Causes and Impacts of Personal Health Information (PHI) Breaches: A Scoping Review and Thematic Analysis

Completed Research Paper

Javad K. Pool **Saeed Akhlaghpour**

Farhad Fatehi **Andrew Burton-Jones**

Abstract

In light of the recent high-profile data breach incidents, and newly updated mandatory data breach notification laws, considerable global attention is forming around the protection of Personal health information (PHI). PHI breaches, generally described as an impermissible use or disclosure of protected personal health information, are extremely consequential for healthcare organizations and their patients and customers. This paper reports on a scoping review and thematic analysis of the literature studying the causes and impacts of PHI breaches. We started our review by identifying over 900 relevant articles, and through a rigorous process, included 28 articles for a detailed synthesis. Our findings highlight a number of direct and indirect causes of PHI breaches and their behavioral and operational impacts. Based on these findings, gaps in the literature are identified and implications for future research are discussed.

Keywords: Privacy, security, personal health information, data breach, health information systems, digital health

Introduction

Extant literature highlights the positive impacts of using digital health records on different measures of performance and quality of care (Buntin et al. 2011; Kohli and Tan 2016). At the same time, digitizing personal health records has generated significant new risks. In July 2018, hackers accessed 1.5 million health records in Singapore's online health system – including the health records of the Prime Minister (Ministry of Communications and Information 2018). This incident was just one of the latest high-profile healthcare data breaches. A full list includes the infamous theft of 78.8 million patient records from Anthem Blue Cross, a US-based health insurance plan provider (Lord 2018), and the online sale of Australian Medicare card details on a darknet auction site (Elton-Pym 2017).

Personal health information (PHI) breaches, generally described as an impermissible use or disclosure of protected personal health information, are extremely consequential. Arguably, from a hacker's perspective, a person's medical record is worth much more than his/her credit card (Humer and Finkle 2014). These records typically contain extensive amounts of sensitive data such as full name, contact details, insurance details, diagnoses, prescriptions, and treatments. Unlike credit card numbers, this information simply cannot be discarded. They generally remain valid for a long time or even permanently. Hence, if personal health records are breached, they can be used for a wide range of fraudulent purposes, including identity theft, insurance fraud, forged prescriptions, and so on.

There is also growing evidence that, in comparison to other industries, healthcare organizations are more vulnerable to data breaches (Gordon et al. 2017). This is partly because in the healthcare settings, typically a large number of actors have access to PHI for the purpose of providing care to patients/customers. Therefore, human errors such as misuse of electronic records may arise and threaten patients' privacy. There are also other factors such as inadequate staffing and funding for IT security and insufficient technology investment that put healthcare organizations at heightened risk. Besides the potentially serious harm to affected individuals, the financial and organizational costs of data breaches, which range from regulatory penalties to brand damage, are devastating for healthcare organizations (Goode et al. 2017; McLeod and Dolezel 2018).

Globally, there is increasing recognition of the importance of protecting personal information. This trend is reflected in the passing of new privacy regulations, such as EU's General Data Protection Regulation (GDPR), Australia's Notifiable Data Breaches (NDB) scheme (both of which came into effect in 2018), and California's Consumer Privacy Act (enforceable from 2020). Recent high-profile data breaches, such as Facebook–Cambridge Analytica scandal further intensified this global attention to privacy.

Given the severity and impact of data-breaches in healthcare, and above-mentioned recent developments, we believe a review of the causes and impacts of PHI breaches are timely and important. To our knowledge, there are no recent similar reviews, particularly with a clear focus on the healthcare sector. By synthesizing the literature on past incidents, we intend to provide deeper insights into the situations where health organizations are prone to cyber threats, and highlight the potential adverse outcomes. To this end, our paper reports on a scoping review with the general research question of "what does the current body of literature tell us about the causes and impacts of PHI breaches?" Our findings can inform health organizations, policymakers, and cybersecurity experts involved in developing and implementing healthcare IT, and help them better ensure and protect patients' PHI. Moreover, this study identifies the current gaps in our accumulated knowledge, and highlights promising avenues for future research.

The rest of the paper is structured as follows. We first elucidate on the details of our scoping review methodology, including article selection and coding process. In the finding section, summaries of the causes and impacts of PHI breaches, as identified in our review, are presented in multiple sub-sections. Finally, we share our reflections on fruitful future research directions, followed by a brief conclusion.

Methods

As outlined below, we conducted a scoping review (Arksey and O'Malley 2005). This type of review is suitable where there is a requirement to cover a general topic with diverse research methods employed, to examine broad research questions and to determine whether carrying out a full systematic review is valuable (Levac et al. 2010).

We followed the guidelines of Arksey and O'Malley (2005) and went through the five stages of "*identifying the research question" (stated above)*, "*identifying relevant studies"*, "*study selection"*, "*charting the data"*, and "*Collating, summarizing and reporting the results"*.

The search for identifying relevant study was conducted in PubMed based on broad expression of "data breach." We searched PubMed from January 4, 2009, to January 1, 2019, using the terms (data Breach*, breach notification, security breach*, information breach*, cybersecurity breach*, privacy breach*,

privacy invasion, unauthorised access, information disclosure*, disclosure of information, disclosing information, disclosing data, disclosing health data, data exposure, information exposure, data leak*, security leak*, cybersecurity leak*, information leak*, leaked data, leaked information, leaked Security). The result of the search has shown in Appendix A. The search strategy was adjusted for some keywords (e.g. data leak, and information leak) as they can be used in some articles with different meaning with is not relevant to this study. Records identified from the database was sent to the citation manager (EndNote X8) for the next step.

