CORA Cork Open Research Archive
Cartlann Taighde Oscailte Chorcaí

Title	Privacy by Design: informed consent and Internet of Things for smart health
Authors	O'Connor, Yvonne;Rowan, Wendy;Lynch, Laura;Heavin, Ciara
Publication date	2017-09-19
Original Citation	O'Connor, Y., Rowan, W., Lynch, L. and Heavin, C. (2017) 'Privacy by Design: Informed Consent and Internet of Things for Smart Health', Procedia Computer Science, 113(Supplement C), pp. 653-658. doi: 10.1016/j.procs.2017.08.329
Type of publication	Article (peer-reviewed)
Link to publisher's version	http://www.sciencedirect.com/science/article/pii/S1877050917317398 - 10.1016/j.procs.2017.08.329
Rights	© 2017 The Authors. Published by Elsevier B.V. under a Creative Commons license - https://creativecommons.org/licenses/by-nc-nd/4.0/
Download date	2026-11-07 08:09:35
Item downloaded from	https://hdl.handle.net/10468/4850



UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 113 (2017) 653–658

Procedia Computer Science

www.elsevier.com/locate/procedia

International Workshop on Universal Design for IoT Smart Health (UDISH 2017)

Privacy by Design: Informed Consent and Internet of Things for Smart Health

Yvonne O'Connor*, Wendy Rowan, Laura Lynch, Ciara Heavin[a]

[a] *Health Information Systems Research Centre, Cork University Business School, University College Cork, Ireland.*

Abstract

Check: I accept the terms and conditions and privacy policy statements associated with this technological artefact! The informed consent process is becoming more of a challenge with the emergence of Internet of Things (IoT) as data may be collected without the digital health citizen being aware. It is argued in this paper that the first phase for universal usability of IoT within the smart health domain is to ensure that digital health citizens (i.e. user of technology) are fully aware of what they are consenting to when they register an account with such technological artefacts. This point is further reinforced by the proposed 'Privacy by Design' requirements associated with the forthcoming General Data Protection Regulation (GDPR). This paper proposes some practical approaches which should be considered when designing and developing IoT for data collection and data sharing within the health domain.

© 2017 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of the Conference Program Chairs.

Keywords: Informed Consent; IOT; Smart Health; Privacy by Design

1. Introduction

Technology advancements within the healthcare domain have moved from medical record keeping experiments in the 1960s[1], clinical decision support systems in 1990s[2] to mobile health applications in recent years[3]. The new wave of technology argued to have an impact on the delivery of healthcare services is known as the Internet of Things (IoT) phenomenon. While the concept of IoT first emerged in 1999[4], it is only in recent times that it has been applied within the healthcare domain. The healthcare industry faces many challenges including, but not limited to,

* Corresponding author. Yvonne O' Connor Tel.: +353-490-3344
E-mail address: Y.OConnor@ucc.ie

1877-0509 © 2017 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of the Conference Program Chairs.
10.1016/j.procs.2017.08.329

resource allocation, aging population, increase of patient admissions to hospitals, management of patient diseases, and the emergence of new diseases[5]. It is argued that the application of IoT can assist with addressing these health-related issues due to the various features and functionalities associated with IoT[6].

IoT has been widely defined across a number of domains, resulting in a lack of consensus around how it is defined[7]. In general, however, a common denominator across these definitions is that IoT refers to the use of the internet to interact with physical objects. Chahid, Benabdellah and Azizi (2017)[8] state that *"The Internet of Things represents a vision in which the Internet extends into the real world including everyday objects. Physical elements are no longer disconnected from the virtual world, but can be controlled remotely and serve as physical access points to Internet services."* As a result, the introduction of IoT from a health perspective has brought about many benefits in the areas of medical equipment and medication control (i.e. anti-counterfeit of medical equipment and medication, real-time monitoring and medical refuse information management), medical information management (i.e. patient information management, medical emergency management, medication storage management, blood information management, error prevention mechanism of pharmaceutical preparations, medical equipment and medication traceability, information sharing, neonatal anti-theft and alarm systems), telemedicine and mobile medical care and health management[9].

