Improving Usability, Safety and Patient Outcomes with Health Information Technology
F. Lau et al. (Eds.)

doi:10.3233/978-1-61499-951-5-382

The eHealth Trust Model: A Patient Privacy Research Framework

Nelson SHEN[a,b,1], John STRAUSS[a,b], Michelle SILVER[a],
Abigail CARTER-LANGFORD[a,c], David WILJER[a,d]
[a]*Institute of Health Policy, Management and Evaluation, University of Toronto, ON*
[b]*Centre for Addiction and Mental Health, Toronto, ON*
[c]*Canada Health Infoway, Toronto, ON*
[d]*University Health Network, Toronto, ON*

Abstract. Patient privacy concerns are often cited as a barrier to health information exchange (HIE) implementations; however, the current understanding of patient perspective is limited due to a fragmented approach to patient privacy research. The limited evidence suggests that the patient privacy perspective is context-dependent and may involve benefit-risk tradeoffs. A standardized approach to the contextual factors would allow for more consistent assessment, providing a better understanding or explanation of the contextual factors influencing the patient privacy perspective and their attitudes towards HIE. This paper describes the development of the eHealth Trust Model—an evidence-based theory-grounded conceptual framework intended to guide future patient privacy research.

Keywords. Privacy, Trust, Conceptual Framework, Health Information Exchange

1. Introduction

Privacy commonly refers to an individual's desire to control or have influence over data about themselves[1]. Patient privacy is an issue on the forefront of health information exchange (HIE) discussions, as HIE involves the process of exchanging personal health information (PHI) electronically between various points in healthcare[2,3]. Although HIE can improve healthcare[4,5], it may also be a source of patient privacy concern—an oft-cited barrier to HIE implementation[6,7]. The aggregation of PHI poses potential privacy risks as thousands of records may be accessed and/or disclosed with a single breach. Furthermore, the increased pace and extended reach of PHI (sometimes unbeknownst to the individual) may influence the patient's perceived control of their PHI, causing privacy concerns[7]. These concerns may erode patient trust in healthcare and undermine effective patient-provider relationships. Without trust, patients may withhold information or avoid seeking care in an attempt to protect themselves from the potential stigma, discrimination, and harm associated the unlawful PHI disclosure. These privacy protective behaviors may be detrimental to the patient care and health [8,9]. For this reason, protecting patient privacy is of fundamental importance.

From a policy perspective, protecting privacy requires a balance between the benefits of innovations against patient rights and interests[10]; however, the privacy

[1] Corresponding Author, Email: nelson.shen@mail.utoronto.ca

discourse often fails to include the patient perspective[11]. The evidence suggests patient privacy needs may be overstated by the healthcare community, overlooking the context-dependency of the patient privacy perspective [12–15]. This context-dependency was highlighted in a recent systematic review[16], where 15% to 78% participants reported privacy concerns across the different studies. The review also found that the evidence was fragmented as theories/frameworks and standardized measures were used in only one-fifth of the studies. As a result, the *ad hoc* approaches limited each study's ability to incrementally contribute to a coherent, generalizable, and transferable explanation or understanding of the patient privacy perspective [17]. To provide a common frame of reference for future privacy research, the eHealth Trust Model (eHTM) was developed.

2. Proposed Privacy Framework: The eHealth Trust Model

2.1. Conceptual Foundation

The eHTM is an evidence-based, theory-grounded framework based on the Antecedent, Privacy Concern, Outcome model (APCO)[18]. While there have been a few comprehensive frameworks derived from extant privacy research[1,18,19], the APCO was selected because it was derived through an extensive multi-disciplinary review. Its broad scope was intended to guide future privacy research and allow researchers to adapt it for use in different contexts and disciplines.

