Contextual Privacy by Design for Integrated Electronic Health Records

The Information Continuum Project

Timothy C. Kariotis†

School of Computing and Information Systems, University of Melbourne, Melbourne, Vic, Australia,
timothy.kariotis@unimelb.edu.au

Megan Prictor

Melbourne Law School, University of Melbourne, Melbourne, Vic, Australia,
megan.prictor@unimelb.edu.au

Kathleen Gray

Health and Biomedical Informatics Centre, University of Melbourne, Melbourne, Vic, Australia,
kgray@unimelb.edu.au

Shanton Chang

School of Computing and Information Systems, University of Melbourne, Melbourne, Vic, Australia,
Shanton.chang@unimelb.edu.au

Darakhshan J. Mir

Department of Computer Science, Bucknell University, Lewisburg, Pennsylvania, USA,
d.mir@bucknell.edu

† Corresponding author

ABSTRACT

Health information technologies, such as integrated electronic health records (iEHR), have been proposed as one way to facilitate more integrated healthcare and address the fragmentation of the healthcare system. An iEHR is an electronic record that is longitudinal, comprehensive, prospective, and person-centred. However, iEHRs raise concerns in health care due to issues of trust, privacy, and confidentiality. This is especially true in mental health care, where the information collected may be especially sensitive. Concerns regarding privacy may lead to people withholding essential information needed for appropriate care. We know that currently, clinicians make decisions based on a range of norms and values related to confidentiality, trust, and risk management when sharing patient information. In this paper, we attempt to view and understand these norms using the theory of contextual integrity, which posits that privacy is the appropriate flow of information determined by context specific information norms. Contextual integrity proposes that if a technology breaches entrenched information norms, it should be evaluated as to its moral and political implications and whether it aligns with the values, goals, and ends of the context. However, if a new technology is justified in breaching information norms, contextual integrity does not describe how these information norms then adapt to the implemented technology. Drawing on technology appropriation theory, we theorise that users will appropriate technology to establish norms that maintain the values, goals, and ends of the context. However, technology may constrain these emergent norms, so appropriated norms are developed. We propose a participatory design method to develop *co-appropriated information norm* for iEHRs. These co-appropriated norms may support the development of design principles that will support users in appropriating technology to align with the values, goals, and ends of the context.

CCS CONCEPTS

• Social and professional topics~Medical records • Social and professional topics~Patient privacy • Applied computing~Health care information systems

KEYWORDS

Electronic Health Records, Privacy, Contextual Integrity, Healthcare, Technology Appropriation

1 Introduction

People with complex and chronic mental health conditions may access several services across health (e.g. general practitioner), mental health (e.g. psychiatrist), and social care services (e.g. housing & homelessness services) [1]. Currently, in Australia, among other countries, these services work in siloes, causing people to 'fall through the gaps' between services, which ultimately leads to poor experiences and poor outcomes [1]. Information sharing is one way to facilitate more collaborative and integrated models of care between these different services. Electronic health records (EHRs) have been proposed as one way to facilitate information sharing; while EHRs tend to allow for information sharing between siloes, they do not readily lead to the integration of information about patients across these siloes in order to provide better care [2]. The 'gold standard' or goal in health informatics is to have an integrated EHR (iEHR), which is longitudinal, person-centred, comprehensive, and prospective [2–4]. An iEHR would link all services and include a record of health information, as well as care plans focussed on the patient's need across the lifespan. Such a record was recommended in the 2014 review into Australian mental health services, but we are yet to see such technology implemented [5]. One of the major concerns with health information technology, especially in mental health, which deals with particularly sensitive and at times stigmatised information, is the issue of privacy. Currently, in health care, information sharing decisions are made by balancing a range of values and norms such as confidentiality, trust, risk management, and promoting best health [6–8]. However, there is limited evidence for the current information norms in mental health, and how these may be violated by an iEHR. Taking the approach of designing privacy into an iEHR is essential due to the specific nature of trust in the health care system. The theory of Contextual Integrity (CI), which views privacy as the appropriate flow of information provides a lens to understand why an iEHR may pose privacy concerns through breaching entrenched information norms. Theories of technology appropriation help explain how new norms may emerge, potentially favouring stakeholders with greater power or control, as technology is appropriated by users in a specific context [9]. We propose using a participatory design approach that recognises the values and norms of a range of stakeholders in the design process to develop, what we term as, co-appropriated norms for an iEHR [10,11]. In addition, we plan to co-develop socio-technical design principles to uphold these norms in mental health contexts.

