobile devices in radiology. *Insights into Imaging* 2018; 9: 247-251. Statement 22nd March, 2018.

68. Ranschaert ER, Van Ooijen, P.M.A., McGinty, G.B., Parizel, P.M. Radiologists' Usage of Social Media: Results of the RANSOM Survey. *Journal of Digital Imaging* 2016; 29: 443-449. DOI: DOI 10.1007/s10278-016-9865-1.

69. Siegmund LA. Social Media in Occupational Health Nursing, helpful or harmful? *Workplace Health & Safety* 2020; 68: 408-414. Research Article.

70. Kaur J, Suri, V. . Whatsapp in obstetrics and gynaecology: necessary evil or blessing in disguise? *Journal of Obstetrics and Gynaecology* 2020. DOI: https://doi.org/10.1080/01443615.2019.1710481.

71. Sultan M, Brown, E.M., Thomas, R.H. Clinicians embracing social media: Potential and pitfalls. *Epilepsy & Behavior, Science Direct* 2019: 7.

72. Bennani A, Sekal, M. Usefulness of WhatsApp for Discussing Difficult Cases in Pathology Practice: A Moroccan Experience. *Turkish Journal of Pathology* 2019; 35: 134-138. DOI: 10.5146/tjpath.2018.01441.

73. Mulrennan S. Medical information and social media in the time of COVID-19. *Respirology* 2020; 25: 578-579. Commentary.

74. Downey A. Clinicians told they can use WhatsApp to share data in face of Covid-19, https://www.digitalhealth.net/2020/03/clinicians-told-they-can-us.. (2020, accessed November 2020 2020).

75. NHS. Instant messaging services a 'vital part of the NHS toolkit' during a crisis, https://www.england.nhs.uk/2018/11/instant-messaging-services-a... (2018, accessed July 2020).

76. H.S.E. National Financial Regulation, Mobile Phone Devices. In: Executive HS, (ed.). *NFR-27*. NFR27 ed. 2017.

77. HSE. *Electronic Communications Policy*. Policy. July 2019 2019. Dublin, Ireland: Health Service Executive.

78. HSE Information Technology (I.T.) Security Policy.

79. H.S.E. Mobile Phone Device Policy. In: Executive HS, (ed.). *2*. Dublin, Ireland2010.

80. Stanton L. WhatsApp Seeks to Comply with Europe's Privacy Rules. *Cybersecurity Policy Report; New York* 2018: 2.

81. Favaretto M, Shaw, D., De Clercq, D., Joda, T., Elger, B.E.,. Big Data and Digitalization in Dentistry: A Systematic Review of the Ethical Issues. *International Journal of Environmental Research and Public Health* 2020; 17. DOI: 10.3390/ijerph17072495.

82. Ramji A, Tamer, D., Cota, C.B., Monteiro, R.L., Lima, C.C.C., Prestia, J., Subbotina, K. Managing Big Data Privacy and Security. *International Law News* 2017; 46: 1-21. Article.

83. Abukar S. Getting Personal, The professional, legal and ethical aspects of confidentiality. *Imagine & Therapy* 2017; 16: 26-28. Confidentiality.

84. Williams CM, Chaturvedi, B.S.R., Chakravarthy, B.S.K. Cybersecurity Risks in a Pandemic. *Journal of Medical Internet Research* 2020; 22: 4. DOI: 10.2196/23692.

85. Bittner JG, Heather J., Logghe, H.J., Kane, E.D., Goldberg, R.F., Alseidi, A., Aggarwal, R., Jacob, B.J. A Society of Gastrointestinal and Endoscopic Surgeons (SAGES) statement on closed social media (Facebook®) groups for clinical education and consultation: issues of informed consent, patient privacy, and surgeon protection. *Society of American Gastrointestinal and Endoscopic Surgeons* 2019; 33: 7.

86. Haug CJ. Turning the Tables — The New European General Data Protection Regulation. *New England Journal of medicine* 2018: 3. DOI: 10.1056/NEJMp1806637.

87. Persia S. DATA SECURITY AND YOUR DENTAL PRACTICE. *Oral health* 2020; 110.

88. Lopes IM, Guarda, T., Oliveira, P. General Data Protection Regulation in Health Clinics. *Journal of Medical Systems* 2020: 44-53. DOI: https://doi.org/10.1007/s10916-020-1521-0.

89. I.G.A. Using Video Conferencing for Service User Consultations. *NHS Website* 2016.

90. H.S.E. planning to introduce new Instant Messaging Service. *Medical Independent*, April 3, 2018 2018.

91. Goodin D. Study shows which messengers leak your data, drain your battery, and more, https://arstechnica.com/information-technology/2020/10/study-shows-which-messengers-leak-your-data-drain-your-battery-and-more/ (2020, accessed 28/10/20 2020).

92. Australian Medial Association and Medical Indemnity Industry Association of Australia. Clinical images and the use of personal mobile devices: A guide for medical students and doctors. Australia 2014.

93. Natarajan S, Nair, A.G. Outsmarted by the smartphone! *Indian Journal of Opthalmology* 2015; 63: 757-758. DOI: 10.4103/0301-4738.171502.

94. HSE. Social Media & Digital Policy - Staff Use Guidelines. Dublin, Ireland: H.S.E. communications, 2017, p. 1-6.

95. O'Brien D. What's Up WhatsApp? *Castlebridge Blog*. Dublin: Castlebridge.ie, 2021.

96. John B, McCreary C and Roberts A. Smartphone and mobile technology use among the dental profession. *Journal of the Irish Dental Association* 2023: 2-5. DOI: 10.58541/001c.67927.

97. John B, McCreary C, Wilcox A, et al. Smartphone Clinical Communication Amongst Irish Dental Professionals. In: *Irish Division IADR* (ed IADR), Online, 5th February, 2021 2021, p.16. Dublin.

98. O'Connor P, Byrne D, Butt M, et al. Interns and their smartphones: use for clinical practice. *Postgrad Med J* 2014; 90: 75-79. 2013/11/15. DOI: 10.1136/postgradmedj-2013-131930.

99. Mobasheri MH, King D, Johnston M, et al. The ownership and clinical use of smartphones by doctors and nurses in the UK: a multicentre survey study. *BMJ Innovations* 2015; 1: 174-181.

100. Johnstone P. The device in your pocket. *RiskWise, Risk management from Dental Protection* 2018: 6-7. Feature.

101. Davies A, Hassey A, Williams J, et al. Creation of a core competency framework for clinical informatics: From genesis to maintaining relevance. *International Journal of Medical Informatics* 2022; 168: 5. 30th October, 2022. DOI: https://doi.org/10.1016/j.ijmedinf.2022.104905.

102. Bain B. Big Banks to pay millions in fines for using WhatsApp. *The Irish Times*, Tuesday 8th August, 14.08, 2023. 2023.

103. ICO. ICO reprimands NHS Lanarkshire for sharing patient data via WhatsApp, https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/08/ico-reprimands-nhs-lanarkshire-for-sharing-patient-data-via-whatsapp/ (2023, accessed 20th March 2024).

104. HSE. *HSE Social Media Staff Use Guidelines*. Guidelines. October 2023. Republic of Ireland: HSE.ie.

105. GMC. *Good Medical Practice*. Guidance Document. 30th January 2024. London: GMC, UK.

106. MC. *Guide to Professional Conduct & Ethics for Registered Medical Practitioners*. Guideline. January 2024. Dublin, Ireland: Medical Council of Ireland.

107. HCPC. *Guidance on the use of social media*. Guidance document. 24th March 2020. London, UK: Health and Care Professions Council.

108. Braun V and Clarke V. Using thematic analysis in psychology. *Qualitative Research in Psychology* 2006; 3: 77-102. DOI: http://dx.doi.org/10.1191/1478088706qp063oa.

109. DDU. *Protecting patient data*. Guidance. 27th January 2023. London, UK: Dental Defence Union.

110. GDC. *Standards for the Dental Team*. 2013. London, England: General Dental Council.

111. The Scottish Government (TSG). *Information governance considerations for staff on the use of instant messaging software in the NHS Scotland.* Blog Post. 16th March 2020. Scotland, UK.: The Scottish Government.

112. UHL. *Mobile Device Management Policy*. Policy. 20th November 2020. Leicester, England.: UHL, Leicester, England.

113. GOSH. *Acceptable Use of ICT Policy*. Policy. 2023. London, England.: Great Ormond St Hospital NHS Trust.

114. The Beacon Hospital. *Mobile Communication Policy*. Policy. 24th January 2022. Dublin, Ireland: The Beacon Hospital.

115. HSE. *Data Protection Policy*. 2019. Republic of Ireland: Health Service Executive.

116. INMO. *Guidance on the use of Instant Messaging in the workplace*. May 2019. Dublin, Ireland: Irish Nurses and Midwives Organisation.

117. NHS. *Use and share information with confidence*. 2nd February 2022. UK: NHS Transformation Directorate.

118. NHS. *Using Mobile Messaging*. 20th December 2022. UK: NHS Transformation Directorate.

119. NHS. *Bring your own device (BYOD) guidance*. 9th August 2023. UK: NHS England Transformation Directorate.

120. QVH. *Social Media and Online Content Policy and Guidance for Staff*. Guidance for staff. 25th April 2022. England, UK: Queen Victoria Hospital NHS Foundation Trust.

121. UHD. *Social Media Policy*. Policy document. October 2020. Dorset, UK.: University Hospitals Dorset, NHS Foundation Trust.

122. UHL. *Health Records Management*. Policy. 28th April 2023. Leicestershire, England: University Hospital Leicester NHS Trust.

123. ICGP. *IT Security for Irish General Practice*. Advice document. January 2020. Dublin, Republic of Ireland.: Irish College of General Practitioners.

124. MDU. *Social media in the Republic of Ireland: top tips for doctors*. 1st August 2023. Republic of Ireland: TheMDU.com.

125. MDU. *Using Social Media*. Guidance. 30th January 2024. London, England, UK.: Medical Defence Union.

126. Medical Protection (MP). *Ask the expert - social media*. Advice/guideline article. 10th June 2020. London, England: MedicalProtection.org.

127. Voigt P, & Von dem Bussche, A. *The EU General Data Protection Regulation (GDPR)*. Cham, Switzerland: Springer, 2017.

128. Data Protection Comission (DPC). *Data Protection Impact Assessments*. 2018. Dublin, Ireland: Data Protection Comission.

129. Morris C, Scott, R. E., Mars, M. WhatsApp in Clinical Practice—The Challenges of Record Keeping and Storage. A Scoping Review. *International Journal of Environmental Research and Public Health* 2021; 18: 18. DOI: doi.org/10.3390/ijerph182413426.

130. NCSC. *Multi-factor authentication for online services*. 3rd December 2018. London, England: National Cyber Security Centre.

131. NCSC. *Using secure messaging, voice and collaboration apps*. Blog Post. 2021. London, UK: National Cyber Security Centre.

132. NCSC. *Bring Your Own Device Security Code - Guidance for organisations on how to chosse, configure and use devices securely*. 13th December 2021. London, UK: National Cyber Security Centre.

133. NCSC. *Secure communications principles*. October 2021. London, UK: National Cyber Security Centre.

134. NCSC. *Device Security Guidance*. 29th June 2021. London, UK: National Cyber Security Centre.

135. Monkman H, Mir, S., Borycki, E.M., Courtney, K.L., Bond J., Kushniruk, A.W. Updating professional competencies in health informatics: A scoping review and consultation with subject matter experts. *International Journal of Medical Informatics* 2023; 170: 9. 20th December, 2022. DOI: doi.org/10.1016/j.ijmedin.2022.104969.

136. Heavin C and Power DJ. Challenges for digital transformation – towards a conceptual decision support guide for managers. *Journal of Decision Systems* 2018; 27: 38-45. 08.05.2018. DOI: https://doi.org/10.1080/12460125.2018.1468697.

137. Angst CM, Block ES, D'Arcy J, et al. When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches. *MIS Quarterly* 2017; 41: 60.

138. Paul M, Maglaras L, Ferrag MA, et al. Digitization of healthcare sector: A study on privacy and security concerns. *ICT Express* 2023; 9: 571-588. 21st February, 2023. DOI: doi.org/10.1016/j.icte.2023.02.007.

139. Verizon. *Verizon 2018 Data Breach Investigations Report*. Report. 2018.

140. Wani TA, Mendoza A and Gray K. BYOD in Hospitals, Security Issues and Mitigation Strategies. In: *Australasian Computer Science Week Multiconference* January 2019, p.21. Melbourne Australia.

141. Wani TA, Mendoza A and Gray K. Hospital Bring-Your-Own-Device Security Challenges and Solutions: Systematic Review of Gray Literature. *Jmir Mhealth and Uhealth* 2020; 8: 14. Review February, 2020. DOI: 10.2196/18175.

142. Wani TA, Mendoza A and Gray K. BYOD security behaviour and preferences among hospital clinicians – A qualitative study. *International Journal of Medical Informatics* 2024; 192: 15. 30th August, 2024. DOI: https://doi.org/10.1016/j.ijmedinf.2024.105606.

143. Sakpal M. *How to Improve Your Data Quality*. 2021. Gartner.

144. Black A and Van Nederpelt P. How to select the right dimensions of Data Quality.

145. Weiskopf NG and Weng C. Methods and dimensions of electronic health record data quality assessment: enabling reuse for clinical research. *J Am Med Inform Assoc* 2013; 20: 144-151. Review 25 June, 2012. DOI: 10.1136/amiajnl-2011-000681.

146. Pool J, Akhlaghpour S and Fatehi F. Health Data Privacy in the COVID-19 Pandemic Context: Discourses on HIPAA. *Navigating Healthcare Through Challenging Times*. IOSPress.nl, 2021, p. 70-77.

147. Ibrahim AM, Abdel-Aziz HR, Mohamed HAH, et al. Balancing confidentiality and care coordination: challenges in patient safety. *BMC Nursing* 2024; 23: 14. DOI: 10.1186/s12912-024-02231-1.

148. DAMA. Dimensions of Data Quality, https://dama-nl.org/dimensions-of-data-quality-en/ (2023, accessed 16th March, 2024 2024).

149. Ballou DP, Pazer, H.L. Modeling Data and Process Quality in Multi-input, Multi-output Information Systems. *Management Science* 1985; 31: 150-162.

150. Nerminathan A, Harrison A, Phelps M, et al. Doctors' use of mobile devices in the clinical setting: a mixed methods study. *Internal Medicine Journal* 2016; 47: 291-298. DOI: doi:10.1111/imj.13349.

151. Lovell T. WhatsApp use in the NHS a 'privacy and clinical safety timebomb'. *EMEA*, April 03, 2019 2019.

152. Heselmans A, Van de Velde. S., Donceel P, et al. Effectiveness of electronic guideline-based implementation systems in ambulatory care settings - a systematic review. *Implementation Science* 2009; 4: 12. Systematic Review 30th December, 2009. DOI: 10.1186/1748-5908-4-82.

153. Carayon P, Wetterneck TB, Rivera-Rodriguez AJ, et al. Human factors systems approach to healthcare quality and patient safety. *Applied Ergonomics* 2013; 45: 14-25. DOI: dx.doi.org/10.1016/j.apergo.2013.04.023.

154. Van de Ven AH. Chapter 4. Building a Theory. *Engaged Scholarship: A Guide for Organizational and Social Research*. Oxford University Press, 2007, pp.43.

155. Sein MK, Henfridsson O, Purao S, et al. Action Design Research. *Management Information Systems Quarterly* 2011; 35: 37-56.

156. Susman G, & Evered, R. An Assessment of the Scientific Merits of Action Research. *Administrative Science Quarterly* 1978; 23: 582-603.

157. Hevner AR, March ST, Park J, et al. Design science in information systems research. *MIS Quarterly* 2004; 28: 75-115. Research Essay.

158. Susman G. Action Research: A Sociotechnical Perspective. In: Morgan G (ed) *Beyond Method: Strategies for Social Research*. Newbury Park, CA, USA.: Sage Publications, 1983, pp.95-113.

159. Sein MK and Rossi M. Elaborating ADR while drifting away from its essence: A commentary on Mullarkey and Hevner. *European Journal on Information Systems* 2018; 28: 21-25. Research Article 01.18.18. DOI: 10.1080/0960085X.2018.1527189.

160. Boeckl K, Grayson, N., Howell, G., Lefkovitz N., Ajmo, J., Craft, R.E., McGinnis, M., Sandlin K., Slivina, O., Snyder, J., Ward, P. *Mobile Device Security Bring Your Own Device (BYOD)*. September, 2023 2023. USA: National Cyber Security Centre.

161. ICO. Bring your own device (BYOD). 14.

162. Foote KD. Data Quality Dimensions. Epub ahead of print 15th February, 2022.

163. DAMA. Dimensions of Data Quality, Working Group Data Quality. Epub ahead of print 01.01.23.

164. Bragg R. *CISSP Training Guide*. 1st. ed. UK: Pearson IT Certification, 2002.

165. Landis TR and Koch GG. The Measurement of Observer Agreement for Categorical Data. *Biometrics* 1977; 33: 159-174.

166. The Data Protection Comission (DPC). The Data Protection Commission, https://www.dataprotection.ie/en (2018, accessed 18th August 2024).

167. Luaner J. Unconscious incompetence. *Postgrad Med J* 2010; 86: 1. Reflection. DOI: 10.1136/pgmj.2010.108423.

168. Russo JE and Shoemaker PJH. Managing Overconfidence. *Sloan Management Review* 1992: 7 - 17.

169. See KE, Morrison EW, Rothman NB, et al. The detrimental effects of power on confidence, advice taking, and accuracy. *Organisational Behavior and Human Decision Processes* 2011; 116: 272-285. 25th August, 2011. DOI: 10.1016/j.obhdp.2011.07.006.

170. Sattler DN, McKnight PE, Naney L, et al. Grant Peer Review: Improving Inter-Rater Reliability with Training. *PLoS One* 2015: 9. Research article.

171. Orlikowski WJ and Lacono CS. Research Commentary: Desperately Seeking the 'IT' in IT Research—A Call to Theorizing the IT Artifact. *Information Systems Research* 2001; 12: 121-134.

172. Twomey MB, Sammon D and Nagle T. The Tango of Problem Formulation: A Patient's/Researcher's Reflection on an Action Design Research Journey. *Journal of Medical Internet Research* 2020; 22: 23. Viewpoint. DOI: http://dx.doi.org/10.2196/16916.

173. Morris C, Scott RE and Mars M. Towards 'Formalising' WhatsApp Teledermatology Practice in KZ-N District Hospitals: Key Informant Interviews. *Int J Environ Res Public Health* 2024; 21: 17. DOI: https://doi.org/10.3390/ijerph21101388.

174. Dentistry.co.uk. 2024 Dentistry Census: key findings, https://dentistry.co.uk/2024/02/08/2024-dentistry-census-key-findings/ (2024, accessed 8th February 2024).

175. John B, McCreary C and Roberts A. Digital Communication. In: Jenkinson J and Woolward J (eds) *A Clinician's Brief Guide to Communication Skills in 21st Century Psychiatry*. UK: Cambridge University Press, In Press.

176. Data Protection Comission (DPC.ie). Special Category Data, https://www.dataprotection.ie/en/organisations/know-your-obligations/lawful-processing/special-category-data (2018, accessed 20th November, 2024 2024).

177. John B, Heavin C and Roberts A. Navigating The Wild West: A Review of Guidance on Clinical Communications using Personal BYOD, IM and Third-Party Apps in The UK and Ireland. *Frontiers In Digital Health* In Press. Scoping Review.

178. Sky News. NHS software provider faces £6m fine after hackers steal tens of thousands of medical records, https://news.sky.com/story/nhs-software-provider-faces-6m-fine-after-hackers-steal-tens-of-thousands-of-medical-records-13192012 (2024, accessed 7th August 2024).

179. Roussi A. Hacked info from Italy security databases sold to rich clients, prosecutors say, https://www.politico.eu/article/private-investigators-hack-state-security-data-milan-italy/ (2024, 2024).

180. O'Kelly E. SETU Waterford campuses hit by cyberattack, Monday classes cancelled, https://www.rte.ie/news/education/2024/1101/1478655-waterford-hack/ (2024, accessed 1st november, 2024 2024).

181. Alter S. Theory of Workarounds. *Communication of the Association for Information Systems* 2014; 34: 1041-1066. March, 2014.

CHAPTER 10 APPENDICES

APPENDIX 1 PAPER 1

frontiers in Digital Health

OPINION
published: 22 March 2022
doi: 10.3389/fdgth.2022.816804

Smartphone Technology for Clinical Communication in the COVID-19 Era: A Commentary on the Concerning Trends in Data Compliance

Bernadette John, Christine McCreary and Anthony Roberts*

Cork University Dental School and Hospital, University College Cork, Cork, Ireland

Keywords: smartphone technology, clinical communication, information governance, data compliance, COVID-19, WhatsApp, education

OPEN ACCESS

Edited by:
Elizabeth Mary Morrow, Research Support NI, Ireland

Reviewed by:
Mark White, Waterford Institute of Technology, Ireland
Jennifer Heath, Bombo Research & Consulting, Australia

****Correspondence:***
Bernadette John
118225957@umail.ucc.ie

Specialty section:
This article was submitted to Health Technology Innovation, a section of the journal Frontiers in Digital Health

Received: *16 November 2021*
Accepted: *24 February 2022*
Published: *22 March 2022*

Citation:
John B, McCreary C and Roberts A (2022) Smartphone Technology for Clinical Communication in the COVID-19 Era: A Commentary on the Concerning Trends in Data Compliance. Front. Digit. Health 4:816804. doi: 10.3389/fdgth.2022.816804

INTRODUCTION

The COVID-19 global pandemic has rightly been the focus of attention for the healthcare workforce and has accelerated the global proliferation and adoption of smartphone and digital technologies for clinical communication and remote consultation (1, 2). This is an understandable development as functionality that enables dialogue between clinicians *via* Instant Messaging (IM) Applications or Apps (e.g., such as WhatsApp and iMessage), and between clinicians and patients through videoconferencing Apps (e.g., such as Zoom and Skype), has never been more important. Clinicians have drawn on the familiar and simple smartphone technology to overcome the communication barriers required for social distancing, reducing the risks associated with face-to-face contact and optimizing efficiencies in healthcare (1), often without adequate training as to potential clinical safety risks or data security incidents. These interventions have often had efficiency of communication at their core but may leave legacy issues that will become apparent as the health emergency passes. These channels have permanently and positively transformed communications, although they also raise professional, ethical, security and legal concerns that are associated with these technologies (3, 4). Clinicians (and their patients) may be in danger of becoming *"ensnared"* in a web of hidden data harvesting. Busy clinicians using smartphones to communicate effectively within their own healthcare teams or directly with patients, could face negative ramifications of these technologies unless the Information Commissioners Office (ICO; UK) or Data Protection Commission (DPC; Ireland) actively regulate to ensure data compliance within the National Health Service (NHS) or Health Service Executive (HSE; Ireland). This article explores the contemporary clinical context and regulatory ramifications within which practicing clinicians are operating. It highlights the need for appropriate guidelines, tools, and education in digital health to enable clinicians to practice in an environment where sensitive patient data can be processed and communicated securely with clarity for patients as to how their data might be used.

CLINICAL COMMUNICATIONS, SMARTPHONE TECHNOLOGY AND APPS

Effective communication is an essential element of good clinical care. However, the traditional methods of communications (e.g., landline telephones, pagers and fax machines) are restrictive. Smartphone technology and communications Apps (including IM) have become ubiquitous in society facilitating cost effective and efficient communication on a "one-to-one" or "one-to-many" basis. For clinicians, the functionality facilitates

conversations and consultations between colleagues and enables the sharing of (potentially sensitive) supplementary voice recordings, images and video at the *"touch of a button"* with WhatsApp being the most cited IM application in healthcare (3).

Presumably as a consequence of the magnitude of the COVID-19 pandemic combined with inadequate investment in communications infrastructure, clinicians have been encouraged to draw on their smartphones or Bring Your Own Devices (BYODs) and Apps (5) (e.g., Skype, iMessage, Zoom) for telemedicine activities. Such functionality has positively enabled online/remote consultations, reviews and test result discussions, patient monitoring and clinical photography, including the use of diagnosis Apps from smartphone images. The patient journey and the working life of clinicians have improved whilst pragmatically bypassing the need for time-consuming additional training or purchase of costly new technology at a time of crisis. Regrettably, the perceived advantage of familiarity of these technologies, contrasts with usage of BYODs potentially introducing data security risks for clinicians which they may not be aware of due to a lack of education and training. Of course, not all patients have an awareness of such technologies, or own a compatible device generating inequality in availability to digital services.

DIGITAL PROFESSIONALISM

Digital Professionalism may be defined as *"the competence or values expected of a professional when engaged in social, digital communication and mobile technology"* [amended from Oxford English dictionary definition of professionalism (6)].

There are clear challenges for how health professionals conduct themselves in a rapidly evolving digital landscape. It has been suggested that Digital Professionalism education and learning should begin in undergraduate training, "given its relevance at all levels" (7).

This issue has recently been acknowledged in the latest Curriculum for Graduating European Dentists (8) which has an Intended Learning Outcome:

"graduating dentists must demonstrate digital professionalism by protecting patient data and the appropriate use of social media and digital communication, mindful of how these activities may force them into ethically challenging situations and/or damage the reputation of the wider profession."

This healthcare exemplar challenges education providers to best equip its graduates for the challenges of modern digital society. Our anecdotal experience indicates that clinicians have a broad range of attitude and behavior with risky behavior by busy clinicians on the frontline being a concern.

RECORD KEEPING AND CLINICAL IMAGES

Record keeping of clinical images and "chat messages" stored on BYOD smartphones shared *via* IM and Apps pose a range of serious safety concerns (9). The clinician initiating a dialogue has responsibilities to ensure that any messages/data and responses are recorded in the patient's notes; IM conversations may be subject to Freedom of Information requests or Subject Access Requests (10). However, downloading of the dialogue and any clinical images to store it in the patient notes or digital healthcare record may not be technically possible and even if so, are these data being promptly deleted from the smartphones by all members of the App group? Clinicians may not be aware that smartphones store deleted images in the *"deleted images"* album for 28 days (2). Further, smartphones must be password protected with image streaming to insecure cloud servers and between networked devices turned "OFF" (2, 10). The storage of clinical images using insecure cloud servers associated with a BYOD is concerning (3, 10). Digital images contain additional Exchangeable Image File Format (EXIF) data from geographical co-ordinates to date, time and device details, so anonymising digital clinical images requires a level of digital literacy that many clinicians do not possess or are unaware of.

DATA SECURITY

The *"minimalisation"* of sensitive patient identifiable data is essential when engaged in clinical communications *via* smartphone Apps due to concerns regarding data security (10). Conversely, clear identification of the patient being discussed is necessary for patient safety as communication failure could result in poor clinical outcomes and avoidable errors (11). The conflict between communication accuracy and patient data security arose pre-COVID-19 with patient care prioritized over the security of patient data (12). The potential for a security breach of patient data is heightened when IM Apps use unregulated servers outside the European economic area. Lack of compliance with data protection requirements regarding data mining, fair processing, records management, and the technical challenges posed by BYOD, are well documented (3, 10).

CYBERCRIME

Healthcare is one of the most targeted sectors for cybercrime globally due to its rich data source and perception as a *"soft target"* (12). Data vulnerability in healthcare is attributable to limited budgetary resources, fragmented governance, cultural behaviors and through the use of obsolete systems unable to support the latest software/updates (13). Regrettably, high risk and critical vulnerabilities in healthcare systems are increasingly targeted by ransomware and the COVID-19 pandemic anecdotally resulted in an increase in malicious cybercrime activity. An example was the successful access and exploitation of personal and health data from a major ransomware attack on the HSE on 14th May 2021 (14). This was a highly significant attack and the largest known against a health service computer system, with massive negative impact on healthcare delivery. Reports that more was paid to ransomware criminals during the first half of 2021 than for the whole of 2020, statistics that could serve as inspiration to other criminals (14) intent on exploiting health systems. A post incident review commissioned by the HSE provided key

learning points for healthcare professions in relation to regular cybersecurity awareness and training for all staff grades (14).

DATA AS A COMMODITY

The business model for many smartphone and App based communications channels involves actively commodifying user data from the device, any networked devices (e.g., fitness trackers) and associated cloud storage. The consequences of "*data harvesting*" by companies such as Meta (owners of WhatsApp and Instagram) and Alphabet (owners of Google, Fitbit, YouTube, Nest) and the "*profiling*" of individuals by exploiting personal data by companies (e.g., Cambridge Analytica) cannot be underestimated or ignored (15). Smartphones have the potential to threaten the security of sensitive patient data and yet, "*the opaque nature of online (including mobile App) tracking, along with the use of data held by mobile operators, is beyond the awareness and understanding of many individuals*" (16). This is acknowledged widely outside of healthcare settings (e.g., auto-manufacturing) where employees are forbidden from using WhatsApp, Snapchat etc. on company issued devices due to data breach concerns (17). Surveillance by Smartphone Apps that harvest the sensitive data, is a genuine concern spanning national, EU and international Data Protection, Information Privacy and Human Rights Laws. Clinicians may be inadvertently enabling the long-term exploitation of patients and their data by third parties (e.g., health insurance companies) or through malicious spyware (e.g., Pegasus).

INFORMATION GOVERNANCE

UK Guidance to clinicians has evolved significantly over recent years. Advice from the National Health Service (NHSX; with a remit for technology, digital and data sharing and transparency and now part of the NHS Transformation Directorate) in October 2020 (5) stated that "*in the current circumstances it could be more harmful not to share health and care information than to share it*". Further, they report that "*The Information Commissioner has assured NHSX that she cannot envisage a situation where she would take action against a health and care professional clearly trying to deliver care*". This assertion is limited to the regulatory action that could be taken by the ICO itself and related specifically to the context of COVID-19. Worryingly, the advice also explicitly endorses the use of "*commercial, off-the-shelf applications such as WhatsApp and Telegram where there is no practical alternative, and the benefits outweigh the risk*".

NHS Clinicians are currently advised to adopt personal BYOD's for video conferencing consultations, home working and mobile messaging (5). Reassurances have been provided for off-the-shelf tools (Skype/WhatsApp) to be used, with implied consent obtained by patient acceptance of the invitation and entering into the consultation (5). However, intentional in inadvertent sharing of patient data could be unlawful as patients only consent to the video consultation and not for their (sensitive) data to be shared further. A clinician (data controller), cannot simply contract their way out of their obligations to the patient (data subject) under the General Data Protection Regulation (GDPR) (18). Helpfully, the European Commission has provided guidance to EU Member States and App developers on how to comply with GDPR and the ePrivacy Directive (19).

GDPR AND HUMAN RIGHTS

The implementation of GDPR in May 2018, created a single legal framework across EU member states on "*the protection of natural persons with regard to the processing of personal data and on the free movement of such data*" (18). This increased the safeguarding of privacy obligations on organizations that process personal data to undertake significant technical and organizational measures to demonstrate compliance.

The protection of personal information is arguably the most pressing concern in defending fundamental freedoms and human rights (20). If a patient feels that their privacy rights have been violated by a clinician using an inappropriate technology, the ICO or DPC could find their assertion that clinicians are free to use such channels challenged. It is noteworthy that since the UK has left the EU, their data protection regulations are likely to diverge so clinicians trained outside the UK will need training supports to raise awareness of any differences.

It is also important to note that not all patients have equal benefit from or access to these technologies and the relationship with discrimination for underserved and marginalized groups, and health inequality must be acknowledged and explored.

CONCLUSION

Smartphone technologies afford clinicians (and their patients) a broad range of highly positive advantages observed acutely during COVID-19. Clinicians have always had the best interests of their patients as a key driver however, the legacy of the well-intended measures undertaken during COVID-19 in relation to patient data and privacy could be felt long after the current emergency ends. Concerns highlighted in this article should be addressed by unambiguous healthcare sector and institutional guidelines with supportive training and education opportunities. Clinicians should be able to access training to optimize appropriate smartphone technologies within regulatory frameworks to overcome data security concerns. Embedding this training into undergraduate curricula, professional CPD requirements and mandatory institutional clinical training would positively encourage digital professionalism.

AUTHOR CONTRIBUTIONS

All authors listed have made a substantial, direct, and intellectual contribution to the work and approved it for publication.

ACKNOWLEDGMENTS

We would like to acknowledge the contribution of Anita Wilcox, information specialist and librarian, for her valuable and constructive suggestions during the preparation of this manuscript.

REFERENCES

1. Barrios V, Cosi n-Sales J, Bravo M, Escobar C, Gamez JM, Huelmos A, et al. Telemedicine consultation for the clinical cardiologists in the era of COVID-19: present and future. Consensus document of the Spanish Society of Cardiology. *Rev Esp Cardiol.* (2020) 73:910–8. doi: 10.1016/j.rec.2020.06.032
2. Rimmer A. Can I receive and store images sent from patients during remote consultations? *BMJ.* (2020) 370:2. doi: 10.1136/bmj.m2675
3. Mars M, Morris C, Scott R. WhatsApp guidelines–what guidelines? a literature review. *J Telemed Telecare.* (2019) 25:524–9. doi: 10.1177/1357633X19873233
4. Masoni M, Guelfi MR. WhatsApp and other messaging apps in medicine: opportunities and risks. *Intern Emerg Med.* (2020) 15:171–3. doi: 10.1007/s11739-020-02292-5
5. NHSX. COVID-19 IG advice. Available online at: https://www.nhsx.nhs.uk/information-governance/guidance/covid-19-ig-advice/ (accessed December 5, 2020).
6. Stevenson A. *Oxford dictionary of English.* USA: Oxford University Press (2010).
7. Gabbard GO. Digital professionalism. *Acad Psychiatry.* (2019) 43:259–63. doi: 10.1007/s40596-018-0994-3
8. McLoughlin J, Zijlstra-Shaw S, Davies J, Field JC. The graduating European dentist—Domain I: professionalism. *Eur J Dent Educ.* (2017) 21:11–3. doi: 10.1111/eje.12308
9. Mars M, Scott R. WhatsApp in Clinical Practice: A Literature Review. In: al. AJMe, Editor. *The Promise of New Technologies in an Age of New Health Challenges.* Amsterdam: IOS Press (2016). p. 82–90.
10. Mistry K. *Information governance considerations for staff on the use of instant messaging software in acute clinical settings* (2018).
11. Toussaint PJ, Coiera E. Supporting communication in health care. *Int J Med Inform.* (2005) 74:779. doi: 10.1016/j.ijmedinf.2005.04.007
12. Martin G, Martin P, Hankin C, Darzi A. Cybersecurity and healthcare: how safe are we? *Br Med J.* (2017) 358:j3179. doi: 10.1136/bmj.j3179
13. Ferreira A, Cruz-Correia R. COVID-19, Cybersecurity and the Human Right to Privacy. *JMIRx Med.* (2020) 2:e21069 doi: 10.2196/21069
14. PwC. *Conti cyber attack on the HSE, Independent Post Incident Review, Commissioned by the HSE Board in conjunction with the CEO and Executive Management Team.* 03 December, 2021 (2021). Dublin, Republic of Ireland: The Board, HSE, Dr Steevens' Hospital, Dublin 8, Ireland.
15. Rabkin J. Revealed: Trump campaign strategy to deter millions of Black Americans from voting in (2016). Available online at: https://www.channel4.com/news/revealed-trump-campaign-strategy-to-deter-millions-of-black-americans-from-voting-in-2016 (accessed December 28, 2020).
16. (@PrivacyMatters) PW. Tweet. *Tweet.* UK: Twitter (2020).
17. Bloomberg. *WhatsApp, Snapchat Banned on Company Devices at Continental.* Windows IT Pro (Online) Chicago. Informa (2018).
18. The EU Parliament TCotE. Regulation (EU) 2016/679 of the European Parliament and The Council of the European Union of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). In: Union OJotE, Editor. *L119/1.* Brussels: For the European Parliament, The President M. Schulz, for the Council of the European Union, The President J.A. Hennis-Plasschaert (2016). p. 88.
19. Comission E. *Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection.* Brussels: EC (2020). p. 14.
20. Markopoulou V, Nieri A, Liaskos J, Zoulias E, Mantas J. Nursing Staff's Awareness of Processing Personal Data According to GDPR. In: al. JMe, editor. *The Importance of Health Informatics in Public Health during a Pandemic.* Amsterdam: IOS Press (2020). p.237–40.