The APCO is a high-level process model outlining the antecedents contributing to *privacy concern* and the resultant outcomes of those concerns. The antecedent constructs consist of *privacy experience, privacy awareness, personality, demographic, and culture*, while the outcome constructs include *perceived risk* and *behavioural reaction*. *Behavioural reaction* is the most prominent outcome since it represents an individual's intention to use an online service and/or technology. *Regulation* and *trust* are proposed to have reciprocal relationships with *privacy concern*, acting as both antecedents and outcomes The APCO also includes the notion of a privacy calculus—a cognitive risk-benefit analysis used by individuals to determine their *behavioural reaction*[20]. The privacy calculus is a common explanation of why individuals engage in information sharing behaviours despite voicing privacy concerns (i.e., the privacy paradox). This dissonance between attitude and behaviour occurs because the perceived benefits offsets the perceived privacy risks of using the technology or service.

2.2. Framework Development

A systematic review[16] and a qualitative study involving patient interviews[21] were conducted to inform the eHTM development. This foundational work was conducted at the Centre for Addiction and Mental Health (CAMH) with approval from their research ethics board (CAMH067/2015). The systematic review[16] assessed the current understanding of the patient privacy perspective of HIE. Insights on adaptations or expansions to the APCO were generated by mapping the evidence to the model. Despite identifying 59 studies, most of the linkages between the APCO constructs were tenuous either because they were infrequently studied, or the evidence was inconsistent in terms of directionality and statistical significance. Of the confirmed linkages, perceived quality of care had a significant effect in mitigating *privacy concerns*. Studies also confirmed that *privacy concerns* reduced patient willingness to share PHI or increased patient

privacy protective behaviours. The privacy calculus was also evident, where *perceived benefit* was positively associated with intention to use health information technology (HIT) and actual use; however, assumptions on the role of the privacy calculus in relation to *privacy concern* and *behavioural reaction* varied across studies. Based on the review findings, the following adaptations were made to the APCO:

- *Privacy concern* was changed to *privacy perspective* to encompass a greater range of privacy views and remove the negative framing of concern;
- *Demographic* was split into *demographic, tech savvy, and healthcare perception* to provide more specificity to patient characteristics;
- *Regulation* was changed to *policy and regulation* to include institutional privacy policies which govern PHI use; and
- *Privacy awareness* was changed to *eHealth awareness* to make it specific to healthcare and HIE.

Following the review, interviews with mental health service users were conducted to understand their privacy perspectives and to validate the constructs in the adapted APCO[21]. While patient participants believed that privacy was important given the stigmatic nature of their PHI, their degree of privacy concern varied depending on their patient experiences. Whether concerned or not, the participants were willing to share their PHI in HIE. They supported HIE because they wanted the best care possible— both directly through clinician or patient use, and indirectly through research and analytics. Participants also held a fatalistic view that privacy breaches are unavoidable in the current digital society and little can be done to protect their PHI privacy. Combined with a general unawareness of their patient privacy rights, participants placed a tremendous level of trust that the healthcare system and their providers will protect patient privacy.

To provide more depth to the *trust* construct, the Web-Trust Model (WTM) [22] was integrated with the adapted APCO. The WTM is an empirically validated model that uses the Theory of Reasoned Action [23] to explain the causality of trust on online behaviours. The WTM posits *disposition to trust* (i.e., the general tendency to willingly depend on others) and *institution-based trust* (i.e., beliefs that the structural conditions exist to ensure a trustworthy transaction) as antecedents to trust in a web-vendor. These antecedents influence the individual's *trusting beliefs* (i.e., perceptions about a vendor's attributes), which leads to *trusting intention* (i.e., decision to engage with the vendor).

Because the *trusting belief-trusting intention* linkage (WTM) mirrors the *trust-behavioural reaction* linkage (APCO), *trust* was renamed *trusting belief* to provide more specificity. This adaptation is appropriate because intention to share information may vary with the recipient. The other WTM constructs fit under the APCO high-level constructs, where, (1) *trusting intention* is represented under *behavioural reaction*; (2) *institution-based trust* is represented under *policy and regulation* and *healthcare perception*; and (3) *disposition to trust* is represented under *personality*.