1.1 Privacy, Contextual Integrity and Technology Appropriation

Contextual integrity views privacy as the appropriate flow of information which stems from context specific information norms [12]. Information norms can be characterised by five dimensions, including the sender, receiver and subject of the information, information type, and transmission principles [12]. If a new technology breaches any of these entrenched information norms, it is said to breach contextual integrity. However, in recognition that norms may change, it is recommended that a technology that prima facie breaches CI be further evaluated [12]. First, the moral and political implications of the new technology should be assessed, and second, it should be assessed whether the new technology upholds the values, norms, and ends of the context [13]. Though CI has been mainly used as an evaluative theory, we propose that it could be extended to conceptualise how norms are adapted once new technology that breaches entrenched information norms is implemented. We propose a method to develop co-appropriated norms for an iEHR and associated socio-technical design principles to uphold these norms.

Nissenbaum outlines that information norms represent a balance or a compromise and that these may favour the powerful in a certain context [13]. This poses some interesting reflections for the design of new technology in healthcare where the balance of power is currently being shifted, to give more information and decision-making capacity to patients, rather than being led by clinicians [14]. The concept of emerging norms aligns with theories of technology appropriation, in that when technology is implemented, there may be an initial misalignment between the technology-as-designed and the entrenched norms of the context [15,16]. Thus, through a process of appropriation, technology is shaped by the users, to become technology-in-practice [17]. The new technology will have a set of 'designed-in-norms' which though may follow the syntactical rules of information norms, are not norms in the true sense. Appropriation theory describes these 'norms' as functional affordances, which are the range of ways a technology could be used [18]. For example, in the case of an iEHR it may allow the clinician (sender) to upload a summary of the health information (information type) about a patient (subject), with their consent (transmission principle) but who receives that information (receiver) depends on the health services patients' accesses. These functional affordances are underpinned by symbolic expressions or a technology spirit, which includes the values, goals and intent of the technology [16,18]. For example, a health information system may have a number of conflicting ‘spirits' in that it could be designed to improve efficiency as well as to improve coordination of care [19]. Designers may negotiate a number of values, goals, and ends, in the development of technology, including their own values [20,21]. We theorise that users will appropriate the information norms to move towards greater alignments with their values, ends, goals in a specific context. Similar to how Nissenbaum theorises that entrenched norms develop from a balance of different values that may favour the powerful [13]. It may be that these emergent norms also favour those with more control over information norms, for example, the health professional [9]. However, this may mean that users appropriate technology in a way that could be counterproductive to the reason the technology was initially justified in breaching information norms. For example, clinicians may be less likely to record detailed sensitive information in a shared record, which may limit the benefits for integrated care [22]. The functional affordances of a technology, which stem from the values designed into the technology may either limit or facilitate this movement towards what could be considered emergent norms, and thus the end-point of this process is appropriated norms. We propose a method to work with all stakeholders to develop co-appropriated norms that recognise the values, ends, and goals of all stakeholders in a specific context.

2 Research Design

To unearth the entrenched norms in the mental health context and develop co-appropriated norms for the use of an iEHR, we draw principles from two participatory design methods, experience-based co-design (EBCD) and action-design research (ADR). Participatory design has a focus on balancing power relationship, learning by doing, and is based in practice; this aligns closely with both contextual integrity focus on the specific context and the values of participation in healthcare [23]. EBCD aims to bring together the many complex stakeholders, including service providers and users, that may engage with a health service or product in an equal space where everyone’s experience is valued in the design process [24,25]. A key principle of ADR is guided emergence, where we start with a concept from the researchers, and this is shaped by the stakeholders in the specific context being explored [26]. In this project, we focus on generating not only co-appropriated information norms but also socio-technical knowledge (design principles). Socio-technical knowledge recognises that technology is impacted by social, organisation and contextual factors, and vice versa [27,28]. Understanding how information norms emerge not just in the use of the technology, but also in the social and organisational spaces that the technology resides in is essential for successful design [29]. In addition, if a technologies ‘spirit’ cannot be changed, certain functional affordances or other parts of the socio-technical system (e.g. workflows or policies) may be designed to support the co-appropriated information norms.

3 Method

We outline our proposed method below in the context of a project we are working on titled the *Information Continuum Project*. Three broad phases are proposed that move between theory and practice in the development of both a general concept of an iEHR, co-appropriated information norms and design principles that uphold these norms.