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

Copyright © 2022 John, McCreary and Roberts. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

APPENDIX 2 BOOK CHAPTER

Jointly commissioned by Cambridge University Press and The Royal College of Psychiatry, "Digital Communication" Book entitled 'A clinicians Brief Guide to Communication Skills in 21st Century Psychiatry', edited by Dr Josie Jenkinson and Dr James Woolward.

Digital communication

Section 3

Summary: This section sets out the skills and essential considerations fundamental for the effective use of digital channels of communication. The importance of the security and privacy of sensitive information will be explored and opportunities for professional development established. Areas covered will include:

- *Digital professionalism*
- *GDPR*
- *Personal privacy, securing devices and online accounts*
- *Social media – and optimising your social media profile*
- *Digital communication – videoconferencing, web chat, instant messaging, and email*
- *Intellectual Property Rights and the appropriate use of material sourced online when teaching and training*

LIMIT - 15000 Words (CURRENTLY 14355 WORDS)

Section 3

Introduction

An advanced level of digital literacy is now an essential requirement for all healthcare professionals. Not only is it necessary that clinicians are fluent with the technical skills for effective digital communication, but they must also have a thorough appreciation of the professional issues raised through the use of the vast array of digital communication channels available, ranging from email to social media.

Initially, digital communication channels were accessible solely via a desktop PC however, a wide range of communication applications (Apps) are now readily available on tablets, Smartphones, Smartwatches, Smart TVs, and Smart Speakers. These Apps offer simple, accessible, sophisticated channels of communication with advances in technology continuing apace. From Instant Messaging (IM) that can readily be enhanced with Smartphone created digital images and video, to video conferencing, digital communications channels have become ubiquitous. The technologies are currently so simple and readily available, they are used for day-to-day domestic communications by all age groups and by commercial companies for the conduct of business. It is now possible to share and broadcast our thoughts and impulses instantly, twenty-four hours a day, with little time to reflect upon or contemplate the potential consequences of the content being shared.

In a clinical context, social, mobile and digital media provide clinicians with a toolkit of effective, contemporary modes of communication, facilitating efficient, timely and high-quality clinical care as well as fostering inter-professional and intra-professional collaborations (1). The requirements for digital solutions to promote efficient communication and remote consultation during the Covid-19 Pandemic health emergency has expedited the adoption of Smartphone technology for clinical communications (2).

As the list of popular current consumer channels evolves, the developers of such technologies further enhance functionality as they strive to remain relevant and compelling to users. As a consequence of this evolution, the terms and conditions of use for each of these channels also require updating and require regular change. It is therefore essential that clinicians are alert to the fact that although most of these channels do not require monetary payment for access, they are most definitely not free of charge. Often, although no financial transaction occurs, users pay for access to the functionality by allowing the platform owners to access and monetise the data on the devices that host them. The commercial exploitation of this data has been coined as "the new oil rush", creating vast fortunes for those companies that generate it. Examples of such companies that exploit these data are Facebook (owners of Instagram, WhatsApp, and Meta/Facebook etc.) to Alphabet (owners of the Google search engine, Google Chrome, Google Maps, YouTube, Nest and Fitbit). These parent companies arguably know more about us than we know about ourselves including our location details, our fitness level (by monitoring our daily step count, the routes we take to work, our political opinions, our browsing history, how long we spend online each day, our call history on our phones and even our ability to control our impulses.

Table 1 provides a summary of popular social media platforms (at the time of writing) and their associated functionalities. It is of note that every platform has multiple functionalities and features in common, each platform has its own unique focus, identity and appeal.

Table 1. Popular current social media platforms and the functionality they offer

	Facebook	Twitter	Instagram	Skype	Youtube	Whatsapp	Zoom	TikTok	LinkedIn	SnapChat
Videos	●	●	●	●	●	●		●	●	●
Video Calls	●		●	●		●	●	●		●
IM	●	●	●	●		●				●
Images	●	●	●	●		●				●
Live streaming	●	●	●		●		●	●	●	
Business use	●	●	●	●	●		●	●	●	
Social use	●	●	●	●	●		●	●		●
Group Chat	●	●	●			●	●			●
Stored Messages	●	●				●	●			
Public	●	●	●		●			●		●

Legend:

Videos – refers to the ability to upload, host, embed or link to films and or JPEG,GIFs etc

IM refers to the capacity to exchange Instant Messages between users.

Images refers to the ability to upload and publish images to the platform

Live streaming is the ability to receive or transmit live audio or video material

Business use indicates that a platform offers a specific set of functions, specifically intended for business users

Social Use indicates that this platform is created for recreational users (some platforms have both)

Group Chat indicates the ability to converse with more than one person at a time

Stored Messages indicates that messages between members are stored and can be retrieved later

Public – the communication and content on these platforms are public by default, although most platforms allow users to select settings that will make at least some of their content private

These platforms and the plethora of functionalities they provide, bring with them a range of issues that any clinician intending to use them socially or professionally needs to be familiar with.

Digital Professionalism

Digital Professionalism has been defined as *"the competence or values expected of a professional when engaged in social, digital communication and mobile technology"* (amended from Oxford English dictionary definition of professionalism (3)).

There are clear challenges for how health professionals conduct themselves in a rapidly evolving digital landscape. It has been suggested that Digital Professionalism education should begin in undergraduate medical training, 'given its relevance at all levels' (4), with specific reference made to the importance of including content on managing boundaries and clinical dilemmas in various online contexts for those on specialist psychiatric training programmes.

This issue has recently been acknowledged in the latest Curriculum for Graduating European Dentists (5). Within the Association for Dental Education in Europe document, there is an Intended Learning Outcome that states, *"graduating dentists must demonstrate digital professionalism by protecting patient data and the appropriate use of social media and digital communication, mindful of how these activities may force them into ethically challenging situations and/or damage the reputation of the wider profession."* This healthcare exemplar challenges dental education providers to best equip its graduates for the challenges of modern digital society, and indeed the full range of healthcare providers could usefully draw on this example.

The speed and ubiquity of technological developments have resulted in a raft of new challenges around data protection, and professional standards. These are seldom acknowledged in the literature despite the information governance risks, threats to personal privacy and patient confidentiality, and ultimately trust in the clinical professions (6). Anecdotal evidence certainly suggests that users seldom take the time to read and understand new terms and conditions for each new update to an App, social network, or operating system, and yet such updates can place information that is meant to be private into the public domain.

The informal and instantaneous nature of communication via social, digital media and mobile technology can pose a serious challenge for all healthcare professionals, who must remain vigilant to the fact that their status in society and the public eye, requires them to always maintain a high standard of conduct. Poorly considered words images and data including location, shared online may expose clinicians and their extended network of family and friends, to criticism from patients, employers, and the mainstream media. Clinicians and student clinicians should ensure that what is to be found about them online is reassuring and not alarming and not jeopardise or undermine their professional standing in society. Adverse content could involve material that clinicians post about themselves, but also material that others might post about them and as such, clinicians should be mindful of the types of responses that their own comments might provoke.

To underscore the importance of vigilance in this area, employers have become aware of the activities of its employees in relation to digital professionalism. In 2017, a report was published outlining disciplinary action against in excess of 1200 NHS staff, including 65 individuals who lost their jobs, for their use of social media and messaging Apps (7). This staff cohort, who ranged from porters to Consultants, engaged in a range of inappropriate

practices. These included sharing confidential patient information online, the publishing of derogatory messages regarding patients and colleagues, to being evidenced as using platforms such as Facebook, Twitter, and WhatsApp while at work. Much of the material that was published threatened professional reputations and patient confidentiality.

It has become evident that many staff have been investigated years after some messages were written, so it is important that new students to the profession actively curate (see Do's and Don'ts) anything shared in the past, as it remains accessible and potentially republishable long into the future. The practice of psychiatry can be extremely stressful, and one should be vigilant not to be lulled into a false sense of security due to the privacy settings on various accounts and networks, avoiding ever using social channels to '*vent*' or let off steam.

Private and professional lives can't always be neatly compartmentalised in the online world and like it or not it is prudent to take time to edit, curate and create a positive online profile. Even those who pride themselves on the fact that there is nothing to be found about themselves online, should not become complacent in relation to their online profile and what is to be found on the internet relating to them in both a professional and personal capacity. Limiting the amount of personal information available about you across all platforms will make it more difficult for anyone to learn about you – from patients with a casual interest, to criminals.

Do's and Don'ts

- Consider what information you are comfortable with sharing about your employer, your patients and your family and perhaps discuss this with your friends and work colleagues. It may be that you decide not to mention that you have children, or that you would not like to share what choices you have made for their care or education while you are at work for example

- Your friends, colleagues and family can add to your digital footprint, every time they mention you online. It might be a useful idea to consider and make them aware if there is anything you would rather they didn't share about you online, particularly if it could make you, your family or your patients vulnerable. For example, if you drive a distinctive car and conduct home visits, or if are going away on holiday and your home will be unattended
- Get someone else to search for or Google you regularly – to ensure that you are happy about what is to be found
- Always scrutinise updates, terms and conditions as well as functionality, permissions and default settings on Apps and social media platforms with each new update. Take time to reconfigure from their default settings as upgrades can often expose personal information when new features are added. Be sure to check what personal information is on your public profile and therefor in the public domain
- Delete any Apps you no longer need, and be aware that if you own an iPhone, deleted Apps will reappear on the dashboard of your phone if you 'Update all' Apps. If you need to remove an App forever for your own privacy (for example Tinder or other dating Apps) it may be a good idea to abandon the Apple operating system and move to Android (but be aware, the use of a different operating system may generate further security implications)
- Try to only download Apps from the App Store or Google Play, as these sites are most likely to host the safest Apps for your device. Search online to ensure that any Apps you have or are contemplating downloading, are well reviewed and is not associated with any information governance risks – many Apps have the right to send and read all digital communications on a device without notifying the owner – as a clinician, this is a dangerous prospect
- Clear your search history and cookies regularly (you can search online for information on how best to do this for your specific devices)
- Be aware that if you sign up to a new platform via Facebook – amongst other things, it can allow the new platform to post on your Facebook timeline without notifying you. It is best to keep all your social media accounts separate, don't make life easy for hackers
- Delete any material and profiles created in the past that no longer appropriately reflect your values or beliefs and be mindful of anything that anyone else has posted about you online. If possible, ask the poster in person, or the moderator of the website or chat room to remove any material that could be problematic
- Actively avoid posting online when emotional, exhausted, or under the influence of any intoxicant
- Consider everything that you publish on digital and social channels as potentially public—from WhatsApp messages to post on an anonymous blog, Instagram, Twitter, Snapchat and TikTok account, to the comments left on a blog post, newspaper, web journal article or online forum, all could turn up for scrutiny tomorrow. Anything shared online can be duplicated and circulated widely. Material posted online anonymously can usually be traced back to its point of origin via the service provider, so it is practically impossible to maintain anonymity online

- When using social media for professional purposes, psychiatrists should safeguard patient confidentiality and avoid sharing any identifiable patient information about patients or colleagues, alive or dead. Even with the proper privacy settings in place, anything posted online may end up being distributed further than intended. The more unusual a clinical presentation is, the easier it is for a patient to be identified
- Images shared online can be very difficult to truly anonymise. Cropped images can sometimes be 'uncropped'- for example if they are embedded in some versions of PowerPoint before editing. Digital photographs usually contain Exchangeable Image File Format (EXIF) data (for example - date, time, geographical co-ordinates of the location where the image was taken, camera settings including the make and model of the device on which the image was created), threatening patient confidentiality. Consider removing metadata from any photographs before you post them online. EXIF data can also be used over time to build up a profile of your movements, so simply resize, edit, and resave images before you post them from the smartphone to remove this data
- Try to make a point of always asking others their permission before sharing their images online, and politely suggest that they might ask you before sharing images of you in the same way
- Never take clinical photographs with a Smartphone or within common commercial Apps such as WhatsApp (these download images by default to the device's photo album and streams between all networked devices) or iMessage. Even if such images are immediately deleted from your device, they can remain in the 'Recently deleted' album on iPhone for another 30 days (8)
- Consent from a patient to create or share images of a clinical issue or test results online is problematic to obtain. Clinical images and data should be kept securely and serve as part of the medical notes. As such, there are specific technical specifications and requirements with regard to the secure storage of this material under General Data Protection Regulations (GDPR (9)). It is not appropriate to store them in the image gallery on a smartphone that is networked to a cloud such as the USA hosted iCloud. Clinicians cannot contract themselves out of their obligations under GDPR with patient consent

- When posting online, The GMC (10) states that if you identify yourself as a doctor in publicly accessible social media, you should identify yourself by name, and be aware that any material written by those who represent themselves as doctors is likely to be taken on trust and may reasonably be taken to represent the views of the profession more widely. Even if not identifying as medical students or doctors on social media, or posting about medical matters, the GMC standards still apply
- Ensure you are respectful of colleagues online, try to give people the benefit of the doubt. Without facial expression, nuance, or intonation from voice, it is easy to jump to conclusions or misinterpret what people are trying to communicate
- Be open and honest regarding any conflicts of interest financial or commercial interests or affiliations with pharmaceutical, healthcare, or biomedical companies, because any of your opinions are likely to be taken on trust and impact on public trust in the profession
- Online discussions around patient care must be anonymised even if restricted to specific, appropriately hosted and secure, professional channels such as doctors.net
- Professional boundaries can become blurred when using social media. As a rule of thumb, it is not a good idea to accept Facebook friend requests from patients or to engage in conversations with patients about their care on your private profiles or publicly accessible social media (Further information can be found in GMC guidance (10, 11))

If the ideas in the suggestions figure make you feel uncomfortable, as you are unsure what qualities would create an authentic taste of who you are on social channels, it could be useful to read the book - *Strengthsfinder 2.0* (12) The book contains a code to access a valuable online tool that will enable you to discover and define your strengths and qualities.

Consider carefully if you are considering using or selecting management filters and tools such as Vanilla (Vanillasocial.co), to scan personal social media accounts for old, potentially objectionable posts and material. A thorough 'Spring Clean' of any potentially toxic or poorly advised material shared in the past may be a very reassuring prospect, particularly for those who have been using popular social media platforms for many years (even since childhood and before entering university), however, connecting a product to and allowing unrestrained access to social media accounts could result in material being identified and used against you.

Some of these sites don't even have terms and conditions or an *"about us"* section on their landing pages where they request your login details.

It is important to choose those whom you engage online carefully, and best to try not to respond negatively to any criticism received via social media. If you feel compelled to respond, try to show restraint, demonstrate patient-centeredness, professionalism, and a willingness to reflect, or else you could try to maintain as neutral a tone as possible. Screengrab anything negative that has been said, recording date, time etc. If you feel you are being bullied or *'trolled'*, you will then have evidence to share with authorities, site moderators etc. if you need to ask for it to be removed or for the commenter to be sanctioned or locked out of the site. Be aware that finding yourself criticised online does not necessarily mean that you have encountered a *troll*. Sometimes 'blocking' someone can simply inflame a situation. Perhaps consider 'muting' someone if their comments are confrontational or upsetting.

The areas of potential medico-legal difficulty in relation to the use of social media described here, are also helpfully summarised in a publication by the Medical Defence Union (13). Alongside their guidance and advice, they provide an advisory helpline telephone number to support clinicians with their response to online criticism.

GDPR

If clinicians are using digital devices to discuss patients and share clinical images etc, the devices, Apps and social media platforms they are using for communication and processing of data must be compliant with GDPR. Indeed, clinicians need to be sure that none of the Apps hosted on their smart devices from Smartwatches to Smartphones threaten the security and

confidentiality of the sensitive patient data.

GDPR (9) was enacted across the EU in May 2018, following four years of discussion and a two year transition period. Aimed at overhauling how organisations (including health services) process data, GDPR provides greater protection and rights for data subjects (including patients) and stipulates specific requirements for the appropriate storage, encryption, and transmission of sensitive data, with violations set to generate financial penalties of up to four percent of annual turnover for NHS hospital trusts and Universities, or twenty million euro (14). In the context of digital communication for healthcare workers, the introduction of GDPR has a major impact on how individuals and organisations operate.

In particular, GDPR stipulates that personal data shall be:

- Held securely and encrypted to specific requirements (256 bits, Official accreditation ISO 27001/27002 for the cloud provider (audited and confirmed at that)
- Not transferred to a country or territory outside the European Economic Area for storage unless it complies with specific requirements

Both of these points are of specific practical importance to psychiatry as the channels that are used for clinical communications must host the data within the EU and also, despite the fact that some of the Apps may indeed encrypt the content of the messages that are shared to the stipulated level, the default permissions within the Apps (for example with WhatsApp) may download images to photo albums of all of the devices that receive the images and stream them to the USA hosted Apple iCloud.

A few special categories of sensitive data exist, and are afforded greater protections under GDPR, health information being one of them, and here again this is relevant to clinicians. Among a raft of new rights for 'data subjects', patients have the right protection against

unauthorised or unlawful processing of their data, to be informed if their data is lost or destroyed or damaged.

Healthcare providers are obliged to allow patients to access the data held on them (through System Access Requests or 'SARs'), patients have the right to portability of their data to another provider if they so wish, and they have the right to amend their data if it is inaccurate and explicit consent of the data subject for data processing. Health systems, such as the NHS, and the clinicians who work within them need a good understanding of current data protection regulations and to work within the terms of GDPR. However, as the UK has left the EU, it is reasonable to assume that the regulations concerning data protection are likely to change and potentially diverge from the GDPR, so it is a good idea to stay in touch with any emerging changes and consider their potential impact on the practicalities for your clinical practice.

Personal privacy, securing devices and online accounts

The incidence of the COVID-19 pandemic has resulted in an a vastly increased number of people working from home and information security professionals(15) have enecdotally reported an increase in malicious activity from cyber criminals seeking to exploit the situation. From malware to ransomware attacks and phishing emails. This real world event has already been successfully exploited to access and exploit personal and health data as evidenced from the major ransomeware attack on the Health Service Executive (HSE) in ireland on 14th May 2021. This was the most significant cybercrime attack on an Irish state agency and the largest known attack against a health service computer system, with massive negative impact on the delivery of healthcare for several weeks. The attack began when a single computer stopped

working and its user clicked on a link, on a message service, when prompted to do so, to reach out for help.

A substantial ransome was demanded and apparently paid in order to release 700 gigabytes of data of patients home addresses and personal details that had been accessed via that computer. The criminals have not yet been identified and the health service continues to try to recover, many months after the incident. Such crimes are obviously very lucrative, and this recent attack having been successful for the perpetrators will only serve to encourage interest from cyber criminals.

Take time to consider how much someone could learn about you, our patients, or your employer, if they accessed one of your devices. Think carefully about what your store and how you protect the material on your devices and allocate time to ensure you are up to date with this regularly.

Clinicians, and indeed all those working in healthcare should be on alert for phishing emails which are fraudulent communications sent by an attacker designed to trick the recipient or victim into revealing sensitive information to the criminal, or to clicking links to download malicious software onto the victims infrastructure such as ransomeware. Avoid clicking on any links within any suspicious communications in case of downloading malware.

It is essential to keep operating systems, software, and Apps up to date, as out of date versions may contain weaknesses which make them easier to hack. When companies release updates, they often fix or 'patch' any weaknesses that have come to light and make them harder for criminals to access. Enable automatic updates across devices and software is essential where possible, and back up all data before any manual updates, as occasionally updates can remove

or change files. Backing up regularly will ensure that there is always a recent copy of the data, to help you to recover if data is lost or stolen. Back up the data on your devices regularly via the an appropriate secure cloud based GDPR compliant service. Your health trust or employer will have a policy with regard to how clinical data is to be stored or backed up – with specific technical specifications and advice for encryption and cloud storage. Think through what you will do if you lose or have your device stolen, whether it be your Bring Your Own Device (BYOD) Smartphone or the laptop provided by your employer. It may be worth investigating how you would wipe your devices remotely - if Mobile Device Management Software (MDM) is not enabled on your devices.

It is also important to back up all data regularly as this will assist with recover any important information if a device is stolen, broken, or mislaid. Seek advice from Information Governance and the IT department within your organisation or alternatively, look to the NCSC.gov.uk and NHS web pages (see Further Reading).

Always make a point of changing passwords and pins from their default settings as this will help to protect devices from unauthorised access. Always use different strong passwords for each online account and save these in your browser (such as Safari, Chrome or Brave), or use a password manager to remember them for you. Consider using different email addresses for a range of activities, for example, one email for banking and online shopping, one for social activity and obviously a separate email account for work. Use separate passwords and a password manager to remember them all. If one email address is receiving a lot of junk mail, it is then easy to abandon it.

Lock or turn off a device when not in use, use a strong password to protect it and enable two-factor authentication (2FA) for all devices and across all accounts. 2FA is a more secure way

to confirm your identity when you are using important online accounts and services such as email, social media, and banking. Even if someone knows your password, they won't be able to access your accounts if you have protected them with 2FA. It is particularly important to use 2FA for your important email accounts as any criminal who gains access to your inbox can use it to reset passwords for other accounts using the 'forgot password' feature. The option to set up 2FA is usually located in the security settings of your accounts where it is referred to as two-step verification. For detailed instructions on how to set up 2FA on services from Gmail to LinkedIn and Outlook, visit the Cyber Aware pages of the National Cyber Security Centre (NCSC.gov.UK). Enable biometrics (Fingerprint or Face recognition) if the devices support this feature.

Only ever use secure Wi-Fi for devices where you access or process any sensitive or work-related data. Public and insecure Wi-Fi poses a high risk for malicious activity, and hackers can easily exploit weak security to exploit confidential data.

An uncovered webcam has the potential to allow surveillance of an office or home environment and since their invention they have proved to be a target for criminals through the exploitation of vulnerabilities or the installation of malware. If a PC or laptop has an integrated webcam, it will not be able to physically unplug it, so a webcam cover can be a very useful and cost-effective option to consider in order to increase personal privacy and security.

Every Smartphone has a unique 16 digital IMEI number that can be used to track or lock it, if it is lost or stollen. Typing *#06# into most android Smartphones will reveal the IMEI. On an Apple device, select the Settings App, click on General and then select About and scroll down to find the IMEI number. Make a note of it and keep it somewhere safe.

Wipe all devices thoroughly before they are upgraded or discarded – this applies to BYOD laptops, phones, PCs, and any wearable technology such as fitness trackers onto which messages may be streamed – speak to your IT department before moving on from a current device used to access sensitive data.

From your birthday to your movements to your home address, it is important to be aware of the sum of the data that could easily be discovered by somebody who searches for information about you across the range of platforms that you use, and how that could be used to compromise your personal security and the potential consequences of that. Your current address may be available via 192.com, and details are drawn from the publicly available electoral role. You can avoid this by ticking the relevant box on the registration form. You may request that your details be removed by completing a C01 record removal form, which can be accessed online. However, if you live in shared accommodation, you may need to discuss this first with your flatmates.

You may wish to set up Google alerts that will notify you by email anytime the Google search engine indexes information about you or your family, or whenever criterial which you provide, such as your name or address are searched for. You can find out how to do this by Googling 'Google Alerts'.

Social media

Social media provides busy clinicians, academics, and students with the ability to maintain a range of 'casual' or social connections, supporting and fostering networking with family, friends, and peers, providing entertainment, distraction as well as valuable social and emotional support.

Among the many ways in which these channels enable communication by clinicians, they offer a means of establishing a diverse network of contacts, irrespective of location, to facilitate speedy consultation and collaboration, professional development, facilitating insight, challenging, and expanding knowledge. Such platforms can empower, enabling clinicians to engage with and advocate for patients and the wider public effectively through campaigning, raising awareness and promoting personal and professional reputations.

"No matter how far you are into your career you can intentionally use social media to become a better professional" (Cunningham, A.M. in (16)).

There is a wide range of social networks available for effective continuous professional development. A powerful example of how social media was used to improve care is the highly influential #hellomynameis campaign that was started by Dr Kate Granger MBE, a hospital doctor who was undergoing treatment for cancer. Dr Granger started a very successful campaign on Twitter for more person-centred, compassionate care, by drawing attention to the importance of the simple, basic step of introductions of staff always introducing themselves to patients. By 2017, the #hellomynameis hashtag had made over 2 billion impressions, resulted in a TEDx talk and now has on-going impact, with a campaign that has become international. More information on this campaign can be found online at hellomynameis.org.uk.

A recent example of how social media (Twitter specifically) has been harnessed in this way was the Irish Medical Organisation's (IMO) campaign to raise awareness and public support for their work around the clock using the hashtag "#WeAreWorking". The IMO successfully encouraged healthcare professionals in December of 2018 to publish images and details of their work via Twitter, delivering twenty-four-hour care, seven days a week (17). These images, along with the associated information regarding number of patients seen, number of consecutive days worked, number of hours on call throughout the holiday period, were truly enlightening to anyone who assumed that the health service provides a nine-to-five, Monday-to-Friday service or is a comfortable career choice. Over a thousand people tweeted and the #WeAreWorking hashtag appeared on 3.8 million timelines and received headlines in the Irish National press (17). The ability to broadcast our thoughts and opinions to a potential audience

Figure 1.

A hashtag (#) symbol, before a keyword or phrase, is a commonly used way to label content on Twitter and Instagram. Anyone sharing content on a relevant topic can add a hashtag label to it, so that others who are interested in a certain topic can easily search for and locate all the content on that particular topic, by clicking on the hashtag. Hashtags can be included anywhere in a Tweet.

of millions can be both daunting and empowering but the benefits of having a positive, professional presence on social channels can far outweigh the risks. It is essential however, to acknowledge and be aware of the dangers posed by engagement with social and digital media, to protect yourself personally as well as to safeguard the interests of patients, employers, colleagues, and your profession.

Popular online communities or forums including Facebook, can offer the option to create private space – accessible by request or by invitation only. Some platforms can even offer the option to participate anonymously, or under an assumed name. However, when such groups are large and requests for membership are high, it is difficult for the moderators to be sure that all of those requesting membership are genuine clinicians, and not journalists, curious members of the public or disgruntled patients. These communities are also potentially not hosted securely for the purposes of maintaining privacy. It can be very difficult to maintain confidentiality or anonymity. One example of how the media can report and misreport such material is exemplified by a piece from The Mail on Sunday in 2015 which sensationalised details of junior doctors plans for their strike in 2015. The popular right wing tabloid newspaper claimed to have exposed "a secret plan of militant junior doctors to con the public and cripple the NHS with a walk out" (18). It published a story filled with photos and quotes of junior doctors to undermine their credibility, when their journalists accessed a 'secret Facebook group' which all proved to be untrue.

Community websites, such as Doctors.net.uk, which was specifically created by The British Medical Association (BMA) for clinical professionals, confirm and verify membership and registration before allowing access, offer a safer platform for facilitating clinical and non-clinical discussion and debates, sharing opinions, giving, and receiving peer support etc. It is still essential to never share data that could identify a patient on any platform, including those specifically designed for clinicians but in particular, commercial platforms, such as Facebook.

There is huge potential for the blurring and erosion of the boundaries between professional and personal relationships through the use of social media, with the possibility of it affecting the nature of workplace relationships and the actual doctor-patient relationship itself.

It is appropriate for doctors to use social media to share private interests, hobbies and opinions in the public domain and it can support the development of meaningful connections with others. Social media enables clinicians to demonstrate how they put their values and interests into action in their day-to-day lives. For example, a clinician can use it to evidence further training or education, attendance at conferences, commitment to teaching, love of sport or exercise, passion for the environment or animal rights, commitment to social inclusion, local politics, campaigns, and research.

A recent review of the literature (19) however, evidenced sparse mention of how platforms such as Facebook Messenger and WhatsApp *"manage, analyse, repurpose, or even disclose the data and content of communication*", commodifying data to pay for the functionality that is offered by these applications. Health service providers must consider carefully before allowing clinical communications via consumer channels to avoid exposing sensitive patient data to the risk of breaking confidentiality (20).

Junior colleagues and students may be less familiar with the practical execution of their newly acquired professional responsibilities when using the technology, including the importance of probity, personal privacy, information governance and safeguarding patient confidentiality. However, on the other hand, experienced professionals have a huge amount to learn from new entrants to the professions who were brought up immersed in social media and digital technology from an early age, and who are familiar and fluent with the functionality and value of such technology. It is important to open the lines of communication and maximise dialogue between the generations within the healthcare professions. There is an obvious potential symbiosis between younger *'Digital Natives'* who can draw on and benefit from the experience and professionalism of accomplished clinicians in this new context and also of

course in the opposite direction where the clinical experience of the older generation can inform the practice of their younger colleagues.

Suggestions for best practice when using social media

- Actively seek peer support from colleagues with a range of professional and social media experience – seasoned professionals new to the online platforms and those who are familiar with the platforms but perhaps new to the profession
- Consider carefully which platforms to engage with when considering discussion of any professional issues, and risk assess these with peers
- Scrutinise the sources of news stories that are served to you via social media and be sure to read any news articles, before republishing the content wider – beware of being flamed by headline and being taken in by fake news!
- Try to follow a range of people online and avoid creating an echo chamber of only those with whom you agree – which can unhealthily polarize views and leave our constructs to go unchallenged
- Endeavour to respond positively to online criticism, social media is a terrific place to showcase patient centredness and professionalism
- Beware of getting drawn into arguments or conflict online
- Avoid writing sentences in capital letters as it can appear angry or manic
- Never use social media when you are exhausted, emotional or under the influence of alcohol or any other intoxicant
- Social media is not an appropriate forum for whistle blowing, and it is essential to use the formal, professional channels available in order to raise issues of concern
- It is a good idea to 'stake your claim' by opening accounts and creating profiles for yourself across several social media platforms, to ensure that the words of another cannot be mistaken for you. Be aware that patients, employers, and colleagues will search for you online, and so you should be mindful that you are happy for your content to be found

Long established legal and ethical standards - principles of professionalism as laid down by the General Medical Council (GMC) continue to apply in the rapidly evolving online world -

see *Further Reading* and the advice included in Good Medical Practice (11) which provides specific guidance for doctors using social media. GMC Guidance on Doctors' use of social media (10), along with useful, best practice guides on the use of social media from The BMA (21-23) The RCPsych (24) and The RCGP (25) are recommended reading for all levels of users. Healthcare provider organisations also have their own local policies and clinicians should familiarise themselves with these. This guidance in combination with peer support and some common sense can support you to safely navigate and maximise the benefits of social and digital media. The mentorship of respected colleagues across the flattened hierarchy of social media, active role models and peer support, can make the digital landscape a safe and friendly place for professionals to build networks and share ideas.

Optimising your social media presence

It can be useful and rewarding to follow and engage with mainstream media TV and broadsheet journalists who write about health, mental health and even psychiatry, on platforms such as Twitter. Obviously, this can allow you to stay in close touch with any emerging press stories concerning your specialist area of interest, but it can also be rewarding in other less obvious ways. It can allow you to build relationships and rapport, strike up conversation regarding the press stories and research, delve deeper into research studies, raise your profile, showcase your knowledge or insight, establish your authority, and even potentially create opportunities for you and your work to gain mainstream media and press attention and reach a wider audience. Examples of colleagues who undertake these types of activities, as well as potentially relevant journalists to follow (at the time of writing) may be found in Appendix 1.

Digital communication – Videoconferencing, web chat, instant messaging, and email

Unfortunately, healthcare is not always safe or effective, and the role that communication failures play in the generation of poor outcomes and avoidable error is now widely discussed and recognised (26). Effective communication is an essential part of good clinical care, yet the traditional method of using landline phones, bleeps or pagers, and indeed fax machines, in clinical areas as a means of communication is far from ideal (27). Gould (28) describes this traditional "*formal*" system of communication in a hospital environment by clinicians as "*outdated and impractical by today's standards*", especially as they point out that it is now possible to instantly transmit "*a myriad of data forms at the touch of a button*," on a smartphone from reports to photos, X-rays, videos to Global Position System (GPS) coordinates. "*If information is the lifeblood of healthcare then communication systems are the heart that pumps it"* (26) and so it is essential that efficient, secure, current communications modalities are available to clinicians to enable them to carry out their work.

Data governance in relation to smartphones and mobile technology is no longer something that clinicians in general and health systems across the EU can afford to ignore.

As previously stated, security and data protection must be a central concern for clinicians who understand that confidential patient data is no trivial issue. Patients disclose intimate personal information with the understanding that it will be stored and communicated in a way that protects their privacy and confidentiality.

Clinical data is arguably the most valuable and sensitive data of all. Typically, communications Apps such as iMessage, WhatsApp, Facebook Messenger App etc. may require access to a range of confidential information on the users' Smartphone, including contact lists (which may be uploaded to servers in the cloud), contact information (physical address, email address, name, phone number etc), calendars (to read and amend entries) email, SMS, iMessage etc.

(to read and send communications to those in the contact lists without notifying the owner), microphone and camera (to enable and support recording of communications), and the image gallery to enable access to, and downloading of, images between users.

Table 2 is an unofficial translation of a table published by the Dutch Data Protection Authority in April 2020, outlining the range of important considerations when selecting video call Apps for communication. The regularity with which App functionality and terms and conditions are updated would suggest that it is an extremely demanding and complex task for anyone, let alone clinicians to remain abreast of the issues posed for the selection of any App for sensitive clinical communications. Current, specialist input would be required from Information Technology, Legal and Information Governance professionals in order to inform the choice of an appropriate communications channel for clinical communications.

Table 2.

Privacy Decision-making aid: Video Call Apps

As of 15 April 2020 UNOFFICIAL TRANSLATION by Christopher Schmidt, CIPP/E CIPM CIPT CBSA

	Discord	FaceTime	Hangouts (Google)	Hangouts Meets (Google)	Houseparty	Jitsi	Messenger (Facebook)	Signal	Skype	Talk (Nextcloud)	Teams (Microsoft)	Whatsapp	Zoom*
What does the app offer?													
(group) chat (text)	■	■	■	■		■	■	■	■	■	■	■	■
1-to-1 calls (audio and/or video)	■	■	■	■	1	■	■	■	■	■	■	■	■
group calls (audio and/or video)	■	■	■	■	■	■	■		■	■	■	■	■
set up and manage yourself (self-hosted)						■				■			
participation in conversation w/o creating an account			■	■		■			2	2	2		2
use in browser	■		■	■	3	■	■		4	■	■	5	■
use on different platforms (cross-platform)	■		■	■	6	■	■	■	■	■	■	■	■
What data does the app collect?													
address book		■	■	■	■		■		■		7	■	
location data		■	■	■	■		■		■		■	■	■
call data	■		■	■	■		■		■		■		■
metadata	■	■	■	■	■		■		■		■	■	■
linking data with data from other products or profiles			■	■			■		■		■	8	
For what purposes does the app process data?													
For using the app	■	■	■	■	■	■	■	■	■	■	■	■	■
For improving the app	■	■	■	■	■		■		■		■	■	■
Show (personalised) advertisements					■		■						9
How does the information flow look like?													
Data Processing Agreement possible				■		10				10	■	11	12
Data transfer to 3rd parties (if so, what data and to whom)	13	14	15	15	16		17		18		19	20	21
Location of data controller	US	US	IRL	IRL	US	10	IRL	US	IRL	10	IRL	IRL	US
data remain in the Netherlands						■		■		■			
data remain in the EU				■		■		■		■	■		
Is the communication secure?													
end-to-end encryption (even the provider of the app cannot access the content of the communication)		■				■	22	■	23	■		■	
encryption of traffic during transfer, so that third parties cannot access it (note: the provider of the app may be able to access it, but this does not mean it will happen).	■	■	■	■		24	■	■	■	■	■	■	■
minimisation of metadata use		■				■		■		■			
encryption by default	■	■	■	■		■		■	■	■	■	■	■
anyone can check source code (open source)						■		■		■			
How does the app make money?													
paid subscription or paid version	25	26		■					27	28	■		29
(personalised) advertisements			■		■		■		■			■	30
donations								■					
otherwise						31						32	
Where can you find information?													
privacy statement (refer to the Dutch original for clickable links)	🔗	🔗	🔗	🔗	🔗	🔗	🔗	🔗	🔗	33	🔗	🔗	🔗
privacy statement in Dutch	■	■	■	■			■		■	33	■	■	

1 Video only
2 After invitation
3 Google Chrome
4 Skype for Web in Microsoft Edge or Google Chrome
5 But, not for video or audio
6 Android, iOS, Google Chrome
7 Mobile/exchange
8 With other Facebook products
9 Please note: when calling via website
10 N/A (self-hosted)
11 Standard agreement
12 For some sectors
13 Metadata and IP data for business purposes, but no sale of data
14 To Apple Subsidiaries and Agents
15 Within Google
16 To public authorities when they so request and to related companies
17 Within Facebook and to external partners
18 To public authorities when they so request
19 Within Microsoft
20 To Facebook and to third parties, but not (yet) for advertising purposes within Facebook
21 To supporting partners, but no sale of data
22 Not for (video) calling; for chatting you have to start this separately in Secret Mode
23 Only in private conversations (see: website)
24 In group discussions
25 Discord Nitro
26 Supplied as standard for new Apple products
27 Skype for businesses
28 The enterprise edition has been paid for
29 There are several subscriptions, but also a free version
30 Please note: when calling via website
31 Project is fully supported by the company (kit)
32 Part of Facebook
33 This depends on the person offering a Nextcloud service

* Be careful when using Zoom. This app is still in development.
** Note: For group calls, there is either no end-to-end encryption, or only with a limited number of participants.
Please note that the AP has not been able to do extensive technical research on the apps. The AP relies on what companies say about how video call apps process your data, for example in their privacy statement.