2.3. The eHealth Trust Model

Mirroring the APCO, the eHTM follows an "Antecedent➔eHealth Trust➔Outcome" process. At the core of the eHTM (fig. 1) are three *eHealth Trust* constructs (i.e., *privacy perspective, trusting belief,* and *policy and regulation*), representing the patient attitude towards confidentiality—trust that the healthcare system (or provider) can and will

uphold its legal obligation to protect the privacy of the entrusted PHI. The eHTM suggests that a patient's *eHealth trust* is contextual, informed by their perceptions, experiences, personal dispositions, and environment. *eHealth Trust* is the primary determinant in a patient's *behavioural reaction* to HIE. These reactions can manifest as the willingness to share PHI, intention to opt-out, or intention to use patient-facing HIT. *Behavioural reaction* may also be influenced by the trade-offs between the *perceived benefit* of HIE and *perceived risk* to privacy (i.e., privacy calculus).

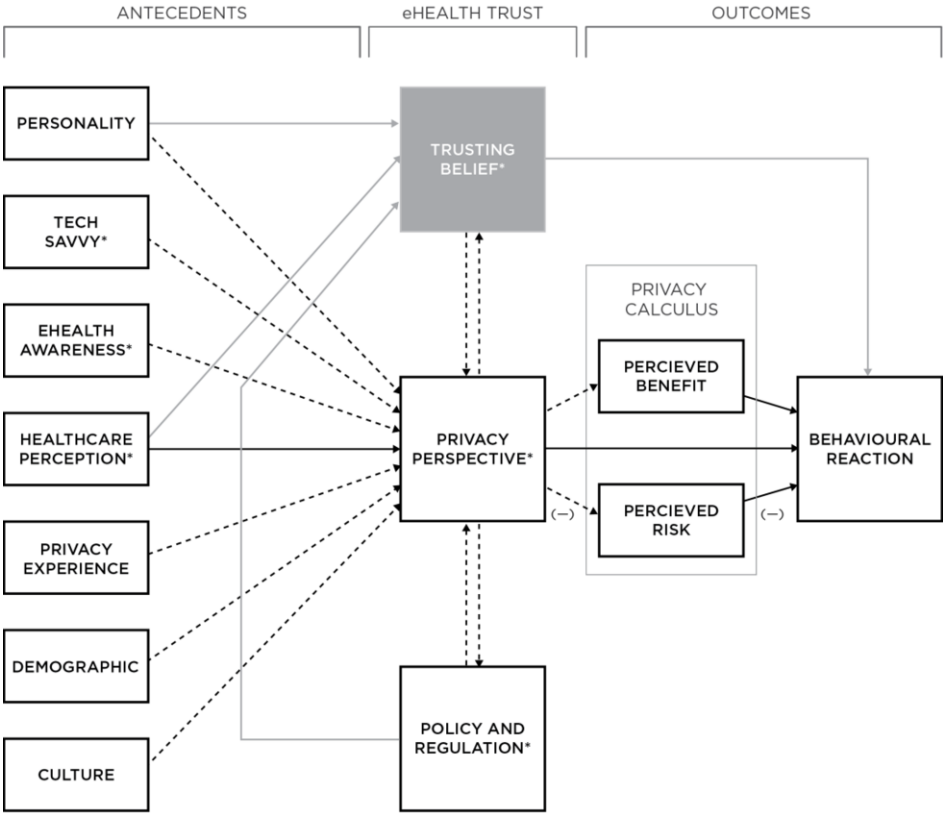

Figure 1. The eHealth Trust Model

The status of the linkages in the eHTM were derived from the systematic review, patient interviews, and the WTM. The linkages included from the WTM (grey arrow) were confirmed through multiple studies by its authors[22]. As discussed, most linkages are tenuous as their relationships were unconfirmed or remain unclear. The confirmed linkages within the model assume there is a positive association between constructs unless otherwise indicated. The eHTM also assumes a positive framing for *behavioural reaction,* defined as "*an individual's intention to electronically share their PHI or use HIT*" (construct definition summary in Table 1). For instance, a positive *healthcare perception* will lead to a positive *trusting belief* and *privacy perspective* which subsequently leads to a positive *behavioural reaction*. A negative *privacy perspective*

may increase the *perceived risk* of HIE, thereby reducing *behavioural reaction* (i.e., opt-out of PHI sharing, non-use of HIT, exercise patient privacy rights).