Conversely, IoT has been criticised from a security and privacy perspective[10]. In 2013, the first IoT botnet was discovered by a researcher at Proofpoint security firm[11]. This had serious implications for the security and privacy of IoT users as this botnet was found to be collecting personal information like users' names and telephone numbers, but also monitored user activities without the user being aware of this data acquisition. It is argued that these security and privacy issues remain nowadays[6]. Although this example did not occur within a healthcare context, it nonetheless highlights that the process of informed consent with IoT needs to be addressed[12]. Informed consent requires that the user of IoT fully understands how/why their data will be utilised and the advantages, disadvantages and achievable outcomes associated with use of their data[13]. However, due to the ubiquitous nature of IoT this is becoming more of a challenge as data may be collected without the digital health citizen being aware.

The remainder of this paper is structured as follows: Section 2 speaks to the concepts of privacy by design, informed consent and universal usability. We argue that all three concepts must be integrated to ensure that universal design for IoT smart health can be achieved. To facilitate this, it is important that the current drawbacks to these approaches (documented in Section 2) are addressed and thus, a proposed practical approach to IoT smart health is provided (Section 3). Section 4 concludes the paper with an overview of future work and the contributions of this research to theory and practice.

2. Privacy by Design, Informed Consent and Universal Usability

From the 25th May 2018, the General Data Protection Regulation (GDPR) will come into effect mandating that data controllers and processors are required to emphasise transparency, security and accountability, while concurrently standardising and strengthening the right of European citizens to data privacy[14]. Essentially, data controllers and processors must embrace 'Privacy by Design'. The concept of Privacy by Design is not new[15]. Instead, it is acquiring more attention in practice and in academia due to the forthcoming GDPR, which if not adhered to will result in financial penalties. Privacy by Design promotes and demands that data controllers and processors are proactive in addressing the privacy implications of any new or upgraded system, procedure, policy or data-sharing initiative, throughout its planning phase and its full lifecycle. Therefore, this concept should be at the forefront of people's minds when IoT is implemented within healthcare scenarios.

One of the central principles underpinning GDPR is to increase digital citizen awareness surrounding consent for data processing and usage. This has considerable implications for data processing and usage in a healthcare context[16]. To ensure digital citizens are informed when consenting to the use of IoT, within the health domain, it is imperative that the needs of the digital citizen are met to guarantee that they have the information they need to make informed choices. The term 'informed consent' stems from the medical practitioner community and was typically defined entirely by rules of disclosure, adequate comprehension, and obtaining signatures[17]. Due to the advancement of technology physical signatures are no longer mandated; instead electronic signatures and/or an activity such as ticking a box are sufficient[18,19]. While electronic consent (eConsent) has not yet widely been adopted[20], it is envisioned that this approach will become more commonplace due to IoT devices[12].

Aforementioned, the aim underpinning the consent process is that participants should be provided with sufficient information to allow him/her to make an informed decision with regards to certain activities (in this context, the use of IoT devices for smart health initiatives specifically pertaining to the collection, analysis and use of sensitive health data). Existing research advocates that there remains a chasm between patient understanding and subsequent data usage by IoT devices[21]. That is, digital health citizens may not be aware that they are consenting for their health-related data to be used for data processing purposes[21]. Some of the commonly cited reasons for the lack of engagement and subsequent understanding associated with the consent process include the length of the policy documents and complex language used[22]. Tassé and Kirby[20] further argue that there is a dearth of standards or guidelines on how to best implement eConsent. Additionally, the authors argue that the requirements related to content of consent vary from one guideline to another, and between jurisdictions[20]. With their work on eConsent, Coiera and Clarke[23] identified four distinct levels of consent (see Table 1). While levels one and four are considered to be easily manageable from a technical perspective, the remaining two levels require more work for expressing patient electronic consent[24].

Table 1. Consent Level

Consent Level	Description
1. General Consent	The digital health citizen consents to give full access to his/her health data.
2. General Consent with specific conditions	The digital health citizen gives a general agreement but some restrictions in terms of the person, data and purpose are defined.
3. General Denial with specific conditions	Complements Consent Type/Level 2 but the priority is given to the restrictions.
4. General Denial	The digital health citizen does not consent to give access to his/her health data.