Operating system vendors such as Apple (iOS) and Google (Android), plus other, non-communication-based Apps on any Smartphone dashboard may additionally access financial information, track purchase history, user's browsing data, search terms, user created content,

and location, health, and fitness information – steps, heart rate etc. Paying for access to the functionality on offer from these Apps by providing ready access to the contents of a doctor's data and potentially that of patients is inappropriate and poses a genuine information governance risk.

Doctors are probably using their own personal Apple or Google accounts where data is analysed for Apple's and Google's own ad-related practices etc and may themselves be compromised by how they personally manage access to their devices and cloud-based accounts. It is important to also be aware that each time a website or even a single newspaper article is accessed via a Smartphone, over a thousand private surveillance mechanisms can be granted access to the data on the device, from the browsing history, to location, to a list of the Apps on the device, the content on each of the Apps, the contact lists, information regarding purchases, details of your life offline and any data on any of the devices at your home that sharing your IP address, including those devices belonging to those who share your home, from flatmates to members of your family – all to generate advertising revenue to the newspaper group that published the article online. This is why institutions from tyre manufacturers to banks and insurance companies, install mobile management software on any mobile device including BYOD, before allowing them to access work related data. Such software helps to govern business related communications, data, and systems accessed via the device and can clear a Smartphone or laptop of all its contents in the event that it is stollen or if an employee leaves the company.

Ideally, all clinical communications should be made via a secure digital tool or channel, approved with regard to NHS information governance standards, and compliant with GDPR. In the USA, where clinicians are obliged to adhere to the requirements of the Health Insurance Portability And Accountability Act (HIPAA) of 1996 (29), the security and privacy of patient's

medical data and communications is protected by the provision of a myriad of institutional digital solutions such as Voalte, Trillion, Tigerflow and Microsoft Teams. Hospitals in the USA, less concerned by budgetary restraints and arguably more risk averse regarding litigation, use expensive institutional solutions, often providing specific devices and digital communications channels for clinicians to use, thus ensuring that patient data is securely stored and communicated. HIPAA (29) is not as comprehensive a standard as GDPR and most of the established solutions being used in the USA are not yet GDPR compliant. It is possible that these solutions will be adapted and become available in the EU in the future.

For example, Microsoft Teams, can now run solely on servers located with the European Economic Area (EEA) thus complying with the requirements of GDPR. It is interesting to note that in the USA, The Department of Health and Human Services which enforces HIPAA compliance, maintains 'technological neutrality for texting'(4). This means that no meaningful compliance standards for texting exist in the USA, so there is no such thing as HIPAA compliant texting. It can therefore be assumed that there is no GDPR compliant texting either.

However, the advice on offer from the NHS and various professional bodies can be not only sparse, but controversial. Healthcare as an industry has not always kept pace with technology (Watson et al 2016) and there is ample recent relevant evidence of personal smartphone and mobile technology use by clinicians for workplace communications in settings in the UK (27, 30-32). In their extensive review of the literature, researchers (33) found in excess of 50 international papers describing studies where WhatsApp or Instagram were being evaluated for use in clinical communications as the primary focus. In one multi-centred, UK-based, pan-specialty, pan-grade survey study of both doctors and nurses, which spanned five separate National Health Service hospital sites in the UK, researchers (31) evaluated ownership and use of tablets and smartphones by healthcare professionals (doctors n=2107) and nurses (n=4069). They reported approximately 98.9% of doctors and 91.5% of nurses owned a

smartphone, with numbers continuing to rise. They found that of the doctor group, 64.7% had used Short Message Service (SMS), 33.1% had used App-based messaging and 46.0% had used their smartphone camera and picture messaging (e.g., to send a photograph of a wound or X-ray to a colleague for an opinion). The corresponding figures in the nurse group were far less at 13.8%, 5.7% and 7.4%, respectively.

The use of mobile/smart devices and Apps in clinical care poses specific and significant security and privacy challenges that must be addressed to ensure data protection and consequently patient safety (27) and to prevent the erosion of patient trust. A fundamental principle of current data protection legislation in the UK and indeed within the EU, is that personal information is to be stored securely, protected against disclosure or destruction of data and against their accidental loss or destruction. Breach of the Data Protection Rules risk exposing clinicians and employer to litigation from an injured party as it may constitute an offence under the GDPR (20).

There is currently a range of specifically created technical solutions for efficient communication of patient details available to use on BYOD Smartphones, if the particular NHS trust or employer is unable to finance the provision of specific devices and integrated communications solutions for clinical communications. These Apps include Hospify, Forward, Careflow Connect, Med Crowd, MedicBleep, Siilo, Signal and Cupris. Clinicians are advised to take a conservative approach to the utilisation and selection of digital channels.

Social, mobile, and digital solutions must be risk-assessed and approved by experts in order to ensure that they are appropriate for processing sensitive data. Clinicians should contact the IT Department or Information Governance Department in their employing health trust; to ensure that Data Protection Impact Assessments (DPIAs) have been conducted on any

technology, channels and Apps being considered for use. Clinicians cannot be expected to dabble in this complex and quickly evolving area where an extremely high level of expertise is required and must be free to immerse themselves in their clinical work. Failing this, professional bodies could create panels of appropriate specialist professionals to create the DPIAs themselves.

A list of expertly risk assessed NHS-approved Apps, or the provision of institutional or enterprise solutions such as Hospify, Near Me, Microsoft Teams or Voalte for use by clinicians are well overdue. Most popular free Apps, such as WhatsApp, are not compliant with the requirements of GDPR and are not secure or appropriate for clinical communications. To ensure that communication is efficient and secure, it is essential that a comprehensive list of the essential functionality and approved Apps for clinicians be established. For example, an online image sharing repository, a cloud-based document sharing solution, an online calendar, a video conferencing/consultation solution, an instant messaging channel, a PDF creator App, dictation software and Apps and a reference manager App.

With regard to each, it would require thorough evaluation from a team of security specialists to meaningfully establish –

- What are the benefits?
- What are the hazards?
- Who might be harmed?

The technology has evolved to a point where it is now essential to collaborate and engage expert IT, information governance and legal professionals in a team in order to complete these risk assessments in order to establish exactly what are the implications for personal, patient, employer privacy.

How to evaluate your technology

Questions that must be answered regarding each include;

- Will images communicated by the App contain EXIF data that could threaten privacy/confidentiality?
- What data is the App accessing and is it at risk of disclosure or exploitation?
- Where is the data stored? Where are their servers? Where is it streamed?
- Who owns the content? Images?
- Any privacy issues referenced online or in the press?
- Any emerging functionality to be aware of? New Terms and Conditions? (Terms and conditions must be reviewed regularly as these are liable to change)
- Does the software or App provide logs of who has accessed the data?
- Is there an ability to log every location where the data is stored?

If video conferencing functionality is required, and Microsoft Teams or Skype for business (for example) is provided by an employer, then that channel must be used, as opposed to the free Skype App or a WhatsApp video call that may be readily to hand. Further, Microsoft Teams may indeed be an appropriate and secure, employer provided solution to enable video conferencing, remote consultation, and collaboration with distant colleagues, but the microphone on a BYOD Bluetooth headset purchased separately could prove to be a security risk and make the communication insecure. So be sure to familiarise yourself with any current workplace policy and press stories with regard to cybercrime or emerging issues with technology. OneDrive is part of the Microsoft Office suite – Google Docs and Dropbox may not be compliant. Always default to the channels and hardware that are provided by your NHS trust, university or employer.

It is also worth considering carefully whether Smart watches, Smart TVs, Smart speakers, Bluetooth and WIFI etc, pose avoidable, genuine risks to the security of patient data, and seeking advice locally from information governance professionals and colleagues in IT before allowing them to be introduced into clinical areas. The recent cyber-attack which paralysed the Irish healthcare system in 2021, at the height of the Covid-19 health emergency should serve to heighten concerns around information security.

The terms and conditions associated with many of these devices mean that they have permission to record anything when they are installed, with the platforms retaining ownership of these recordings. This can make them inappropriate for clinical settings. Wearable technology such as Smart watches, Smart Glass and even fitness trackers must be carefully risk assessed and scrutinised before wearing during clinical practice, as they may pose a risk to patient privacy. Features such as Bluetooth can mean they could be a security risk.

The NHS published well informed Information Governance considerations and risks around the use of instant messaging software in clinical settings in 2018 (34) which was useful and informative, but it failed to offer any practical guidance around information that is communicated by clinicians daily via BYOD mobile devices.

It is best to avoid creating Clinical images with a BYOD Smartphone—unless a specific, secure, employer approved solution, device or App has been made available for this purpose. Images shared by iMessage or WhatsApp, for example, on an iPhone are currently downloaded to the Apple iCloud by default whether the recipient opens the message or not. Digital images are then streamed between networked devices (iPad, Mac) and iCloud by default. If it is imperative that if a clinician uses WhatsApp to share images, these features must be disabled on their Smartphone. Digital images created using a Smartphone and transmitted using most

popular Apps are often compressed to save space (so contain minimal additional data), but this should never be taken for granted. The terms and conditions of use for Apps often update and can alter substantially with each new update, settings can readily change so that an image can contain details from geographical co-ordinates, to date, time, make and model of device etc. All confidential patient data, including clinical images are required to be stored securely with the patient's medical notes, and if in digital form, they are required to be encrypted. Before sharing any digital image via any App, it is important to be clear about any additional EXIF data that is contained within the image, especially if that image is of a confidential nature.

From digital dialogue (including email, instant messaging, and web/video chat) to the use of dictation Apps, accessing test results online, and scheduling appointments in an online diary, the clinician's role involves access to and communication of confidential, sensitive data. This necessitates a certain level of technical literacy, especially now as the BYOD) Smartphone has become ubiquitous in the workplace. Images of test results, radiographs, clinical signs, taken via a Smartphone (for example via an iPhone) in a doctor's pocket, can be suggested for potential upload to social Apps such as Facebook or Instagram by default. The more unusual a clinical presentation is, the more identifiable the patient will be.

Anonymised cropped clinical images shared in PowerPoint presentations sometimes only require an 'un-crop' command to reveal the entire original image. A photograph, cropped to show an image of a patient's eye, could be labelled with the patient's name automatically, if it is uploaded to Facebook. Facial recognition technology being used by Facebook is currently that powerful.

Patient appointments or operation schedules should never ever be hosted on free commercial services such as a personal Google Calendar. Investigate the tools provided by employers –

NHS and Universities. Microsoft Office applications currently offers a secure and appropriate enterprise diary feature that meets this requirement. Many businesses are now advising employees not to access social networks or download software or Apps on any device used to process work-related data (35).

There are several steps we should all take, around our behaviour on social and digital channels to ensure the privacy of sensitive data.

Suggestions for Best Practice when engaged in Digital Communications

- Communication and storage of patient data must comply with GDPR – so insist on risk assessed solutions for clinical work, seek advice from the IT department/information governance department of your organisation and ask to be sign posted to appropriate secure enterprise or approved solutions
- Never allow anyone else to access or use the digital devices you use for work related data
- Disable message notifications on your device's lock screen – do not allow messages to stream onto fitness trackers for example
- Set all devices to lock out after a short period of not being used
- Fit a privacy filter/film to the screens of any device used to access confidential data, specifically BYOD laptops or PCs that are used in shared spaces
- If it is not possible to download copies of messages regarding specific patients into their notes, record information regarding communications, colleagues consulted, and decisions made in the patients notes or records

- Minimising the amount of patient identifiable data communicated in any digital message, but remain vigilant to the fact that it must be clear to the person you are communicating with, who the patient is that you are discussing
- Comprehensive medical records are essential, and conversations may be subject to freedom of information requests or subject access requests so must be recorded in the medical notes
- Turn off image/message streaming between networked devices, and to the cloud. Unlink Apps on Smart devices from the image library on your smart devices.

If the use of BYOD and commercial, non-medical digital solutions were to stop immediately, healthcare across the NHS would be a lot less efficient. However, we must be sure to make informed choices regarding the solutions we use. Such measures include turning off any unnecessary functionality or permissions to maximise the security of the data, turning on any security features that are available, avoiding public Wi-Fi, and considering the use of a Virtual Private network (VPN) and lobby for training, guidance, and provision of appropriate secure solutions. It is important to note in the meantime that any decisions made on any digital messaging platform must be recorded on the patient's notes (Siegel et al. 2016). Anyone who stops working at a particular hospital or clinical area must be removed from the message group. Keep patient identifiable data shared via these channels to the absolute minimum.

In October 2020, NHSX (the UK Government unit responsible for setting national policy and developing best practice for NHS technology, digital and data, including sharing and transparency) issued specific advice (36), regarding the use of communications tools to aid clinicians in their work during the COVID-19 pandemic, when the use of efficient digital communications and remote consultations was suddenly perceived as urgent. In their Digital

COVID-19 guidance for clinicians The RCPsych (37) attempted to paraphrase the NHSX (36) around digital clinical communications noting:

> *"It is fine to use video conferencing tools such as Skype, WhatsApp, Facetime as well as commercial products designed specifically for this purpose."*

Further;

> "the consent of the patient or service user is implied by them accepting the invite and entering the consultation".

Reliance was placed on assurances provided by the Information Commissioner (ICO) to NHSX that she could not envisage a situation where she would act against a health and care professional who was clearly trying to deliver care. However, these observations need to be treated with caution, not least because of the unprecedented context in which it was issued.

Where the NHSX advice references consent – this appears to be a reference to consent from the patient to the *nature* of the consultation – i.e. Video consultation online rather than face to face consultation. There is a risk that healthcare professionals reading that guidance would assume that the patient's agreement to proceed by way of a remote consultation could be relied upon as discharging the controller's obligations in respect of data processing. However, a data controller (in this case the clinician, or their employer) cannot evade their compliance obligations by pointing to the patient's agreement to a remote consultation.

The patient's consent could - if it meets the exacting requirements of consent under the GDPR – provide a lawful basis for processing under Article 6 (38) and a suitable exemption for the purpose of Article 9 (39) (Special category data) of the UK GDPR. However, if the communications platform which the controller has selected does not meet the requirements of the UK GDPR, the patient's consent to a remote consultation cannot remedy or excuse that compliance failure. The UK GDPR does not provide any mechanism for data controllers to

contract out of their compliance obligations. What the NHSX and RCPsych guidance do not stress is that the controller's obligations to undertake appropriate due diligence before selecting a particular communications platform are not altered either by the existence of a pandemic or comforting words from the ICO.

So far as the ICO's position is captured in the NHSX document, there are two important points to note. Firstly, it is limited to regulatory action being taken by the ICO of their own volition and does not impact the data subject's rights to bring a claim. Secondly, it applies a risk-based approach which is very context specific i.e., the COVID pandemic. Many medical consultations may relate to matters which have a significant impact on health and well-being and may involve life or limb threatening conditions, where the absence of a consultation may cause real harm. Indeed, the guidance specifically endorses off the shelf solutions only "where there is no practical alternative, and the benefits outweigh the risks". The vexed question which remains is how well equipped are health and care professionals to meaningfully appraise specific communications channel or platform on their own.

Since the beginning of the pandemic, many employers – including those from the financial services, banking and insurance, have conducted DPIAs, created relevant policy, provided training, back-up support and appropriate technology to accommodate the processing of sensitive data when remote working. From the provision of specific dedicated hardware to secure communications channels to Mobile Device Management (MDM) – which can provide a range of useful options including the ability to remotely wipe devices that are stollen or lost) solutions for BYOD. Health systems and employers must be clear that any sensitive patient data is processed and stored in a way that will facilitate their prompt compliance with any requests for access from a Subject Access Requests (SAR). This is important as a SAR may be served when a staff member has gone on holiday or has moved on to other employment. NHS

employers must make similar investments in technology and security to ensure safe remote consultations, communications and working.

It is imperative that doctors take security issues into careful consideration when recommending digital health tools to patients for use on their own Smartphones and devices, as vulnerable patients may be less able to weigh up the benefits and hazards of such Apps for themselves. Specialist, professional advice should always be sought before recommending any Apps or digital solution to patients.

Suggestions for best practice when using Videoconferencing, web chat and instant messaging

- Guidance signposting a specific approved channel (such as Microsoft Teams or Near me), hardware and secure internet connection provided by your employer must be followed. Details should be found on your intranet via the Information Governance, or IT training team
- Good lighting and an uncluttered background are important and should not be ignored. It is best to try to choose a position where the day light is shining directly onto your face, never sit with a window behind you as it will interfere with how clearly you are seen
- During the consultation it is best to look straight into the camera and not into the eyes of the patient who you are talking to
- When engaged in video conferencing with a patient, it is important to ensure that the patient feels they can confide in a clinician and that you are in an appropriate private location, not overheard. If they are in a public place to avail of public Wi-Fi, suggest that they could consider alternative arrangements and perhaps reschedule

- Try to be sensitive to the patient's level of digital literacy and confidence with the technology to determine whether any video consultation or screening is likely to be effective
- Secure Wi-Fi must always be used in order to ensure privacy, a Virtual Private Network (VPN) may be appropriate
- Ask the patient if they are also using secure, password protected Wi-Fi
- Any notes that are taken must be kept securely, encrypted, and not streamed to any insecure cloud services on BYOD

Professional communications via email

Senior clinicians and medical educators often lament the recent phenomenon of junior staff and students taking a less formal, over-familiar tone with them in email while many millennials have abandoned email completely. It is important to consider demeanour in all written professional communications, as would be appropriate in oral dialogue. It is also important to strive to maintain a formal tone, with introductions and salutations in written communications to patients and all professional colleagues.

Email containing confidential patient data, should be communicated only via secure organisational email addresses, and not via any insecure or commercial, private account such as Gmail or Yahoo, which may not be secure. If such accounts must be used, for example, when communicating with a patient to their private email address, it is important to follow any employer information security policy which should be in place identifying what can and cannot be done. One simple, sensible solution, in the absence of this, is that the sensitive data be attached to the email as a password protected enclosure, and the pre-agreed

password communicated separately, perhaps by text. This process doesn't have to be complicated; the same password can be used again and again.

It is essential that we never say anything in an email that we would not happily say to or about someone in person. It is never appropriate to engage in gossip, bullying or speculation for example about a colleague (at all) and certainly not on work related email or any digital channels. Any communication written concerning any individual within an organisation, can ultimately be handed over to them for their inspection upon request (as per the requirements of an SAR), so it is important to bear that in mind. For this reason, it is also important to remember that all such communications should not be destroyed or deleted.

Younger people, brought up in this age of digital technology are less likely to check their email regularly, preferring to use different technologies for communications, so it is worth remembering that some communications – such as reminders regarding appointments for example, are best communicated via different channels such as SMS digital messaging. Email accounts are commonly congested with SPAM email, including everything from shopping receipts to information about promotions from retailers, so it is important to never use work related email accounts for anything other than professional related communications. It can be easy to miss important communications if we receive a huge volume of email.

It should go without saying that we need to resist the urge to "reply to all" in emails or 'CC' in people, when emails are received, suggesting meeting times or organising events – this is also an irritating source of email congestion. One useful tip, when taking annual leave and setting an 'out of office' notification, is to leave a message saying that your inbox is full, and asking that people phone you upon your return – generally, if people receive such an automated

email in reply to a request, they will go and solve their issue with someone else – freeing you up to spend your first two days after your return to actually get on with some work!

Endeavour to resist the urge to answer any digital communications, including those made via digital messenger, concerning work related issues or regarding patients when under the influence of alcohol/on holiday etc. Clinicians require their down time to recover and return to work refreshed.

Suggestions for best practice when using email

- When emailing any sensitive data via an insecure email account - sensitive data be attached to the email as a password protected enclosure
- SARs are to be expected and it is essential that we never say anything in an email that we would not happily say to or about someone in person, any email communications should not be destroyed or deleted
- Never use work related email accounts for anything other than professional related communications

Intellectual Property Rights and the appropriate use of material sourced online when teaching and training

It is a common misconception that material sourced online can be freely used for teaching and scholarly work, so long as it is not used to generate income. Despite the fact that plagiarism and the importance of gaining permission and providing acknowledgement for the contribution made in research and publications is widely understood, the proliferation of new technology that enables downloading, copying, reworking and republication of media sourced from the internet has resulted in a raft of intellectual property violations.

Intellectual Property consists of inventions, creations of the mind, literary and artistic works, photographs, images and symbols and the names used in commerce. It is protected by law, through creative commons licenses, patents, trademarks, and copyright. Universities and research institutions have been said to be the factories of the knowledge economy. It is intellectual property rights that provide a mechanism whereby such institutions can safely capitalise on the knowledge that they generate within the economic sectors.

Students, researchers, clinicians, and academics commonly appear to be ignoring the fact that search engines such as Google and Bing are not repositories of free images, music, journal articles and other material. It is essential that the ownership and permissions around the use of images selected for use on slides, posters, educational material and websites including blogs is established before they are uploaded, and rights established and appropriately paid for or attributed.

Internet sourced photographs and illustrations are commonly to be found on academic university assignments from essays to posters, slide presentations, reports and notes, educational materials, and virtual learning materials. While these materials remain internal, they may be covered by one of the various licensing agreements held by universities and health trusts. However, these works can and often are re-published online, hosted on public-

facing institutional and commercial platforms such as Prezi, SlideShare, blogs and Pinterest without due permissions, acknowledgement, or respect of the originator's rights.

It is naive to assume that visual media companies such as Getty Images, Alamy etc, newspapers, commercial publishers, photographers, musicians will happily ignore violations to their copyright or be satisfied if users offer to remove or delete such material, simply because it is being used for scholarly work or in material concerned with the health or welfare of others. Copyright owners are within their rights to pursue substantial claims for lost royalties and loss of income plus expenses.

A number of websites are available where free to use stock images can be sourced online – most universities have a page on their intranet signposting staff to advice and signposting a range of these including:

Unsplash.com - a photo discovery platform for free to use, high-definition photos that can be downloaded and use to embellish any project

Pexels.com – free to use stock photos and videos from a global network of creators

Pixabay.com is a vibrant community of creatives, sharing copyright free images and videos. All contents are released under the Pixabay License, which makes them safe to use without asking for permission or giving credit to the artist - even for commercial purposes.

Commons.Wikimedia.org is a global movement whose mission is to bring free educational content to the world, providing an online repository of free-use images, sounds and other media.

There is a potentially useful exception for teaching, or "illustration for instruction", in Section 32 (40) of the Copyright, Designs and Patents Act 1988 (CDPA). This can cover the reuse of text, images, or film - in principle any medium, provided that fulfil the requirements:

- teaching for a non-commercial purpose
- the author/ source is adequately acknowledged
- it is fair dealing with the material

In order to satisfy the fair dealing test, it is essential that due consideration is given to whether its use is likely to damage the interests of the rights owner – the author or the publisher. It is always best to seek advice from a Knowledge and Information Professional such as a librarian at the institution where the teaching will take place. For example, if all or a large part of a published textbook were being reproduced, it could be argued that the publishers and authors interests are being damaged, but if brief selected extracts were being shared, then it could probably not be proven – so seek advice and acknowledge on the teaching material, poster or presentation that this advice has been sought, it is important to acknowledge the rights of others and demonstrate the importance of professionalism in this issue.

In principle, the Section 32 Copyright 'illustration for instruction' exception could be relied upon to cover the use of copyright-protected images in a secure online teaching environment, on a Virtual Learning Environment (VLE) such as Moodle, depending on the details in each case. This could potentially include live online teaching sessions and also making the material available for students to access at their convenience, such as flipped lectures and lecture recordings. However, clarify with the university where you are teaching, to confirm that if using Section 32 exemption, students are registered at the site where the teaching is being delivered, and not, for example, interns or a visiting delegation of academics.

Suggestions for best practice in the use of material sourced online when teaching and training

- Only ever use images, film, and music to embellish your work that you have created yourself or that you have established permission to use
- Do not distribute copies of any materials for teaching unless you have established that you are working within the law
- Always be sure to acknowledge that the materials used to enhance and embellish academic presentations are sourced ethically and within the law and role model professionalism in this area
- Reverse search any images you are intending to use to embellish slides using Google images. To investigate the origin of an image you might like to use from the Internet try to search for it using Google - Right click on the image, Copy the image address, Go to Google images, Click on the camera icon to Search by image
- Download the Little Guide to Copyright by JISC for simple explanations of Creative Commons licenses and copyright (41)

ACKNOWLEDGEMENTS

We would like to thank Stewart Duffy MD, Partner and Solicitor, Radcliffes Le Brasseur for his advice in relation to GDPR and the use of digital channels for communications during the COVID-19 pandemic.

Table 2 is reproduced with the kind permission of Christopher Schmidt, Magister of Law, Law Tutor, Jones Day, Frankfurt, Germany. Permission has also been requested from the authors of the original work - the Dutch Supervisory Authority/Autoriteit Persoonsgegevens in Holland.

FURTHER READING

Centre for the protection of national infrastructure (2021)– My digital footprint. https://www.cpni.gov.uk/security-campaigns/my-digital-footprint (accessed 10th November 2021)

Hopkinson, C. (2020) Working from home advice. University of Oxford https://infosec.web.ox.ac.uk/article/working-from-home-advice (Accessed 10th November, 2021)

National Cyber Security Centre (2021) Improve your online security today. https://www.ncsc.gov.uk/cyberaware/home (accessed 10th November 2021)

National Cyber Security Centre (2021) Social media: how to use it safely. https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely (accessed 10th November 2021)

National Cyber Security Centre (2021) Top tips for staying secure – online password managers. https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers (accessed 10th November 2021)

National Cyber Security Centre (2021) Dealing with suspicious emails and text messages. Version 2.0. https://www.ncsc.gov.uk/guidance/suspicious-email-actions (accessed 10th November 2021)

British Medical Association (2018) Ethics Guidance on Social Media BMA Guidance. BMA.org.uk

British Medical Association (2013) Medical Students Ethics Toolkit. BMA.org.uk

British Medical Association (2018) Social Media Guidance for Doctors BMA.org.uk (https://www.bma.org.uk/advice/employment/ethics/social-media-guidance-for-doctors - accessed 20th December 2018)

British Medical Association (2018) Social Media – Practical Guidance and Best Practice BMA.org.uk

General Medical Council (2017) Confidentiality: good practice in handling patient information. GMC-uk.org (http://www.gmc-uk.org/Confidentiality2017. pdf_69037815.pdf – accessed 20th December, 2018)

General Medical Council (2013) Doctors' use of Social Media. GMC-uk.org https://www.gmc-uk.org/-/media/documents/doctors-use-of-social-media_pdf-58833100.pdf

General Medical Council (2013) GMC guidance: *Maintaining a Professional Boundary Between You and Your Patient*. GMC-uk.org. (https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/maintaining-a-professional-boundary-between-you-and-your-patient - accessed 01 December, 2019)

General Medical Council (2013) Financial and commercial arrangements and conflicts of interest. GMC-uk.org (http://www.gmc-uk.org/guidance/ethical_ guidance/21161.asp– accessed 20th December, 2018)

General Medical Council (2011) Making and using visual and audio recordings of patients. GMC-uk.org (http://www.gmc-uk.org/guidance/ethical_ guidance/making_audiovisual.asp– accessed 20th December, 2018)

General Medical Council (2016) Professional Behaviour and Fitness to Practise: Guidance for Medical Schools and their Students. GMC-uk.org (http://www.gmc-uk.org/education/ undergraduate/professional_behaviour.asp – accessed 20th December, 2018)

General medical Council (2019) Good medical practice. (https://www.gmc-uk.org/-/media/documents/good-medical-practice---english-1215_pdf-51527435.pdf?la=en, accessed October 2019) April, 2019.

ICO (2016) Guide to the General Data Protection Regulation (GDPR) (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ Accessed 1st January, 2019

The Medical Defence Union (2018) Using Social Media. TheMDU.com (https://www.themdu.com/guidance-and-advice/guides/guide-to-social-media - Accessed 20th December, 2018)

NHS Digital (2018) NHS and Social Care Data off-shoring and the use of public cloud services. (https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/nhs-and-social-care-data-off-shoring-and-the-use-of-public-cloud-services - Accessed 4th January, 2019)

Rimmer A. (2018) How Can I remain Professional on Social Media. BMJ, Careers, 2017;359:j5206 (https://www.bmj.com/content/359/bmj.j5206 Accessed 1st January, 2019)

Rimmer A. (2018) Doctors' use of Facebook, Twitter, and WhatsApp is the focus of 28 GMC investigations. BMJ 2017;358:j4099 https://www.bmj.com/content/358/bmj.j4099?ijkey=73f04235035f37ee75a8c7b3c5508d934ed5f04c&keytype2=tf_ipsecsha (Accessed 10th October, 2018)

Rimmer, A. (2017) Hidden risks your smartphone poses to your career. British Medical Journal, 2017;359:j4896, 26th October, 2017. (http://www.bmj.com/content/359/bmj.j4896 Accessed 19th September, 2018)

Royal College of Psychiatrists (2020) Digital COVID-19 guidance for clinicians. London: RCPsych, London. (https://www.rcpsych.ac.uk/about-us/responding-to-covid-19/responding-to-covid-19-guidance-for-clinicians/digital-covid-19-guidance-for-clinicians. Accessed 21st October 2021).

Royal College of General Practitioners (2013) Social media highway code. RCGP.org.uk (http://www.rcgp.org.uk/social-media– accessed 20th December, 2018)

Walters S., Owen G. Adams S. (2015) Dirty tricks of militant strike doctors: Junior medics' cynical attempt to plunge NHS into crisis with mass walkout revealed in secret Facebook group The Daily Mail. 8th November, 2015. (**https://www.dailymail.co.uk/news/article-3308808/Junior-medics-cynical-attempt-plunge-NHS-crisis-mass-walkout-revealed-secret-Facebook-group.html** - accessed 20th November 2019)

REFERENCE LIST

1. Chan WS, Leung AY. Use of Social Network Sites for Communication Among Health Professionals: Systematic Review. Journal of medical Internet research. 2018;20(3):e117.
2. Barrios V, Cosı´n-Sales, J., Bravo, M., Escobar, C., Gamez, J.M., Huelmos, A., Cortes, C.O., Egocheaga, I., Garcı´a-Pinilla, J.M., Jimenez-Candil, J., Lo´pez-de-Sa´, E., Llergo, J.T., Obaya, J.C., Pallares-Carratala´, V., Sanmartın, M., Vidal-Perez, R., Cequier, A. Telemedicine consultation for the clinical cardiologists in the era of COVID-19: present and future. Consensus document of the Spanish Society of Cardiology. Rev Esp Cardiol. 2020:9.
3. Stevenson A. Oxford dictionary of English: Oxford University Press, USA; 2010.
4. Gabbard GO. Digital Professionalism. Acad Psychiatry. 2019;43(3):259-63.
5. McLoughlin J, Zijlstra-Shaw S, Davies J, Field J. The graduating European dentist—Domain I: professionalism. European Journal of Dental Education. 2017;21:11-3.
6. Drake TM, Claireaux HA, Khatri C, Chapman SJ. WhatsApp with patient data transmitted via instant messaging? Am J Surg. 2016;211(1):300-1.
7. Rimmer A. Doctors' use of Facebook, Twitter, and WhatsApp is the focus of 28 GMC investigations. The BMJ. 2017;358(j4099).
8. Rimmer A. Can I receive and store images sent from patients during remote consultations? The BMJ. 2020;370(m2675):2.
9. Regulation (EU) 2016/679 of the European Parliament and The Council of the European Union of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 216/679 (2016).
10. GMC. Doctors' use of social media. London: GMC; 2013.
11. GMC. Good Medical Practice, Working with doctors Working for patients. London: GMC; 2013.
12. Rath T. Strengths Finder 2.0. New York: Gallup Press; 2007.
13. MDU. Using Social Media. Advice for maintaining professional integrity and boundaries on social media. London: Medical Defence Union; 2020.
14. John B. Are you ready for General Data Protection Regulation? The BMJ. 2018;360(k941):2.
15. C. H. Working from Home advice [Web page]. Oxford: Oxford.ac.uk; 2020 [updated Thursday 19th march at 16.00; cited 2022 10th January, 2022]. Available from: https://www.infosec.ox.ac.uk/article/working-from-home-advice.
16. Rimmer A. How can I remain professional on social media? BMJ. 2017;359(j5206).
17. IMO. Irish Medical Organisation Annual Report 2018. 2019 March 29th 2019.
18. Walters S, Owen, G., Adams, S. Dirty tricks of militant strike doctors: Junior medics' cynical attempt to plunge NHS into crisis with mass walkout revealed in secret Facebook group. The Mail on Sunday. 2015 8th November 2015.
19. Chan WSY, Leung, A.Y.M. Use of Social Network Sites for Communication Among Health Professionals: Systematic Review. Journal of Medical Internet Research. 2018;20(3):12.