Table 1. Definitions of eHealth Trust Model constructs (NB: * denotes original APCO constructs)

Domain Construct	Definition
eHealth trust	
Privacy perspective	An individual's beliefs, attitudes, and concerns about the electronic sharing of their personal health information.
Trusting belief	An individual's willingness to become vulnerable to the actions of another party.
Policy and regulation	An individual's knowledge of and attitudes towards the protection and use of their electronic personal health information.
Antecedents	
Privacy experience*	The extent to which individuals have been exposed to or have been a victim of information abuses.
eHealth awareness	An individuals' general awareness of health information technology. This includes experience with, knowledge of, and attitudes toward health information technology.
Healthcare perception	An individual's attitudes and beliefs about the healthcare system and their personal health.
Demographic	Differences based on the shared characteristics of a population.
Tech savvy	An individual's knowledge of, attitudes towards, and experience with technology.
Culture*	The attitudes, customs, and beliefs that distinguishes one group of people from another.
Outcomes	
Perceived benefit*	The degree to which an individual believes the electronic sharing of their personal health information can help themselves and others.
Perceived risk*	The degree to which an individual believes the electronic sharing of their personal health information will result in a loss or harm.
Behavioural reaction*	An individual's intention to electronically share their personal health information or use health information technology.

3. Discussion and Conclusion

With the increasing investments into interoperable HIT, it is important to understand patient privacy expectations on how their data is and will be used. The eHTM is a comprehensive evidence and theory-based framework intended to provide a logical and structured guide to thinking about patient privacy research, evaluation, and the discussion. By providing a common frame of reference, the eHTM aims to address the fragmented approaches to patient privacy research, allowing future research to incrementally contribute to the understanding of the patient privacy perspective. The foundational work presented here demonstrates the utility of a guiding framework (i.e., APCO) in building and extending the evidence. The work to date suggests that patient experience, value proposition, and trust are equally important factors to include in the discussion about patient privacy—all seldom explored in extant literature.

Like its predecessor in the APCO, the eHTM is intentionally broad to allow for the flexible application to suit various contexts and the informational needs of its users. The HIE framing focuses the eHTM on PHI uses rather than specific HIT, allowing for continued applicability as the digital health landscape evolves new innovative uses of PHI. This iteration of the eHTM will be further refined through a Delphi study focused on establishing content validity, marrying evidence and theory with the practical experience of privacy experts. Future research will leverage existing data from the Canada Health Infoway privacy survey [24] to establish criterion and construct validity of the model.

References

[1] F. Bélanger, and R.E. Crossler, Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems, *MIS Q* **35** (2011) 1017–1041.

[2] W. Hersh, A. Totten, K. Eden, B. Devine, P. Gorman, S. Kassakian, S.S. Woods, M. Daeges, M. Pappas, and M.S. McDonagh, *Health Information Exchange*, Elsevier, 2015.

[3] M.M. Mello, J. Alder-Milstein, K. Ding, and L. Savage, Legal Barriers to the Growth of Health Information Exchange—Boulders or Pebbles?, *Milbank Q* **96** (2018) 110–143.

[4] C.S. Kruse, and A. Beane, Health Information Technology Continues to Show Positive Effect on Medical Outcomes: Systematic Review, *J. Med. Internet Res.* **20** (2018) e41.

[5] W.R. Hersh, A.M. Totten, K.B. Eden, B. Devine, P. Gorman, S.Z. Kassakian, S.S. Woods, M. Daeges, M. Pappas, and M.S. McDonagh, Outcomes From Health Information Exchange: Systematic Review and Future Research Needs, *JMIR Med. Informatics.* **3** (2015) e39.