3.1 Define New Technology, Current Context & Breach of CI

Phase 1 involved, defining the concept of an iEHR, defining the current context of mental health care, and assessing whether the concept of an iEHR would breach contextual information norms as per CI theory. We started with a broad concept idea of an iEHR drawing on seminal literature to understand the key principles of what the iEHR would do. In this project we have drawn on the international standard organization’s definition of an EHR for integrated care [2], Dyke et al.’s [3] definition of a patient-centred longitudinal care plan, and the recommendation from the 2014 review of Australian mental health services [5] to outline a concept for a system to improve information sharing across the mental health system, which we’ve termed an iEHR. We specifically are trying to capture the ‘spirit’ of what was outlined in the 2014 review from a policy perspective. We also are completing a scoping review into how EHRs more broadly have been used and appropriated in mental health contexts, and to potential functional affordances. We also thoroughly define the context that is mental health care and healthcare. This includes extricating the current information norms within this context, and the values underpinning them. This was done through a review of the literature and interviews with service providers [30]. We have concluded that an iEHR will breach the current contextual information norms because currently, the majority of information sharing between different healthcare sectors is event specific. As described in the example in 1.1 any future clinicians may potentially have access to an iEHR, which is different from the current information norms where the treating clinician curates the information about a patient for a specific clinician [31].

3.2 Align Technology with Context

Once we identified how iEHRs breaches contextual integrity, we reflected on whether this may be justified through a reflection on the moral and political implications of the new technology, and whether it aligns with the values, goals, and ends of the context. Some EHRs give service users access to their record; this allows them to have easy access to the information being shared about them. This aligns with a move in healthcare towards the greater democratisation of health information [14]. iEHRs may also support the current shift towards more team-based, integrated models of care in mental health [7].

3.3 Co-Design Ideal Norms (Figure 1)

We have accepted that the iEHR breaches contextual information norms but that this is potentially justified. Phase 3 aims to develop co-appropriated norms for an iEHR. To do this, we plan to work through two design cycles, to shape the co-appropriated information norms and the design principles to uphold them. The first phase involves working with focus groups of stakeholders to unearth the information norms different stakeholders would gravitate towards with the introduction of an iEHR. In this project, we plan to use a story-completion method, where we start with several story-boards that represent the key information sharing situations we discovered in Phase 1. This story-board will introduce the broad concept of an iEHR, and participants in the focus group will be asked to complete the story. A discussion will be facilitated to explore the information norms in each story-board. In the Information Continuum Project, we plan to work with service users, service providers, carers, health administrators, health informaticians, and lawyers. The reason for doing this is that though clinicians may be the senders and receivers of information, a range of other stakeholders may also manage this information. Consequently, other stakeholders may guide service provider decisions around appropriate transmission principles.

The findings from the stakeholder focus groups will be analysed thematically. All the findings will be synthesised, and the researchers will develop these into a draft list of socio-technical design principles. We expect that the norms created may not align perfectly across all stakeholders, so we will develop a range of potential design guidelines that could meet these different information norms. These will be taken back to a co-design group that includes representatives from all stakeholder groups for further discussion. The findings from this focus group will be synthesised into a second draft of both co-appropriated norms and design principles and sent back to all participants for further feedback. We plan to present these design principles at an industry conference to get feedback on how they might be implemented in the design of an iEHR. The output of this process should be a set of design guidelines that industry can use when designing iEHRs in mental health contexts, that will ensure the appropriate flow of information.