20. ESR. The new EU General Data Protection Regulation: what the radiologist should know. Insights Imaging. 2017;8:5.
21. BMA. Social media, ethics and professionalism, BMA guidance. London: BMA.org.uk; 2018.
22. BMA. Ethics of social media use London: BMA.org.uk; 2020 [updated 8th September 2020. Available from: https://www.bma.org.uk/advice-and-support/ethics/personal-ethics/ethics-of-social-media-use.
23. BMA. Social media, Practical guidance and best practice. London: BMA.org.uk; 2020.
24. RCPsych. Social Media Staff and Members Policy: May 2020. London: RCPsych; 2020.
25. RCGP. Social media highway code. RCGP; 2013.
26. Toussaint PJ, Coiera E. Supporting communication in health care. International journal of medical informatics. 2005;74(10):779.
27. Martin G, Janardhanan P, Withers T, Gupta S. Mobile revolution: a requiem for bleeps? Postgrad Med J. 2016;92(1091):493-6.
28. Gould G, Nilforooshan, R., . WhatsApp Doc? British Medical Journal. 2016;2:109-10.
29. Control CfD. Health Insurance Portability and Accountability Act of 1996 (HIPAA) USA: CDC.gov; 1996 [Available from: https://www.cdc.gov/phlp/publications/topic/hipaa.html.
30. Johnston MJ, King, D., Arora, S., Behar, N., Athanasiou, T., Sevdalis, N., Darzi, A.,. Smartphones let surgeons know WhatsApp: an analysis of communication in emergency surgical teams. The American Journal of Surgery. 2015;209:45-51.
31. Mobasheri MH, King D, Johnston M, Gautama S, Purkayastha S, Darzi A. The ownership and clinical use of smartphones by doctors and nurses in the UK: a multicentre survey study. BMJ Innovations. 2015;1(4):174-81.
32. O'Sullivan DM, O'Sullivan E, O'Connor M, Lyons D, McManus J. WhatsApp doc? BMJ Innovations. 2017;3(4):238-9.
33. Kamel-Boulos MN, Guistini, D.M., Wheeler, S. Instagram and WhatsApp in Health and Healthcare: An Overview. Future Internet. 2016;8(37):14.
34. Mistry K. Information governance considerations for staff on the use of instant messaging software in acute clinical settings: NHS England; 2018 [updated 09.11.18. NHS England Publications Gateway Reference: 08496].
35. Bloomberg. WhatsApp, Snapchat Banned on Company Devices at Continental. Windows IT Pro (Online) Chicago. 2018 June 6, 2018.
36. NHSX. COVID-19 IG advice [web page]. United Kingdom: National health Service, Digital; 2020 [Guidance for patients and service users; Information governance advice for NHS staff]. Available from: https://www.nhsx.nhs.uk/information-governance/guidance/covid...
37. RCPsych. Digital COVID-19 guidance for clinicians London: RCPsych; 2020 [updated 21st May 2020. Available from: https://www.rcpsych.ac.uk/about-us/responding-to-covid-19/responding-to-covid-19-guidance-for-clinicians/digital-covid-19-guidance-for-clinicians.
38. GDPR, Lawful basis for processing, Article 6 (2021).
39. Special Category Data, GDPR, Article 9, Article 9 (2021).
40. Copyright, Designs and Patents Act 1988. Sect. Part 1, Chapter 111, Education, Section 32 (1988).
41. JISC. The Little Guide to Copyright. In: www.jiscdigitalmedia.ac.uk, editor. 1 ed. London: JISC; 2016. p. 2.

APPENDIX 1. Some suggestions for journalists to follow on Twitter (at the time of publication) include:

- Hugh Pym, @bbcHughPym – BBC News Health Editor covering all aspects of health (UK and Global). Politics and economics of the NHS
- Laura Donnelly - @lauradonnlee - Health Editor of The Telegraph
- Denis Campbell @denis-campbell, Guardian and Observer health writer
- Slavea Chankova @SlaveaChankova - Health Correspondent, The Economist.com
- Shaun Lintern @ShaunLintern – Health Correspondent at The Independent

It can equally be useful to follow the Twitter accounts of journalists or editors of specialist scholarly publications and journals you would like to contribute to. For example:

- Fiona Godlee @fgodlee – Editor in Chief, the BMJ
- Rebecca Coombes @rebeccacoombes Medical Journalist, head of news and Views, the BMJ
- Richard Hurley @rich_hurley – Features and debates editor at the BMJ

Suggested potential Twitter account or role models for clinicians to follow in your area of expertise via Twitter could include:

- Wendy Burn @wendyburn – Past President Royal College of Psychiatrists, Consultant Psychiatrist
- Anthony David @ProfTonyDavid - Director of UCL Institute of Mental Health
- Michael Farrell @MichaelFarrellE - Professor and Addiction Scientist, Director of Drug and Alcohol Research Centre, Australia

- Ian Hickie @ian_hickie - Co-Director of the Brain and Mind Centre at the University of Sydney, Australia
- Keith Humphreys @KeithNHumphreys - Prof at Stanford California, Public Policy Advisor and writer at Washington Post
- Dr Kate Lovett @DrKateLovett – President, Lead for recruitment, Past Dean Royal College of Psychiatrists, Consultant Psychiatrist
- Geraldine Strathdee @DrG_NHS - Former National Clinical Director, mental health England
- Simon Wessely @WesselyS – Director of Kings Centre for Military Health Research, Kings College London, past president of Royal College of Psychiatrists
- Jenny Drife @DrifeJenny - Psychiatrist working with rough sleepers in South London
- Ben Goldacre @bengoldacre, Academic and Science Author (Bad Science and Bad Pharma), Senior Clinical Research Fellow, Scientist, Physician, popular "stats geek" – Oxford
- Matthew Hotopf @MatthewHotopf Mental health researcher and psychiatrist at King's College Institute of Psychiatry, Psychology and Neurosciences. Director of the National Institute for health Research, Maudsley Biomedical Research Centre
- Carmine M. Pariante - @ParianteLab, The Institute of Psychiatry, Psychology and Neurosciences at Kings College London. Psychiatrist & researcher @SPILabKCL. Writer & Editor @inspirethemind @BrainBehavImm, @BBI_Health. President @ISPNE
- Psychiatric Trainees Committee @RCPsychTrainees
- Royal College of Psychiatrists @RCPsych
- Individual RCPsych faculty accounts as these are starting to look really interesting - eg @RCPsychOldAge

A Twitter hashtag to search and be aware of:

- #ChoosePsychiatry – for information and dialogue about careers

The Mental Elf (www.nationalelfservice.net) – website and blog for mental health research and guidance. Summaries that highlight evidence-based publications relevant to mental health practice in the UK and further afield.

APPENDIX 3 PAPER 2

Journal of Dentistry 122 (2022) 104112

Contents lists available at ScienceDirect

Journal of Dentistry

journal homepage: www.elsevier.com/locate/jdent

Smartphone technology for communications between clinicians – A scoping review

Bernadette John *, Christine McCreary, Anthony Roberts

Cork University Dental School & Hospital, University College Cork, Wilton, Cork, Ireland

ARTICLE INFO

Edited by: C.D. Lynch

Keywords:
Smartphone
Clinical communication
Whatsapp
Apps
Instant messaging

ABSTRACT

Objectives: This scoping review aims to review explore, assess, and map the literature to inform clinical practice regarding communication between clinicians. Specific Apps/channels used were identified and assessed with a focus on data security with key concepts and knowledge gaps identified.

Data: The Joanna Briggs Institute framework is followed, with search results reported as per the *PRISMA ScR for scoping reviews* guidelines.

Sources: A systematic search strategy encompassing EBSCO and OneSearch databases was conducted - two identical searches, (June and October 2020) limited to English language articles published 2016–2020. A narrative synthesis was used to integrate and report the findings.

Study selection: Sixty-six publications were selected. Twelve from EBSCO, thirty-five from OneSearch, nineteen were hand searched. Sixteen of the publications were research studies, nine were literature reviews, twenty-six were editorial, one was a newspaper article and fourteen were grey literature. Instant Messaging (40%, $n = 23$), image sharing (41%, $n = 24$), and video conferencing (19%, $n = 11$) were functions most popular with clinicians. WhatsApp, generic instant messaging, Facebook messenger, ZOOM, and Skype are evidenced as channels for communication between clinicians within the EU. A sizeable proportion of the publications (38%; $n = 25$) failed to identify or adequately address technical security concerns and requirements around privacy and data protection.

Conclusions: Clinicians use smartphones /Apps to communicate clinical information with each other. The security and privacy issues arising from their communication of sensitive data is absent or only superficially acknowledged within the literature.

Clinical significance: Clinician's need clearer guidance on the use of smartphone technology for clinical communications.

1. Introduction

There is growing international concern around the use of digital modalities for clinical communication [1–23]. A systematic review of the utilisation of Social Networking Sites for communication amongst health professionals in frontline clinical practice by Chan and Leung [1] is one example of such concern. Conducted prior to the strict stipulations required for General Data Protection Regulation (GDPR) [24], this international study clearly identifies limitations around technical insight, risks to the protection of sensitive data, professionalism and liability posed by the use of popular consumer digital communications channels. The education and training of health professionals and the necessity for policy were identified as areas of importance for future research.

GDPR came into force across the EU on the 25th May 2018, following a two year "run-in" preparation period, to safeguard data privacy. This regulation increased obligations for organisations that process personal data within member states. Health Information is considered to be the most confidential of all types of personal information [25] and organisations that process personal data are required to adopt significant new technical and organisational measures to demonstrate their GDPR compliance. Data subjects (all individuals within the EU) gained a raft of new legal rights regarding the processing of their data including the right of access, the right of rectification, the right to erasure, the right to restrict processing and the right to object to their data being processed [26].

The COVID-19 pandemic has heightened the urgency for digital

* Corresponding author.
E-mail address: 118225957@umail.ucc.ie (B. John).

https://doi.org/10.1016/j.jdent.2022.104112
Received 2 February 2022; Received in revised form 21 March 2022; Accepted 25 March 2022
Available online 10 April 2022
0300-5712/© 2022 The Author(s). Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

solutions to aid remote consultation and communication [27] for the benefit of patient care and evidently has expedited the adoption of smartphone technology [28]. Concerns are intensifying, that current clinical communications practice has the potential to compromise data privacy and data protection with smartphones, popular Apps and social media - technology that commodifies patient data [10,11,16,29,30]. The acquisition of patient data is possible through a variety of current advertising technologies including tracking and data profiling, analytics, location data, third party sharing of data, data brokers, surveillance technology and networked devices. These have the potential to violate privacy regulations and legislation including GDPR and the European Convention of Human Rights [31]. De Benedictis et al. [3] speculated that the use of WhatsApp in healthcare may represent an extreme version of "backdoor adoption" which occurs when easy and familiar technology is embraced to meet a requirement. Unfortunately, this adoption is often without the appropriate formal approval or assessment from senior healthcare or IT management regarding the opportunities and risks that these innovations might bring along with them. The requirements for appropriate policy, technical evaluation and risk assessment should not be ignored.

In order to map existing literature and emerging evidence in this broad area and to clarify key concepts, identify gaps in the knowledge and guide future research and policy, a scoping review was identified as the 'next logical step' [32] and is the focus of this study.

It was anticipated that for this scoping review to be effective, it would be necessary to draw upon the full range of published literature, from quantitative research (surveys to establish the prevalence of smartphone and App use), qualitative studies (used to discover any problems with the specific technologies), to policies, editorial and press articles, including a range of outlets, from academic literature to Health Service policy and general press outlets, across the full range of clinical practice, in order to generate evidence that is relevant to the current practice of dentistry.

2. Methods

2.1. Overview

A scoping review protocol was developed guided by the Joanna Briggs Institute framework (JBI)(32). Thus, an overview of the literature was mapped to address the broad research questions. A data extraction (selection and coding) protocol was developed around PICO (Population/Intervention or exposure/Comparator/Outcome).

2.2. Objectives and research questions

For the purpose and objectives of this review the questions asked were: What are the common smartphone functionalities being used by clinicians in Europe to communicate sensitive patient data at present? What specific consumer Apps/channels are used most by clinicians for clinical communications? Are security issues acknowledged, explored, and appropriately mitigated for in relation to the consumer channels being used, with a specific focus on GDPR compliance?

2.3. Identifying relevant studies and eligibility criteria

Publications in the English language since 2016 were reviewed as most trade publications and grey literature on technology uses the English Language. Translating publications through Google translate was deemed not to be satisfactory as it translates literally and can miss nuances. Research studies, literature reviews, press releases, newspaper articles, editorial in journals and grey literature including government and health service policy papers were all included.

2.4. Eligibility criteria

Articles were included if they if they had content on clinical communication, clinical consultation or general clinical communications via consumer Apps, or social media. Papers were included if they raised issues relevant for patient privacy, patient data, GDPR, Data protection and Data compliance using consumer digital channels. The focus of this study was communication between clinicians and as such, papers were excluded if they were concerned with communication between clinicians and patients. No effort was made to include only papers that concerned communications between dental clinicians, as it was felt that this would be too restrictive and was unlikely to generate enough evidence.

Although the purpose of this study is focussed on the use of consumer social media and Apps within the EU, their functionality is identical worldwide and the issues around their implementation by clinicians are global. For this reason, it was planned *a priori* to include international papers.

As 2016 was the year when the two-year run-in period for the implementation of GDPR commenced, only papers published from 2016 were included in the search. Searching older publications would not have provided the appropriate currency for this study. Platforms, functionality, and the digital landscape is evolving so quickly that a recent and focussed time interval was important to achieve relevance. A very small number of policy documents could be included outside this date range if nothing more recent, that still appears to be informing current clinical practice could not be identified.

2.5. Evidence searches

Search results are reported as per the *Preferred Reporting Items for Systematic Reviews and Meta-Analyses extension (PRISMA ScR) for scoping reviews* guidelines (see Appendix Table A1.). Comprehensive literature searches were conducted following consultation with Anita Wilcox, an expert information specialist.

The OneSearch discovery system (a search of approximately 200 databases including ProQuest databases, EBSCO databases including

Table A1
PRISMA SCr review checklist.

IDENTIFY THE REPORT AS A SCOPING REVIEW		
TITLE	1.	Title Yes
ABSTRACT	2.	Structured summary Yes
INTRODUCTION	3.	Rationale Yes
4.	Objectives Yes	
METHODS	5.	Protocol and registration N/A
6.	Eligibility criteria Yes	
7.	Information sources Yes	
8.	Search Yes	
9.	Selection of sources of evidence Yes	
10.	Data charting process Yes	
11.	Data items Yes	
12.	Critical appraisal of individual sources of evidence N/A	
13.	Synthesis of results	
RESULTS	14.	Selection of sources of evidence Yes
15.	Characteristics of sources of evidence Yes	
16.	Critical appraisal within sources of evidence N/A	
17.	Results of individual sources of evidence Yes	
18.	Synthesis of results Yes	
DISCUSSION	19.	Summary of evidence Yes
20.	Limitations Yes	
21.	Conclusions Yes	
FUNDING	22.	Funding Yes N/A

Business Source Complete, CINAHL, Science Direct, JStor, IEEE, BMJ, Nature, Royal Society of Chemistry, and many more, simultaneously for information which eliminates the need to hand search all of them individually). EBSCO was additionally hand searched specifically because OneSearch includes articles from peer reviewed journals, not trade/commercial publications, or grey literature in EBSCO. A systematic search strategy within these two system/databases was conducted and individual journal titles were included if they were deemed relevant to the project (e.g., the Journal of Dentistry). Hand searches were also conducted to identify substantive or scholarly information that has not been formally peer-reviewed or published. The full search was performed twice (once on 24th June 2020, and once again on 20th October 2020); thus, ensuring all possible new publications and current content on this fast-moving topic were included.

Databases were searched with subsequent search terms:

OneSearch - Zoom OR WhatsApp OR patient data OR patient privacy keywords used in a basic search. OneSearch (2nd search); use of smartphone OR Zoom OR WhatsApp AND patient privacy OR health data at risk. Limiters selected were Medicine, Public Health, Nursing, Computer Science and Law.

As OneSearch Discovery system or search engine also searches EBSCO databases, a different search string was utilised in searching the database separately to establish if it were possible to capture anything new. For example, if Covid 19 was used with OneSearch it could have eliminated the articles without that word, and some very good, relevant articles would have been missed.

No limiter was used in the initial basic search of OneSearch. The abstracts of 1000 results were read, and articles were selected according to our inclusion criteria. Subsequently limiters used included Conference Proceedings, Trade Publication Articles, Data Sets, Journal Articles, Magazine Articles and Newspaper Articles. Date limitations were applied as described above.

For the first EBSCO search - Zoom, video communications, impact, COVID-19 OR clinical consultation OR (patient, data security and privacy) were used. Expanders - equivalent subjects Search modes were applied - Boolean/Phrase For EBSCO. For the second EBSCO search - Zoom OR Skype OR social network* OR WhatsApp OR clinical communication OR communication Apps OR patient privacy OR GDPR or general data protection regulation OR patient data. Limiter used: Published Date: 2016–2021.

For both EBSCO and OneSearch the results were displayed by relevance. Hence, it was accepted that these are the most relevant to the topic. The OneSearch Discovery system displays only 1000 items per search. Also, although EBSCO saves all the searches, it does not indicate which search yielded the most articles. It is therefore assumed that if the system ranked the results by relevance, one would find the appropriate articles within the displayed results.

2.6. Selecting the evidence

All references identified on the databases listed in the search strategy were uploaded to reference management software (EndNote X9). Any duplicates were identified and removed.

Eligibility and relevance of the papers were assessed and confirmed in two phases:

1 In the first phase, titles and abstracts were examined by one reviewer, before the full texts of the articles were downloaded and identified as being potentially eligible using the pre-set inclusion and exclusion criteria. These articles were then screened to confirm their eligibility
2 In the second phase, any doubts surrounding inclusion of a paper were discussed and agreed with the second reviewer.

2.7. Data extraction

All articles selected had data extracted on their characteristics by a single reviewer, charted on a Microsoft Excel spreadsheet (See Appendix Table A2) standardised for final inclusion in the Scoping review. Articles were coded by the following characteristics: Subject concerning clinical communications, author, year, book title, journal title, classification of publication (study, literature review, press release, newspaper article, general information article in journal, grey literature including government papers), title of article, main concept of article, which functionality the article concerns, the specific consumer smartphone channel being discussed, and if the article concerns EU or Non-EU communications. The evaluation of the literature was further coded and grouped into those publications that were mitigated for technical security concerns accurately, including the requirements of data protection and GDPR, and those that did not.

One characteristic of scoping reviews of note is that a formal assessment of research methodological quality of the included studies is generally not performed. This is because a scoping review is designed to provide an overview of the existing evidence base regardless of quality [32].

2.8. Synthesis of results

The broad nature of this scoping review and the heterogeneity of the included publications made meta-analysis impossible. Full-text PDF articles were downloaded, individually uploaded into Endnote, and then imported into NVIVO qualitative data analysis software with the full text available for qualitative syntheses. NVIVO enabled the visualisation of data, the processing, analysis, and summarisation of text in relation to (I) the functionality being used for current clinical communications practice, (II) the specific consumer smartphone channels being used, (III) whether security concerns had been mitigated for, and (IV) the technical compliance with GDPR. The articles were evaluated for the quality of the content they contained and were grouped into categories as follows:

Positive content: An indication of a high level of technical understanding concerning the modality being described and/or fluency with the legal issues posed by such channels.

Negative content: Content that gives rise to debate or disagreement or controversy. Further, content that indicated superficial or outdated understanding of technical issues posed for data privacy regarding current smartphone and App technology and regulations, such as GDPR.

A narrative qualitative synthesis of the findings was then conducted from the selected publications.

2.9. Risk of bias (quality) assessment

The relevance and eligibility of the articles included in this review were assessed and critically appraised by one reviewer before being scrutinised and confirmed by a second reviewer, risk of bias was not applicable as this is a scoping review.

3. Results

3.1. Study selection

The first search of the OneSearch database search yielded 15 papers, the second search of OneSearch yielded 44 papers, a total of 59 papers combined. A first search of EBSCO resulted in 25 papers and a second yielded 24–49 in total from EBSCO. The first-hand search yielded 31 papers and the second 36, 67 papers in total. 175 papers from all searches identified by OneSearch, EBSCO database and hand searching, respectively (Fig. 1). After removal of 47 duplicates, 128 records were screened, and 38 records excluded based on not meeting the eligibility criteria. A total of 90 full text articles were assessed for eligibility.

Table A2
Data extraction microsoft excel spreadsheet.

Search Type	Included in CLINICAL COMMS	Negative/Positive	Authors	Year	Book	Title	Journal Title	Study	Literature Review	Press Release	Newspaper article	General information article in journal	Grey Literature (including governmental papers)	Title	MAIN CONCEPT 1 - Functionality required for current clinical Communications in healthcare?	MAIN CONCEPT 2 - Smartphone Channel being used	MAIN CONCEPT 3 - Technical insight & compliance with GDPR	MAIN CONCEPT 4 - Ethics EU
OneSearch1	Y	Negative	Markeland (2017)	2017	0	0		0		0	0	0	n	(Zoom Launches Industry's First Scalable Cloud-Based Video Telehealth Solution; Video Communication Providers Have Temporarily Waived Business Solution Integration	Video consultation software for telehealth		ZOOM	NO	NON EU, Canada
OneSearch1	Y	Positive	Watson et al. (2016)	2016	0	The American Journal of Surgery		0		0	0	0	n	A response to an article - "Ensuring safe communication in healthcare: a response to 'Smartphones in surgery' and 'Smartphones in surgeons know whatsapp: an analysis of smartphone adoption in emergency surgical teams'	Instant messaging among surgical clinicians		Whatsapp	NO	EU NO/UK/HIH, UK, but published in a USA journal
OneSearch1	Y	Positive	Mosko, A. 2018	2018	0	JMIR Medical Informatics		X		0	0	0	0	The use of communication apps by medical staff in the australian health care system: Survey study on prevalence and use	Communication Apps		Whatsapp	NO, BUT LEGAL COMPLIANCE AND PRIVACY ISSUES ACKNOWLEDGED	NON EU, Australia
OneSearch1	N	Positive	Gamon L. (2018)	2018	0	0		0		0	0	0	X X	Whatsapp seeks to comply with Europes Privacy Rules	Not successfully clinical, but security of instant messaging		Whatsapp	Whatsapp signed 'an undertaking' to not share data with Facebook. This was prior to implementation of GDPR. Therefore Whatsapp was not GDPR compliant	Relevant to all in EU
OneSearch1	Y	Positive	John B. (2018)	2018	0	Wiki		X		0	0	X X		Are you ready for General Data Protection Regulation?	Yes, communications in healthcare		Whatsapp, dropbox, instant messaging, (another comment, happily, none chosen, thankfulness, info and cute)	Yes - issues posed by GDPR for the use of comms apps discussed	Relevant to all in EU
OneSearch1	Y	Positive	Chen, W.S.Y., & Leung 2016	2016	0	Journal of Medical Internet Research		X	X		0	0	X	Use of social network sites for communication among health professionals: systematic review	Yes, communications in healthcare		Social Networking Sites	Risks to data protection acknowledged	Non EU - Hong Kong
OneSearch1	N	Positive	Mosawi I. (2020)	2020	0	American Journal of Nursing Reserch		X		X	0	X X		Are Patient Privacy and Health Information Confidentiality Between Nurses and Patients and Health Systems Challenge Privacy Expectations and Laws	Non communications channels specifically		Telehealth/google companies etc	MENTIONS AMR ACKNOWLEDGES GDPR	NON EU - USA
OneSearch1	FAILED	Negative	El Hadidy et al. (2017)	2017	0	Irish Journal of Medical Science		X		0	0	0	0	Smartphones in clinical practice: students' experience of two Dutch Paediatric teaching hospitals	Clinical Comms - Medics		Medical Apps, Whatsapp,	Not mentioned	EU - Ireland
OneSearch1	N	Positive	Mehta, I. (2020)	2020	0	ThinkerMike.com		X		0	0	0	X X	Don't believe Zoom 'its video calls are not encrypted and be safe	Universal - not clinical comms specifically		Zoom	Not mentioned	EU - Ireland
OneSearch1	Y	Positive	Dalfiandola A. R. et	2016	0	Plos One		X		0	0	0	0	Whatsapp in hospital? An empirical investigation of individual perceptions and behavioral characteristics of use	Nurses and physicians		Whatsapp	Not mentioned specifically, although mentions that data privacy protection issues acknowledged	EU - Italy
OneSearch2	Y	NEGATIVE	Gould, D. & Hothersall (2018)	0	0	BMJ Innovations, 01/2018, Volume 0, Issue 0		X	0	0	0	0	0	WhatsApp Ouch!	Doesn't really concern itself at all with data protection or privacy and states that doctors will continue to use routes of communication that are more efficient and useful.	UK			0
OneSearch2	Y	NEGATIVE	Elliott, P. (2017)	2017	0	(Palo Alto, CA), Hamlet 7, Volume 9, Issue 3		X	0	0	0	0	0	The Use of WhatsApp Smartphone Messaging as an Orthopaedic Clinical Adjunctive Tool for Telemedicine: An Overview	No. Says whatsapp is easy, inexpensive and intrusion 'only when you want it to be' - so information handled arrangement to doesn't get	Web		Totally ignores the GDPR issues raised by the use of Whatsapp	0
OneSearch2	Y	NEGATIVE	Giordano V. et al. (2017)	2017	0	Interactive journal of medical research, 07/2017, Volume 6, Issue 2		X	0	0	0	0	0	WhatsApp Messenger as an Adjunctive Tool for Telemedicine: An Overview	Totally ignores issues around security of data	Read		ARTICLE TOTALLY IGNORES PRIVACY AND GDPR ISSUES SPECIFICALLY - FIRST FOR GDPR WAS 2 YEARS PRIOR TO MAY 2018	0
OneSearch2	Y	POSITIVE	Mosom, M. et al. (2020)	2020	0	Internet and emergency medicine, 01/2020, Volume 15, Issue 2		X	0	0	0	X	0	WhatsApp and other messaging apps in medicine: opportunities and risks	Absolutely spells out that Whatsapp is not gdpr compliant.	Italy		Included as relevant	0

(continued on next page)

Table A2 (*continued*)

OneSearch2	Y	POSITIVE	Hawkes, N. (2018)	2018	0	BMJ, 03/2018, Volume 360		X	0	0	0	X	0	Study records on WhatsApp	Yes, specifically	UK		Included as deemed relevant	0
OneSearch2	Y	NEGATIVE	Gulacti (2018)	2018	0	Journal of medical systems, 04/2018, Volume 42, Issue 6		X	0	0	0	0	0	An Analysis of WhatsApp Usage for Communication Between Consulting and Resigning Physicians	No. Totally ignores issues around privacy of data	Turkey		THIS 2018 ARTICLE IS FROM TURKEY AND TOTALLY IGNORES ISSUES SURROUNDING THE USE OF WHATSAPP	0
OneSearch2	Y	NEGATIVE	Bleck, L. Et al. (2003)	2020	0	Encephalomyelitidis/ence, 05/2003, Volume 51		X	0	0	0	0	0	Reactions and countermeasures of medical oncologists towards the Mobile messaging with patients	No mention at all of data security	Italy		Included as deemed relevant	0
OneSearch2	N	POSITIVE	Martinengo (2020)	2020	0	BMJ, 03/2020, Volume 368		X	0	0	0	0	0		Some good advice around maintaining privacy and the chromic adhering to data protection laws, recommending set name+locations in patients notes and identifying scope of use - but addressed in channel before it is commenced	Singapore, Hong Kong and Imperial College London, UK	Yes		0
OneSearch2	Y	POSITIVE	Kara, O. (2020)	2020	0	Journal of medical systems, 02/2020, Volume 44, Issue 4		X	0	0	0	X	0	Secure Instant Messaging Application in Prenatal Care	1928 grading time as an alternative to whatsapp	Israel		0	0
OneSearch2	N	POSITIVE	Fasoulakis, M. (2020)	2020	0	International journal of environmental		X	X	0	0	0	0	Big Data and Digitalization in Dentistry: A Systematic Review of the Ethical Issues	Data security issues raised continuously throughout this study	Sweden	No		0
OneSearch2	Y	NEGATIVE	ESR (2018)	2018	0	Insights into Imaging, 04/2018, Volume 9, Issue 2		X	0	0	0	X	0	Business aspects of the European Society of Radiology's (ESR) position on the proper use of mobile devices in radiology	It just mentions that security is an issue with no acknowledged / Whatsapp involvement	European	0		0
OneSearch2	N	POSITIVE	Spencer, A. & Patel, R.(2016)	2016	0	Nursing management (Harrow, London, England), 01/2016, Volume 23, Issue 1		X	0	0	0	X	0	Applying the Data Protection Act 2018 and General Data Protection Regulation principles in healthcare settings	Explanation of GDPR as applied to specific cases, but none clinical comms using a smartphone	UK and Ireland	0		0
OneSearch2	Y	POSITIVE	Jain, H. K. (2016)	2016	0	Indian Journal of Disease in Education, 12/2016, Volume 194, Issue 12		X	0	0	0	X	0	Mobile device and app use in pandemic emergency care: a survey of attitudes and practice in the UK and Ireland	Point is not that the NHS approved the use of communications, but seems during emergency....this study looks to measure harm caused by such apps - but that may not be evidenced yet.	Ireland	0		0
OneSearch2	Y	POSITIVE	Rosner A. (2020)	2020	0	BMJ, 07/2020, Volume 370		X	0	0	0	X	0	Can I receive and store clinical images on my mobile device using secure messaging?	Yes	UK		0	0
OneSearch2	Y	POSITIVE	Nanji, K. (2017)	2017	0	International Low Flows, 04/2017		X	0	0	0	X	0	Managing Big Data Privacy and Security	Relevant to Healthcare in general, internationally with specific advice for the EU	Canada, USA, Brazil,	0		0
OneSearch2	Y	POSITIVE	Akubar, K. (2017)	2017	0	Imaging & Therapy Practice, 05/2017		X	0	0	0	X	0	Getting Personal	Specifically mentions issues around obligations for clinicians with regard to data security, and the importance of to data and images sharing	UK	0		0
OneSearch2	Y	POSITIVE	RCN 2018	2018	0	Nursing Standard, 12/2018, Volume 32, Issue 30		X	0	0	0	0	0	Survey suggests widespread use of instant messaging apps to discuss patient care	This article states that many NHS employers have banned the use of WhatsApp, but are asking that nurses risk their registration by sharing confidential information on photos about patients without consent	UK	0		0
OneSearch2	Y	NEGATIVE	Ramchaeni, E. (2016)	2016	0	Journal of Digital Imaging, 08/2016, Volume 29, 483-487		X	0	0	0	0	0	Radiologists' usage of social media in practice: Results of the RANDOM survey	Mentions issues around risk to patient confidentiality and potential medicolegal implications	The Netherlands, USA, Belgium	0		0
OneSearch2	Y	NEGATIVE	Siegmund, L.A. (2020)	2020	0	Workplace health & safety, 08/2020, Volume 68, Issue 8		X	X	0	0	0	0	Social Media in Occupational Health Nursing: Helpful or Harmful? by Siegmund, Lisa Anne	outlines the functionality within whatsapp for example and ignores the risks to patient privacy it poses - specifically and deliberately breaking patient confidentiality as opposed to technical issues of compliance or functionality	UK		0	0

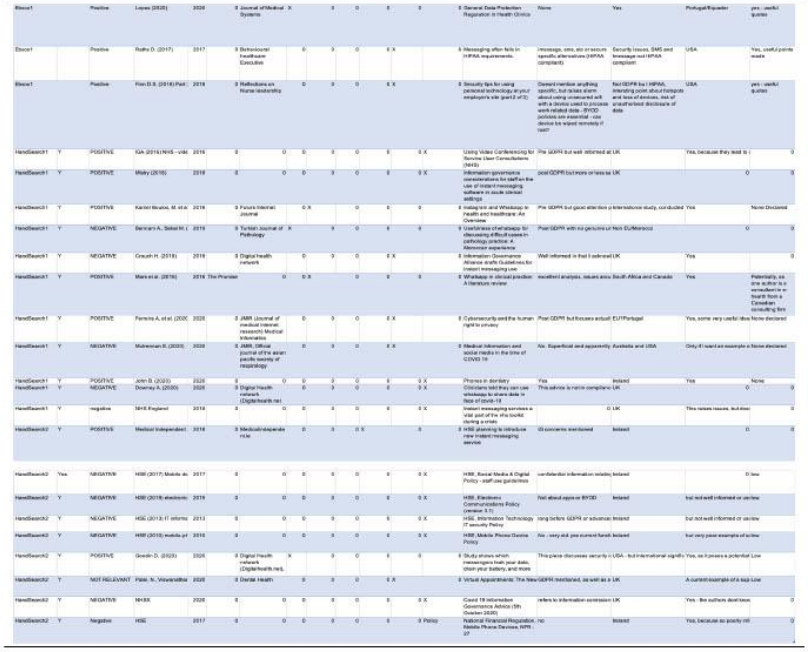
(continued on next page)

Table A2 (*continued*)



(*continued on next page*)

Table A2 (*continued*)



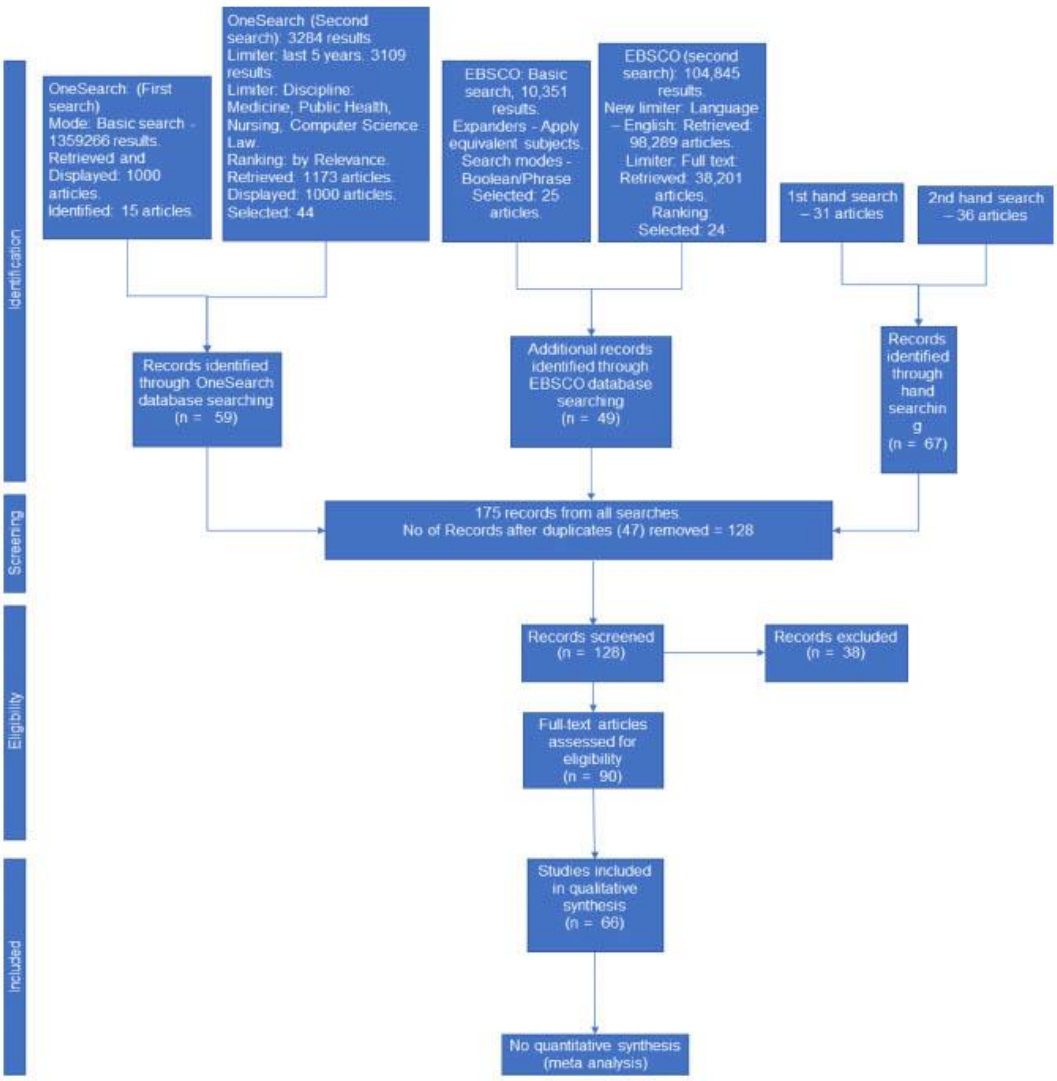


Fig. 1. Prisma 2009 Flow Diagram, RESULTS (June – Oct 2020).

Discussions with a second reviewer were undertaken when there was ambiguity whether to include (or exclude) papers with a final yield of 66 records included for the final qualitative synthesis. The 24 articles that were excluded at this point were found to be focused on a range of interesting but irrelevant areas, from the use of public social media platforms by clinicians for professional networking or medical education purposes, to the utilisation of consumer Apps for patient peer support, the information governance risks posed by hacked medical devices, the evolving risks within Apps and current statistics to be aware of regarding the use of specific consumer Apps such as WhatsApp.