[6] C.S. Kruse, V. Regier, and K.T. Rheinboldt, Barriers over time to full implementation of health information exchange in the United States, *J. Med. Internet Res.* **16** (2014).

[7] K.B. Eden, A.M. Totten, S.Z. Kassakian, P.N. Gorman, M.S. McDonagh, B. Devine, M. Pappas, M. Daeges, S. Woods, and W.R. Hersh, Barriers and facilitators to exchanging health information: A systematic review, *Int. J. Med. Inform.* **88** (2016) 44–51.

[8] B.A. Malin, K.E. Emam, and C.M. O'Keefe, Biomedical data privacy: problems, perspectives, and recent advances, *J. Am. Med. Inform. Assoc*. **20** (2013) 2–6.

[9] O. Ben-Assuli, Electronic health records, adoption, quality of care, legal and privacy issues and their implementation in emergency departments, *Health Policy* **119** (2015) 287–297.

[10] A. Acquisti, L. Brandimarte, and G. Lowenstein, Privacy and Human Behaviour in the Age of Information, *Science.* **347** (2015) 509–515.

[11] S. Lewis, *Securing a Bright Health Information Future*, in: C.M. Flood (Ed.), Data Data Everywhere, Carleton University Press, Kingston, ON, Canada, 2011: pp. 253–266.

[12] E. Bäck, and K. Wikblad, Privacy in hospital., *J. Adv. Nurs.* **27** (1998) 940–945.

[13] P. Sankar, S. Moran, J.F. Merz, and N.L. Jones, Patient perspectives on medical confidentiality, *J. Gen. Intern. Med.* **18** (2003) 659–669.

[14] D. McGraw, J.X. Dempsey, L. Harris, and J. Goldman, Privacy as an enabler, not an impediment: building trust into health information exchange, *Health Aff. (Millwood)* **28** (2009) 416–427.

[15] N.T. Shaw, A. Kulkarni, and R.L. Mador, Patients and health care providers' concerns about the privacy of electronic health records: A review of the literature, *Electron. J. Heal. Informatics*. **6** (2011).

[16] N. Shen, T. Bernier, L. Sequeira, J. Strauss, M. Silver, A. Carter-Langford, and D. Wiljer, Understanding Patient Privacy Perspective on Health Information Exchange: A Systematic Review., *Submitted for publication,* (2018).

[17] P. Nilsen, Making sense of implementation theories, models and frameworks, *Implement. Sci.* **10** (2015) 1–13.

[18] H.J. Smith, T. Dinev, and H. Xu, Information Privacy Research: An Interdisciplinary Review, *MIS Q.* **35** (2011) 989–1015.

[19] Y. Li, Theories in online information privacy research : A critical review and an integrated framework, *Decis. Support Syst.* **54** (2012) 471–481.

[20] M.J. Culnan, and P.K. Armstrong, Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation, *Organ. Sci.* **10** (1999) 104–115.

[21] N. Shen, L. Sequeira, J. Strauss, M. Silver, A. Carter-Langford, and D. Wiljer, Patient privacy perspectives on health information exchange in a mental health context: A qualitative study., *Submitted for publication,* (2018).

[22] D.H. McKnight, V. Choudhury, and C. Kacmar, Developing and Validating Trust Measures for e-Commerce: An Integrative Typology, *Inf. Syst. Res.* **13** (2002) 334–359.

[23] M. Fishbein, and I. Ajzen, *Belief, Attitude, Intention and Behaviour: An Introduction to Theory and Research*, Addison-Wesley, 1975.

[24] Earnscliffe Strategy Group, 'What Canadians Think': Canadians' perspectives on privacy of personal health information in the context of digital health, 2017. https://www.infoway-inforoute.ca/en/component/edocman/3348-earnscliffe-survey-on-electronic-health-information-and-privacy/view-document?Itemid=101.