From the previous step, 904 articles were retrieved (appendix B). Box 1 details the inclusion and exclusion criteria, which constitutes the study selection stage of our scoping review. Subsequent Figure 1 summarises the selection process from identification to the inclusion of articles into the study.

Box 1. **Details of Study Selection (Inclusion/Exclusion Criteria)**

Inclusion
Database: PubMed
Language: English
Text availability: Full text
Publication dates: 2009/01/04-2019/01/01
Source type: Journal (original /research articles), peer review
Subject area:
-*Data Breaches*: Unauthorised access, use, collection, and disclosure of health information (See examples of data breaches provided at The Office of the Australian Information Commissioner (2018)
-*Personal health information (PHI):* Individual information (related to the physical or mental health of a person or other information) collected, transmitted and/or maintained electronically by a health service provider (Chernyshev et al. 2018)
Type of system: Systems containing PHI related to study setting
Data: Electronic
***Participants*:** Individuals (users committed unauthorized access, hackers, staff, healthcare professionals, students (Medical, physician assistant (PA), and allied health)) or organization (see study setting)
Study setting: Health services and organizations providing the services: (the definition of service providers adopted from The Office of the Australian Information Commissioner (2016)
Outcome: Identifying the causes and impacts of data breaches
Exclusion
Source type: Review, opinion; perspective, view, letter, comment and response, conference paper (in book series), Symposium proceedings paper
Subject area:
-*Solely describe*: protocols, encryption, algorithms or formulas, mathematical models, law/rule and ethics, simulation, learning models, implementation, design or architecture, development of computer programs, modeling language (e.g. UML)
-Disclosing information for improving care delivery, using a fictional case study
Data: non-electronic, e.g. paper data

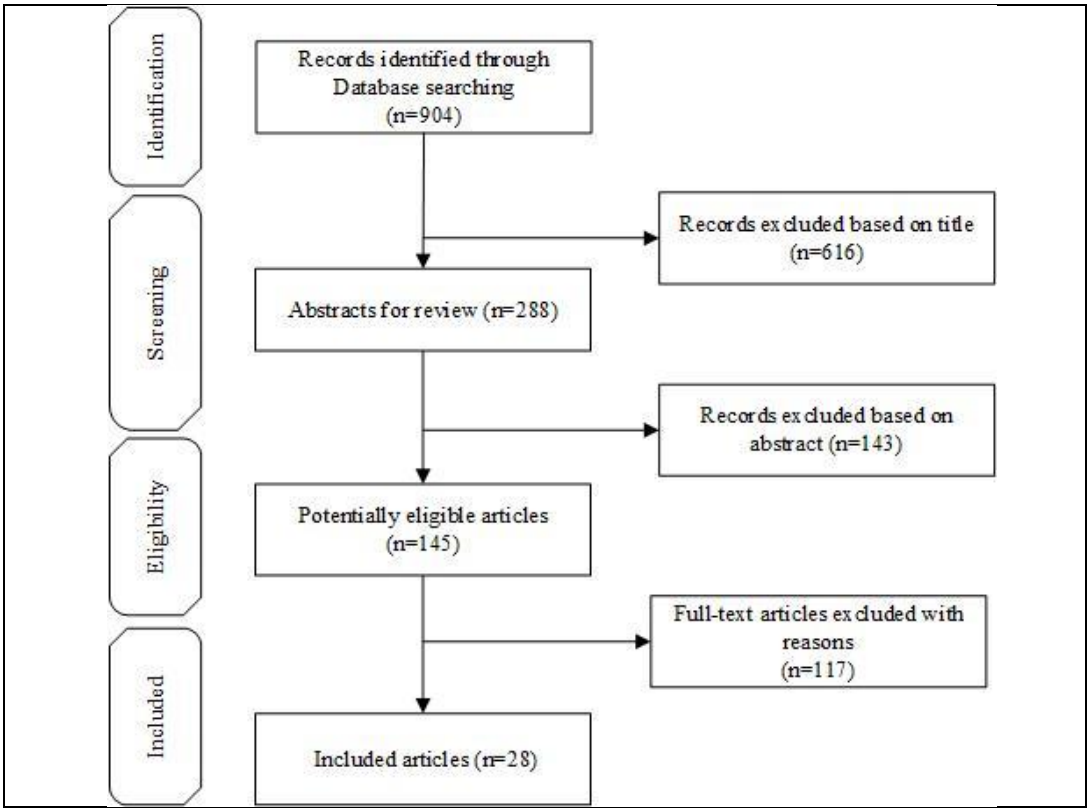

Figure 1. PRISMA Diagram of The Study Selection Process for the Scoping Review

Subsequently, detailed data of the 28 included articles were collected. The data covers authors (year), journal, country, methods, context, systems, level of analysis, and employed theory (see Appendix C). We performed a thematic analysis (Braun and Clarke 2006) to identify and report relevant findings (causes and impacts of PHI breaches) from these studies.

Findings

Study Characteristics

A large number of data breach studies (as shown in Table 1), have been recently conducted, with 64% of the included articles published between 2016 and 2018. As the results highlight, a large body of data breach literature seems to have originated from North American (especially, U.S.) samples, with few insights into other regions. There is considerable diversity in terms of the settings of the studies, with a significant portion of them conducted in hospital settings.