Sixteen of the publications were studies, 9 were literature reviews, 26 were editorials, 1 was a newspaper article and 14 were grey literature. Seventeen publications were from the UK, ten were from Ireland, eight were from the USA and 7 were international collaborations. Four were from Italy, two were from Portugal, two were from Spain, three were collaborations within the EU and one was from Holland. The rest were from a variety of countries outside the EU, including Switzerland, Canada, Hong Kong, Australia, South Africa, Turkey, Israel, India, Morocco, and Turkey. Publications covered a range of clinical specialities, from primary care to paediatrics, radiology, oncology, orthopaedics, dermatology, obstetrics and gynaecology to cardiology, pathology, and emergency medicine. The disciplines of clinicians described as using smartphone technology and Apps for clinical communications were mainly doctors, but also included dentists and

nurses. Several papers included the generic term *clinicians*.

3.2. Themes

Three themes and two sub-themes were identified, based on the objectives and research questions.

3.2.1. Theme 1: smartphone functionality used by clinicians in Europe to communicate sensitive patient data

The most popular functionality for clinicians in the literature was evidenced as image sharing as described in 41% ($n = 24$) of the articles, closely followed by instant messaging at 40% ($n = 23$) and video conferencing with 19% ($n = 11$).

3.2.2. Theme 2: specific apps/channels are used most and are they compliant with the current GDPR policy and legislation

WhatsApp (owned by Facebook) was the consumer App most reported as popular with clinicians with 42% ($n = 33$) papers that named a specific channel, evidencing its use. WhatsApp is not compliant with current GDPR policy and legislation and its use raises a raft of privacy and technical data security concerns as evidenced in the literature [3,10–12,14–16,23,33]. Generic Instant Messaging (such as iMessage) was also extremely popular with 28% ($n = 22$) of the mentions of its use by clinicians, again, this functionality is not compliant with GDPR and raises concerns for data security [17,19,34]. Facebook Messenger was specifically named as used by 17% ($n = 13$) clinicians. This App, which is owned by Facebook, hosts its data in the USA and for that reason and various others, it is not deemed secure enough to be GDPR compliant. Video conferencing App Zoom was evidenced as popular in 8% ($n = 6$) of the papers that named a specific channel. The use of Zoom raises a range of security concerns is not GDPR compliant [35,36]. Skype was described as used in 5% of papers ($n = 4$). Skype also has been associated with a range of security issues and is not compliant with GDPR requirements or current legislation [23].

3.2.3. Theme 3: acknowledgement, exploration, and mitigation of security issues

A sizeable proportion of the publications around Smartphone and App use for clinical communications (37.87% ($n = 25/66$) [2,4,27,28,37–56] either fail to appropriately acknowledge, totally ignore, or mitigate for technical security concerns, including issues concerning data protection, from HIPAA (in the case of USA publications) to GDPR.

Each publication was categorised as either a 'Positive Publication' or a 'Negative Publication'. Content that was identified as Positive, including content that evidenced a high level of technical fluency, made up sixty two percent of the publications [1,3,5,7–12,14–23,26,29,30,33–36,57–68], with general information articles or editorial from journals making up most of these publications. Studies made up 19% ($n = 8$) of these well-informed papers published. 15% ($n = 6$) were literature reviews. 2% or 1 paper was a newspaper article. 49% ($n = 20$) were general information articles such as editorials in clinical journals. 15% ($n = 6$) of the positive publications around the use of these modalities were grey literature.

The timeline of material being published that was defined as Negative and did not mitigate for technical security concerns and/or the requirements of GDPR or contained controversial content from 2016 to 2020 is insightful (see Fig. 2). One paper was included from 2010 [55], and another from 2013 [54] as they were the only policies that could be found from the HSE that were intended to inform clinicians on their use of 'mobile phone' and information technology. These documents are currently available online and although they may have been well informed when published, some of the technology described and the content concerning it is obsolete and could be responsible for misleading current clinical practice. These documents contained information that were deemed both negative and positive but must currently be classified as Negative as it was published prior to the era of smartphones and the prolific popularity of Apps on Bring Your Own Device (BYOD) smartphones for clinical communications.

During 2016 and 2017 the predominance was for Negative content to be published, material that evidenced superficial understanding of the data protection or technical issues to be published, while well informed or Positive publications were largely silent. From 2018 this trend reversed, particularly in 2018 where there was a predominance of Positive, well-informed content, and content that demonstrated technical insight but nevertheless 12% ($n = 3$) of all poor advice recorded was also published in 2018. This is probably due to the heightened awareness of issues around data protection and data security due to the implementation of GDPR. Positive publications become sparse again in 2019 but in 2020, pandemic year, both types of publication proliferate again. Fifty-six percent ($n = 14$) of all the Negative quality material has been published since the implementation of GDPR. This is hugely significant, because when clinicians are under most pressure to use smartphone channels to facilitate efficiency and social distancing, the literature is providing conflicting information regarding the safety of the use of consumer Apps and smartphone functionality for clinical communications.

The following matrix (Fig. 3) illustrates the same information by year, content type and type of publication. In 2016 and 2017, poorly informed Negative content dominated, emanating exclusively from research Studies. In 2018, the year of Positive content, demonstrating technical insight, most emanates from general information articles in journals and grey literature. In 2019, and particularly 2020, Negative content once again emerges from general information articles, grey literature, literature reviews and studies, but these sources also published Positive content which all came once again from general information articles (editorials) in clinical journals in the main (Fig. 4).

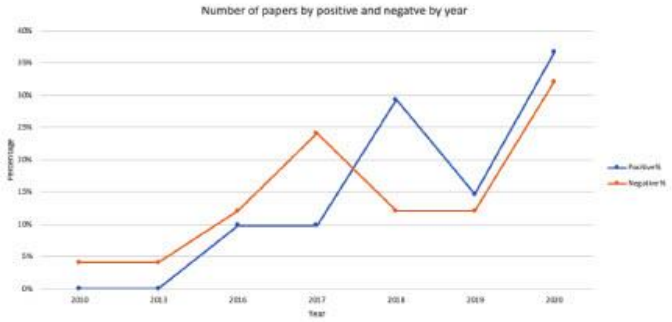


Fig. 2. Illustration of number of papers by positive and negative by year.

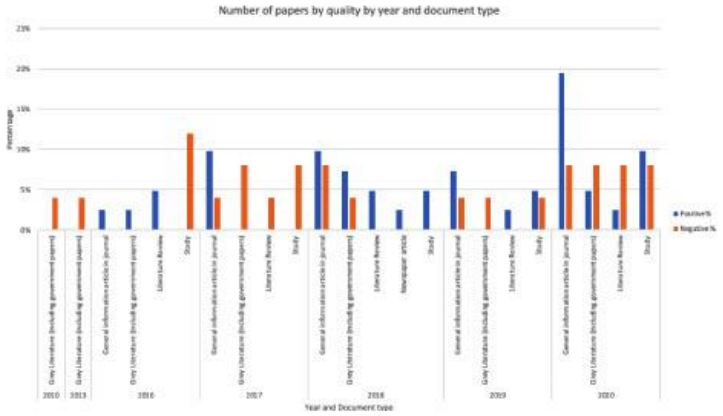


Fig. 3. Illustration of number of papers by year and document type.

Year	Sum of Positive	Sum of Negative	Positive%	Negative %
2010				
Grey Literature (including government papers)	0	1	0%	4%
2013				
Grey Literature (including government papers)	0	1	0%	4%
2016				
General information article in journal	1	0	2%	0%
Grey Literature (including government papers)	1	0	2%	0%
Literature Review	2	0	5%	0%
Study	0	3	0%	12%
2017				
General information article in journal	4	1	10%	4%
Grey Literature (including government papers)	0	2	0%	8%
Literature Review	0	1	0%	4%
Study	0	2	0%	8%
2018				
General information article in journal	4	2	10%	8%
Grey Literature (including government papers)	3	1	7%	4%
Literature Review	2	0	5%	0%
Newspaper article	1	0	2%	0%
Study	2	0	5%	0%
2019				
General information article in journal	3	1	7%	4%
Grey Literature (including government papers)	0	1	0%	4%
Literature Review	1	0	2%	0%
Study	2	1	5%	4%
2020				
General information article in journal	8	2	20%	8%
Grey Literature (including government papers)	2	2	5%	8%
Literature Review	1	2	2%	8%
Study	4	2	10%	8%
Grand Total	**41**	**25**	**100%**	**100%**

Fig. 4. Supporting data for number of papers by positive and negative.

4. Discussion

4.1. Summary of evidence

Image sharing [4,9,10,12–15,18,20,21,34,40,41,43,44,46,48,58,69,70], instant messaging [2,4,9,14,15,17–20,34,39–41,44,46,51,56,62,67,70–72] and video conferencing [1,2,4,9,14,15,17–20,34,39–41,44,46,51,56,62,67,70,72] are functions that are evidenced as popular and necessary for current clinical practice in general but may therefore be assumed to be of relevance to current dental practice specifically. Of significance here is the fact that if a Bring Your Own Device (BYOD) mobile phone is used to create a clinical image, it contains Exchangeable Image File Format (EXIF) data by default, from date and time to geographical co-ordinates where the image was taken. Any image created on a smartphone is also streamed by default to all of the networked devices associated with the smartphone (for example a smartwatch, tablet, laptop, and PC) via the cloud – in the case of the iCloud – this is located outside the EU and is not GDPR compliant. The processes required to anonymise and store a digital image securely requires a level of digital literacy that is not evident in many of the articles that describe the use of this functionality. If digital images are shared between clinicians via an instant messaging service such as WhatsApp, it is potentially downloaded by default into the image album on all the devices that receive it, and streamed to their networked devices, ultimately stored in

their insecure clouds also.

4.2. Popular consumer Apps for clinical communications

It is evident that WhatsApp, generic instant messaging, iMessage, Facebook Messenger, Zoom and Skype are extremely popular, perhaps even endemic consumer Apps, amongst healthcare professionals, despite concerns that the use of such modalities raise. The functionality offered by consumer Apps are paid for by allowing the developers to access and exploit the data on a device, and if these modalities are being used by clinicians for sensitive communications, they are being paid for by enabling the App owners to access sensitive patient data.

4.3. GDPR

The GDPR does not allow sensitive data of EU citizens to be stored on cloud located outside the EU. This regulation applies to all EU member states without the intervention of national parliaments. If a hospital or health system is faced with a request for access to personal data (Subject Access Request or SAR) they are obliged to produce the information so that data subject or patient can correct or delete it and it is mandatory therefor that health systems, such as the HSE or NHS know where and how data is stored. This requirement is currently impossible to comply with when clinicians use WhatsApp. Issues such as this are clearly described and articulated by some authors including Masoni & Guelfi [16] illustrating their well-informed insight.

The installation of most consumer Apps from WhatsApp, online calendars, Dropbox, to Google drive on any smartphone, allows the uploading of contact lists, images and messages to servers outside the EU [73] meaning that it is virtually impossible to comply with GDPR requirement for entities such as the HSE and NHS to be able to locate all of the data being processed on a patient if requested. The business model for consumer Apps is to collect, process and monetise data from their users. Masoni & Guelfi [16] state that WhatsApp is not GDPR compliant or indeed compliant with HIPAA in the USA. Some authors clearly articulate the mechanisms of consumer Apps, how companies data mine devices, monetise the data they contain, and the security issues Apps pose. Chen [35] describes a black box of company secrecy in his evaluation of Zoom and lists several steps that can be taken to improve privacy if no other channel is available.

A number of publications included in the review contain information that is open to dispute, could be termed as controversial and were therefor classified as Negative. NHSX [56] published advice online for clinicians around their use of messaging Apps such as WhatsApp, Facetime (owned by Apple) and Skype in November 2020, and this serves as a good example of this type of content. This publication stated that clinicians in the UK are free to adopt their BYOD to facilitate the use of video conferencing for consultations, home working and mobile messaging.

4.4. Consent for processing

Reassurances are provided regarding off the shelf tools from Skype to WhatsApp as acceptable to use, with the patient or service user *implying consent* by accepting an invitation and commencing the consultation. However, it can be argued that assuming consent from a patient to their data being shared by Apps like Zoom or WhatsApp, could be perceived as unlawful, if what we are asking patients to do is to allow the clinician to contract out of GDPR data protection obligations; in effect, asking patients to agree that they are not going to be subject to the law. Where this advice refers to consent, it is specifically consent to the nature of the consultation i.e., video rather than face-to-face, rather than (GDPR) consent for any aspect of the data processing. A data controller cannot evade their legal obligations by seeking to get the patient's consent. If the patient "consented" to opting out of the GDPR, that could not preclude the regulator from acting for a breach of the regulations as the requirements which must be met to achieve GDPR compatible consent are exacting.

Consent to engage in a remote consultation, even if it were GDPR compatible, is not the same as consent to the sharing of related data within the platform's insecure ecosystem. A patient's remedy for a breach would be under the GDPR, on the basis that the Controller cannot contract their way out of the obligations to the Data Subject. This advice was published, two years after the implementation of GDPR and four years after the two-year run-in period prior to the implementation of GDPR, to inform clinicians of the communications channels they could use during the COVID-19 Pandemic emergency. It states that the Information Commissioner has assured NHSX that she cannot envisage a situation where she would act against a health care professional trying to deliver care.

Two specific issues are troubling regarding the articulation of the ICO's position is in this document.

1 The advice is limited to regulatory action being taken by the ICO itself.
2 A context specific risk-based approach is taken i.e., the COVID-19 pandemic.

These are not clearly explained to the busy clinicians who may be drawing on this advice. Many medical and indeed dental consultations may relate to matters which have a significant impact on health and well-being and may involve life or limb threatening conditions where the absence of a consultation may result in genuine harm. This advice document specifically endorses consumer channels only *"where there is no practical alternative, and the benefits outweigh the risks"*. The advice contained in this document is relevant only for the duration of the current health emergency and is not a carte blanche to use these modalities for clinical communications.

Twenty-five papers are concerned more with the usefulness of the functionality available from smartphone Apps and BYOD and fail to acknowledge or consider the risks associated with them. They may superficially endorse the importance of obtaining and recording consent, and of minimising patient identifiable information, but they ignore the fact that EXIF data is embedded in digital photographs by default, or that images may be streamed by default between networked devices and hosted in an inappropriately secured cloud that is not GDPR compliant. There is no mention of the dangers posed by facial recognition software in any of the papers reviewed and several of the papers draw quite concerning conclusions:

"We can conclude that WhatsApp instant messaging system is a useful and rapid tool to share information between healthcare professionals in the real world" [42].

It is our view that WhatsApp may indeed be useful and rapid as a modality, but it is not an appropriate communications solution for clinical communications as it is not GDPR or even HIPAA compliant.

The number of papers achieving publication despite the fact that they contain poor quality content (technical and or legal) on the use of Apps for clinical communication is noteworthy. The fact that the numbers of poorly informed articles reduced the year that GDPR was implemented (2018) was encouraging. However, as the COVID-19 Pandemic struck in 2020, when the requirement for remote consultation and efficient digital communications became essential, the number of poorly informed papers achieving publication increased again and that is most concerning. These publications are misleading and will cause issues in clinical practice as busy clinicians need to be able to access well informed content to inform their clinical practice.

5. Conclusion

There is a dearth of evidence of genuinely secure channels being used to communicate sensitive patient data between clinicians within the EU, and a sizeable proportion of publications in the clinical journals fail to

explore or even acknowledge the technical security considerations necessary to ensure the security of confidential patient data to meet the requirements of GDPR.

There are gaps in the knowledge around what constitutes an appropriately secure digital communications channel and the process for risk assessing and approval of such channels for secure communication of sensitive clinical data. Research studies trialling, comparing, and evaluating the use of the various secure enterprise solutions would be extremely valuable (such as Hospify or Near Me). It is also important to establish why clinicians are using insecure consumer channels as opposed to selecting free or cheap to use secure consumer channels (such as Signal or Siilo) for clinical communications. It can be speculated that busy clinicians are simply poorly informed, potentially due to the complete absence of leadership, relevant sign posting and current policy via health systems such as the NHS or the HSE, and lack of training. This of course coupled with the ready availability of insecure technology with which clinicians are already fluent, via their BYOD mobile phones.

General Data Protection Regulation (GDPR) within the EU sign posts specific technical and security requirements for the processing of sensitive data, including health data, and the European Convention of Human Rights (article 8 and convention 108) cannot be ignored.

Clear, well-informed advice, policy, regulation, and training is evidently required to mitigate for security concerns, constraints and technical requirements around privacy and data protection regulation and legislation, in relation to the modalities being used.

Funding

No funding was sought or provided. The source of evidence for the study was the databases within the library of the university.

Ethical approval

As this is a scoping literature review, no data collected from human subjects. Ethical approval was not required.

Patient and public involvement

Patients and/or the public were not involved in the design, conduct or reporting of this research.

Author contributions

This scoping review was conducted as part of a PhD study by Bernadette John under the academic supervision of Dr Christine McCreary and Prof Anthony Roberts.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

We would like to acknowledge the contribution of Anita Wilcox, information specialist and librarian, for her valuable and constructive suggestions during the preparation of this manuscript. We are also grateful to Dr Stewart Duffy, a healthcare regulatory lawyer, for his insight regarding GDPR and the law.

References

[1] W.S.Y. Chan, A.Y.M. Leung, Use of social network sites for communication among health professionals: systematic review, J. Med. Internet Res. 20 (3) (2018) 12.
[2] Crouch H. Information governance alliance drafts guidelines for instant messaging use [Online journal]. digitalhealth.net 2018 [updated 02.03.18. The Information Governance Alliance (IGA) has drafted guidelines for clinicians using instant messaging for work purposes, hailing such systems as a 'useful tool' but highlighting the possibility of 'serious' data security concerns. 2022. Available from: https://www.digitalhealth.net/2018/03/information-governance-alliance-guidelines-instant-messaging-use/.
[3] A. De Benedictis, E. Lettieri, C. Masella, L. Gastaldi, G. Macchini, C. Santu, D Tartaglini, WhatsApp in hospital? An empirical investigation of individual and organizational determinants to use, PLoS One 14 (1) (2019) 13.
[4] T.S. El Hadidy, A.E. Alshafei, A.E. Mortell, E.M. Doherty, Smartphones in clinical practice: doctors' experience at two Dublin paediatric teaching hospitals, Ir. J. Med. Sci. 187 (2017) 9.
[5] O. Ezra, A. Toren, O. Tadmor, E. Katorza, Secure instant messaging application in prenatal care, J. Med. Syst. 44 (73) (2020) 72–75.
[6] D. Fattore, M. Delfino, G. Fabbrocini, Legal, medical, and ethical implications of instant messaging application use in dermatology, Int. J. Dermatol. 58 (2019) 195–207.
[7] D.S. Finn, K.W. Dion, Security tips for using personal technology at your employer's site, Reflect. Nurs. Leadersh. 43 (2) (2018) 8. In this issue, https://www.reflectionsonnursingleadership.org/.../more-features/Vol43_2_security-tips-for-using-personal-technology-at-your-employer-s-site%5B3/5/2019, 2018. (Accessed 11 April 2022).
[8] N. Hawkes, Sixty seconds on WhatsApp, BMJ 360 (1041) (2018) 1.
[9] H.K. Jahn, I.H. Jahn, D. Roland, M.D. Lyttle, W. Behringer, Mobile device and app use in paediatric emergency care: a survey of departmental practice in the UK and Ireland, Arch. Dis. Child. 104 (12) (2019) 1203–1207, 12/2019.
[10] B. John, Are you ready for general data protection regulation? BMJ 360 (k941) (2018) 2.
[11] John B. Phones in dentistry. Bitesize - official newsletter of the Dental Council of Ireland. 2020 July 2020.
[12] M.N. Kamel-Boulos, D.M. Guistini, S. Wheeler, Instagram and WhatsApp in health and healthcare: an overview, Future Internet 8 (37) (2016) 14.
[13] M. Mars, C. Morris, R. Scott, SelfieTelemedicine – What are the legal and regulatory issues? Transforming healthcare through innovation in digital health 254 (2018) 53–62, https://doi.org/10.3233/978-1-61499-914-0-53.
[14] M. Mars, R. Scott, A.J.M.E Al, WhatsApp in clinical practice: a literature review, editor. The Promise of New Technologies in an Age of New Health Challenges. 231 of Studies in Health Technology and Informatics, IOS Press, 2016, pp. 82–90.
[15] M. Mars, C. Morris, R. Scott, WhatsApp guidelines – what guidelines? A literature review, J. Telemed. Telecare 25 (9) (2019) 524–529.
[16] M. Masoni, M.R. Guelfi, WhatsApp and other messaging apps in medicine: opportunities and risks, Intern. Emerg. Med. 15 (2020) 171–173.
[17] Mistry K. Information governance considerations for staff on the use of instant messaging software in acute clinical settings: NHS England; 2018 [updated 09.11.18. NHS England Publications Gateway Reference: 08496]. 2022.
[18] A. Nikolic, N. Wickramasinghe, D. Claydon-Platt, V. Balakrishnan, P. Smart, The use of communication apps by medical staff in the Australian health care system: survey study on prevalence and use, JMIR Med. Inform. 6 (1) (2018) 7.
[19] D. Raths, Messaging often fails HIPAA requirements, Behav. Healthcare Exec. 37 (Summer) (2017) 44–45.
[20] R.C.N., Survey suggests widespread use of instant messaging apps to discuss patient care, Nurs. Stand. 32 (30) (2018) 1.
[21] A. Rimmer, Can I receive and store images sent from patients during remote consultations? BMJ 370 (m2675) (2020) 2.
[22] A. Spencer, S. Patel, Applying the data protection act 2018 and general data protection regulation principles in healthcare settings, Nurs. Manag. 26 (1) (2019) 34–40.
[23] L. Watson, F. Pathiraja, A. Depala, B. O'Brien, S. Beyzade, Ensuring safe communication in health care: a response to Johnston et al. on their paper "Smartphones let surgeons know WhatsApp: an analysis of communication in emergency surgical teams, Am. J. Surg. 211 (1) (2016) 2.
[24] Regulation (EU) 2016 679 of the European parliament and the council of the European union of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General data protection regulation), 216/679 (2016).
[25] E. Mehraeen, M. Ghazisaeedi, J. Farzi, Security challenges in healthcare cloud computing: a systematic review, Glob. J. Health Sci. 9 (2016) 12.
[26] BSR, The new EU general data protection regulation: what the radiologist should know, Insights Imaging 8 (2017) 5.
[27] K. Iyengar, G.K. Upadhyaya, R. Vaishya, V. Jain, COVID-19 and applications of smartphone technology in the current pandemic, Diabetes India Diabetes Metab. Syndr. 14 (2020) 733–737. Clinical Research & Reviews.
[28] V. Barrios, J. Cosı´n-Sales, M. Bravo, C. Escobar, J.M. Gamez, A. Huelmos, C. O. Cortes, I. Egocheaga, J.M. Garcı´a-Pinilla, J. Jimenez-Candil, E. Lo´pez-de-Sa, J. T. Llergo, J.C. Obaya, V. Pallares-Carratala, M. Sanmartın, R. Vidal-Perez, A. Cequier, Telemedicine consultation for the clinical cardiologists in the era of COVID-19: present and future. Consensus document of the Spanish Society of Cardiology, Rev. Esp. Cardiol. 73 (11) (2020) 910–918, https://doi.org/10.1016/j.rec.2020.06.032.
[29] A. Ferreira, R. Cruz-Correia, COVID-19, Cybersecurity and the Human Right to Privacy, JMIR Publications, 2020, p. 14.
[30] I.M. Wielawski, Are patient privacy and health data at risk? AJN 120 (4) (2020) 2.
[31] European Convention on Human Rights - Right to respect for private and family life, (1994).

[32] M.D.J. Peters, H. Khalil, P. McInerney, D. Parker, C. Baldini Soares, Guidance for conducting systematic scoping reviews, Int. J. Evid. Based Healthc. 12 (2015) 141–146.
[33] Bloomberg WhatsApp, Snapchat banned on company devices at continental. Windows IT Pro (Online) Chicago. 2018 June 6, 2018.
[34] L. Martinengo, P. Spinazze, J. Car, Mobile messaging with patients, Br. Med. J. 368 (2020) 884.
[35] B. Chen, Zoom is Easy to Use, and Easy to Bomb, New York Times, 2020, 9th April 2020;Sect. B.5.
[36] Mehta I. TheNextWebcom (Blog) [Internet]2020 1st April 2020. [cited 2020 30.11.2020]. Available from: https://search.proquest.com/docview/2384679846?accountid=14504.
[37] Marketwired, Zoom launches industry's first scalable cloud- based video telehealth solution, Marketwired (2017) 2017, 20th April.
[38] G. Gould, R. Nilforoushan, WhataApp doc? Br. Med. J. 2 (2016) 109–110.
[39] P. Ellanti, A. Moriarty, F. Coughlan, T. McCarthy, The use of WhatsApp smartphone messaging improves communication efficiency within an orthopaedic surgery team, Cureus 9 (2) (2017), https://doi.org/10.7759/cureus.1040.
[40] V.K.H. Giordano, A. Godoy-Santos, W. Dias Belangero, R.E. Santos Pires, P. Labronici, WhatsApp messenger as an adjunctive tool for telemedicine: an overview, Interact. J. Med. Res. 6 (2) (2017) 1–9, https://doi.org/10.2196/ijmr.6214. http://www.i-jmr.org/2017/2/e11/.
[41] U. Gulacti, U. Lok, S. Hatipoglu, H. Polat, An analysis of WhatsApp usage for communication between consulting and emergency physicians, J. Med. Syst. 40 (130) (2016), https://doi.org/10.1007/s10916-016-0483-8.
[42] L. Biasi, R. Bordonaro, N. Borsellino, A. Butera, M. Caruso, S. Cordio, I. Di Cristina, F. Ferraù, D. Giuffrida, H. Soto Parra, M. Spada, P. Tralongo, R. Valenza, F. Verderame, S. Vitello, P. Zerilli, P. Dario, A. Firenze, V Gebbia, Reactions and countermeasures of medical oncologists towards the incoming COVID-19 pandemic: a WhatsApp messenger-based report from the Italian college of chief medical oncologists, Ecancermedicalscience 14 (2020) 12.
[43] E.S.R., ESR paper on the proper use of mobile devices in radiology, Insights Imaging 9 (2018) 247–251.
[44] E.R. Ranschaert, P.M.A. Van Ooijen, G.B. McGinty, P.M. Parizel, Radiologists' usage of social media: results of the RANSOM survey, J. Digit. Imaging 29 (2016) 443–449.
[45] L.A. Siegmund, Social media in occupational health nursing, helpful or harmful? Workplace Health Saf. 68 (9) (2020) 408–414, https://doi.org/10.1177/2165079920935779.
[46] J. Kaur, V. Suri, Whatsapp in obstetrics and gynaecology: necessary evil or blessing in disguise? J. Obstet. Gynaecol. (2020) (Lahore).
[47] M. Sultan, E.M. Brown, R.H. Thomas, Clinicians embracing social media: potential and pitfalls, Epilepsy Behav. Sci. Direct 115 (2019) 7, https://doi.org/10.1016/j.yebeh.2019.106462.
[48] A. Bennani, M. Sekal, Usefulness of WhatsApp for discussing difficult cases in pathology practice: a moroccan experience, Turkish J. Pathol. 35 (2) (2019) 134–138.
[49] S. Mulrennan, Medical information and social media in the time of COVID-19, Respirology 25 (2020) 578–579.
[50] Downey A. Clinicians told they can use WhatsApp to share data in face of COVID-19 2020 [updated 19th March 2020. Available from: https://www.digitalhealth.net/2020/03/clinicians-told-they-can-us.
[51] N.H.S. Instant messaging services a "vital part of the NHS toolkit" during a crisis: NHSX; 2018 [cited 2020. 9th November 2018: [News]. Available from: https://www.england.nhs.uk/2018/11/instant-messaging-services-a.
[52] National Financial regulation mobile phone devices NFR, 27, (2017).
[53] H.S.E., HSE Electronic Communications Policy, HSE, Dublin, Ireland, 2019, pp. 1–22.
[54] H.S.E., Information Technology (I.T.) Security Policy, HSE, Dublin, Ireland, 2013, pp. 1–15.
[55] Mobile phone device policy, (2010). H.S.E.
[56] NHSX. COVID-19 IG advice [Web page]. United Kingdom: National Health Service, Digital; 2020 [Guidance for Patients and Service users; Information Governance Advice For NHS Staff]. Available from: https://www.nhsx.nhs.uk/information-governance/guidance/covid-19-ig-advice/.
[57] L. Stanton, WhatsApp Seeks to Comply With Europe's Privacy Rules, Cybersecurity Policy Report, New York, 2018, p. 2.
[58] M. Favaretto, D. Shaw, D. De Clercq, T. Joda, B.E. Elger, Big data and digitalization in dentistry: a systematic review of the ethical issues, Int. J. Environ. Res. Public Health 17 (7) (2020) 2495, https://doi.org/10.3390/ijerph17072495.
[59] A. Ramji, D. Tamer, C.B. Cota, R.L. Monteiro, C.C.C. Lima, J. Prestia, K. Subbotina, Managing big data privacy and security, Int. Law News 46 (1) (2017) 1–21.
[60] S. Abukar, Getting personal, the professional, legal and ethical aspects of confidentiality, Imagine Therapy 16 (5) (2017) 26–28.
[61] C.M. Williams, B.S.R. Chaturvedi, B.S.K Chakravarthy, Cybersecurity risks in a pandemic, J. Med. Internet Res. 22 (9) (2020) 4.
[62] J.G. Bittner, J. Heather, H.J. Logghe, E.D. Kane, R.F. Goldberg, A. Alseidi, R. Aggarwal, B.J. Jacob, A society of gastrointestinal and endoscopic surgeons (SAGES)statement on closed social media (Facebook®) groups for clinical education and consultation: issues of informed consent, patient privacy, and surgeon protection, Soc. Am. Gastrointest. Endosc. Surg. 33 (2019) 7.
[63] C.J. Haug, Turning the tables – The new European general data protection regulation, N. Engl. J. Med. 379 (3) (2018) 207–209, https://doi.org/10.1056/NEJMp1806637.
[64] S. Persia, Data security and your dental practice, Oral Health 110 (4) (2020) 92.
[65] I.M. Lopes, T. Guarda, P Oliveira, General data protection regulation in health clinics, J. Med. Syst. 44 (53) (2020), https://doi.org/10.1007/s10916-020-1521-0.
[66] I.G.A., Using Video Conferencing For Service User Consultations, NHS Website, 2016.
[67] H.S.E., Planning to Introduce New Instant Messaging Service, Medical Independent, 2018. April 3, 2018.
[68] Goodin D. Study shows which messengers leak your data, drain your battery, and more 2020 [Study shows which messengers leak your data, drain your battery etc.]. 2022. Available from: https://arstechnica.com/information-technology/2020/10/study-shows-which-messengers-leak-your-data-drain-your-battery-and-more/.
[69] Australian Medial Association MIIAoA. Clinical images and the use of personal mobile devices A guide for medical students and doctors. In: AMA M., editor. Australia 2014. p. 18.
[70] S. Natarajan, A.G Nair, Outsmarted by the smartphone!, Indian J. Opthalmol. 63 (10) (2015) 757–758.
[71] W.S. Chan, A.Y. Leung, Use of social network sites for communication among health professionals: systematic review, J. Med. Internet Res. 20 (3) (2018) e117.
[72] H.S.E., Social Media & Digital Policy - Staff Use Guidelines, H.S.E. Communications, Dublin, Ireland, 2017, pp. 1–6.
[73] O'Brien D. Castlebridge blog [Internet]. Dublin: Castlebridge.ie. 2021. [cited 2021 20th January 2021]. Available from: https://castlebridge.ie/2021/01/20/whats-up-whatsapp/.

APPENDIX 4 PUBLICATION 4, PAPER 3.

PEER-REVIEWED

Smartphone and mobile technology use among the dental profession

Précis

Technical support and digital professionalism training are required to facilitate the appropriate use of smartphone technology for dental clinicians practising in the Republic of Ireland.

Abstract

Statement of the problem: Smartphone technologies have changed the landscape of digital communication across society. The Covid-19 pandemic has accelerated the adoption of and requirement for technical solutions to facilitate remote clinical communications. Despite the benefits of smartphones in a clinical communication context, there are risks associated with their use.

Purpose of the study: The primary purpose of this study was to determine the extent of smartphone use among dental professionals in the Republic of Ireland (ROI). In addition, we sought to determine the perception and knowledge of potential pitfalls, risks, and limitations of these technologies among the same population. A smaller cohort of UK dental professionals was surveyed for comparison.

Materials and methods: An online quantitative survey was distributed to evaluate dental professionals' knowledge and understanding of the risks and limitations of smartphone and mobile technology, providing general understanding of the current use of smartphone technology in healthcare in the ROI and the UK.

Results: A total of 123 responses were received from dental professionals in the ROI (UK: n=77). The majority of dental professionals confirmed that they were aware of the risks associated with smartphone use and perceived that they were adequately skilled in digital professionalism. However, concerning practice regarding the communication of sensitive patient data was identified, with the potential for these data to be stored on insecure devices and cloud servers. Many ROI and UK dental professionals confirmed that they would need support to remove patient-identifying data when trading in their device.

Conclusions: App, smartphone and mobile device ownership among dental professionals for clinical communications is widespread in the ROI (and UK), with respondents using their devices to send images (photos and radiographs) to one another. However, the risks of such activities are only partly acknowledged, with many having a lack of insight into data security.

Journal of the Irish Dental Association Published online January 2023

Introduction

There is an ever-increasing accessibility and availability of smartphone and mobile technology across society. The functionality of these 'bring your own devices' (BYODs) is vast, enabling a range of current media-rich communications between users.[1] From simple text messaging or image sharing (clinical photos and/or radiographs), to video conferencing, the intention of digital clinician communications is to improve patient care.[2] These technologies were widely adopted across healthcare during the Covid-19 pandemic, when minimising in-person meetings led to the heightened use of BYODs and digital solutions to aid remote and efficient clinical communication between clinicians and their patients.[3] Clinical communications using BYODs have been the subject of a recent scoping



Bernadette John
BSc (Hons) PG Dip RGN RM PHN
Cork University Dental School and Hospital
University College Cork

Christine McCreary
MA MD FDS(OM)RCPS FFD RCSI
Senior Lecturer/Consultant in Oral Medicine
Cork University Dental School and Hospital
University College Cork

Anthony Roberts
BSc(Hons) BDS(Hons) PhD FDS RCPS(Glasg) FDS(Rest Dent) FFD RCSI FHEA
Professor/Consultant in Restorative Dentistry
Cork University Dental School and Hospital
University College Cork

Corresponding author: Bernadette John E: 116225957@umail.ucc.ie

Table 1: Age and gender demographics of respondents.

	Republic of Ireland			United Kingdom		
Age (years)	Female	Male	Total	Female	Male	Total
20-29	5 (6%)	1 (2%)	6 (5%)	6 (13%)	–	6 (8%)
30-39	20 (26%)	3 (7%)	23 (19%)	17 (36%)	5 (17%)	22 (29%)
40-49	16 (21%)	9 (20%)	25 (20%)	14 (30%)	7 (23%)	21 (27%)
50-59	21 (27%)	15 (33%)	36 (29%)	8 (17%)	11 (37%)	19 (25%)
60-69	15 (19%)	14 (30%)	29 (24%)	2 (4%)	6 (20%)	8 (10%)
>70	–	4 (9%)	4 (3%)	–	1 (3%)	1 (1%)
Total	77 (63%)	46 (37%)	123 (100%)	47 (61%)	30 (39%)	77 (100%)

Table 2: Dental professional and employment demographics.