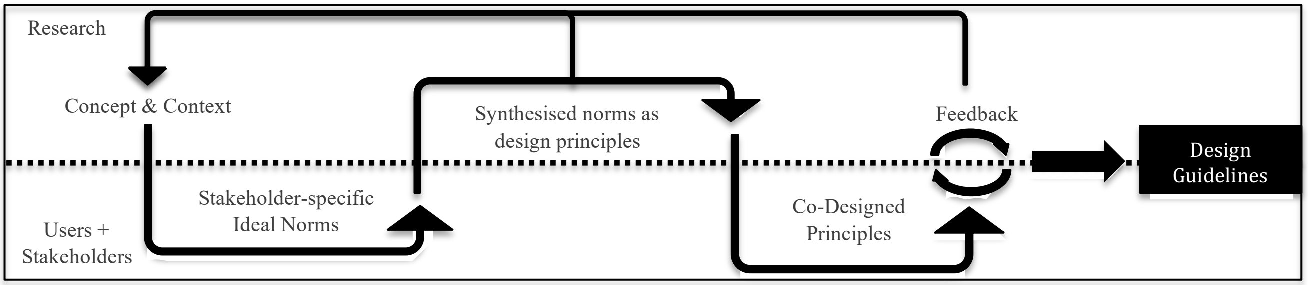

Figure 1: Method Outline

4 Implications

Trust is essential in healthcare, especially mental health care, where people put trust in the clinicians when they share sensitive and potentially highly stigmatised information [32]. Implementation of new technology poses a risk to trust in health care due to concerns regarding privacy and confidentiality [33]. Thus, we need an approach to design technology that will uphold people's privacy. Contextual integrity provides a theoretical standpoint on privacy that aligns with much of what we already know about information sharing in health. We know that electronic health records breach contextual integrity, but that this may be justified due to moral and value-based reasons. However, once we implement an iEHR new norms may emerge as users appropriate the technology. Taking a participatory design approach, we propose a method to develop co-appropriated norms and design principles for an iEHR in mental health. We see this is the first step in a broader design process, to design an iEHR for implementation and evaluation in a mental health context.

REFERENCES

[1] S.J. Lee, E. Crowther, C. Keating, and J. Kulkarni, What is needed to deliver collaborative care to address comorbidity more effectively for adults with a severe mental illness?, *Australian & New Zealand Journal of Psychiatry*. **47** (2013) 333–346. doi:10.1177/0004867412463975

[2] International Organisation for Standardisation, 20514 Draft Technical Report: EHR Definition Scope and Context, ISO, 2015. https://www.iso.org/standard/39525.html.

[3] P.C. Dykes, L. Samal, M. Donahue, J.O. Greenberg, A.C. Hurley, O. Hasan, T.A. O'Malley, A.K. Venkatesh, L.A. Volk, and D.W. Bates, A patient-centered longitudinal care plan: vision versus reality, *Journal of the American Medical Informatics Association : JAMIA*. **21** (2014) 1082–1090. doi:10.1136/amiajnl-2013-002454.

[4] S. Garde, P. Knaup, E.J. Hovenga, and S. Heard, Towards semantic interoperability for electronic health records, *Methods of Information in Medicine*. **46** (2007) 332–343. doi: 10.1160/ME5001

[5] National Mental Health Commission, The National Review of Mental Health Programmes and Services, NMHC, Sydney, NSW, 2014. http://www.mentalhealthcommission.gov.au/our-reports/contributing-lives,-thriving-communities-review-of-mental-health-programmes-and-services.aspx.

[6] S.K. Fitch, Trust, Information-Sharing and the Doctor–Patient Relationship: A Multi-Method, Empirical-Ethics Study of New Zealand General Practice, (2017). https://researchspace.auckland.ac.nz/handle/2292/33558

[7] M.A. Rothstein, The Hippocratic Bargain and Health Information Technology, *J Law Med Ethics*. **38** (2010) 7–13. doi:10.1111/j.1748-720X.2010.00460.x.

[8] J. Firn, N. Preston, and C. Walshe, Ward social workers' views of what facilitates or hinders collaboration with specialist palliative care team social workers: A grounded theory, *BMC Palliative Care*. **17** (2018) 7. doi: 10.1186/s12904-017-0214-z

[9] P.M. Leonardi, and S.R. Barley, What's Under Construction Here? Social Action, Materiality, and Power in Constructivist Studies of Technology and Organizing, *ANNALS*. **4** (2010) 1–51. doi:10.5465/19416521003654160.

[10] D.J. Mir, Y. Shvartzshnaider, and M. Latonero, It Takes a Village: A Community Based Participatory Framework for Privacy Design, in: 2018 IEEE European Symposium on Security and Privacy Workshops, IEEE, 2018: pp. 112–115. doi: 10.1109/EuroSPW.2018.00022

[11] R.Y. Wong, and D.K. Mulligan, Bringing Design to the Privacy Table: Broadening" Design" in" Privacy by Design" Through the Lens of HCI, in: 2019 CHI Conference on Human Factors in Computing Systems, ACM, 2019: pp. 262-278. doi: 10.1145/3290605.3300492.

[12] H. Nissenbaum, Privacy in Context: Technology, policy, and the integrity of social life, Stanford University Press, 2009.

[13] H. Nissenbaum, Contextual Integrity Up and Down the Data Food Chain, *Theoretical Inquiries in Law*. **20** (2019). http://www7.tau.ac.il/ojs/index.php/til/article/view/1614.