In some cases, informed consent from digital health citizens is not required for IoT devices[25]. It is argued that the latter is caused by many small-to-medium enterprises entering the IoT marketplace possessing minimum knowledge around privacy policies and the rights of end-users[25,26]. The IoT community is criticised for not going out of their way to highlight how data is being collected and implications of analysis and potential multiple uses of that data in the future. This is exacerbated by the lack of regulation, policy and guidelines[27].

With IoT devices, it is argued[28] that universal usability should be embraced when developing new healthcare systems. In simplistic terms, universal usability refers to a technological solution that can be used by every member of society independent of technology type and users' socio-demographic details[29]. Achieving universal usability of IoT devices is desirable. Three challenges in attaining universal usability are reported by Shneiderman[30]. These challenges include technology variety, user diversity and gaps in user knowledge (each concept is further described in Table 2).

Although universal usability and eConsent present some challenges, implementing Privacy by Design principles can help address these in the context of IoT within the health domain. The next section describes a proposed practical approach for software/hardware developers to consider.

3. Proposed Practical Approach

As part of funded research project, we have explored the user experience of eConsent when registering for a Health Social Network (HSN – PatientsLikeMe), it was found that users had very little understanding when agreeing to the Privacy Policy (PP) and Terms and Conditions (T&C) of this site. Although users are giving eConsent on current HSN platforms, the option to retain a level of control or choice over the privacy of their Personal Health Information (PHI) is limited. Participants from our study expressed a clear desire to have more control over the privacy and security levels of their PHI. It emerged that digital health citizens would whole heartedly welcome a new approach to the eConsent arena, one which offers improved transparency and understandability. Further findings indicated

that some of the system settings available in Facebook, in terms of offering users a level of control over their data, could be translated to other platforms e.g. HSNs and other IoT devices.

This short paper leverages the lessons that have been learned from a previous similar case study, by briefly outlining the challenges of universal usability in the provision of eConsent, incorporating IoT as part of the next phase of this research project. Indeed, universal usability implies the use of a single system to meet all needs. Figure 1 provides an overview of how best to design and develop an IoT for use within the healthcare domain. In doing so, it is hoped that the data produced by IoT devices is understandable and meaningful for different digital health citizens.

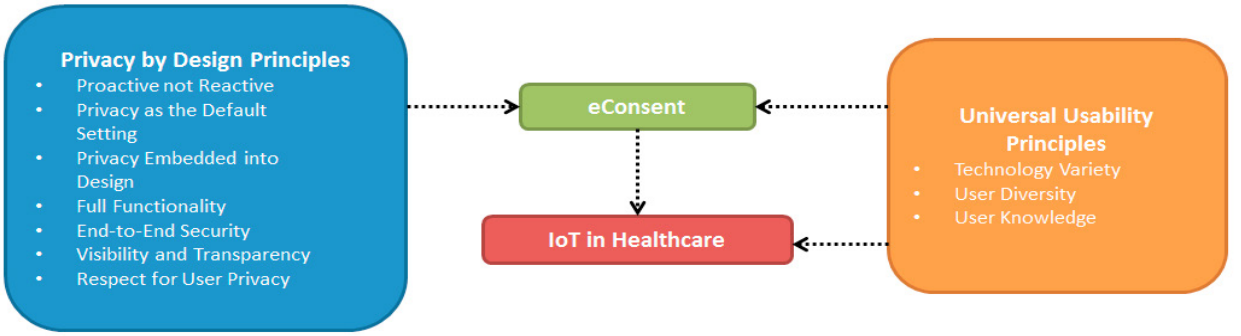


Figure 1. Proposed Practical Solution

It is from these explorations into the user experience of eConsent, that steps to move forward with the development and improvement of eConsent processes can move apace. Based on our research into the eConsent process when registering to use a HSN, the following Table (2) highlights the practical steps that could be taken in the enhancement of IoT for the end user.