	Republic of Ireland	United Kingdom
Dental role	Total	Total
Dentist	92 (75%)	55 (71%)
Dental specialist	22 (18%)	18 (24%)
Dental hygienist	1 (1%)	0 (0%)
Clinical dental technician	0 (0%)	1 (1%)
Dental nurse	8 (6%)	3 (4%)
Main employment		
Public sector	45 (37%)	55 (71%)
Private sector	78 (63%)	22 (29%)

review, which demonstrated knowledge gaps around digital security and risk assessment for the security of clinical data.[3] Health professionals must demonstrate the appropriate competence or skill when using digital media (digital professionalism), and yet security and privacy issues are often absent from or only superficially acknowledged in the published literature.

Despite the clear advantages of improved clinical communication for all, the implementation of the European Union (EU) General Data Protection Regulation (GDPR)[4] resulted in increased regulatory requirements around the technology for hosting and processing sensitive data. This, along with the catastrophic cyberattack on the Health Service Executive (HSE) in 2021, resulted in growing concern around the use of digital modalities for clinical communication for everyone involved in current healthcare/dental practice in Ireland.[2] Given their ubiquitous nature and the potential for sensitive patient data to become compromised, it is timely to determine the culture of smartphone use among the dental profession.

Materials and methods

An online questionnaire was adapted (with the permission of the authors) from relevant published studies in the Republic of Ireland (ROI) and the United Kingdom (UK)[3,5] to explore BYOD smartphone and mobile technology use among dental professionals. Ethical approval was granted (UCC Ref: 018-131) for dissemination of a Google Form weblink to dentists and the wider dental profession (dental specialists, dental hygienists, dental nurses, etc.). The invitation to complete the questionnaire provided a convenient sample open to any dental care professional in the ROI (and UK). The questionnaire included the anonymous demographic characteristics of each individual, current use of BYOD smartphones and mobile technology for communicating patient data, and the level of perceived risk associated with their use. The questionnaire was a blend of closed- and open-style questions to allow free text/elaboration. The ROI questionnaire was distributed as a weblink across a number of organisations: Cork University Dental School and Hospital (May 2020); a Dental Council of Ireland newsletter to all registrants (August 2020); an Irish Dental Association webinar (October 2020); online attendees to the Irish Division of the International Association of Dental Research (February 2021); and, the Orthodontic Society of Ireland (March 2021). Plans for wider dissemination at face-to-face conferences that had been planned were curtailed due to the Covid-19 pandemic. UK dissemination of the questionnaire was undertaken through the British Dental Association and the British Association of Oral Surgeons. The resulting data are presented descriptively with no statistical analysis undertaken.

Results

Respondent demographics

A total of 123 dental professionals from the ROI and 77 dental professionals from the UK completed the online survey. A similar gender balance was observed between the ROI (females n=77; 63%) and UK (females n=47; 61%) (Table 1). A wide age range for respondents was observed, with respondents in the 20-29 and >70 year categories in both jurisdictions. The majority of ROI respondents were in the 50- to 59-year age category (n=36; 29%), and for the UK the largest number of responses were seen in the 30- to 39-year age category (n=22; 29%).

The vast majority of ROI respondents were dentists in general practice (n=92; 75%), or dentists in specialist practice (n=22; 18%), with smaller numbers of dental hygienists, dental technicians and dental nurses (Table 2). A similar distribution pattern was observed for respondents from the UK.

The demographic relating to employment type differed between the ROI and the UK – a much higher percentage of respondents work in the private sector in the ROI (n=78; 63%) than in the UK (n=22; 29%).

Current use of smartphones and mobile technology for communicating patient data

High levels of smartphone use were observed among respondents (ROI 98%; UK 100%), with the Apple iPhone the most popular device (ROI n=78; 63%, and UK n=58; 75%). Android devices were less popular in the ROI (n=41; 33%) and UK (n=18; 23%), with the remainder using "other devices".

Respondents were asked to answer questions in the following domains (Table 3):

- Technological skills: A majority of respondents from both jurisdictions (ROI n=105; 85%; UK n=71; 92%) perceived that they had an "appropriate level of technological skill to use a smartphone", although this belief was not evenly distributed across employment type in the ROI. The majority of those ROI respondents who perceived that they did not

Table 3: Current use of smartphones and mobile technology for communicating patient data.

			Republic of Ireland			United Kingdom		
			Total	Public	Private	Total	Public	Private
1	Technological skills	Yes	105 (85%)	42 (34%)	63 (51%)	71 (92%)	50 (65%)	21 (27%)
		No	18 (15%)	3 (2%)	15 (12%)	6 (8%)	5 (6%)	1 (1%)
2	Usefulness	Yes	95 (77%)	34 (28%)	61 (50%)	70 (91%)	49 (64%)	21 (27%)
		No	28 (23%)	11 (9%)	17 (14%)	7 (9%)	6 (8%)	1 (1%)
3	Sending images by instant messaging and/or app	Yes	78 (63%)	21 (17%)	57 (46%)	48 (62%)	35 (46%)	13 (17%)
		No	45 (37%)	24 (20%)	21 (17%)	29 (38%)	20 (26%)	9 (12%)
4	Currently have patient/ clinical information on smartphone	Yes	62 (50%)	13 (10%)	49 (40%)	29 (38%)	22 (29%)	7 (9%)
		No	61 (50%)	32 (26%)	29 (24%)	48 (62%)	33 (43%)	15 (19%)
5	Multiple devices streaming between each other	Yes	36 (29%)	12 (10%)	24 (20%)	22 (29%)	15 (19%)	7 (9%)
		No	87 (71%)	33 (27%)	54 (44%)	55 (71%)	40 (52%)	15 (19%)
6	Devices streaming to the cloud	Yes	61 (50%)	21 (17%)	40 (33%)	30 (39%)	21 (27%)	9 (12%)
		No	62 (50%)	24 (20%)	38 (31%)	47 (61%)	34 (44%)	13 (17%)

Table 4: Level of perceived risk associated with smartphone and mobile technology use.

			Republic of Ireland			United Kingdom		
			Total	Public	Private	Total	Public	Private
1	Risk awareness	Yes	94 (76%)	38 (31%)	56 (46%)	67 (87%)	47 (61%)	20 (26%)
		No	29 (24%)	7 (6%)	22 (18%)	10 (13%)	8 (10%)	2 (3%)
2	Skilled in digital professionalism	Yes	66 (54%)	25 (20%)	41 (33%)	50 (65%)	34 (44%)	16 (21%)
		No	57 (46%)	20 (16%)	37 (30%)	27 (35%)	21 (27%)	6 (8%)
3	Awareness of IT support available	Yes	25 (20%)	7 (6%)	18 (15%)	23 (30%)	13 (17%)	10 (13%)
		No	98 (80%)	38 (31%)	60 (49%)	54 (70%)	42 (55%)	12 (16%)
4	Would value IT support	Yes	114 (93%)	42 (34%)	72 (59%)	74 (96%)	53 (69%)	21 (27%)
		No	9 (7%)	3 (2%)	6 (5%)	3 (4%)	2 (3%)	1 (1%)

possess an appropriate level of technological skill to use a smartphone were in the private sector. Only six UK respondents felt that they did not have the technological skills to use a smartphone, with one of these being in the private sector.

- Usefulness: The majority of ROI respondents (n=95; 77%) confirmed that they found their smartphones useful for the meaningful exchange of clinical information (UK n=70; 91%) and this occurred in both public and private sectors.
- Sending images by messaging: Of the ROI respondents, the majority (n=78; 63%) confirmed that they use or have used their smartphones to communicate images, via WhatsApp or standard picture messaging, with a similar pattern observed in the UK (n=48; 62%). Of the ROI respondents who confirmed sending images, the majority were from the private sector.
- Patient/clinical information stored on their smartphone: Half of ROI respondents confirmed that they had or might have clinical information currently stored on their BYOD smartphones and, of these, the majority worked in the private sector. UK respondents who had patient/clinical information stored on their smartphone were mostly public sector.
- Multiple streaming devices: The majority of ROI respondents (n=90; 73%) confirmed that they own multiple smart devices and, of these, almost one-third (n=36; 29%) confirmed that data does (or has the potential to) stream between these devices, with respondents in both the public and private sectors, a finding also seen in the UK.
- Streaming to the cloud: Half of ROI respondents confirmed that their devices did (or had the potential to) stream sensitive patient data to the cloud, an activity that was observed in both the public and private sectors, with similar results seen among UK responses.

Level of perceived risk associated with smartphone and mobile technology use

Respondents were asked to answer questions in the following domains (Table 4):

- Risk awareness: The majority of the respondents from the ROI (n=94; 76%) considered themselves aware of the risks associated with the use of smartphones and smart devices for the communication of work-related data; respondents were in both the public and private sector, with a similar UK trend (n=67; 87%).
- Skilled in digital professionalism: Approximately half of ROI dental professionals believed themselves to be skilled in digital professionalism (n=66; 54%); respondents were in both public and private sector, with a similar UK trend (n=50; 65%).
- Awareness of need for IT support: The majority of ROI respondents (n=98; 80%) were unaware of any IT supports for wiping or 'cleaning' BYODs at the point of trading in, trading up or abandoning devices. A similarly high percentage of UK respondents reported a lack of awareness of such IT support (n=54; 70%).
- Value of IT support: Respondents in the ROI (n=114; 92.6%) agreed that IT support when trading in devices would be useful (UK, n=74; 96%). The highest levels of value for such IT support were observed in the ROI private and UK public sectors.

Discussion

This study used an online questionnaire distributed to a convenient sample of dental care professionals in the ROI and UK, and demonstrates that smartphone and mobile technology use is widespread. No attempt was made to match the

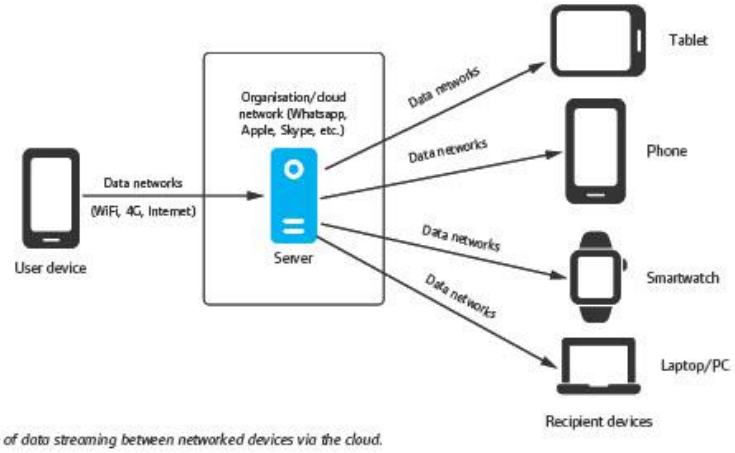


FIGURE 1: Illustration of data streaming between networked devices via the cloud.

demographics of ROI respondents with those of the UK; rather, the data was collated for trend comparison. Respondents confirmed that their smart devices are useful for the meaningful exchange of clinical information to assist patient management. However, while dental professionals may allow the exchange with a positive intention, the results confirm the use of inappropriate and insecure messaging apps[7] and video conferencing channels (e.g., WhatsApp and Zoom)[8] for the communication of sensitive patient data. Dental professionals currently practising within the EU (and UK) are obliged to work within the requirements of the GDPR. A minority of clinicians use SMS to communicate patient clinical information, contravening their GDPR obligations.[7] Accepting the limitations of the study, clinicians are mainly unaware of the potential for sensitive data to be obtained and exploited,[2] and yet clinicians ignoring GDPR may threaten patient confidentiality and bring the profession into disrepute. For the avoidance of doubt, the use of instant messaging and commercial Apps such as WhatsApp for clinical communications is insecure and not GDPR compliant.[7]

With regard to level of perceived risk, a large majority of dental professionals in the ROI confirmed that they had the appropriate level of technological skill to use a smartphone. Given the number of respondents confirming the streaming and storage of confidential patient data to additional networked devices (laptops, smartwatches, iPads, etc.), this confidence seems misplaced. This study raises information governance concerns regarding the potential for numerous insecure locations where sensitive patient data is being stored and points to an unmet need for further clinician training in this area.

A larger proportion of ROI dental professionals who practise privately responded to the questionnaire than in the UK sample, and report sending clinical images insecurely and storing patient information on insecure devices in concerning numbers. This may be a consequence of a lack of access to enterprise/institutional technology supports that might be available in the public sector (e.g., the HSE) and also suggests a requirement for private sector training. Only half of the ROI cohort were confident to confirm that their BYODs were not streaming work-related data to their associated non-institutional clouds, further highlighting the potential for sensitive patient data breaches. It appears to be poorly understood that the likes of the Apple iCloud are hosted in unregulated servers outside the European Economic Area (EEA), and therefore are not GDPR compliant. Figure 1 illustrates the potential for smart devices to stream data between networked devices via potentially non-GDPR-compliant and insecure cloud servers, an issue that is poorly acknowledged in the literature.[3]

The professional, ethical, security and legal concerns posed by popular messaging apps are established.[2,7,8] However, the wider functionalities associated with these modalities, including the selection of secure channels to communicate patient data, the data security issues posed by information streaming between networked devices, the streaming of sensitive patient data to insecure cloud servers, and the cleaning of devices before they are abandoned, traded in, or traded up, provide further areas for concern. Poor awareness regarding phone stewardship (protecting and being responsible for the data held on a mobile phone)[10] also evidences a requirement for digital professionalism and technical training for even the most experienced dental professionals. Despite lack of insight with regard to data security, there is a high level of recognition among professionals that supports the requirement for tasks such as wiping devices of patient-identifying data in the public and private sectors.

Conclusions

App, smartphone, and mobile device ownership among dental professionals for clinical communications is widespread in the ROI (and UK), with this study demonstrating that dental professionals are using their devices to send images (photos and radiographs) to one another. The risks associated with these activities are only partly acknowledged, with many dental professionals evidencing a lack of insight into data security. Dental professionals may benefit from mobile device management software to remove data when required, online portals to securely store and manage clinical images, and digital professionalism training. Some of these solutions are emerging in the UK's National Health Service (NHS), and could be included as part of professionalism and ethics training provided to clinicians through their indemnity organisation, which has flagged concerns in professional publications.[11]

We conclude that there is an unmet need for technical solutions, technical support, and digital professionalism training to facilitate the appropriate use of

smartphone technology for dental clinicians practising in the ROI. Until these supports are in place, it is essential for dental professionals to engage in the use of smartphone and mobile technology for the dissemination of clinical data with caution as they try to best serve their patients.

References

1. Rimmer, A. Can I receive and store images sent from patients during remote consultations? *BMJ* 2020; 370: m2675.
2. John, B., McCreary, C., Roberts, A. Smartphone technology for clinical communication in the Covid-19 era: a commentary on the concerning trends in data compliance. *Front Digit Health* 2022; 4: 816604.
3. John, B., McCreary, C., Roberts, A. Smartphone technology for communications between clinicians – a scoping review. *J Dent* 2022; 122: 104122.
4. The EU Parliament TCotE. Regulation (EU) 2016/679 of the European Parliament and The Council of the European Union of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*. Union OJotE, (ed.). L119/1. Brussels: For the European Parliament, The President M. Schulz, for the Council of the European Union, The President J.A. Hennis-Plasschaert, 2016, p. 88. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.
5. O'Connor, P., Byrne, D., Butt, M., *et al.* Interns and their smartphones: use for clinical practice. *Postgrad Med J* 2014; 90 (1060): 75-79.
6. Mobasheri, M.H., King, D., Johnston, M., *et al.* The ownership and clinical use of smartphones by doctors and nurses in the UK: a multicentre survey study. *BMJ Innovations* 2015; 1: 174-181.
7. Masoni, M., Guelfi, M.R. WhatsApp and other messaging apps in medicine: opportunities and risks. *Intern Emerg Med* 2020; 15 92): 171-173.
8. Chen, B. Zoom is easy to use, and easy to bomb. *New York Times*, April 9, 2020.
9. Mars, M., Morris, C., Scott, R. WhatsApp guidelines – what guidelines? A literature review. *J Telemed Telecare* 2019; 25 (9): 524-529.
10. Mars, M., Morris, C., Scott, R. Selfie telemedicine – what are the legal and regulatory issues? In: Ginige, J.A. Maeder, A.J. (eds.). *Transforming Healthcare Through Innovation in Digital Health: Selected Papers from Global Telehealth*. Amsterdam: IOS Press, 2018, pp.53-62.
11. Johnstone, P. The device in your pocket. *RiskWise, Risk management from Dental Protection* 2018: 6-7.

CPD questions

To claim CPD points, go to the MEMBERS' SECTION of www.dentist.ie and answer the following questions:

IDA irish dental association CPD

1. What is the name of the EU regulation that was implemented across the EU in 2018 concerning data protection and privacy?.

- ○ Copyright and Patient Privacy Directive (CPPD)
- ○ General Data Protection Regulation (GDPR)
- ○ Privacy and Data Processing Regulation (PDPR)
- ○ General Data Privacy Rule (GDPR)

2. The majority of dental professionals stated that they had the clinical skills to use a smartphone to communicate patient data:

- ○ and on further questioning they demonstrated that they knew how to keep patient data secure.
- ○ thus confirming that they require no further training, support or policy regarding the issue of data privacy.
- ○ so patients should rest assured that their privacy is protected when sharing private information with dental professionals
- ○ yet they agreed in large numbers that they currently had patient information stored on their smartphones and streaming to their associated clouds.

3. Digital professionalism was outlined as an area of required competence for graduating dentists in Europe in 2017 under the domain of professionalism. This concerns:

- ○ the use of workplace technology to improve patient care
- ○ the protection of patient data through the appropriate use of digital communications and was explicitly highlighted in an effort to avoid damage to the wider profession by bringing it into disrepute, undermining the trust that the public hold in dental professionals
- ○ undergraduate training only and is not an issue for clinicians who have been in practice for a number of years
- ○ the GDPR and concerns awareness for newly graduating clinicians so that they work within practice guidelines

APPENDIX 5 PUBLICATION 5. PRESENTATION.

IADR PowerPoint Slides presented to Irish Division of IADR, 5th February, 2021, online.









SMARTPHONE CLINICAL COMMUNICATION AMONGST IRISH DENTAL PROFESSIONALS

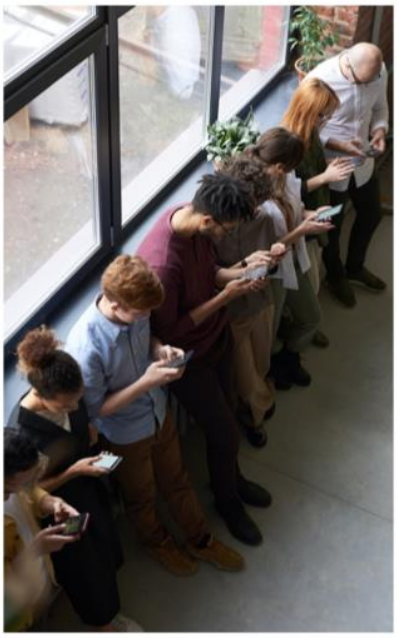
Irish Division IADR 5th February 2021

Bernadette John, Christine McCreary, Anita Wilcox, Anthony Roberts.

A TRADITION OF INDEPENDENT THINKING

UCC

University College Cork, Ireland
Coláiste na hOllscoile Corcaigh



Digital Professionalism

The competence or skill expected of a professional when engaged in social and digital communication

(amended from Oxford English Dictionary definition of 'Professionalism')





ADEE 2017 The Graduating European Dentist

Domain I: Professionalism

1.1.8 Demonstrate digital professionalism by protecting patient data, and the appropriate use of **social media and digital communication**, mindful of how these activities may force them into ethically challenging situations and/or damage the reputation of the wider profession (bring it into disrepute).

McLoughlin J. , Zijlstra-Shaw S., Davies J.R., Field J.C.) Eur J Dent Educ. 2017;21(Suppl. 1):11–13

Objective

To determine

- the prevalence of smartphone ownership and
- trends in usage of clinical communication & digital professionalism

amongst the Irish Dental Profession



Methods

A Google form questionnaire was developed

Ethical Approval sought and obtained (SREC) UCC Log 2018-131

Distributed in 2020 to the Dental Profession

- via Email (~200 staff & PG students)
- via Dental Council letter (~500 Dental Council Registrants)
- via Webinar given to the Irish Dental Association

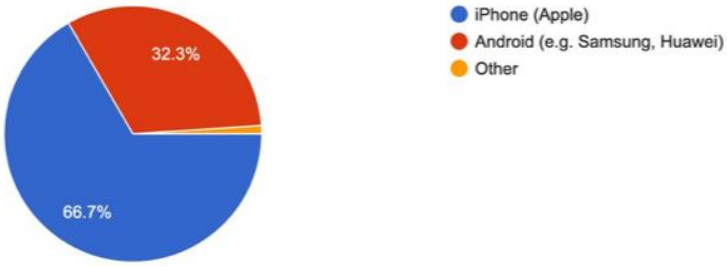
https://forms.gle/PvAUpKiScRsictAm9

UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

Results - 1

Smartphone usage amongst dental professionals

- n=98 Total respondents
  - n=96 (98%) confirmed that they owned a smartphone
  - n=64 (66.7%) Apple;
  - n=31 (32.3%) Android;
  - n=1 (1%) Other

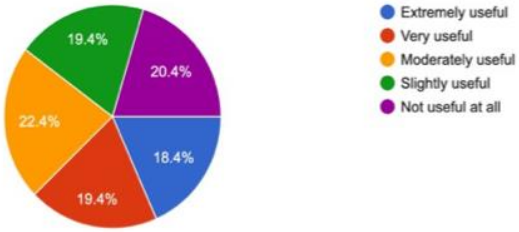


UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

Results - 2

Smartphone usefulness for meaningful exchange of information

- n=78 (79.6%) found their smartphone useful
  - n= 18 (18.4%) Extremely useful
  - n= 19 (19.4%) Very useful
  - n= 22 (22.4%) Moderately useful
  - n= 19 (19.4%) Slightly useful
  - n= 20 (20.4%) Not useful at al

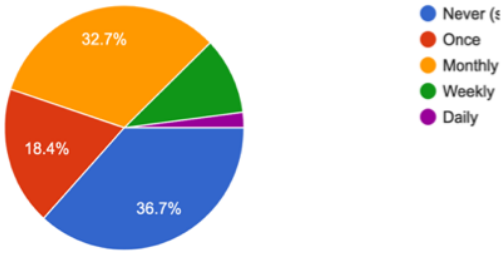


UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

Results - 3

Smartphone used to photograph patient related clinical information to share with a colleague

- n=62 (63.3%) had used this functionality
  - n= 36 (36.7%) Never
  - n= 18 (18.4%) Once
  - n= 32 (32.7%) Monthly
  - n= 10 (10.2%) Weekly
  - n= 2 (2%) Daily

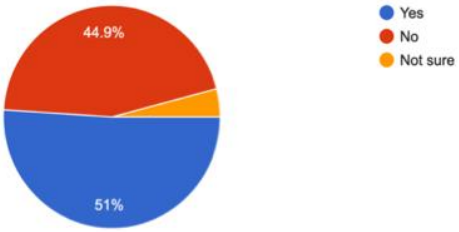


UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

Results - 4

Clinicians' awareness of patient related clinical information stored on their Smartphone

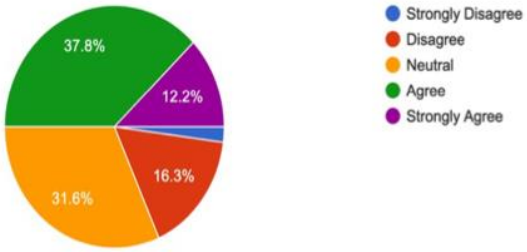
- n= 50 (51%) Yes
- n= 44 (44.9%) No
- n= 4 (4.1%) Not sure



Results - 5

"I am adequately skilled in digital professionalism."

- n= 37 (37.8%) Strongly Disagree
- n= 16 (16.3%) Disagree
- n= 31 (31.6%) Neutral
- n= 37 (37.8%) Agree
- n= 12(12.2%) Strongly Agree



Results - 6

N=30 (31%) of respondents confirmed that they had data streaming to another device

N=51 (52%) confirmed that their data was streaming to cloud-based services

N=92 (94%) perceived the need for support to clean/wipe their smartphone before trading in/up their device

Conclusions

- Smartphone technology is prevalent among Irish Dentists (Apple most common)
- Large number of dentists use Smartphones for meaningful exchange of information
- Worrying number of photographs of clinical information being taken to share with colleagues
- Inadequate personal skills in Digital Professionalism and a perceived training need identified
- Data streaming to other devices (including cloud-based services) – the security of the data is concerning
- Perceived need for assistance when trading up devices



Discussion

- High usage of Smartphone Devices amongst dental professionals
- Dental professionals are exchanging clinical information / photographs
  - Data protection, privacy, liability and professionalism
  - The European Convention on Human Rights
  - GDPR
- Storage of this information clearly an issue (Device / Cloud)
- Perception of adequate skills in Digital Professionalism

- **Dentists require urgent signposting to secure, compliant digital solutions**

- Impact of COVID-19 Pandemic
  - Work patterns
  - Data collection/questionnaire distribution



UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

THANK YOU

URL to the still active questionnaire

https://forms.gle/PvAUpKiScRsictAm9

UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

Potentially Compliant choices for clinical communications

INSTANT MESSAGING

- Medic Bleep
- MedCrowd
- Siilo
- Hospify
- CareFlow Connect
- Forward

VIDEO CONSULTATION WITH PATIENTS

Attend Anywhere

VIDEO COLLABORATION BETWEEN CLINICIANS

- Microsoft Teams
- Cisco Web Ex

APPENDIX 6 ABSTRACT, IADR PRESENTATION

Title *(no more than 10 words)*	**IADR, 5th February, 2021.** **Abstract for conference presentation** **Smartphone clinical communication amongst Irish Dental Professionals.**
Objectives	Effective communication between clinicians is essential in health care settings including Dentistry. Smartphone technology is ubiquitous in modern society and clinical practice due to its cost effective and efficient communication functionality. The purpose of this study was to determine the prevalence of smartphone ownership and clinical communication in the Irish Dental Profession, trends in usage and Digital Professionalism.
Methods	A Google form questionnaire was developed and distributed in 2020 to the dental profession via email (196 dental staff & 13 post graduate students at UCC), via letter (500 Irish Dental Council members through a letter with a URL to the still active questionnaire (https://forms.gle/PvAUpKiScRsictAm9)) and during a webinar given to the Irish Dental Association (more respondents welcome).
Results	A total of 98 responses were received with 96 (98%) of respondents confirming they owned a smartphone (n=64% Apple; n=31% Android; n=3% Other). Respondents reported the use of SMS / iMessage (n=49; 50%) or App-based messaging (e.g. WhatsApp n=51; 52%) to communicate patient related clinical information to colleagues. Many respondents (n=49; 50%) perceived inadequate personal skills in 'Digital Professionalism'. Patient-related clinical information was stored on the smartphones of n=50 (51%) respondents with n=30 (31%) having data streaming to another device and n=51 (52%) having data streaming to cloud-based services. A large number of respondents n-=92 (94%) perceived the need for support to clean/wipe their smartphone before trading in/up their device.
Conclusions	Smartphone technology is highly prevalent among Irish dentists with many (approx. 50%) using their device to communicate patient related clinical information (including photographs) without appropriate GDPR compliance.

	The security of the information is concerning, especially as these patient data may (inadvertently) be streamed to other devices or stored insecurely on remote cloud-based servers. Dentists require urgent signposting to secure digital solutions and training on Digital Professionalism.

APPENDIX 7 LETTER OF ACCEPTANCE FROM PUBLISHER FOR BOOK CHAPTER

CAMBRIDGE UNIVERSITY PRESS

To Whom it may Concern

This is to confirm that Bernadette John is a co-author of the chapter "Digital Communication" together with Professor Anthony Roberts and Dr Christine McCreary, for the book entitled "A Clinician's Brief Guide to Communication Skills in 21st Century Psychiatry" edited by Dr Josie Jenkinson and Dr James Woollard. The book will be a co-publication between Cambridge University Press and the Royal College of Psychiatrists.

Bernadette's chapter has been accepted for publication and we are hoping that the book should have a 2023 publication date.

Bernadette's contribution is very much appreciated.

Yours sincerely

O Boult.

Olivia Boult
Editor, Medicine
The Academic Group / Cambridge University Press
University Printing House / Shaftesbury Road / Cambridge CB2 8BS
oboult@cambridge.org
www.cambridge.org

APPENDIX 8 DATA EXTRACTION MICROSOFT SPREADSHEET (CHAPTER 3.)

Search Type	Included AS CLINICAL COMMS	Negative/Positive	Authors	Year	Book Title	Journal Title	Study	Literature Review	Press Release	Newspaper article	General information article in journal	Grey Literature (including government papers)	Title	MAIN CONCEPT 1 - Functionality required for current clinical Communications in healthcare?	MAIN CONCEPT 2 - Smartphone Channel being used	MAIN CONCEPT 3 - Technical ineight, compliant with GDPR	MAIN CONCEPT 4 - EU/non Eu
OneSearch1	Y	Negative	Marketwired (2017)	2017	0	0	0		0	0	0	x	0 Zoom Launches Industry's First Scalable Cloud-Based Video Telehealth Solution: Video Communication Provider's New Telehealth Service Features Epic Integration	Video consultation software for telehealth	ZOOM	NO	NON EU, Canada
OneSearch1	Y	Positive	Watson et al. (2016)	2016	0	The American Journal of Surgery	0		0	0	0	X	0 A response to an article - "Ensuring safe communication in healthcare: a response to Johnston et al on their paper "Smartphones let surgeons know whatsapp: an analysis of communication in emergency surgical teams"	Instant messaging among surgical clinicians	Whatsapp	NO	EU RESEARCH, UK, but published in a USA journal
OneSearch1	Y	Positive	Nikolic A. 2018	2018	0	JMIR Medical Informatics	X		0	0	0	0	0 The use of communication apps by medical staff in the australian health care system: Survey study on prevalence and use	Communication Apps	Whatsapp	NO, BUT LEGAL COMPLAINCE AND PRIVACY ISSUES ACKNOWLEDGED	NON EU. Australia
OneSearch1	N	Positive	Stanton L. (2018)	2018	0	0	0		0	0	0	0	X Whatsapp seeks to comply with Europes Privacy Rules	Not necessarily clinical, but security of instant messaging	Whatsapp	Whatsapp signed 'an undertaking' to not share data with facebook. This was prior to implementation of GDPR. Potentially Whatsapp was not GDPR compliant	Relevant to all in EU
OneSearch1	Y	Positive	John B. (2018)	2018	0	BMJ	0		0	0	0	X	0 Are you ready for General Gata Protection Regulation?	Yes, communications in healthcare	Whatsapp, dropbox, instant messaging, careflow connect, hospify, med crowd, medicbleep, siilo and cupris	Yes - issues posed by GDPR for the use of comms apps discussed	Relevant to all in EU
OneSearch1	Y	Positive	Chan, W.S.Y., & Leun	2018	0	Journal of Medical Internet Research	0	X		0	0	0	0 Use of social network sites for communication among health professionals; systematic review	Yes, communications in healthcare	Social Networking Sites	Risks to data protection acknowledged	Non EU - Hong Kong
OneSearch1	N	Positive	Wielawski I. (2020)	2020	0	American Journal of Nursing Reports	0		0	0	0	X	0 Are Patient Privacy and health Data at Risk? Partnerships between tech companies and health systems challenge privacy expectations and laws	Not communications channels specifically	facebook/google companies etc	MENTIONS AND ACKNOWLEDGES GDPR	NON EU - USA
OneSearch1	FALSE	Negative	El. Hadidiy et al. (201	2017	0	Irish Journal of Medical Science	X		0	0	0	0	0 Smartphones in clinical practice: doctors' experience at two Dublin Paediatric teaching hospitals	Clinical Comms - Medics	Medical Apps, Whatsapp,	Not mentioned	EU - Ireland
OneSearch1	N	Positive	Mehta, I. (2020)	2020	0	TheNextWeb.com	0		0	0	0	0	X Don't believe Zoom: its video calls are not encrypted end to end	Universal - not clinical comms specifically	Zoom	Not mentioned	EU - Holland
OneSearch1	Y	Positive	DeBenedictis A. Et al	2019	0	Plos One	X		0	0	0	0	0 Whatsapp in hospital? An empirical investigation of individual and organisational determinants of use	Nurses and physicians	Whatsapp	Not mentioned specifically, although securitiey and privacy protection issues acknowledged	EU - Italy
OneSearch2	Y	NEGATIVE	Gould, G. & Nilforoosh	2016	0	BMJ Innovations, 07/2016, Volume 2, Issue 3	X	0	0	0	0	0	WhatsApp Doc?	Doesnt really concern itself at all with data protection or privacy and states that doctors will continue to use modes of communication that are most efficient and useful.	UK	Yes - Mentions the information governance bulletin from the NHS (since removed) that forbids the use of Whatsapp as not appropriate for clinical comms	0
OneSearch2	Y	NEGATIVE	Ellanti, P. (2017)	2017	0	(Palo Alto, CA), 02/2017, Volume 9, Issue 2	X	0	0	0	0	0	The Use of WhatsApp Smartphone Messaging Improves Communication Efficiency within an Orthopaedic Surgery Team	No. Says whatsapp is easy, inexpensive and reliable! Only acknowledges that information must be anonymised but doesnt get	Irish	Totally ignores the GDPR issues raised by the use of Whatsapp	0
OneSearch2	Y	NEGATIVE	Giordano V. et al. (201	2017	0	Interactive journal of medical research, 07/2017, Volume 6, Issue 2	0	X	0	0	0	0	WhatsApp Messenger as an Adjunctive Tool for Telemedicine: An Overview	Totally ignores issues around security of data	Brazil	ARTICLE TOTALLY IGNORED PRIVACY CONCERNS AND GDPR SPECIFICALLY - PREP FOR GDPR WAS 2 YEARS PRIOR TO MAY 2019	0
OneSearch2	Y	POSITIVE	Masoni, M. et al. (202	2020	0	Internal and emergency medicine, 03/2020, Volume 15, Issue 2	0	0	0	0	X	0	WhatsApp and other messaging apps in medicine: opportunities and risks	Absolutely spells out that Whatsapp is not gdpr compliant	Italy	Included as relevant	0