As evident in the table, a wide range of systems were examined, with EHR/EMR, and then HIS, being the most common ones. An interesting finding from table 1 is that most studies employed quantitative methods and worked on the individual level of analysis. Finally, there are relatively few studies that explicitly applied a theory. The review reveals that only six articles (21%), all at individual level of analysis, tested theories, namely self-determination theory, information systems success, health belief model (HBM), preventive health behavior, theory of acceptance and use of technology, health information system security threat lifecycle (HISSTL), and deterrence theory.

Table 1. Overview of the Studies Characteristics

Variable	Number of studies	Percentage
Year of publication		
2016-2018	18	64
2013-2015	7	25
2009-2012	3	11
Country		
North America (the USA and Canada)	16 (13,3)	57
Europe (UK, Switzerland, Multiple-countries)	5 (3,1,1)	18
Asia (Taiwan, China, Israel)	5 (3, 1, 1)	18
Australia	2	7
Setting		
Medical centers	2	7
Hospital	9	32
Academic centers	4	14
Business associates	1	4
Multiple-setting	3	11
Not applicable (N/A)	5	18
Other	4	14
Systems		
EMR/EMR	9	32
Health information system (HIS)	6	21
Mobile phones	5	18
Multiple-system	1	4
Desktop computer	1	4
Online platform	2	7
Portable device	1	4
Ultrasound	1	4
No particular system	2	7
Method		
Quantitative	18	64
Qualitative	2	7
Mix	4	14
Other	4	14
Level of analysis		
Individual	19	68
Organizational	7	25
IT artifact	2	7

Thematic Analysis

We started our thematic coding with the five categories of data breach causes (Wikina 2014) in mind. Our analysis confirmed the applicability of these categories as direct causes of data breaches, but also other themes emerged. We labeled these as indirect causes. Behavioral and operational impacts were the other main themes that emerged from our coding. More details on the outcome of our coding process for causes and impacts are summarized in table 2 and the subsequent sections.

Table 2. Causes and Impacts of PHI Breaches

Themes*			Examples of studies using this theme	No.	%**
Causes	*Direct*	Unauthorised access/disclosure	Calhoun et al. (2018), Firdouse et al. (2018), Yaraghi and Gopal (2018), Gabriel et al. (2018), Guo et al. (2018), Hepp et al. (2018), Müthing et al. (2017), Hassidim et al. (2017), Drolet et al. (2017), Blanke et al. (2016), Tieu et al. (2015), Prochaska et al. (2015), Eikey et al. (2015), Wikina (2014), Baskaran et al. (2013), Elger (2009)	16	57
		Hacking/IT incident	Yaraghi and Gopal (2018), Gabriel et al. (2018), Wikina (2014), Müthing et al. (2017)	4	14
		Improper disposal	Yaraghi and Gopal (2018), Gabriel et al. (2018), Wikina (2014), Moggridge (2017)	4	14
		Loss	Yaraghi and Gopal (2018), Gabriel et al. (2018), Blanke et al. (2016), Wikina (2014)	4	14
		Theft	Yaraghi and Gopal (2018), Gabriel et al. (2018), Blanke et al. (2016), Wikina (2014)	4	14
	Indirect	Non-compliance	Kuo et al. (2018), Calhoun et al. (2018), Kuo et al. (2017), Sher et al. (2017), Eikey et al. (2015), Sethi et al. (2014) Hepp et al. (2018)	7	25
		Ineffective use	Meehan et al. (2018)	1	4
		Awareness	Firdouse et al. (2018), Elger (2009), Fernando and Dawson (2009)	3	11
		Third-party applications	Firdouse et al. (2018)	1	4
		Organizational characteristics	Fernando and Dawson (2009), Gabriel et al. (2018)	2	7
Impacts	*Behavioral*	Privacy concerns	Kisekka and Giboney (2018)	1	4
		Health information sharing	Kisekka and Giboney (2018), Zhou (2018), Walker et al. (2016), Agaku et al. (2014)	4	14
		System use	Tieu et al. (2015)	1	4
		Trust	Tieu et al. (2015), Agaku et al. (2014), Croll (2011)	3	11
	Operational	Care quality	Kisekka and Giboney (2018)	1	4
		System success	Kisekka and Giboney (2018)	1	4

*Certain articles cover more than once categories; ** Percentage based on the number of included studies

Causes

Direct Causes

US Department of Health and Human Services defines five main known causes of breaches, namely, unauthorized access/disclosure, hacking/IT incident, improper disposal, loss, and theft that lead to a direct breach of PHI. As detailed below, we found that this categorization convincingly covers the causes found in our sample.

Unauthorized Access/Disclosure

The majority of studies in our sample investigated unauthorized access/disclosure of PHI as the main reason of data breaches in various forms such as authorized employees or third parties involving in an unauthorized use (Kierkegaard 2012). Take Memorial Hermann Hospital in the U.S., for an example, where a former employee accessed the electronic medical records of more than 10000 customers (Bhuyan et al. 2016). Unauthorized access can also be committed by medical and health science students when they have not received comprehensive privacy training (Calhoun et al. 2018).