Table 2. Proposed Practical Approach

Privacy by Design Principle	Description[14,31]	Proposed Solution
Proactive not Reactive	Seeks to anticipate and prevent privacy-invasive events before they happen.	Constantly updated anti-virus, anti-malware, anti-ransom ware in place. Protection of data guaranteed to user.
Privacy as the Default Setting	Seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected.	All user data is kept private. Access by third parties is requested from user and agreement sought prior to disclosure.
Privacy Embedded into Design	Embedded into the design and architecture of the system.	The eConsent process must be clearly articulated from the start. Terms and conditions and privacy policy statements must be clearly located by the user.
Full Functionality	Seeks to accommodate all legitimate interests and objectives in a positive-sum, win-win manner, not through a dated, zero-sum approach where unnecessary trade-offs are made.	Transparency and honesty in platform design by provider. The elimination of bias in design and the promotion of trustworthiness to the end user.
Privacy as the Default Setting	The digital health citizen gives a general agreement but some restrictions in terms of the person, data and purpose are defined.	This coincides with the different levels of consent that digital health citizens can decide from. Digital health citizens should be able to set the level of privacy which best suits their needs.
End-to-End Security	Must detail the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security	The encryption of identifiable user details and personal health information i.e. full name, DOB, email, health condition,

	measures are essential to privacy, from start to finish.	medication etc.

Table 3. Proposal Practical Approach (continued)

Privacy by Design Principle	**Description**	**Proposed Solution**
Visibility and Transparency	(1) To inform users about privacy risks and their implications; and (2) to be as open and transparent as possible.	eConsent must move away from text-heavy and jargon-based documentation to a more visual approach, with voice-over capabilities, to easily inform the user.
Respect for User Privacy	Requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.	This coincides with the different levels of consent that digital health citizens can decide from.
Universal Usability Principle	**Description**	**Proposed Solution**
Technology Variety	Supporting a broad range of hardware, software, and network access.	The eConsent process must adapt to the user's devices/network. This should be an automatic process which is not disruptive to the user.
User Diversity	Accommodating users with different skills, knowledge, age, gender, disabilities, disabling conditions (mobility, sunlight and noise), literacy, culture, income, and so forth.	By moving to a more visual approach with voice over capabilities the eConsent process is more accessible to a broader range of users. eConsent could be delivered across multiple modalities and multiple languages.
Gaps in User Knowledge	Bridging the gap between what users know and what they need to know.	The eConsent process must highlight in simple language (and across a variety of languages) what the terms and conditions/privacy policy document imply. Introducing a quiz on the statements could be a beneficial step in identifying what users know and understand about the terms and conditions.

4. Conclusion

Privacy by design and the introduction of a universal usability principle has the potential to carry IoT into the next phase – where users are not just a customer but a partner of the process. While our empirical work to date has not examined eConsent from an IoT perspective, we argue that the underlying concepts are pertinent across IS in health. The findings from understanding the level of citizen awareness in the provision of eConsent through health social networks may be leveraged to inform our understanding when it comes to IoT. In light of GDPR and the proliferation of IoT in health, we recognise that this is a timely opportunity to develop best practice guidelines for designers, medical/health care professionals, and researchers. Most importantly, we need to further engage with the provision of eConsent in IoT for citizens who need to have all of the relevant information available to them to support them to make better and more informed decisions about opting in or out.

Acknowledgement

We would like to acknowledge Wellcome Trust Grant for funding CHASM Project Seed Award 201607/Z/16/Z

References

1 Goldschmidt PG. HIT and MIS: Implications of Health Information Technology and Medical Information Systems. Communications of the ACM, 2005: 48(10): 68-74.

2 Austin C. J. and Boxerman S. B. 2003. Information Systems for Healthcare Management. Chicago, USA, Health Administration Press.

3 Dwivedi YK, Shareef MA, Simintiras AC, Lal B & Weerakkody V. A generalised adoption model for services: A cross country comparison of mobile health (m-health). Government Information Quarterly, 2016: 33(1), 174-187.

4 Kulik J, Heinzelman W & Balakrishnan, H. Negotiation-Based Protocols for Disseminating Information in Wireless Sensor Networks [J]. Wireless Networks, 2002: 8, (2-3).

5 Gabutti I, Mascia D & Cicchetti A. Exploring "patient-centered" hospitals: a systematic review to understand change. BMC health services research, 2017: 17(1), 364.