OneSearch2	Y	POSITIVE	Hawkes, N. (2018)	2018	0	BMJ, 03/2018, Volume 360	0	0	0	0	X	0	Sixty seconds on . . . WhatsApp	Yes, specifically	UK	Included as deemed relevant	0
OneSearch2	Y	NEGATIVE	Gulacti (2016)	2016	0	Journal of medical systems, 04/2016, Volume 40, Issue 6	X	0	0	0	0	0	An Analysis of WhatsApp Usage for Communication Between Consulting and Emergency Physicians	No. Totally ignores issues around privacy of data	Turkey	THIS 2016 ARTICLE IS FROM TURKEY AND TOTALLY IGNORES PRIVACY ISSUES AROUND THE USE OF WHATSAPP	0
OneSearch2	Y	NEGATIVE	Blasi, L. Et al. (2020)	2020	0	Ecancermedicalscience, 05/2020, Volume 14	X	0	0	0	0	0	Reactions and countermeasures of medical oncologists towards the	No mention at all of data security	Italy	Included as deemed relevant	0
OneSearch2	N	POSITIVE	Martinengo (2020)	2020	0	BMJ, 03/2020, Volume 368	X	0	0	0	0	0	Mobile messaging with patients	Some good advice around documenting consent to use channel, adhering to data protection laws, documenting all communications in patients notes and clarifying scope of what can be discussed on channel before it is commenced	Singapore, Hong Kong and Imperial College London, UK	Yes	0
OneSearch2	Y	POSITIVE	Ezra, O. (2020)	2020	0	Journal of medical systems, 02/2020, Volume 44, Issue 4	0	0	0	0	X	0	Secure Instant Messaging Application in Prenatal Care	YES! piloting Siilo as an alternative to whatsapp	Israel	0	0
OneSearch2	N	POSITIVE	Favaretto, M. (2020)	2020	0	International journal of environmental research and	0	X	0	0	0	0	Big Data and Digitalization in Dentistry: A Systematic Review of the Ethical Issues	Data security issues raised continuously throughout this piece	Swiss	No	0
OneSearch2	Y	NEGATIVE	ESR (2018)	2018	0	Insights into Imaging, 04/2018, Volume 9, Issue 2	0	0	0	0	X	0	European Society of Radiology paper on the proper use of mobile devices in radiology	It just mentions that security issues must be acknowledged? Wholely inadequate	European	0	0
OneSearch2	N	POSITIVE	Spencer, A. & Patel, S	2019	0	Nursing management (Harrow, London, England), 01/2019, Volume 26, Issue 1	0	0	0	0	X	0	Applying the Data Protection Act 2018 and General Data Protection Regulation principles in healthcare settings	Explanation of GDPR as applied to specific cases, but none clinical comms using a smartphone	UK and Ireland	0	0
OneSearch2	Y	POSITIVE	Jahn, H.K. (2019)	2019	0	Archives of Disease in Childhood, 12/2019, Volume 104, Issue 12	X	0	0	0	0	0	Mobile device and app use in paediatric emergency care: a survey of departmental practice in the UK and Ireland	Points out that the NHS approved the use of Whatsapp for clinical comms during emergency ...this study looks to measure harm caused by such apps - but that may not be evidenced yet.	Ireland	0	0
OneSearch2	Y	POSITIVE	Rimmer A. (2020)	2020	0	BMJ, 07/2020, Volume 370	0	0	0	0	X	0	Can I receive and store images sent from patients during remote consultations?	Yes	UK	0	0
OneSearch2	Y	POSITIVE	Ramji, Al. (2017)	2017	0	International Law News, 09/2017	0	0	0	0	X	0	Managing Big Data Privacy and Security	Relevant to Healthcare in general, internationally with specific advicee for the EU	Canada, USA, Brazil,	0	0
OneSearch2	Y	POSITIVE	Abukar, S. (2017)	2017	0	Imaging & Therapy Practice, 08/2017	0	0	0	0	X	0	Getting Personal	Specifically considers issues around obligations for clinicains with regard to data protection act 1998 in relation to data and images sharing	UK	0	0
OneSearch2	Y	POSITIVE	RCN 2018	2018	0	Nursing Standard, 03/2018, Volume 32, Issue 30	X	0	0	0	0	0	Survey suggests widespread use of instant messaging apps to discuss patient care	this article states that many NHS employers have banned these apps - quotes the RCN as stating that nurses risk their registration by sharing confidential information or photos about patients without consent	UK	0	0
OneSearch2	Y	NEGATIVE	Ranschaert, E. (2016)	2016	0	Journal of Digital Imagine (2016) 29:443-449	X	0	0	0	0	0	Radiologists usage of social media: Results of the RANSOM survey	Mentions issues around risk to privacy for patients but no meaningful exploration	The Netherlands, USA, Belgium	0	0
OneSearch2	Y	NEGATIVE	Siegmund, L.A. (2020	2020	0	Workplace health & safety, 09/2020, Volume 68, Issue 9	0	X	0	0	0	0	Social Media in Occupational Health Nursing: Helpful or Harmful?by Siegmund, Lee Anne	outlines the functionlality within whatsapp for example and ignores the risks to patient privacy it poses - concerns itself with deliberately breaking patient confidentiality as opposed to technical issues of compliance or functionality	UK	0	0

OneSearch2	Y	NEGATIVE	Kaur J. Suri V. (2020)	2020	0	Journal of obstetrics and gynaecology, 02/2020	0	0	0	0	X	0	WhatsApp in obstetrics and gynaecology: necessary evil or blessing in disguise?	Totally ignores issues around security of data	India	0	0
OneSearch2	N	POSITIVE	Bloomberg (2018)	2018	0	Bloomberg, Windows IT Pro, 06/2018	0	0	0	0	0	X	WhatsApp, Snapchat Banned on Company Devices at Continental	This article shows how businesses are concerned that Whatsapp puts sensitive data at risk and the actions that businesses are taking top mitigate for that risk	USA publication concerning German auto manufacturer	0	0
OneSearch2	Y	POSITIVE	Williams C.M. (2020)	2020	0	Journal of medical Internet research, 09/2020, Volume 22, Issue 9	0	0	0	0	X	0	Cybersecurity Risks in a Pandemic	interesting quotes around health care organisations being a cybercrime target during a pandemic	USA	0	0
OneSearch2	Y	POSITIVE	Bittner J.G. (2019)	2019	0	Surgical Endoscopy, 01/2019, Volume 33, Issue 1	0	0	0	0	X	0	A Society of Gastrointestinal and Endoscopic Surgeons (SAGES) statement on closed social media (Facebook®) groups for clinical education and consultation: issues of informed consent, patient privacy, and surgeon protection	0	USA	0	0
OneSearch2	N	POSITIVE	Haug, C. (2018)	2018	0	The New England journal of medicine, 07/2018, Volume 379, Issue 3	0	0	0	0	X	0	Turning the Tables — The New European General Data Protection Regulation	Very useful quotes on the meaning and implications of GDPR	European	0	0
OneSearch2	N	POSITIVE	ESR (2017)	2017	0	Insights into imaging, 06/2017, Volume 8, Issue 3	0	0	0	0	X	0	The new EU General Data Protection Regulation: what the radiologist should know by European Society of Radiology (ESR)	some useful quotes	UK	0	0
Ebsco1		Positive	Persia S. (2020)	2020		0 Oral Health		0	0	0	0 X		0 DATA SECURITY AND YOUR DENTAL PRACTICE.	Not specifically about smartphone technology but data security	Doesnt mention	Non EU - Canada	Yes, because it articulates the issues raised by data breaches for dental practices and the scale of the existing issues in Canada. It also explains regulations in Canada
Ebsco1		Positive	Chen , B. (2020)	2020		0 New York Times, NY		0	0	0	0 X		0 Zoom Is Easy to Use, and Easy to Bomb: [Business/Financial Desk]	Not specifically about smartphone tecnology but Zoom	Not mentioned	NOT EU, BUT USA with global significance	Yes, because it describes issues posed by the use of zoom - ZOOM AND USA, BUT RELEVANT POINTS
Ebsco1		Negative	Barrios, V. et al. (2020	2020		0 Rev Esp Cardiol.	X		0	0	0	0	0 Telemedicine consultation for the clinical cardiologists in the era of COVID-19: present and future. Consensus document of the Spanish Society of Cardiology.	None specifically mentioned	This article skims over security issues but mentions the importance of adhering to legislation	EU - Spain	Yes, This article mentions 'data protection legislation, ' and for this reason states that only tools using data encryption should be used and informed consent recorded in electronic patient record. The researchers dont appear to know what they dont know - read in detail in case I am
Ebsco1		Positive	Mars (2018) copy	2018		0 Studies in Health Technology & Informatics		0 X		0	0	0	0 Selfie Telemedicine – What Are he Legal and Regulatory Issues?	Smartphones, instant messaging Apps, eamil	This article raises issues around legal obligations - so potentially yes, full article requested	EU	Yes - requested via inter library loan
Ebsco1		Positive	Fattore, D., et al. (2011	2019		0 International Journal of Dermatology		0	0	0	0 X		0 Legal, medical, and ethical implications of instantmessaging application use in dermatology	Mobile technologies	"Few doctors are aware of the possible misunderstandings in communication with patients and of the risks related to noncompliance with privacy legislations" - GDPR specifically mentioned	EU - Italy	Yes - because it usefully raises issues that I raise all the time regarding compliance with GDPR
Ebsco1		Positive	Jimenez-Rodriguez, D	2020		0 International Journal of Environmental Research and Public Health	X		0	0	0	0	0 Increase in Video Consultations During theCOVID-19 Pandemic: Healthcare Professionals'Perceptions about Their Implementation and Adequate Management	An unamed specific Telehealth platform	Regulations mentioned, but not GDPR specifically	EU - Spain	Yes, because this research actually evaluated issues around the implementation of a dedicated video-telehealth tool, not a commercial free social App and it establisehd the issues it raised
Ebsco1		Negative	Iyengar, K. et al. (2020	2020		0 Diabetes & Metabocilc Syndrome: Clinical Research & Reviews		0 X		0	0	0	0 COVID-19 and applications of smartphone technology in the currentpandemic	Zoom, skype, facetime, instant messaging	Not concerned with privacy or security at all, no mention of GDPR or other regulations	Non EU - India	Somewhat, because it totally ignores issues around patient privacy - it even advocates the use of Zoom for group counselling - taken out of context it could lead to breaking GDPR
Ebsco1		Negative	Sultan, M. et al. (2019	2019		0 Epilepsy & Behavior		0	0	0	0 X		0 Clinicians embracing social media: Potential and pitfalls	Social Media in general	GDPR not mentioned	EU - UK	Yes
Ebsco1		Positive	Mars M. (2019)	2019		0 Journal of Telemedicine & Telecare		0 X		0	0	0	0 WhatsApp guidelines - what guidelines?	Whatsapp	No guidelines exist on whatsapp use	South Africa and Canada	Yes

Ebsco1		Positive	Lopes (2020)	2020		0	Journal of Medical Systems	X		0	0	0	0	0	General Data Protection Regulation in Health Clinics	None	Yes	Portugal/Equador	yes - useful quotes
Ebsco1		Positive	Raths D. (2017)	2017		0	Behavioural healthcare Executive		0	0	0	0	X		0	Messaging often fails in HIPAA requirements.	imessage, sms, etc or secure specific alternatives (HIPAA compliant)	Security issues, SMS and Imessage not HIPAA compliant	USA	Yes, useful points made
Ebsco1		Positive	Finn D.S. (2018) Part 2	2018		0	Reflections on Nurse leadership		0	0	0	0	X		0	Security tips for using personal technology at your employer's site (part 2 of 3)	Doesnt mention anything specific, but raises alarm about using unsecured wifi with a device used to process work related data - BYOD policies are essential - can device be wiped remotely if lost?	Not GDPR bu t HIPAA, intersting point about hotspots and loss of devices, risk of unauthorised disclosure of data	USA	yes - useful quotes
HandSearch1	Y	POSITIVE	IGA (2016) NHS - vide	2016		0	0		0	0	0	0	0	X	Using Video Conferencing for Service User Consultations (NHS)	Pre GDPR but well informed ab	UK	Yes, because they lead to	0
HandSearch1	Y	POSITIVE	Mistry (2018)	2018		0	0		0	0	0	0	0	X	Information governance considerations for staff on the use of instant messaging software in acute clinical settings	post GDPR but more or less sa	UK	0	0
HandSearch1	Y	POSITIVE	Kamel Boulos, M. et a	2016		0	Future Internet Journal		0	X	0	0	0	0	Instagram and Whatsapp in health and healthcare: An Overview	Pre GDPR but good attention p	International study, conducted	Yes	None Declared
HandSearch1	Y	NEGATIVE	Bennani A., Sekal M. (	2019		0	Turkish Journal of Pathology	X		0	0	0	0	0	Usefulness of whatsapp for discussing difficult cases in pathology practice: A Moroccan experience	Post GDPR with no genuine ur	Non EU/Morocco	0	0
HandSearch1	Y	NEGATIVE	Crouch H. (2018)	2018		0	Digital health network		0	0	0	0	X		0	Information Governance Alliance drafts Guidelines for instant messaging use	Well informed in that it acknowl	UK	Yes	0
HandSearch1	Y	POSITIVE	Mars et al. (2016)	2016	The Promise	0		0	X		0	0	0	0	Whatsapp in clinical practice: A literature review	excellent analysis, issues arou	South Africa and Canada	Yes	Potentially, as one author is a consultant in e-health from a Canadian consulting firm
HandSearch1	Y	POSITIVE	Ferreira A, et al. (2020	2020		0	JMIR (Journal of medical internet research) Medical Informatics		0	0	0	0	X		0	Cybersecurity and the human right to privacy	Post GDPR but focuses actuall	EU?Portugal	Yes, some very useful idea	None declared
HandSearch1	Y	NEGATIVE	Mulrennan S. (2020)	2020		0	JMIR, Official journal of the asian pacific society of respirology		0	0	0	0	X		0	Medical Information and social media in the time of COVID 19	No. Superficial and apparently	Australia and USA	Only if I want an example o	None declared
HandSearch1	Y	POSITIVE	John B. (2020)	2020		0	0		0	0	0	0	0	X	Phones in dentistry	Yes	Ireland	Yes	None
HandSearch1	Y	NEGATIVE	Downey A. (2020)	2020		0	Digital Health network (Digitalhealth.net		0	0	0	0	0	X	Clinicians told they can use whatsapp to share data in face of covid-19	This advice is not in compliano	UK	0	0
HandSearch1	Y	negative	NHS England	2018		0	0		0	0	0	0	0	X	Instant messaging services a vital part of the nhs toolkit during a crisis	0	UK	This raises issues, but does	0
HandSearch2	Y	POSITIVE	Medical Independent	2018		0	Medicalindependent.ie		0	0	0	X		0	0	HSE planning to introduce new instant messaging service	IG concerns mentioned	Ireland	0	0

HandSearch2	Yes	NEGATIVE	HSE (2017) Mobile de	2017	0	0	0	0	0	0	0	X	HSE, Social Media & Digital Policy - staff use guidelines	confidential information relating	Ireland	0	low		
HandSearch2	Y	NEGATIVE	HSE (2019) electronic	2019	0	0	0	0	0	0	0	X	HSE, Electronic Communications Policy (version 3.1)	Not about apps or BYOD	Ireland	but not well informed or use	low		
HandSearch2	Y	NEGATIVE	HSE (2013) IT informa	2013	0	0	0	0	0	0	0	X	HSE, Information Technology IT security Policy	long before GDPR or advances	Ireland	but not well informed or use	low		
HandSearch2	Y	NEGATIVE	HSE (2010) mobile-pl	2010	0	0	0	0	0	0	0	X	HSE, Mobile Phone Device Policy	No - very old. pre current functi	Ireland	but very poor example of a	low		
HandSearch2	Y	POSITIVE	Goodin D. (2020)	2020	0	Digital Health network (Digitalhealth.net),	X	0	0	0	0	0	Study shows which messengers leak your data, drain your battery, and more	This piece discusses security is	USA - but international signific	Yes, as it poses a potential	Low		
HandSearch2	Y	NOT RELEVANT	Patel, N., Viswanathar	2020	0	Dental Health		0	0	0	0	X	0	Virtual Appointments: The New	GDPR mentioned, as well as a	UK	A current example of a sup	Low		
HandSearch2	Y	NEGATIVE	NHSX	2020	0	0	0	0	0	0	0	X	Covid 19 Information Governance Advice (5th October 2020)	refers to information comission	UK	Yes - the authors dont knov		0	
HandSearch2	Y	Negative	HSE	2017	0	0	0	0	0	0	0	Policy	National Financial Regulation, Mobile Phone Devices, NFR - 27	no	Ireland	Yes, because so poorly infe		0	

APPENDIX 9 SURVEY TOOL REPUBLIC OF IRELAND

A Study of the Prevalence and Factors influencing the Use of Smartphone and Mobile Technology for the Communication of Patient Data by Clinicians in the Republic of Ireland

Thank you for agreeing to participate in this research project. You have indicated that you are a DENTIST or a DENTAL CARE PROFESSIONAL and we are seeking your views and current practice in the use of personal mobile technology in your clinical roles/ workplace.

* Indicates required question

CHARACTERISTICS OF PARTICIPANT

About you

1. (1.0) Please select your AGE *

Mark only one oval.

- ◯ 20-29 years
- ◯ 30-39 years
- ◯ 40-49 years
- ◯ 50-59 years
- ◯ 60-69 years
- ◯ 70 years or greater
- ◯ Prefer not to say

2. (1.1) Please select your GENDER *

Mark only one oval.

- ◯ Female
- ◯ Male
- ◯ Non-binary
- ◯ Prefer not to say

3. (1.2) Who is your MAIN employer? *

Mark only one oval.

- ◯ Health Service Executive (HSE)
- ◯ Voluntary Sector
- ◯ Private Sector
- ◯ Not employed - Part Time Student
- ◯ Not Employed - Full Time Student
- ◯ Third Level Institution
- ◯ Not Currently Employed
- ◯ Other: _____

4. (1.3) Details of place of MAIN Employment: *

Mark only one oval.

- ◯ Health Service Executive (H.S.E.)
- ◯ Voluntary Sector
- ◯ Private Sector - General Dental Practice
- ◯ Third Level Institution
- ◯ Not currently employed
- ◯ Other: _____

5. (1.4) YEARS since first registration of a Dentist or Dental Care Professional : *

Mark only one oval.

- ◯ Less than 1 year
- ◯ 1-2 years
- ◯ 3-5 years
- ◯ 6-10 years
- ◯ Over 10 years
- ◯ N/A

6. (1.5) Details of registrations with The Dental Council of Ireland *

Check all that apply.

- ☐ Dentist
- ☐ Dental Hygienist
- ☐ Dental Nurse
- ☐ Clinical Dental Technician
- ☐ Not registered with The Dental Council of Ireland
- ☐ Other: _____

7. (1.6) Current role details (for which you are MAINLY employed): *

Mark only one oval.

- ◯ Dentist
- ◯ Dental Hygienist
- ◯ Dental Nurse
- ◯ Clinical Dental Technician
- ◯ Clinical Teacher
- ◯ Lecturer
- ◯ Working in research
- ◯ Working in an administrative post
- ◯ Postgraduate student (MPhil, PhD)
- ◯ Not currently employed
- ◯ Other: _____

8. (1.7) HIGHEST level of educational attainment: *

Mark only one oval.

- ◯ Certificate
- ◯ Diploma
- ◯ Bachelor's degree (BDS)
- ◯ Post- graduate Qualification (e.g. certificate, diploma)
- ◯ Master's degree (MSc)
- ◯ Doctoral Degree (PhD)
- ◯ Other: _____

9. (1.8) LOCATION of employment: *

Mark only one oval.

- Connaught
- Ulster
- Munster
- Leinster (except County Dublin)
- County Dublin
- The Islands
- Other: _____

10. (1.9) With regard to your SPECIALITY, do you work MAINLY in: *

Mark only one oval.

- Dental Public Health
- Endodontics
- Periodontics
- Prosthodontics
- Restorative Dentistry
- Oral Medicine
- Oral Radiology
- Oral Surgery
- Orthodontics
- Student
- Non-clinical post (e.g. researcher)
- Other: _____

To identify rationale for and prevalence of the use of personal Bring your own Device (B.Y.O.D.) Smartphone and Mobile Technology to transmit patient data by Clinicians in the Republic of Ireland. Please consider each of the following questions in turn. Politely, we request that once you have selected an answer from the options provided, that you don't return to questions and amend your previous answers on the basis of the information learned/provided.

11. (2.0) Do you own a Smartphone? *

Check all that apply.

- [ ] Yes
- [ ] No (Skip to question (2.2))

12. (2.1) What type of Smartphone do you own (if you have more than one, what is the MAIN phone you use at/for work)?

Mark only one oval.

- ◯ iPhone (Apple)
- ◯ Android (e.g. Samsung, Huawei)
- ◯ Other

13. (2.2) In relation to the following statement, please select the response that reflects YOUR PERCEPTION: "I have the technological skills to use a Smartphone". *

Mark only one oval.

- ◯ Strongly Disagree
- ◯ Disagree
- ◯ Neutral
- ◯ Agree
- ◯ Strongly Agree

14. (2.3) How USEFUL do you find your Smartphone in helping you with the MEANINGFUL EXCHANGE OF CLINICAL INFORMATION? -e.g To assist with assessment, diagnosis, treatment or any part of the overall management a patient. *

Mark only one oval.

- ◯ Extremely useful
- ◯ Very useful
- ◯ Moderately useful
- ◯ Slightly useful
- ◯ Not useful at all

15. (2.4) Have you used your Smartphone to communicate PATIENT RELATED CLINICAL INFORMATION to colleagues using: *

Mark only one oval per row.

	Never	Once	Monthly	Weekly	Daily
SMS text or iMessage?	◯	◯	◯	◯	◯
An App based messaging service (e.g. WhatsApp)?	◯	◯	◯	◯	◯

16. (2.5) Have you ever used your Smartphone to PHOTOGRAPH patient related clinical information to share with a colleague (for example: photographing a patient's wound or X-ray or test result to consult a colleague for an opinion)? *

Mark only one oval.

- ◯ Never (skip to question (2.7))
- ◯ Once
- ◯ Monthly
- ◯ Weekly
- ◯ Daily

17. (2.6) Did you SEND the photograph(s) as standard multimedia/picture messages or using an App based messaging service (such as WhatsApp)?

Mark only one oval.

- ◯ Standard multimedia/picture message ONLY
- ◯ App based messaging service (such as WhatsApp) ONLY
- ◯ BOTH by Standard multimedia/picure messages and App based messages

18. (2.7) Do you currently have any patient related clinical information STORED on your Smartphone? (NOTE: the answer to this question will be 'Yes' if you have previously sent such information via text messages or App based messaging services and not manually deleted the information afterwards. Further, any deleted photos, are usually subsequently stored in a file named 'deleted photos' on your Smartphone and associated cloud, for 30 days by default). *

Mark only one oval.

- ◯ Yes
- ◯ No
- ◯ Not sure

19. (2.8) Please indicate how often you use the following FUNCTIONALITY of your Smartphone to help you with your clinical activities at work. *

Check all that apply.

	Not used	Less than once a month	Once a month	2 to 3 times a month	Once a week	2-3 times a week	Throughout the day, each day
Phone calling	☐	☐	☐	☐	☐	☐	☐
SMS messaging	☐	☐	☐	☐	☐	☐	☐
Picture/ multi-media messaging	☐	☐	☐	☐	☐	☐	☐
App based messaging (e.g. whatsApp)	☐	☐	☐	☐	☐	☐	☐
Employer issued Email	☐	☐	☐	☐	☐	☐	☐
Private Email – e.g. Gmail or Yahoo Email	☐	☐	☐	☐	☐	☐	☐
Employer issued video conferencing e.g. Skype for Business/ Microsoft Teams	☐	☐	☐	☐	☐	☐	☐
Zoom, Skype, Facetime, Facebook Messenger etc.	☐	☐	☐	☐	☐	☐	☐

20. (2.9) Do you own any other form of Smart device (e.g. Tablet, Smartwatch, Fitness tracker etc.)? *

Mark only one oval.

- ◯ Yes
- ◯ No

21. (2.10) What other types of device do you own? *

Check all that apply.

- ☐ Apple Smartwatch
- ☐ Android Smartwatch
- ☐ Windows Smartwatch
- ☐ Fitbit
- ☐ Jawbone
- ☐ Other brand of fitness tracker
- ☐ Tablet Device (iPad, Android Tablet etc.)
- ☐ None
- ☐ Other: _____

22. (2.11) Do your Smartphone and mobile technology devices (Fitness Tracker, Tablet, Smartwatch, Laptop etc) stream and share work related material between each-other? *

Mark only one oval.

- ◯ Yes
- ◯ No
- ◯ Maybe
- ◯ I do not own multiple devices

23. (2.12) Do your B.Y.O.D.s stream work related data to the cloud? *

Mark only one oval.

- ◯ Yes
- ◯ No
- ◯ Maybe

24. (2.13) Are you expected to use any particular Apps for clinical communications? *

Mark only one oval.

- ◯ Yes
- ◯ No (If no, please skip to question (2.15))

25. (2.14) Please list any Apps that you are required to use for clinical communications:

26. (2.15) Since the COVID 19 Pandemic, are you MORE FREQUENTLY using Smartphone App based communications tools for clinical communications? *

Mark only one oval.

- ◯ Yes
- ◯ No
- ◯ Maybe

27. (2.16) Since the COVID 19 Pandemic, have you started to engage in VIDEO CONSULTATIONS with patients or clinical colleagues? *

Mark only one oval.

- ◯ Yes - via laptop or desktop computer
- ◯ Yes - via Smartphone
- ◯ Both of the above
- ◯ No
- ◯ Other: _____

28. (2.17) Since the COVID 19 Pandemic, are you and your clinical colleagues using any of these video conferencing tools to consult with colleagues or patients? *

Check all that apply.

- ☐ Microsoft Teams - via laptop or desktop computer
- ☐ Microsoft Teams - via Smartphone
- ☐ Zoom - via laptop or desktop computer
- ☐ Zoom - via Smartphone
- ☐ Skype - via laptop or desktop computer
- ☐ Skype - via Smartphone
- ☐ Skype For Business - via laptop or desktop computer
- ☐ Skype For Business - via Smartphone
- ☐ WhatsApp - via laptop or desktop computer
- ☐ WhatsApp - via Smartphone
- ☐ Facetime - via laptop or desktop computer
- ☐ Facetime - via Smartphone
- ☐ Facebook Messenger - via laptop or desktop computer
- ☐ Facebook Messenger - via Smartphone
- ☐ No - I am not using any of these tools
- ☐ Other: _____

29. (2.18) Have you been required to use Apps for any other purpose – such as PDF creator Apps? *

Mark only one oval.

- ◯ Yes
- ◯ No (if no, please skip to question (2.20))

30. (2.19) Please list the Apps are you required to use and for what purpose? (eg. PDF creator Apps)

31. (2.20) Since the COVID 19 Pandemic, are you using more Smartphone Apps to process work related data? *

Mark only one oval.

- ◯ Yes
- ◯ No
- ◯ Unsure

TO EVALUATE YOUR LEVEL OF FAMILIARITY WITH THE GUIDELINES AND RISKS

32. (3.0) In relation to the following statement, please select the response that reflects YOUR PERCEPTION: "I am aware of the risks associated with the use of Smartphones/Smart devices for the communication of work related data." *

Mark only one oval.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

33. (3.1) DIGITAL PROFESSIONALISM has been defined as "the competence or values expected of a professional when engaged in social, digital communication and mobile technology ". Consider the statement above and respond to the following - "I am adequately skilled in digital professionalism." *

Mark only one oval.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

34. (3.2) Consider the scenario where you are about to replace your mobile device: Are you aware of any IT support or training with regard to how you can CLEAN or WIPE your B.Y.O.D. of any patient identifiable data when you trade in or trade up? *

Mark only one oval.

- No (Please skip the next question and go to question (3.4))
- Yes

35. (3.3) Could you please list where this support would come from? (eg. main employer)

36. (3.4) Do you feel that such support would be/is useful? *

Mark only one oval.

- Yes
- No

37. (3.5) Is there anything else you feel could have been usefully included in this questionaire? If so, please feel free to leave a note below.

38. (3.6) Would you be happy to take part in an an in depth FOLLOW UP interview, to provide more details as part of this study? *

Mark only one oval.

- No
- Yes (if so, could you please provide your contact details below)

39. (3.7) Address;

40. (3.8) Telephone number

41. (3.9) Email Address

Thank you....

42. Any data provided will be processed and stored securely in accordance with UCC's Data Protection Policy and procedures and in compliance with the Data Protection Acts 1988 - 2018 ("DPA"). The DPA allows us to process your data because you have provided your explicit consent. You are entitled to withdraw your consent at anytime. If you do withdraw your consent, we will no longer process your personal data and will take steps to delete all reference to your data securely. Your personal data will be retained for 12-months when it will be securely destroyed. If you wish to correct/amend your personal details, please contact me, Bernadette John, at 118225957@umail.com or Dr Christine McCreary (c.mccreary@ucc.ie). If you wish to access your data or have any further queries or concerns with regard to the way your personal data is being processed, please contact the University's Information Compliance Manager (email foi@ucc.ie or telephone +353 (0)21 4903949. You have a right to complain to the Data Protection Commission about the way in which we process your personal data. Details of how to lodge a complaint can be found on the Data Protection Commission website at https://www.dataprotection.ie/docs/Making-a-Complaint-to-the-Data-Protection-Commissioner/r/18.htm Please press 'Submit' below to complete your submission and that you have read and understood the above.

This content is neither created nor endorsed by Google.

Google Forms

APPENDIX 10 SURVEY TOOL UK

A Study of the Prevalence and Factors influencing the Use of Smartphone and Mobile Technology for the Communication of Patient Data by Clinicians in the UK and Republic of Ireland.

Thank you for agreeing to participate in this research project. You have indicated that you are a DENTIST or a DENTAL CARE PROFESSIONAL working in the UK, and we are seeking your views and current practice in the use of personal mobile technology in your clinical roles/workplace.

* Indicates required question

CHARACTERISTICS OF PARTICIPANT

About you

1. (1.0) Please select your AGE *

Mark only one oval.

- ◯ 20-29 years
- ◯ 30-39 years
- ◯ 40-49 years
- ◯ 50-59 years
- ◯ 60-69 years
- ◯ 70 years or greater
- ◯ Prefer not to say

2. (1.1) Please select your GENDER *

Mark only one oval.

- Female
- Male
- Non-binary
- Prefer not to say

3. (1.2) Who is your MAIN employer? *

Mark only one oval.

- National Health Service
- Voluntary Sector
- Private Sector
- Not employed - Part Time Student
- Not Employed - Full Time Student
- Third Level Institution
- Not Currently Employed (Skip to (1.4))
- Other: _____

4. (1.3) Details of place of MAIN Employment: *

Mark only one oval.

- National Health Service
- Voluntary Sector
- Private Sector - General Dental Practice
- Third Level Institution
- Not currently employed
- Other: _____

5. (1.4) YEARS since first registration of a Dentist or Dental Care Professional : *

Mark only one oval.

- ◯ Less than 1 year
- ◯ 1-2 years
- ◯ 3-5 years
- ◯ 6-10 years
- ◯ Over 10 years
- ◯ N/A

6. (1.5) Details of registrations with The General Dental Council of Ireland *

Check all that apply.

- ☐ Dentist
- ☐ Dental Hygienist
- ☐ Dental Nurse
- ☐ Clinical Dental Technician
- ☐ Not registered with The Dental Council of Ireland
- ☐ Dental Therapist
- ☐ Dental Technician
- ☐ Orthodontic Therapist
- ☐ Other: _____

7. (1.6) Current role details (for which you are MAINLY employed): *

Mark only one oval.

- ◯ Dentist
- ◯ Dental Hygienist
- ◯ Dental Nurse
- ◯ Clinical Dental Technician
- ◯ Clinical Teacher
- ◯ Lecturer
- ◯ Working in research
- ◯ Working in an administrative post
- ◯ Postgraduate student (MPhil, PhD)
- ◯ Not currently employed
- ◯ Dental Therapist
- ◯ Dental Technician
- ◯ Orthodontic Therapist
- ◯ Other: _____

8. (1.7) HIGHEST level of educational attainment: *

Mark only one oval.

- ◯ Certificate
- ◯ Diploma
- ◯ Bachelor's degree (BDS)
- ◯ Post- graduate Qualification (e.g. certificate, diploma)
- ◯ Master's degree (MSc)
- ◯ Doctoral Degree (PhD)
- ◯ Other: _____

9. (1.8) LOCATION of employment: *

Mark only one oval.

- ◯ Scotland
- ◯ Northern ireland
- ◯ Wales
- ◯ England
- ◯ The Islands (Shetland, Isle of Man, Isle of Wight, etc)
- ◯ Other: _____

10. (1.9) With regard to your SPECIALITY, do you work MAINLY in: *

Mark only one oval.

- ◯ Dental Public Health
- ◯ Endodontics
- ◯ Periodontics
- ◯ Prosthodontics
- ◯ Restorative Dentistry
- ◯ Oral Medicine
- ◯ Oral Radiology
- ◯ Oral Surgery
- ◯ Orthodontics
- ◯ Student
- ◯ Non-clinical post (e.g. researcher)
- ◯ General Dental Practice
- ◯ Other: _____

To identify rationale for and prevalence of the use of personal Bring your own Device (B.Y.O.D.) Smartphone and Mobile Technology to transmit patient data by Clinicians in the Republic of Ireland. Please consider each of the following questions in turn. Politely, we request that once you have selected an answer from the options provided, that you don't return to questions and amend your previous answers on the basis of the information learned/provided.

11. (2.0) Do you own a Smartphone? *

Check all that apply.

- [ ] Yes
- [ ] No (Skip to question (2.2))

12. (2.1) What type of Smartphone do you own (if you have more than one, what is the MAIN phone you use at/for work)?

Mark only one oval.

- ◯ iPhone (Apple)
- ◯ Android (e.g. Samsung, Huawei)
- ◯ Other

13. (2.2) In relation to the following statement, please select the response that reflects YOUR PERCEPTION: "I have the technological skills to use a Smartphone". *

Mark only one oval.

- ◯ Strongly Disagree
- ◯ Disagree
- ◯ Neutral
- ◯ Agree
- ◯ Strongly Agree

14. (2.3) How USEFUL do you find your Smartphone in helping you with the MEANINGFUL EXCHANGE OF CLINICAL INFORMATION? -e.g To assist with assessment, diagnosis, treatment or any part of the overall management a patient. *

Mark only one oval.

- ◯ Extremely useful
- ◯ Very useful
- ◯ Moderately useful
- ◯ Slightly useful
- ◯ Not useful at all

15. (2.4) Have you used your Smartphone to communicate PATIENT RELATED CLINICAL INFORMATION to colleagues using: *

Mark only one oval per row.

	Never	Once	Monthly	Weekly	Daily
SMS text or iMessage?	◯	◯	◯	◯	◯
An App based messaging service (e.g. WhatsApp)?	◯	◯	◯	◯	◯

16. (2.5) Have you ever used your Smartphone to PHOTOGRAPH patient related clinical information to share with a colleague (for example: photographing a patient's wound or X-ray or test result to consult a colleague for an opinion)? *

Mark only one oval.

- ◯ Never (skip to question (2.7))
- ◯ Once
- ◯ Monthly
- ◯ Weekly
- ◯ Daily

17. (2.6) Did you SEND the photograph(s) as standard multimedia/picture messages or using an App based messaging service (such as WhatsApp)?

Mark only one oval.

- ◯ Standard multimedia/picture message ONLY
- ◯ App based messaging service (such as WhatsApp) ONLY
- ◯ BOTH by Standard multimedia/picure messages and App based messages

18. (2.7) Do you currently have any patient related clinical information STORED on your Smartphone? (NOTE: the answer to this question will be 'Yes' if you have previously sent such information via text messages or App based messaging services and not manually deleted the information afterwards. Further, any deleted photos, are usually subsequently stored in a file named 'deleted photos' on your Smartphone and associated cloud, for 30 days by default). *

Mark only one oval.

- ◯ Yes
- ◯ No
- ◯ Not sure

19. (2.8) Please indicate how often you use the following FUNCTIONALITY of your Smartphone to help you with your clinical activities at work. *

Check all that apply.

	Not used	Less than once a month	Once a month	2 to 3 times a month	Once a week	2-3 times a week	Throughout the day, each day
Phone calling	☐	☐	☐	☐	☐	☐	☐
SMS messaging	☐	☐	☐	☐	☐	☐	☐
Picture/ multi-media messaging	☐	☐	☐	☐	☐	☐	☐
App based messaging (e.g. whatsApp)	☐	☐	☐	☐	☐	☐	☐
Employer issued Email	☐	☐	☐	☐	☐	☐	☐
Private Email – e.g. Gmail or Yahoo Email	☐	☐	☐	☐	☐	☐	☐
Employer issued video conferencing e.g. Skype for Business/ Microsoft Teams	☐	☐	☐	☐	☐	☐	☐
Zoom, Skype, Facetime, Facebook Messenger etc.	☐	☐	☐	☐	☐	☐	☐

20. (2.9) Do you own any other form of Smart device (e.g. Tablet, Smartwatch, Fitness tracker etc.)? *

Mark only one oval.

- ◯ Yes
- ◯ No

21. (2.10) What other types of device do you own? *

Check all that apply.

- ☐ Apple Smartwatch
- ☐ Android Smartwatch
- ☐ Windows Smartwatch
- ☐ Fitbit
- ☐ Jawbone
- ☐ Other brand of fitness tracker
- ☐ Tablet Device (iPad, Android Tablet etc.)
- ☐ None
- ☐ Other: _____

22. (2.11) Do your Smartphone and mobile technology devices (Fitness Tracker, Tablet, Smartwatch, Laptop etc) stream and share work related material between each-other? *

Mark only one oval.

- ◯ Yes
- ◯ No
- ◯ Maybe
- ◯ I do not own multiple devices

23. (2.12) Do your B.Y.O.D.s stream work related data to the cloud? *

Mark only one oval.

- ◯ Yes
- ◯ No
- ◯ Maybe

24. (2.13) Are you expected to use any particular Apps for clinical communications? *

Mark only one oval.

- ◯ Yes
- ◯ No (If no, please skip to question (2.15))

25. (2.14) Please list any Apps that you are required to use for clinical communications:

26. (2.15) Since the COVID 19 Pandemic, are you MORE FREQUENTLY using Smartphone App based communications tools for clinical communications? *

Mark only one oval.

- ◯ Yes
- ◯ No
- ◯ Maybe

27. (2.16) Since the COVID 19 Pandemic, have you started to engage in VIDEO CONSULTATIONS with patients or clinical colleagues? *

Mark only one oval.

- ◯ Yes - via laptop or desktop computer
- ◯ Yes - via Smartphone
- ◯ Both of the above
- ◯ No
- ◯ Other: _____

28. (2.17) Since the COVID 19 Pandemic, are you and your clinical colleagues using any of these video conferencing tools to consult with colleagues or patients? *

Check all that apply.

- ☐ Microsoft Teams - via laptop or desktop computer
- ☐ Microsoft Teams - via Smartphone
- ☐ Zoom - via laptop or desktop computer
- ☐ Zoom - via Smartphone
- ☐ Skype - via laptop or desktop computer
- ☐ Skype - via Smartphone
- ☐ Skype For Business - via laptop or desktop computer
- ☐ Skype For Business - via Smartphone
- ☐ WhatsApp - via laptop or desktop computer
- ☐ WhatsApp - via Smartphone
- ☐ Facetime - via laptop or desktop computer
- ☐ Facetime - via Smartphone
- ☐ Facebook Messenger - via laptop or desktop computer
- ☐ Facebook Messenger - via Smartphone
- ☐ No - I am not using any of these tools
- ☐ Other: _____

29. (2.18) Have you been required to use Apps for any other purpose – such as PDF creator Apps? *

Mark only one oval.

- ◯ Yes
- ◯ No (if no, please skip to question (2.20))

30. (2.19) Please list the Apps are you required to use and for what purpose? (eg. PDF creator Apps)

31. (2.20) Since the COVID 19 Pandemic, are you using more Smartphone Apps to process work related data? *

Mark only one oval.

- ◯ Yes
- ◯ No
- ◯ Unsure

TO EVALUATE YOUR LEVEL OF FAMILIARITY WITH THE GUIDELINES AND RISKS

32. (3.0) In relation to the following statement, please select the response that reflects YOUR PERCEPTION: "I am aware of the risks associated with the use of Smartphones/Smart devices for the communication of work related data." *

Mark only one oval.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

33. (3.1) DIGITAL PROFESSIONALISM has been defined as "the competence or values expected of a professional when engaged in social, digital communication and mobile technology ". Consider the statement above and respond to the following - "I am adequately skilled in digital professionalism." *

Mark only one oval.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

34. (3.2) Consider the scenario where you are about to replace your mobile device: Are you aware of any IT support or training with regard to how you can CLEAN or WIPE your B.Y.O.D. of any patient identifiable data when you trade in or trade up? *

Mark only one oval.

- No (Please skip the next question and go to question (3.4))
- Yes

35. (3.3) Could you please list where this support would come from? (eg. main employer)

36. (3.4) Do you feel that such support would be/is useful? *

Mark only one oval.

- Yes
- No

37. (3.5) Is there anything else you feel could have been usefully included in this questionaire? If so, please feel free to leave a note below.

38. (3.6) Would you be happy to take part in an an in depth FOLLOW UP interview, to provide more details as part of this study? *

Mark only one oval.

- No
- Yes (if so, could you please provide your contact details below)

39. (3.7) Address;

40. (3.8) Telephone number

41. (3.9) Email Address

Thank you....

42. Any data provided will be processed and stored securely in accordance with UCC's Data Protection Policy and procedures and in compliance with the Data Protection Acts 1988 - 2018 ("DPA"). The DPA allows us to process your data because you have provided your explicit consent. You are entitled to withdraw your consent at anytime. If you do withdraw your consent, we will no longer process your personal data and will take steps to delete all reference to your data securely. Your personal data will be retained for 12-months when it will be securely destroyed. If you wish to correct/amend your personal details, please contact me, Bernadette John, at 118225957@umail.com or Dr Christine McCreary (c.mccreary@ucc.ie). If you wish to access your data or have any further queries or concerns with regard to the way your personal data is being processed, please contact the University's Information Compliance Manager (email foi@ucc.ie or telephone +353 (0)21 4903949. You have a right to complain to the Data Protection Commission about the way in which we process your personal data. Details of how to lodge a complaint can be found on the Data Protection Commission website at https://www.dataprotection.ie/docs/Making-a-Complaint-to-the-Data-Protection-Commissioner/r/18.htm Please press 'Submit' below to complete your submission and that you have read and understood the above.

This content is neither created nor endorsed by Google.

Google Forms

APPENDIX 11 ENTITIES CONTACTED (PUBLICATION 6, PAPER 4.)

Number	Name	"X" Handle	Contact Details	Country
1	Royal College of Anaesthetists	@RCoAnews		UK
2	British Dental Association (BDA)		enquiries@bda.org	UK
3	Faculty of Dental Surgery at The Royal College of Surgeons	@FDS_RCS		UK
4	Faculty of Dental surgery of Edinburgh (Royal College of Surgeons of Edinburgh)	@RCSEdFDS		UK
5	Royal College of Emergency Medicine	@RCollEM	communications@rcem.ac.uk	UK
6	Royal College of General Practitioners	@RCGP		UK
7	Faculty of Intensive Care Medicine	@FICMNews		UK
8	Royal College of Obstetricians and Gynaecologists	@RCObsGyn		UK
9	Faculty of Occupational Medicine	@FOMNews		UK
10	Royal college of Ophthalmologists	@RCOPhth		UK
11	Royal College of Paediatrics and Child Health	@RCPCH		UK
12	Royal College of Pathologists	@RCPATH	comms@rcpath.org	UK
13	Faculty of Pharmaceutical Medicine	@FacultyPharmMed		UK
14	Royal College of Physicians of Edinburgh	@RCPEdin		UK
15	Royal College of Physicians of Ireland	@RCPI_news		Ireland
16	Royal College of Physicians	@RCPhysicians		UK
17	Royal College of Physicians and Surgeons of Glasgow	@rcpsglasgow		UK
18	Royal College of Psychiatrists	@rcpsych	press@rcpsych.ac.uk	UK
19	Royal College of Psychiatrists in Scotland		pressscotland@rcpsych.ac.uk	UK
20	Faculty of Public Health	@FPH	JulianRyder@fph.org.uk news@fph.org.uk	UK
21	Royal College of Radiologists	@RCRadiologists		UK
22	Faculty of Sexual and Reproductive Health	@FSRH_UK		UK

23	Royal College of Surgeons of Edinburgh	@RCSEd	pressoffice@rcsed.ac.uk rcsed@tigerbond.com comms@rcsed.ac.uk	UK
24	Royal College of Surgeons of England	@RCSnews	PressOffice@rcseng.ac.uk (+44) 20 7869 6053	UK
25	Royal college of Surgeons of Ireland	@RCSI_Irl		Ireland
26	Faculty of Sport and Exercise Medicine UK	@FSEM_UK		UK
27	Royal College of Nursing	@RCN	Contact Box on RCN Website	UK
28	Royal College of Midwives	@MidwivesRCM	Contact Box on RCM Website	UK
29	Nursing and Midwifery Board of Ireland	@NMBI	EducationandGuidance@NMBI.ie	Ireland
30	Irish Nurses and Midwives Organisation (INMO)		aileen.garrihy@inmo.ie	Ireland
31	Health Service Executive (HSE)	@HSELive	Kavish.Naicker@hse.ie	Ireland
32	General Medical Council (GMC)	@GMCUK	gmcpress@gmc-uk.org standards@gmc-uk.org (+44) 161 923 6602	UK
33	Irish Medical Council	@MedCouncilIRL	educationandtraining@mcirl.ie rachael.kelly@mcirl.ie	Ireland
34	College of Anaesthesiologists of Ireland	@COAIrl		Ireland
35	MediSec (professional indemnity)	@MedisecIreland	info@medisec.ie	Ireland
36	Irish College of General Practitioners	@ICGPnews	library@icgp.ie	Ireland
37	Irish College of Ophthalmologists	@eyedoctorsIRL D39@IALabs @Vision_Irl		Ireland
38	The Irish Dental Association (IDA)	@IrishDentists		Ireland
39	Dental Council of Ireland	@DentalCouncilPr	Ino@dentalcouncil.ie	Ireland
40	The British Association of Oral Surgeons (BAOS)	@BAOS_UK		UK
41	The British Orthodontic Society (BOS)	@BOSbraces		UK
42	Irish Society for Dentistry for Children	@isdc_ie		Ireland
43	Orthodontic Society of Ireland	@Orthosocirl- OSI		Ireland

44	Queen Victoria hospital trust		qvh.communications@nhs.net	UK
45	The Medical Defence Union (MDU)	@the_mdu		UK
46	The British Medical Association (BMA)		SAdmin@bma.org.uk support@bma.org.uk SAdmin@bma.org.uk (+44) 300 123 1233	UK
47	Princess Royal University Hospital (PRUH), CEO	@AngelaHelleur		UK
48	Midwife for the Highlands and Islands, Confidential personal communication - asking for her NHS Trust policy			UK
49	The Nursing and Midwifery Council (NMC)	@NMCnews	media@nmc-uk.org	UK
50	St Vincents hospital		Dataprotection@st-vincents.ie dataprotection@st-vincents.ie	Ireland
51	Great Ormond St Hospital (GOSH)		SAR@gosh.nhs.uk media@gosh.nhs.uk	UK
52	General Dental Council (GDC)	@GDC_UK	communications@gdc-uk policyinbox@gdc-uk.org	UK
53	Medical Protection (MP)	@MPS_Medical	education@medicalprotection.org replyeventsupport@medicalprotection.org	UK
54	The Mater Private Hospital	@materprivate	dataprotectionofficer@materprivate.ie	Ireland
55	Blackrock Health (Private Health Group)		dpo@blackrockhealth.ie	Ireland
56	Blackrock Clinic (Private Hospital)		DPO@Blackrock-clinic.com	Ireland
57	Hermitage Clinic (Private Hospital)		dpo@hermitageclinic.ie	Ireland
58	Galway Clinic (Private Hospital)		dpo@galwayclinic.com	Ireland
59	The Beacon Hospital (Private Hospital)		dataprotection@beaconhospital.ie margaret.callanan@beaconhospital.ie	Ireland
60	St James Hospital		dataprotection@stjames.ie	Ireland
61	National Health Service (NHS)	@NHSuk		UK
62	Cork University Hospital (CUH)	@CUH_Cork		Ireland

63	The Dental Defence Union (DDU)	@the_ddu		Ireland
64	University Hospital Dorset NHS Trust (UHD)		richard.moremon@uhd.nhs.uk	UK
65	Kings College Hospital NHS Trust		kch-tr.FOI@nhs.net https://www.kch.nhs.uk/document/freedom-of-information-request-form	UK
66	Leicestershire Partnership NHS Trust		https://www.leicspart.nhs.uk/about/freedom-of-information-requests/ website	UK
67	The Mater (HSE Public Hospital)		info@mater.ie (+353) 1 803 2333	Ireland
68	Leicestershire Partnership NHS Trust		LPT.DataPrivacy@nhs.net	Ireland
69	The Wellcome Trust		https://wellcome.org/who-we-are/contact-us	UK

APPENDIX 12 DATA DIMENSION ARTEFACT VERSION 1.0 (DDA V1.0)

1				
2	**RESEARCH QUESTION**		**SMARTPHONE AND MOBILE TECHNOLOGY FOR THE COMMUNICATION OF PATIENT DATA**	
3	**Dimensions**		**Characteristic**	
4				**Paper 1**
6	**1.Accuracy**		Does the publication cite or align with credible cyber security sources?	
7			Do the authors describe how to use free third-party Apps on BYOD for secure and confidential communication?	
8	**2.**		Is a clear rationale for the use of a free third-party App described?	
9	**Completeness**		Has a formal risk assessment been conducted and has the need for such (a DPIA in the EU) been explained?	
10		**2.1 Confidentiality**	Does the publication consider and describe compliance with applicable laws and regulations, such as GDPR in the EU or HIPAA in the US?	
12			Do the authors verify that the App does not access sensitive metadata in exchange for access to its functionality, or do they describe how to limit its access?	
13			Is it specified that BYOD should never access free Wi-Fi if hosting or processing sensitive data?	

14			Is it stated that unauthorised users must be prevented from accessing any device on which sensitive data is hosted?	
15			Do authors forbid the hosting of any suspicious Apps on the BYOD along with the free of charge communications App?"	
16		**2.2 Integrity**	Are data encryption, data security in transit and at rest, and server location and security explicitly considered?	
17			Is configuration of the App (e.g., disabling image and data streaming to networked devices and unsecured cloud servers/hosts) addressed?	
18			Are security settings, password protection and MFA of App discussed?	
19			Is the requirement for regular training or briefings on security awareness and ongoing scrutiny of the App explained?	
20		**2.3 Availability**	Has the network capacity, network coverage, power usage, and data accessibility been evaluated?	
21			Are there clear instructions provided regarding record keeping of chat/images in the patient record, such as regularly scheduled downloading and deletion of sensitive data from both the senders' and receivers' Apps and devices?	
22	**3. Currency**		Is the publication date after May 2018?	
23			Are there scheduled updates, or does the content come from a source that regularly provides updated information?	
24	**4. Relevance**		Is guidance provided on how to use the relevant functionality for maximum security and in compliance with data protection regulations?	

25			Have the legal and ethical issues concerning informed consent from patients been discussed and explained?	
26	**5. Clarity**		Is the terminology in the publication readily understood?	
27			Is it easy to interpret the publication to influence clinical practice?	
28	**6. Credibility**		Is the content applicable to a specific jurisdiction? For instance, if it's published within the EU (or UK), GDPR requirements must be specified and adhered to, but if it's the USA, the requirements for HIPAA must apply.	
29			Is the source of this publication credible to clinicians?	
30			Is the publication free of sponsorship and is there no bias declared?	
31	**7. Accessible**		Is the content of this paper freely accessible?	

APPENDIX 13 GLOSSARY OF TERMS FOR DATA DIMENSION ARTEFACT

Glossary	
Bluetooth	Is a standard for the short-range wireless interconnection of mobile phones, computers and other electronic devices.
BYOD	Bring Your Own Device, bring your own personally owned technology - phone, laptop, tablet rather than an officially provided device.
GDPR	General Data Protection Regulation (2018) as stipulated for use across the European Union, and currently also being adhered to by the UK.
MFA - Multi Factor Authentication	Multi Factor Authentication - is an electronic method of authentication which grants the user access to a digital resource such as an app only after successfully presenting two or more pieces of evidence to an authentication mechanism.
Sovereignty of data	Data sovereignty is the idea that data are subject to the laws and governance structures of the nation where they are collected. The concept of data sovereignty is closely linked with data security, cloud computing, network sovereignty and technological sovereignty.
Suspicious App	A suspicious or malicious App is an App that potentially acts as malware, that may steal data or harm the device on which it is hosted.
Third Party App	An App that was not created by the same party that created the device on which it is hosted. When downloading such Apps it is usually a condition of use that you allow the App to access some functionality as well as access to your data. Generally, this data is used to generate income by allowing targeted advertising, but it can also be used for more harmful purposes if it falls into the wrong hands.
Wi-Fi	A facility allowing computers, smartphones, tablets, laptops and other devices to connect to the internet or to communicate with one another wirelessly within a particular area.

APPENDIX 14 DATA DIMENSION ARTEFACT V1.0 (DDA V1.0) INFORMATION SHEET

Title:	**Data Quality Dimensions - BYOD, IM & Third-party Apps for the Communication of Data between clinicians**
Purpose:	The purpose of this model is to measure the quality of advice in guidelines that inform the use of BYOD, IM & Third-party Apps on BYOD for communication between clinicians.
Key Question:	What jurisdiction does the advice and guidelines outlined in this publication pertain to?
How to use the model:	These seven dimensions of data quality aim to assess the quality of the guidance provided to support the secure communication of sensitive data between clinicians. The following provides detail of the dimension and sub-dimensions with supporting definitions/explanations of each of these.
Instructions:	Complete rows 7 onwards with a YES/NO answers using the dimensions to be checked for within each publication. Under each dimension there are sub-dimensions to check against in each publication.

Column	Description	Definition	Defined By		
Row 6 to 7	**Accuracy**	Draws upon and aligns with the latest guidance from reputable cybersecurity sources like the National Cyber Security Centre (NCSC) in Ireland and/or the UK, the National Institute of Standards and Technology (NIST)	**Row 6** References or corresponds with credible cyber security sources.	**Row 7** Details secure/sensitive communications between professionals using BYOD and free of	

		in the USA, or insights from a software assurance professional/security analyst who has conducted specific App vetting. The document must explicitly mention widely used, free of charge, third-party communication Apps (e.g., WhatsApp, Signal, Trello).		charge, third party Apps.	
Row 8 to 20	**Completeness**	Refers to the inclusion of all necessary data attributes or values and does not overlook any significant security concerns related to App vulnerabilities, usage, and deployment.	**Row 8** A clear rationale or justification for the use of a free of charge, third party App (e.g. requirement for specific functionality or efficiency) should be established. This is necessary in	**Row 9** A full formal risk assessment (such as a Data Protection Impact Assessment (DPIA) if within the EU) on App(s) is described in the publication or the authors acknowledge the requirement for such	**Row 10** Relevant legislation and regulations such as GDPR (within the EU) or HIPAA (within the USA) considerations should be acknowledged and any

			order to establish an informed decision regarding the level of risk the clinician, as Data Processor, is prepared to accept.	to be carried out by Data Processors wishing to implement the use of a free of charge, third party App for secure communications?	compliance requirements described.
			Row 11 Metadata should not be exploited in exchange for functionality (if this is the case, efforts should be described to minimise access to this).	**Row 12** BYOD not to access free Wi-Fi or Bluetooth if hosting sensitive data.	**Row 13** No unauthorised users to access the device on which sensitive data is hosted (don't share device with your children!).

			Row 14 No suspicious Apps should be hosted on the BYOD on which the communications App is hosted.	**Row 15** Data encryption, protection of data in transit and at rest, the security and location of servers explained and explored.	**Row 16** Configuration of App to minimise risk – specific clear advice e.g. disable streaming of images and data to networked devices and insecure cloud servers/hosts for backup described as appropriate.

			Row 17 Settings, MFA of App and password protection of device.	**Row 18** Regular training on security awareness and continuous, ongoing scrutiny of the App.	**Row 19** Network capacity, network coverage, power usage, data accessibility established.
			Row 20 Record keeping of data (including dialogue, "chat", images) in patient record (e.g. regular scheduled downloading and subsequent deletion of sensitive data stored on App and device of both		

			sender and receiver(s)).		
Row 21 to 22	**Currency**	Pertains to the timeliness of the data. The publication needs to be shaped by the latest technical capabilities, given the rapidly evolving nature of technology and security threats, as well as changing legislation and regulations. It is essential for the publication to have a publication date, post-GDPR, preferably with scheduled updates, to maintain relevance and accuracy.	**Row 21** Publication date - at a minimum, must be post May 2018, post implementation of GDPR (but preferably within the last 2 years due to constantly advancing technology).	**Row 22** Updates scheduled (from a source that will update content regularly and remove or archive when no longer current (if this is a journal article, is it current enough to be relevant?).	

Row 23 to 24	**Relevant**	Concerns the inclusion of pertinent aspects of the topic that directly impact current clinical practice. This may involve adhering to ethical and legal obligations, such as obtaining explicit informed consent from patients before discussing their cases via a third-party App on the clinician's BYOD with the clinical team.	**Row 23** Provides detailed instructions on the use of current functionality of a relevant App to enhance security and ensure compliance with legislation, such as GDPR. For instance, it may recommend avoiding the backup of WhatsApp to an insecure cloud and propose generating a PDF of chat and images for download and storage in patients'	**Row 24** Ethical and legal Issues concerning informed consent from patients discussed and described.	

			digital or hard copy medical notes.		
Row 25 to 26	**Clarity**	Refers to the ease with which users can comprehend the advice, and the use of terminology that is easily understood.	**Row 25** Terminology readily understood.	**Row 26** Easy to interpret and to influence clinical practice.	
Row 27 to 29	**Credible**	Denotes the reliability of the publisher of the content. This might include recognised entities such a clinical defence union, healthcare providers such as the HSE/NHS, Royal Colleges, or	**Row 27** Concerns the jurisdiction in which the data is being processed, and the	**Row 28** A source credible to clinicians.	**Row 29** Free from sponsorship and no evidence of bias declared.

		reputable journals such The Lancet or the BMJ. The author should be an acknowledged expert in these issues, and the advice should be impartial, devoid of commercial sponsorship, or accompanied by a clear declaration of no bias.	professionals are working.		
Row 30	**Accessible**	Refers to the ease with which a publication can be accessed and retrieved. The full text publication should be fully and freely accessible to all clinicians. There should be full transparency of every source of information, unless the source of the publication is an authority on cyber security.	**Row 30** Open access (i.e. no subscription or membership should be required to access the publication).		

APPENDIX 15 DATA DIMENSION ARTEFACT V2.0 (DDA V 2.0)

1			**REVIEWER ID NO.**	
2	**RESEARCH QUESTION**		**SMARTPHONE TECHNOLOGY FOR THE COMMUNICATION OF PATIENT DATA**	
3	**Dimensions**		**Characteristic**	
4				**Paper 1**
6	**1.Accuracy**		Does the publication cite and align with credible cyber security sources?	
7			Is a description of how to use IM or third-party Apps on a BYOD smartphone for secure and confidential communication provided?	
8	**2. Completeness**		Is a clear rationale for the use of IM or third-party App on a personal BYOD smartphone for clinical communications described?	
9			Has the requirement for a formal risk assessment (for e.g. a DPIA in the EU) been explained?	
10		**2.1 Confidentiality**	Are regulations (such as GDPR (EU) or HIPAA (US)) and their relevance to BYOD, IM, and third-party Apps discussed and obligations described?	
11			Is verifying that an App does not access sensitive metadata in exchange for functionality, or steps to limit such access, discussed?	
12			Is it specified that BYOD should never access free Wi-Fi if hosting or processing sensitive data?	
13			Is it stated that unauthorised users must be prevented from accessing any device on which sensitive data is hosted?	

14			Is the importance of avoiding the installation of any suspicious Apps on personal BYOD devices used for confidential professional communication explained?	
15		**2.2 Integrity**	Are requirements regarding server location, data encryption, data security in transit and at rest, and relevance to BYOD, IM and third-party App clearly described?	
16			Are requirements for configuring of any third-party App (e.g., disabling image and data streaming to networked devices and unsecured cloud servers) explicitly described?	
17			Are security settings, password protection and MFA of device and or Apps discussed?	
18			Is the requirement for regular training or briefings on security stipulated?	
19			Is the need for a regular, scheduled review of the App clearly communicated?	
20		**2.3 Availability**	Is evaluation of the network capacity, network coverage, power usage, and data accessibility discussed?	
21			Are there clear instructions for record keeping of chat/images in patient records, inc. scheduled recording / downloading & deletion of confidential data from senders' & receivers' Apps & devices?	
22	**3. Timeliness**		Is the publication date after May 2018?	

23			Are there scheduled updates, or is the content from a source that regularly provides updated information? Is this publication recent enough to be relevant?	
24	**4. Relevance**		Does the guidance cover using relevant functionality for maximum security and compliance with data protection regulations?	
25			Are the legal and ethical issues of obtaining informed consent from patients discussed and explained in relation to the processing of their data on personal BYOD devices, IM or third-party Apps?	
26	**5. Clarity**		Is the terminology easily understood?	
27			Is the advice easy to interpret and apply in clinical practice?	
28	**6. Credibility**		Is the content specific to a jurisdiction, such as specifying GDPR requirements (EU/UK) or HIPAA requirements (USA)?	
29			Is the source of this publication credible to clinicians?	
30			Publication contains declaration of no bias, or no evidence of sponsorship or bias present	
31	**7. Accessible**		Is this publication freely accessible?	

APPENDIX 16 DATA DIMENSION ARTEFACT V2.0 (DDA V2.0) INSTRUCTION SHEET

Title:	**Data Quality Dimensions - BYOD, IM & Third-party Apps for the Communication of Data between clinicians**
Purpose:	The purpose of this model is to measure the quality of advice in briefing documents, guidelines or policies that inform the use of Personal BYOD smartphones, IM and third-party Apps for communication between clinicians.
Key Question:	What jurisdiction does the advice and guidelines outlined in this publication pertain to?
How to use the model:	These seven dimensions of data quality aim to assess the quality of the guidance provided to support the secure communication of sensitive data between clinicians. The following provides detail of the dimension and sub-dimensions with supporting definitions / explanations of each of these.
Instructions:	Complete rows 7 onwards with a YES / NO answers using the dimensions to be checked for within each publication. Under each dimension there are sub-dimensions to check against in each publication.

Column	Description	Definition	Defined By

Row 6 to 7	**Accuracy**	Draws upon and aligns with the latest guidance from reputable cybersecurity sources like the National Cyber Security Centre (NCSC) in Ireland and/or the UK, the National Institute of Standards and Technology (NIST) in the USA, or insights from a software assurance professional/security analyst who has conducted specific App vetting. The document must explicitly mention widely used third-party communication Apps (e.g., WhatsApp, Signal, Trello), IM, and or personal BYOD smartphones.	**Row 6** References or corresponds with credible cyber security sources.	**Row 7** Details secure/sensitive communications between professionals using personal BYOD, IM or third-party Apps.	

Row 8 to 21	**Completeness**	Refers to the inclusion of all necessary data attributes or values and does not overlook any significant security concerns related to personal BYOD smartphones, IM or third-party App vulnerabilities, usage, and deployment.	**Row 8** A clear rationale or justification for the use of personal smartphones, IM, and / or third-party App (e.g. requirement for specific functionality or efficiency) should be established. This is necessary in order to establish an informed decision regarding the level of risk the clinician, as Data Processor, is prepared to accept.	**Row 9** A full formal risk assessment (such as a Data Protection Impact Assessment (DPIA) if within the EU) on device and or App(s) should be described or acknowledge by the authors as a requirement for Data Processors wishing to implement the use of personal BYOD smartphone, IM, or third-party App for secure communications.	**Row 10** Relevant legislation and regulations such as GDPR (within the EU) or HIPAA (within the USA) considerations should be acknowledged and any compliance requirements described.

			Row 11 Metadata should not be exploited in exchange for functionality (if this is the case, efforts should be described to minimise access to this).	**Row 12** BYOD not to access free Wi-Fi or Bluetooth if hosting sensitive data. Advise on the use of VPNs and secure Wi-Fi practices such as encrypted Wi-Fi connections requiring a password and protected by WPA3 encryption.	**Row 13** No unauthorised users to access the device on which sensitive data is hosted (don't share device with your children!).
			Row 14 No suspicious Apps should be hosted on the BYOD on which the communications App is hosted.	**Row 15** Data encryption, protection of data in transit and at rest, the security and location of servers explained and explored.	**Row 16** Configuration of App to minimise risk – specific clear advice (for e.g. disable streaming of images and data to networked devices and insecure cloud

					servers/hosts for backup) provided.
			Row 17 Settings, MFA of App and password protection of device.	**Row 18** Is the requirement for regular training or briefings on security stipulated?	**Row 19** Is the need for a regular, scheduled review of the App clearly communicated?
			Row 20 Is evaluation of the network capacity, network coverage, power usage, and data accessibility discussed?	**Row 21** Are there clear instructions for record keeping of chat/images in patient records, including scheduled	

				downloading and/or transcribing and deletion of confidential data from senders' and receivers' Apps and devices?	
Row 22 to 23	**Timeliness**	Pertains to the timeliness of the data. The publication needs to be shaped by the latest technical capabilities, given the rapidly evolving nature of technology and security threats, as well as changing legislation and regulations. It is essential for the publication to have a publication date, post-GDPR, preferably with scheduled updates, to maintain relevance and accuracy.	**Row 22** Publication date - at a minimum, must be post May 2018, post implementation of GDPR (but preferably within the last 2 years due to constantly advancing technology).	**Row 23** Updates scheduled (from a source that will update content regularly and remove or archive when no longer current (is publication current enough to be relevant?).	

Row 24 to 25	**Relevant**	Concerns the inclusion of pertinent aspects of the topic that directly impact current clinical practice. This may involve adhering to ethical and legal obligations, such as obtaining explicit informed consent from patients before discussing their cases via a third-party App on the clinician's BYOD with the clinical team.	**Row 24** Provides detailed instructions on the use of current functionality of a relevant App to enhance security and ensure compliance with legislation, such as GDPR. For instance, it may recommend avoiding the backup of WhatsApp to an insecure cloud and propose generating a PDF of chat and images for download and storage in patients' digital or hard copy medical notes.	**Row 25** Ethical and legal Issues concerning informed consent from patients discussed and described.	

Row 26 to 27	**Clarity**	Refers to the ease with which users can comprehend the advice, and the use of terminology that is easily understood.	**Row 26** Terminology readily understood.	**Row 27** Easy to interpret and to influence clinical practice.	
Row 28 to 30	**Credible**	Denotes the reliability of the publisher of the content. This might include recognised entities such a clinical defence union, healthcare providers such as the HSE/NHS, Royal Colleges, or reputable journals such The Lancet or the BMJ. The author should be an acknowledged expert in these issues, and the advice should be impartial, devoid of commercial sponsorship, or accompanied by a clear declaration of no bias.	**Row 28** Concerns the jurisdiction in which the data is being processed, and the professionals are working.	**Row 29** A source credible to clinicians.	**Row 30** Free from sponsorship and no evidence of bias, or publications includes declaration of no bias.
Row 31	**Accessible**	Refers to the ease with which a publication can be accessed and retrieved. The full text publication should be fully and freely accessible to all clinicians. There should be full transparency of every source of	**Row 30** Open access (i.e. no subscription or membership should be required to access the publication).		

		information, unless the source of the publication is an authority on cyber security.			

APPENDIX 17 FOCUS GROUP SCRIPT

Introduction Script

for

Focus Group Discussions

Shandon Room, Oral Health Services Centre

Wednesday 26th June 9 – 14.00 pm.

Group A. Students,09.30 – 12.00, Group B. Qualified clinicians, 12.00 – 14.00

Welcome and Introduction:

Good morning everyone. Thank you all for being here today and for your willingness to participate in this focus group. My name is Bernadette John, and I am currently a PhD candidate at the dental school here at UCC. By background, I am a nurse with over 10 years of experience working in a medical school in the UK. Since 2007, I have been lecturing on Digital Professionalism, focusing on the opportunities and threats that social media and mobile technology pose to the professions.

Purpose of the Study:

The purpose of today's session is to gather your valuable feedback on a Model we have developed. This model is designed to help clinicians assess the quality of data used in clinical guidelines, specifically in the context of how smartphones and mobile technology might be used by clinicians for communicating patient data. Your insights will be instrumental in refining this tool to ensure it meets the practical needs of (future) clinicians like yourselves.

Structure of the Session:

We will begin with a brief overview of the artefact, which you have had the chance to review. Following this, we will go through a series of questions to understand your experience and thoughts about the tool. This will be an open discussion, and I encourage

everyone to share their honest opinions, whether positive or negative. Your feedback is important for the success of this project.

Confidentiality:

I want to assure you that all your responses will be kept confidential and used solely for the purposes of this research. Your names will not be associated with any of the feedback you provide.

Getting Started:

Let's start by briefly going around the room and introducing ourselves, and then we can dive into the discussion. Please feel free to speak openly and share your thoughts. Your input is incredibly valuable. Thank you again for being here, and let's get started.

Questions:

I have a set of questions to guide our discussion:

1. How long did it take you to use the Data Dimensions artefact to assess a single paper?
2. Do all of the dimensions and sub-dimensions included resonate with you? Why or why not?
3. Can you envisage using this artefact/tool in the future? Why or why not?
4. Based on your experience/opinion, are the data dimensions presented in the artefact complete/exhaustive? Why or why not? What is missing?
5. In your opinion, how could the data dimensions and supporting instruction guide be improved?
6. Would you recommend the use of the data dimensions artefact to a colleague? Why or why not?
7. Would you like to add any additional comments or provider further feedback on the artefact?

APPENDIX 18 STUDY SPECIFIC TRAINING

PG6009 Graduate Information literacy attended, and assessment passed, 10-12th February, 2020 – 5 credits acquired to complete year 1

PG7016 Systematic Reviews for the health Sciences completed, 27th – 29th May 2021, 5 credits acquired to complete year 2

PG7048 PhD Generic and Transferable Skills Portfolio (14 hours credit achieved for study days attended with QDA training on NVIVO software), 1500-2000 word write up to be completed. 5 Credits to be acquired to complete year 3

APPENDIX 19 ETHICAL APPROVAL (SOCIAL RESEARCH ETHICS APPROVAL FROM UCC)

Log 2018-131 - Approved

From: Ethics Committee, Social Research (srec@ucc.ie)

To: bernadettejhn@yahoo.co.uk

Date: Thursday, 30 April 2020 at 16:08 BST

Dear Bernadette
The Social Research and Ethics Committee has now approved your application Log 2018-131 entitled "A Study of the Prevalence and Factors influencing the Use of Smartphone and Mobile Technology for the Communication of Patient Data by Clinicians in the Republic of Ireland."

The committee wishes you every success with your research.
All the best
Liz

Please Note – if you wish to make any amendment/changes to research methods etc for this application you will need to submit an application amendment request which you can find at this link https://www.ucc.ie/en/research/support/ethics/socialresearch/faqs/#amendment-requests

The amendment below (January 2024) to the original Ethics approval was requested as one academic supervisor had retired and the data needed to be shared with an additional academic supervisor.

Re: SREC Application

From: Ethics Committee, Social Research (srec@ucc.ie)

To: C.Heavin@ucc.ie; bernadettejhn@yahoo.co.uk

Cc: a.roberts@ucc.ie

Date: Thursday, 4 January 2024 at 15:31 GMT

Dear Ciara and Bernadette,

The Social Research and Ethics Committee has now approved your application Log **2023-293** entitled "Smartphone and mobile technology for the communication of patient data ".

The Committee wishes you every success with your research.

Kind regards,
Maria

Maria FitzGerald Houlihan | Research Ethics Support| SREC| University College Cork | srec@ucc.ie
Website: https://www.ucc.ie/en/research/support/ethics/socialresearch/

The additional amendment below was required (in June 2024) as additional data was required and the original permission to conduct this research had elapsed.

Re: SREC ethics amendment request form

From: Ethics Committee, Social Research (srec@ucc.ie)

To: C.Heavin@ucc.ie; bernadettejhn@yahoo.co.uk

Date: Tuesday, 4 June 2024 at 08:54 BST

Dear Bernadette and Ciara,

The Social Research and Ethics Committee has now approved your amendment to application Log **2023-293A1-** entitled "Smartphone and mobile technology for the communication of patient data ".

In the event that research data collection extends beyond **30/06/2025,** please notify **srec@ucc.ie** via email.

The Committee wishes you every success with your research.

Kind regards,
Maria

Maria FitzGerald Houlihan | Research Ethics Support| SREC| University College Cork | srec@ucc.ie
Website: https://www.ucc.ie/en/research/support/ethics/socialresearch/