[14] J. Calvillo, I. Román, and L.M. Roa, How technology is empowering patients? A literature review, *Health Expectations*. **18** (2015) 643–652. doi:10.1111/hex.12089.

[15] A. Majchrzak, R.E. Rice, A. Malhotra, N. King, and S. Ba, Technology adaptation: The case of a computer-supported inter-organizational virtual team, MIS Quarterly. (2000) 569–600. doi: 10.2307/3250948

[16] G. DeSanctis, and M.S. Poole, Capturing the complexity in advanced technology use: Adaptive structuration theory, *Organization Science*. **5** (1994) 121–147. doi:10.1287/orsc.5.2.121

[17] W.J. Orlikowski, Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations, *Organization Science*. **11** (2000) 404–428. doi:10.1287/orsc.11.4.404.14600.

[18] M.L. Markus, and M.S. Silver, A foundation for the study of IT effects: A new look at DeSanctis and Poole's concepts of structural features and spirit, *Journal of the Association for Information Systems*. **9** (2008) 5. https://aisel.aisnet.org/jais/vol9/iss10/5

[19] N.F. Doherty, C.R. Coombs, and J. Loan-Clarke, A re-conceptualization of the interpretive flexibility of information technologies: redressing the balance between the social and the technical, *European Journal of Information Systems*. **15** (2006) 569–582. doi:10.1057/palgrave.ejis.3000653

[20] M. Akrich, The De-Scription of Technical Objects, in: Shaping Technology/Building Society, The MIT Press, Cambridge, 1997: pp. 205–224.

[21] M. Flanagan, D.C. Howe, and H. Nissenbaum, Embodying Values in Technology: Theory and Practice, in: J. van den Hoven, and J. Weckert (Eds.), Information Technology and Moral Philosophy, Cambridge University Press, Cambridge, 2008: pp. 322–353. doi:10.1017/CBO9780511498725.017.

[22] I. Cairns, M. Jonas, and K. Wallis, The Ethics of Sharing: How Do Social Workers Decide What to Record in Shared Health Records?, *Ethics and Social Welfare*. **12** (2018) 348–369. doi:10.1080/17496535.2017.1384849.

[23] R. Luck, What is it that makes participation in design participatory design?, *Design Studies*. **59** (2018) 1–8. doi:10.1016/j.destud.2018.10.002.

[24] P. Bate, and G. Robert, Experience-based design: from redesigning the system around the patient to co-designing services with the patient, *BMJ Quality Safety*. **15** (2006) 307–310. doi:10.1136/qshc.2005.016527

[25] D. Szebeko, and L. Tan, Co-designing for Society, *Australasian Medical Journal (Online)*. **3** (2010) 580. doi:10.4066/AMJ.2010.378

[26] M. Sein, O. Henfridsson, S. Purao, M. Rossi, and R. Lindgren, Action Design Research, Management Information Systems Quarterly. 35 (2011) 37–56. http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A871353&dswid=-4773

[27] E. Coiera, Four rules for the reinvention of health care, *Bmj*. **328** (2004) 1197–1199. doi:10.1136/bmj.328.7449.1197

[28] D.F. Sittig, and H. Singh, A new socio-technical model for studying health information technology in complex adaptive healthcare systems, in: Cognitive Informatics for Biomedicine, Springer, 2015: pp. 59–80. doi:10.1136/qshc.2010.042085.

[29] R. Lamb, S. Sawyer, and R. Kling, A social informatics perspective on socio-technical networks, *AMCIS 2000 Proceedings*. (2000) 1. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1490&context=amcis2000

[30] T. Kariotis, M. Prictor, K. Gray, and S. Chang, Mind the Gap: Information Sharing between Health, Mental Health and Social Care Services, in: HIC 2019*,* in press.

[31] T. Kariotis, M. Prictor, S. Chang, and K. Gray, Evaluating the Contextual Integrity of Australia's My Health Record, in: Context Sensitive Informatic Conference 2019, in press.

[32] J. Radden, Notes towards a professional ethics for psychiatry, *Australian and New Zealand Journal of Psychiatry*. **36** (2002) 52–59. doi:10.1046/j.1440-1614.2002.00989.x.

[33] N. Shen, T. Bernier, L. Sequeira, J. Strauss, M.P. Silver, A. Carter-Langford, and D. Wiljer, Understanding the patient privacy perspective on health information exchange: A systematic review, *International Journal of Medical Informatics*. **125** (2019) 1–12. doi:10.1016/j.ijmedinf.2019.01.014.