A previous study found that a large majority of residents, fellows, and students used their personal mobile phone to save and transfer clinical images (Guo et al. 2018). Although the majority of surgeons received HIPAA compliance training and were familiar with the regulations of electronic communication, most of them using their personal phone to communicate PHI by text message, indicated by Drolet et al. (2017). Notwithstanding the lack of security about this mode of communication, it can be assumed that one potential reason of using personal devices for communication of PHI by students is ease of use (Prochaska et al. 2015). This highlights the pivotal role of insider threat prevention in the data breach incident and understanding the pattern of organizational failure.

Despite the fact that healthcare organizations investing on security infrastructures as a proactive strategy to reduce the likelihood of experiencing security failure (Kwon 2014), employees and students can cause a violation of privacy by access sharing (Hassidim et al. 2017). Baskaran et al. (2013) reported that a great number of studied participants disturbingly shared their personal passwords between staff to access PHI. One possible explanation for this inappropriate behavior is that they have underestimated the seriousness of the PHI breach impacts (Elger 2009). Similar to this adverse trend also be detected at the artefactual level of security analysis where mHealth applications exposed user credentials via insecure connections (Muthing et al. 2017).

Hacking/IT Incident

Comparing to other types of data breach, hacking/IT incidents are not the most common cause of data breaches (in terms of the number of incidents). However, they were found to affect the largest number of people (over 120 million individuals among cover entities), based on Yaraghi and Gopal's (2018) analysis of reported data from 2009 to 2017 in the U.S. A look at the more recent data from January 2019, reveals a similar pattern. Hacking/IT incidents constitute 9 out of 18 reported breaches among covered entities and business associates in the US. These 9 incidents had serious repercussions on the society as 256,070 individual were affected. Gabriel et al. (2018) reported similar findings in hospital settings in particular, i.e., while the number of hacking/IT incidents ranked four among six types of causes, their serious consequences were the highest, affecting over 4,600,000 individuals. In general, OCR data shows hacking incidents are critical and modeling methods to predict why and how such a breach occurs need to be applied to provide better protection of PHI.

Improper Disposal

Compared to hacking/IT incidents, typically fewer breaches are caused by improper disposal. Yaraghi and Gopal (2018) found from breach data of eight years (started from 2009) the least cause with minimal individual effected among not only covered entities but also business associates was improper disposal.

Because health media data can be recovered, medical equipment such as imaging systems containing PHI must be inspected by applying recovery methods before they are returned to lease companies, or sold to third parties. A multiple-method study (preliminary disk inspection, deletion methods, and file

recovery) in ultrasound systems found that PHI could be recovered, even if the data was deleted based on systems' own instructions (Moggridge 2017). Hence, there seems to be a need for updated and more stringent requirements and standards for proper disposal of PHI.

Loss

Loss of data, stored in digital media or electronic devices, may occur due to health information technology malfunction or human-related errors (Palojoki et al. 2016). This phenomenon should be investigated from a sociotechnical viewpoint, i.e., both the health information technology shortcomings and user errors should be considered in a holistic manner (Sittig and Singh 2011). However, a limited body of literature investigated data breach in terms of loss while the interpretations were based on secondary data provided by OCR. Wikina (2014) study was the first attempt, in our sample, to study IT use and causes of breaches. He indicated theft and loss as affecting more individuals is of critical importance to society compared to hacking or IT incidents. In subsequent years, however, digital transformation in the US healthcare reverse this trend to IT hacking (Yaraghi and Gopal 2018).

Theft

As indicated in the OCR reports, theft incidents were committed in a variety of systems from portable devices to network servers. In this case of crime, often the same features that enable the ease of use of digital records (e.g., a centralized database that allows remote access to all health records) also facilitate ease of theft (Arthur Conklin and McLeod 2010). In the US context, research has shown theft is the most common type of breach and in terms of impact on individuals was far higher than the other three data breaches, after Hacking/IT Incident (Gabriel et al. 2018; Yaraghi and Gopal 2018).

Indirect Causes

In our thematic analysis, we identified a number of indirect causes. Although these elements do not readily result in a data breach, they can indirectly facilitate a data breach incident.

Non-compliance

One important factor contributing to the violation of privacy and disclosure of PHI is the lack of compliance. According to American Institute of Certified Public Accountants' (AICPA), it is the second most serious concern in the context of IT management (Warkentin et al. 2011), thereby resulting organizations in costs of failure (Kwon and Johnson 2013).

Past research on continuance compliance intention has highlighted the role of users' habit formation for compliance with privacy. For example, Kuo et al. (2018) tested the relationship between motivations (intrinsic and extrinsic), habit and intention in complying with EMR privacy policy. They found that motivational factors such as self-efficacy and perceived usefulness led to the formation of habits, which in turn led to a continuance intention to comply with the privacy policy.

Privacy and security rule violations often happened when medical and health science student disclosed PHI for non-care related delivery/operations. For example, Calhoun et al. (2018) reported in one case of breach, a student submitted an assignment with a patient's personal information despite his attempt to cover it up. The patient was then identified by faculty and staff members.

In some organizations, there were collaborating challenges to protect patient privacy because of different perceptions among organizational roles. For example, it is reported that from the users' viewpoints, they tend to not log out of their account since the process of logging in and logging out is a computational inconvenience while the IT staff believe this behavior may disturb the patient privacy (Eikey et al. 2015). Similarly, in a qualitative evaluation of the IT security program, Hepp et al. (2018) found unlocked workstations as a common cause of security breaches.

Ineffective use

In our data extraction, we found only one study focused on the ineffective use of systems and its potential impact on patient privacy invasions. According to the responses of a sample of residents, one

of the outcomes of ineffective use of technology, inexperience with EMR for example, is a possible data breach such as data loss(Meehan et al. 2018).

Awareness

Security awareness highlighted in the information system literature as a countermeasure to reduce IT misuse and enhance employee's compliance behavior (Bulgurcu et al. 2010; D'Arcy et al. 2009). Hence, the lack of security awareness poses a risk of data breaches to the organization. A recent study by Firdouse et al. (2018) highlighted the safety and security concerns regarding the use of texting for clinical communications. The authors argue that there is a need for regulatory guidance and awareness to help physicians decide on what constitutes a reasonable use of texting. It is reported that poor privacy and security awareness training can lead to underestimating the seriousness of situations where PHI protection is required, and thus, result in a confidentiality breach (Elger 2009; Fernando and Dawson 2009).

Third-party applications

Despite the importance of mobile applications in healthcare, there is a paucity of empirical researches that analyze the role of third-party applications as a cause of data breach. As third-party applications such as Apple iMessage, and WhatsApp messaging, become increasingly popular in health institutions, cybersecurity experts raise concerns about text messages security. For example, cybercriminals can use data mining and take advantage of the vulnerabilities of text messaging software that often automatically archives texts for 5 years or more (Firdouse et al. 2018)

Organizational characteristics

Three main organizational characteristics related to data breach were described in the included studies, namely, size, budget, and type. With regards to organizational size, while small health organizations have limitations in allocating financial resources to IT security investments, the evidence of data breaches in the US surprisingly suggests that larger hospitals have a higher possibility of data breaches (Gabriel et al. 2018). Fernando and Dawson (2009) found that privacy and security training in healthcare workplaces are unlikely to be functionally optimal with inadequate budgets. Finally, with regards to hospital type, Gabriel et al. (2018) found the risk of data breaches in pediatric and teaching hospitals are higher than other types of hospitals.

Impacts

Once healthcare organizations encounter serious security incidents, such as data breaches, a variety of adverse impacts are likely. In particular, if proper remedial actions in response to the breach are not taken appropriately at the very earliest opportunity, patient/customers' attitudes and behaviors, as well as systems operations can be impacted. In the study, we labeled the main theme of impacts as behavioral and operational.

Behavioral Impacts

Privacy concerns

As the applications of using electronic records to enhance patient care become increasingly important and ubiquitous in the digital health environment, the challenges of accessing and controlling personal health data and addressing privacy concerns become more salient (Angst and Agarwal 2009). Kisekka and Giboney (2018) found that when health systems are not secure in terms of protecting personal information, privacy concerns will increase. They emphasized system security is part of system quality in the information system model. In fact, data breaches compromise the security of health systems and consequently, patients will have a negative perception about system safeguard against privacy invasion. Hence, it is logical to assume that serious privacy concerns arise as an outcome of a data breach.

Health information sharing

Patients who use online health services have an expectation to control the privacy of their PHI. In situations where the services are perceived to be less confidential and can lead to authorized access, they are unlikely to disclose health information (Zhou 2018).

Fear of failure to preserve PHI by healthcare providers is a barrier in patients' information sharing (Agaku et al. 2014), as it may prevent organizations from improving health service delivery. This interpretation differs from that of Walker et al. (2017) who found that the effects of privacy and security concerns on patients' PHI sharing were minimal and constant. Their explanation was that customers experiencing excellent care are willing to accept the potential risk of breaches associated with PHI. This view proposes that high quality of care in some situations may reduce the perceived importance of a potential data breach.

System use

This theme is central to the information systems literature and consequential for health systems' future (Recker et al. 2019; Wu and Du 2012), as it improves organizational effectiveness and efficiency during which the users accurately operate the systems to fulfill their task (Burton-Jones and Grange 2013; Burton-Jones and Straub 2006). However, designed goals of the system typically cannot be achieved in case of system failures or privacy scandals. For instance, poor security measures and inappropriate responses to data breaches raise users' privacy concerns, which in turn can hinder effective use of health information system. This problem has been indicated in the case of online patient portal use in a general hospital (Tieu et al. 2015). For example, as a barrier to portal use, caregivers were concerned about the vulnerability of the system to hackers and breach of confidentiality regarding diagnoses and medications data. By providing a highly secured system for disclosing health information for the purpose of care delivery, health organizations may enable patients to use portal frequently and effectively than if privacy breach concerns not addressed in practices.

Trust

While the concept of trust has long been a consideration from a number of perspectives, especially as a determinant of IT acceptance, the negative impact of data breaches on trust needs further research as there is currently limited empirical evidence in this domain. Agaku et al. (2014) emphasized weak security measures of PHI will undermine patients' trust and confidence in their healthcare providers. Highlighting the important and complex roles of trust in patients' decision making, Croll (2011) presented a privacy model and a full set of policies for healthcare to define the relationship between confidentiality, trust, privacy, and security. It was found that different type of data breaches could threaten to erode individuals trust in the organization. Similarly, it is shown that users who experienced data breaches in the past, were more likely to distrust organization security measures (Tieu et al. 2015).

Operational Impacts

Our review revealed the operational impacts of data breaches such as *care quality* and *system success* were studied less frequently in the existing literature.

Care quality

In the integrated healthcare, the availability of information in EHR has a critical role for providers to maintain and improve care quality (Amato et al. 2015). Yet, health service excellence can be effected when data breach incidents occur or privacy and security concerns are expressed. For example, Kisekka and Giboney (2018) found that some privacy concerns, such as access to EHR by unauthorized individuals, decrease perceived patient care quality.

System success

In our sample, only one attempt was made to investigate the impact of a data breach on system success. Kisekka and Giboney (2018) argue that the success of health care technologies depends on having effective security controls and sufficient safeguards in place. There is clearly a need for further studies

to identify the links between data breach incidents and the potential success of healthcare information systems.

Concluding Remarks and Future Directions

With the increasing proliferation of digital health technologies, PHI breaches are becoming a mounting concern for healthcare organizations. Breaches can negatively impact individual behavior and organizational performance. To address this issue and protect PHI, there are regulatory and institutional forces that drive healthcare organizations to invest in security and privacy (Angst et al. 2017). However, still there is an ongoing need to systematically collect the evidence related to the causes and impacts of PHI breaches, and further theorize the phenomena

In this paper, we reviewed empirical studies of data breaches published from 2009 to 2018. Our thematic analysis revealed a considerable variety of direct and indirect causes, as well as behavioral and operational impacts of PHI breaches. Our review confirmed that PHI breaches had impacts on individuals and system operation. Hence, they can be a veiled threat to successful and meaningful digital health transformations. We expect that identifying causes and impacts of PHI breaches can help healthcare organizations in developing preventive measures and remedial actions, in achieving resilience when facing a breach.

Our scoping review highlights several directions for future research. In terms of the level of analysis, most studies in our sample investigated data breaches from an individual perspective, e.g., unauthorized access/disclosure of data by individuals. It is surprising that no study conducted at more than one level of analysis. By performing multilevel analyses, future research can provide a richer explanation of why organizations are vulnerable to data breaches and how they can craft effective responses and mitigate the risk. With regards to methodologies, few studies in our sample applied a mixed method approach. A data breach is a complex phenomenon and hackers find diverse and innovative ways to find vulnerabilities and attack organizational systems. To study this vibrant topic, there is a need for future studies that use mixed methods such as interviews, observations, risk predictions, and IT artifact analysis. Not surprisingly, our review uncovers heavy gravitation toward the US samples, with a limited number of studies in other regions. This provides a promising avenue for further investigations in other countries, particularly with considering and theorizing the impacts of cross-cultural differences.

Finally, we echo Lowry et al.'s (2017) call for the effective use of "powerful" IS theories in security and privacy research. As discussed earlier, only around 21% of the articles in our sample explicitly used a theory. This is understandable given that different disciplinary norms govern the field of Medical Informatics. Still, we believe further attention to IS theories can materialize cross-disciplinary benefits (Chiasson et al. 2007). In particular, we identified several themes that were not included in any theoretical model in our sample. These themes were hacking/IT incident, improper disposal, loss, and theft (among direct causes), and ineffective use, and third-party applications (among indirect causes). We invite IS and Medical Informatics researchers to use these findings and engage in further theorizing the impactful phenomenon of "data breach" in healthcare settings and other contexts.

Supplementary Material (Appendices A–C)

Appendices (anonymized) are available online at https://goo.gl/tLuatT

References

Agaku, I. T., Adisa, A. O., Ayo-Yusuf, O. A., and Connolly, G. N. 2014. "Concern About Security and Privacy, and Perceived Control over Collection and Use of Health Information Are Related to Withholding of Health Information from Healthcare Providers," *Journal of the American Medical Informatics Association* (21:2), pp. 374-378.

Amato, F., De Pietro, G., Esposito, M., and Mazzocca, N. 2015. "An Integrated Framework for Securing Semi-Structured Health Records," *Knowledge-Based Systems* (79), pp. 99-117.

Angst, C. M., and Agarwal, R. 2009. "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion," *MIS Quarterly*. (33:2), pp. 339-370.

Angst, C. M., Block, E. S., D'arcy, J., and Kelley, K. 2017. "When Do It Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches," *MIS Quarterly* (41:3).

Arksey, H., and O'Malley, L. 2005. "Scoping Studies: Towards a Methodological Framework," *International Journal of Social Research Methodology* (8:1), pp. 19-32.

Arthur Conklin, W., and McLeod, A. 2010. "Information Security Foundations for the Interoperability of Electronic Health Records," *International Journal of Healthcare Technology and Management* (11:1-2), pp. 104-112.

Baskaran, V., Davis, K., Bali, R. K., Naguib, R. N., and Wickramasinghe, N. 2013. "Managing Information and Knowledge within Maternity Services: Privacy and Consent Issues," *Informatics for Health and Social Care* (38:3), pp. 196-210.

Bhuyan, S. S., Bailey-DeLeeuw, S., Wyant, D. K., and Chang, C. F. 2016. "Too Much or Too Little? How Much Control Should Patients Have over Ehr Data?," *Journal of medical systems* (40:7), p. 174.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp. 523-548.

Buntin, M. B., Burke, M. F., Hoaglin, M. C., and Blumenthal, D. J. H. a. 2011. "The Benefits of Health Information Technology: A Review of the Recent Literature Shows Predominantly Positive Results," *Health affairs* (30:3), pp. 464-471.

Braun, V., and Clarke, V. 2006. "Using Thematic Analysis in Psychology," *Qualitative research in psychology* (3:2), pp. 77-101.

Burton-Jones, A., and Grange, C. 2013. "From Use to Effective Use: A Representation Theory Perspective," *Information systems research* (24:3), pp. 632-658.

Burton-Jones, A., and Straub, D. 2006. "Reconceptualizing System Usage: An Approach and Empirical Test," *Information systems research* (17:3), pp. 228-246.

Calhoun, B. C., Kiel, J. M., and Morgan, A. A. 2018. "Health Insurance Portability and Accountability Act Violations by Physician Assistant Students: Applying Laws to Clinical Vignettes," *Journal of Physician Assistant Education* (29:3), pp. 154-157.

Chernyshev, M., Zeadally, S., and Baig, Z. 2018. "Healthcare Data Breaches: Implications for Digital Forensic Readiness," *Journal of Medical Systems* (43:1), p. 7.

Chiasson, M., Reddy, M., Kaplan, B., and Davidson, E. 2007. "Expanding Multi-Disciplinary Approaches to Healthcare Information Technologies: What Does Information Systems Offer Medical Informatics?," International Journal of Medical Informatics (76 Suppl 1), pp. S89-97.

Croll, P. R. 2011. "Determining the Privacy Policy Deficiencies of Health Ict Applications through Semi-Formal Modelling," *International journal of medical informatics* (80:2), pp. e32-38.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

Drolet, B. C., Marwaha, J. S., Hyatt, B., Blazar, P. E., and Lifchez, S. D. 2017. "Electronic Communication of Protected Health Information: Privacy, Security, and HIPAA Compliance," *The Journal of hand surgery* (42:6), pp. 411-416.

Eikey, E. V., Murphy, A. R., Reddy, M. C., and Xu, H. 2015. "Designing for Privacy Management in Hospitals: Understanding the Gap between User Activities and It Staff's Understandings," *International journal of medical informatics* (84:12), pp. 1065-1075.

Elger, B. S. 2009. "Violations of Medical Confidentiality: Opinions of Primary Care Physicians," *British Journal of General Practice* (59:567), pp. e344-352.

Elton-Pym, J. 2017. "Medicare Data Breach Is the Tip of the Iceberg in the World of Australian Dark Web Fraud." Retrieved 24/02/2019, 2018, from https://www.sbs.com.au/news/medicare-data-breach-is-the-tip-of-the-iceberg-in-the-world-of-australian-dark-web-fraud

Fernando, J. I., and Dawson, L. L. 2009. "The Health Information System Security Threat Lifecycle: An Informatics Theory," *International journal of medical informatics* (78:12), pp. 815-826.

Firdouse, M., Devon, K., Kayssi, A., Goldfarb, J., Rossos, P., and Cil, T. D. 2018. "Using Texting for Clinical Communication in Surgery: A Survey of Academic Staff Surgeons," *Surg Innov* (25:3), pp. 274-279.

Gabriel, M. H., Noblin, A., Rutherford, A., Walden, A., and Cortelyou-Ward, K. 2018. "Data Breach Locations, Types, and Associated Characteristics among Us Hospitals," *American Journal of Managed Care* (24:2), pp. 78-84.

Goode, S., Hoehle, H., Venkatesh, V., and Brown, S. A. 2017. "User Compensation as a Data Breach Recovery Action: An Investigation of the Sony Playstation Network Breach," *MIS Quarterly* (41:3).

Gordon, W. J., Fairhall, A., and Landman, A. 2017. "Threats to Information Security—Public Health Implications," *New England Journal of Medicine* (377:8), pp. 707-709.

Guo, D., Phan, N., Ho, K., Pawlovich, J., and Kitson, N. 2018. "Clinical Texting among Medical Trainees of the University of British Columbia [Formula: See Text]," *Journal of cutaneous medicine and surgery* (22:4), pp. 384-389.

Hassidim, A., Korach, T., Shreberk-Hassidim, R., Thomaidou, E., Uzefovsky, F., Ayal, S., and Ariely, D. 2017. "Prevalence of Sharing Access Credentials in Electronic Medical Records," *Healthcare informatics research* (23:3), pp. 176-182.

Hepp, S. L., Tarraf, R. C., Birney, A., and Arain, M. A. 2018. "Evaluation of the Awareness and Effectiveness of It Security Programs in a Large Publicly Funded Health Care System," *Health Information Management Journal* (47:3), pp. 116-124.

Humer, C., and Finkle, J. 2014. "Your Medical Record Is Worth More to Hackers Than Your Credit Card." *Reuters* Retrieved 24/02/2019, from https://uk.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924

Kierkegaard, P. 2012. "Medical Data Breaches: Notification Delayed Is Notification Denied," *Computer Law & Security Review* (28:2), pp. 163-183.

Kisekka, V., and Giboney, J. S. 2018. "The Effectiveness of Health Care Information Technologies: Evaluation of Trust, Security Beliefs, and Privacy as Determinants of Health Care Outcomes," *Journal of Medical Internet Research* (20:4), p. e107.

Kohli, R., and Tan, S. S.-L. 2016. "Electronic Health Records: How Can Is Researchers Contribute to Transforming Healthcare?," *MIS Quarterly* (40:3), pp. 553-574.

Kuo, K. M., Chen, Y.a C., Talley, P. C., and Huang, C. H. 2018. "Continuance Compliance of Privacy Policy of Electronic Medical Records: The Roles of Both Motivation and Habit," *BMC Medical Informatics and Decision Making* (18:1), p. 135.

Kuo, K. M., Talley, P. C., Hung, M. C., and Chen, Y. L. 2017. "A Deterrence Approach to Regulate Nurses' Compliance with Electronic Medical Records Privacy Policy," *Journal of Medical Systems* (41:12), p. 198.

Kwon, J. 2014. "Proactive Versus Reactive Security Investments in the Healthcare Sector," *MIS Quarterly* (38:2), pp. 451-471.

Kwon, J., and Johnson, M. E. 2013. "Health-Care Security Strategies for Data Protection and Regulatory Compliance," *Journal of Management Information Systems* (30:2), pp. 41-66.

Levac, D., Colquhoun, H., and O'Brien, K. K. 2010. "Scoping Studies: Advancing the Methodology," *Implementation science* (5:1), p. 69.

Lord, N. 2018. "Top 10 Biggest Healthcare Data Breaches of All Time." *Data Insider* Retrieved June 25, 2018, 2018, from https://digitalguardian.com/blog/top-10-biggest-healthcare-data-breaches-all-time

Lowry, P. B., Dinev, T., and Willison, R. 2017. "Why Security and Privacy Research Lies at the Centre of the Information Systems (Is) Artefact: Proposing a Bold Research Agenda," *European Journal of Information Systems* (26:6), pp. 546-563.

McLeod, A., and Dolezel, D. 2018. "Cyber-Analytics: Modeling Factors Associated with Healthcare Data Breaches," *Decision Support Systems* (108), pp. 57-68.

Meehan, R., Kawalec, J., Caldwell, B., and Putman, D. 2018. "Proficiency of First-Year Podiatric Medical Residents in the Use of Electronic Medical Records," *Perspectives in Health Information Management* (15:Winter), p. 1c.

Ministry of Communications and Information. 2018. "Statement by Mr S Iswaran, Minister-in-Charge of Cybersecurity, on the Cyber-Attack on Singhealth's It System, During Parliamentary Sitting on 6 August 2018," in: *Cyber Security, Personal Data*. Singapore: Ministry of Communications and Information.

Moggridge, J. 2017. "Security of Patient Data When Decommissioning Ultrasound Systems," *Ultrasound* (25:1), pp. 16-24.

Muthing, J., Jaschke, T., and Friedrich, C. M. 2017. "Client-Focused Security Assessment of Mhealth Apps and Recommended Practices to Prevent or Mitigate Transport Security Issues," *JMIR Mhealth Uhealth* (5:10), p. e147.

Palojoki, S., Pajunen, T., Saranto, K., and Lehtonen, L. 2016. "Electronic Health Record-Related Safety Concerns: A Cross-Sectional Survey of Electronic Health Record Users," *JMIR medical informatics* (4:2).

Prochaska, M. T., Bird, A. N., Chadaga, A., and Arora, V. M. 2015. "Resident Use of Text Messaging for Patient Care: Ease of Use or Breach of Privacy?," *JMIR medical informatics* (3:4), p. e37.

Recker, J., Indulska, M., Green, P., Burton-Jones, A., and Weber, R. 2019. "Information Systems as Representations: A Review of the Theory and Evidence," *Journal of the Association for Information Systems* (In Press).

Sher, M. L., Talley, P. C., Cheng, T. J., and Kuo, K. M. 2017. "How Can Hospitals Better Protect the Privacy of Electronic Medical Records? Perspectives from Staff Members of Health Information Management Departments," *Health Information Management Journal* (46:2), pp. 87-95.

Sittig, D. F., and Singh, H. 2011. "Defining Health Information Technology–Related Errors: New Developments since to Err Is Human," *Archives of internal medicine* (171:14), pp. 1281-1284.

The Office of the Australian Information Commissioner, O. 2016. "Is My Organisation a Health Service Provider?."

The Office of the Australian Information Commissioner, O. 2018. "Which Data Breaches Require Notification."

Tieu, L., Sarkar, U., Schillinger, D., Ralston, J. D., Ratanawongsa, N., Pasick, R., and Lyles, C. R. 2015. "Barriers and Facilitators to Online Portal Use among Patients and Caregivers in a Safety Net Health Care System: A Qualitative Study," *Journal of Medical Internet Research* (17:12), p. e275.

Walker, D. M., Johnson, T., Ford, E. W., and Huerta, T. R. 2017. "Trust Me, I'm a Doctor: Examining Changes in How Privacy Concerns Affect Patient Withholding Behavior," *Journal of Medical Internet Research* (19:1), p. e2.

Warkentin, M., Johnston, A. C., and Shropshire, J. 2011. "The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention," *European Journal of Information Systems* (20:3), pp. 267-284.

Wikina, S. B. 2014. "What Caused the Breach? An Examination of Use of Information Technology and Health Data Breaches," *Perspective Health Information Management* (11), p. 1h.

Wu, J., and Du, H. 2012. "Toward a Better Understanding of Behavioral Intention and System Usage Constructs," *European Journal of Information Systems* (21:6), pp. 680-698.

Yaraghi, N., and Gopal, R. D. 2018. "The Role of HIPAA Omnibus Rules in Reducing the Frequency of Medical Data Breaches: Insights from an Empirical Study," *The Milbank Quarterly* (96:1), pp. 144-166.

Zhou, J. 2018. "Factors Influencing People's Personal Information Disclosure Behaviors in Online Health Communities: A Pilot Study," *Asia-Pacific Journal of Public Health* (30:3), pp. 286-295.