6 Hu F, Xie D & Shen S. On the application of the internet of things in the field of medical and health care. Paper presented at the Green Computing and Communications (GreenCom), IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing, 2013.

7 Tommasetti A, Vesci M & Troisi O. The internet of things and value Co-creation in a service-dominant logic perspective. Data Management in Pervasive Systems 2015: pp. 3-18. Springer.

8 Chahid Y, Benabdellah M & Azizi A. Internet of things security. Paper presented at the International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS), 2017.

9 Hu F, Xie D & Shen S. On the application of the internet of things in the field of medical and health care. Paper presented at the Green Computing and Communications (GreenCom), IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing, 2013.

10 Weber RH. Internet of Things–New security and privacy challenges. Computer law & security review, 2010: 26(1), 23-30.

11 Yang Y, Wu L, Yin G, Li L, & Zhao H. A Survey on Security and Privacy Issues in Internet-of-Things. IEEE Internet of Things Journal. 2017: April.

12 Neisse R, Baldini G, Steri G & Mahieu V. Informed consent in Internet of Things: The case study of cooperative intelligent transport systems. Paper presented at the 23rd International Conference on Telecommunications (ICT), 2016.

13 Bäumer U, von Oelffen S & Keil M. 2017. Internet of Things: Legal Implications for Every Business. The Palgrave Handbook of Managing Continuous Business Transformation (pp. 435-458): Springer.

14 GDPR website: https://www.dataprotection.ie/docs/GDPR/1623.htm

15 Dickie N, & Yule A. Privacy by design prevents data headaches later. Strategic HR Review, 2017: 16(2), 100-101.

16 Rumbold JMM & Pierscionek B. The effect of the General Data Protection Regulation on medical research. Journal of Medical Internet Research, 2017: 19(2).

17 Faden RR & Beauchamp TL. 1986. A history and theory of informed consent. New York: Oxford University Press

18 O'Keefe CM, Greenfield P & Goodchild A. A decentralised approach to electronic consent and health information access control. Journal of Research and Practice in Information Technology, 2005: 37(2), 161-178.

19 Budin-Ljøsne I, Teare HJ, Kaye J, Beck S, Bentzen HB, Caenazzo L et al. Dynamic Consent: a potential solution to some of the challenges of modern biomedical research. BMC Medical Ethics, 2017: 18(1), 4.

20 Tassé AM & Kirby E. Is written informed consent outdated? The European Journal of Public Health, 2017: 27(2), 195-196.

21 Whitmore A, Agarwal A & Da Xu L. The Internet of Things--A survey of topics and trends. Information Systems Frontiers, 2015: 17(2), 261.

22 McKee R. Ethical issues in using social media for health and health care research, Health Policy, 2013: 110(2-3), 298-301.

23 Coiera E & Clarke R. "e-consent: the design and implementation of consumer consent mechanisms in an electronic environment,"Journal of the American Medical Informatics Association, 2004: vol. 11, no. 2, pp. 129–140, 2004

24 Pruski C. e-crl: A rule-based language for expressing patient electronic consent. Paper presented at the Second International Conference on eHealth, Telemedicine, and Social Medicine, 2010. ETELEMED'10.

25 Privacy Advisor article: https://iapp.org/news/a/is-notice-and-consent-possible-with-the-internet-of-things/

26 Ebersold K & Glass R. The Internet of Things:A Cause for Ethical Concern. Issues in Information Systems, 2016: 17(IV), 145-151.

27 Bäumer U, von Oelffen S & Keil M. 2017. Internet of Things: Legal Implications for Every Business. The Palgrave Handbook of Managing Continuous Business Transformation (pp. 435-458): Springer.

28 Harper S. Is there design-for-all? Universal Access in the Information Society 2007: 6:111. Doi:10.1007/s10209-007-0071-2.

29 Forbes A. 2006. Issues Involved in the Development of Internet-Based GIS Applications.

30 Shneiderman B. Universal usability. Communications of the ACM, 2000: 43(5), 84-91.

31 Cavoukian A. Privacy by Design, The 7 Foundational Principles, Implementation and Mapping of Fair Information Practices. Available online at@ https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf