2020

On the Complexity of Health Data Protection-in-Practice: Insights from a Longitudinal Qualitative Study

Javad Pool
The University of Queensland, j.pool@uq.net.au

Saeed Akhlaghpour
University of Queensland, s.akhlaghpour@business.uq.edu.au

Andrew Burton-Jones
University of Queensland, abj@business.uq.edu.au

On the Complexity of Health Data Protection-in-Practice: Insights from a Longitudinal Qualitative Study

Completed research paper

Javad Pool
UQ Business School
The University of Queensland
Brisbane, Australia
Email: j.pool@uq.net.au

Saeed Akhlaghpour
UQ Business School
The University of Queensland
Brisbane, Australia
Email: s.akhlaghpour@business.uq.edu.au

Andrew Burton-Jones
UQ Business School
The University of Queensland
Brisbane, Australia
Email: abj@business.uq.edu.au

Abstract

Digitalization of healthcare presents opportunities for improving the quality of healthcare services and promises economic benefits. However, the success of digital health and the benefits cannot be actualized without considering health data protection practices in the process of healthcare service delivery. Despite the criticality of protecting health data in the system use lifecycle (from recording to consuming and taking informed actions), there is a paucity of research to investigate this complex phenomenon. Using longitudinal qualitative data on a state-wide digital health transformation project, we contextually theorize the practices for protecting health data. Our study reveals five types of health data protection-in-practice, namely data minimization, informal encoding, accuracy, improving cyber-awareness, and appropriate access management. Our results provide new insights into information system use (especially, effective use), and highlight practices that can improve health data protection.

Keywords Cybersecurity, data privacy, effective use, data protection, digital health, electronic medical records.

1 Introduction

The transformation to digital health provides opportunities for healthcare providers to enhance their efficiency and the quality of health care delivery (Bernardi et al. 2019; Venkatesh et al. 2016). The widespread adoption and use of digital health systems such as Electronic Health Records (EHR), the Internet of Medical Things (IoMT) devices, and mobile health (mHealth) is offering greater connectivity and revolutionizing the care delivery landscape from remote monitoring to precision medicine (Grewal et al. 2020). More importantly, the Covid-19 crisis is facilitating the shift toward digital health transformation and the use of digital health technologies (e.g., telehealth) (Wosik et al. 2020).

As health organizations transforming from traditional systems to digital systems, challenges for protecting digital assets and customer data are increasing. These challenges are originated from both inside of organizations (improper use) and external cyber threats to digital health assets (hacking/IT incidents) (Alshehri et al. 2016; Hempel et al. 2020; Pool et al. 2019). Kim and Kwon (2019) indicated that while healthcare can get benefit from EHR (e.g., improved patient care quality), digitized health data (e.g., within EHRs) and their usage can give rise to health data breaches. Thus, to minimize the risk of data breaches and unpacking the benefit of digital health, data protection practices must be an integral part of system use. Failures in protecting health data can have an impact on care quality and result in harm to patients (Choi et al. 2019; Pool et al. 2020; Tidy 2020).

Past research has investigated a variety of aspects of health IT transformation, adoption, and use (Bernardi and Exworthy 2020; Findikoglu and Watson-Manheim 2016). However, our understanding of how users practice data protection and the complexity of healthcare environments for effective data protection are limited. For translating digital health investments to business value, organizations need to consider the effective use of health information systems (Burton-Jones and Volkoff 2017). In this paper, we argue that practices related to data protection are important for effective use of health IT. To reach data protection goals, such as accuracy and safeguarding the confidentiality of personal data, managers and users need to shift their perspective from the adoption of digital health to effective and personal data protection (PDP)-aware use of digital health systems. Limited studies on the linkages between system use and health data protection leave use-related practices for effective data protection unexplored. Inspired by calls for theorizing with being explicit about the context (Davison and Martinsons 2016), constructing a contextualized theory of effective use (Burton-Jones and Volkoff 2017), and distinctive theorizing of personal health data privacy (Agarwal et al. 2010), we seek to address this theoretically and practically important knowledge gap based on the analysis of qualitative data from a state-wide digital health transformation between 2015 and 2019. Through this theory development study on health data protection-in-practice, we aim to inform healthcare practitioners on effectively protecting health data and materializing the benefits of digital health.

The rest of the paper is structured as follows. The next section provides a background on past research on Effective Use Theory and representing the scope of the study. Next, a methodical approach that was used is explained. Finally, qualitative results are provided followed by a brief conclusion and future research directions.

2 Background

Effective Use Theory (Burton-Jones and Grange 2013) proposes studying how system use facilitates users to attain a goal-oriented activity (task) and improves performance (the desired end). To provide a concept mapping of Effective Use Theory, we conducted a bibliometric analysis via VOSviewer (Van Eck and Waltman 2010). This analysis reflects 214 articles indexed in the Scopus database, and have cited Effective Use study (Burton-Jones and Grange 2013). Figure 1 represents a network visualization of Effective Use related studies. The links in the diagram are based on the co-occurrences of authors' keywords and the size of the nodes represents the frequency of articles on a specific topic.

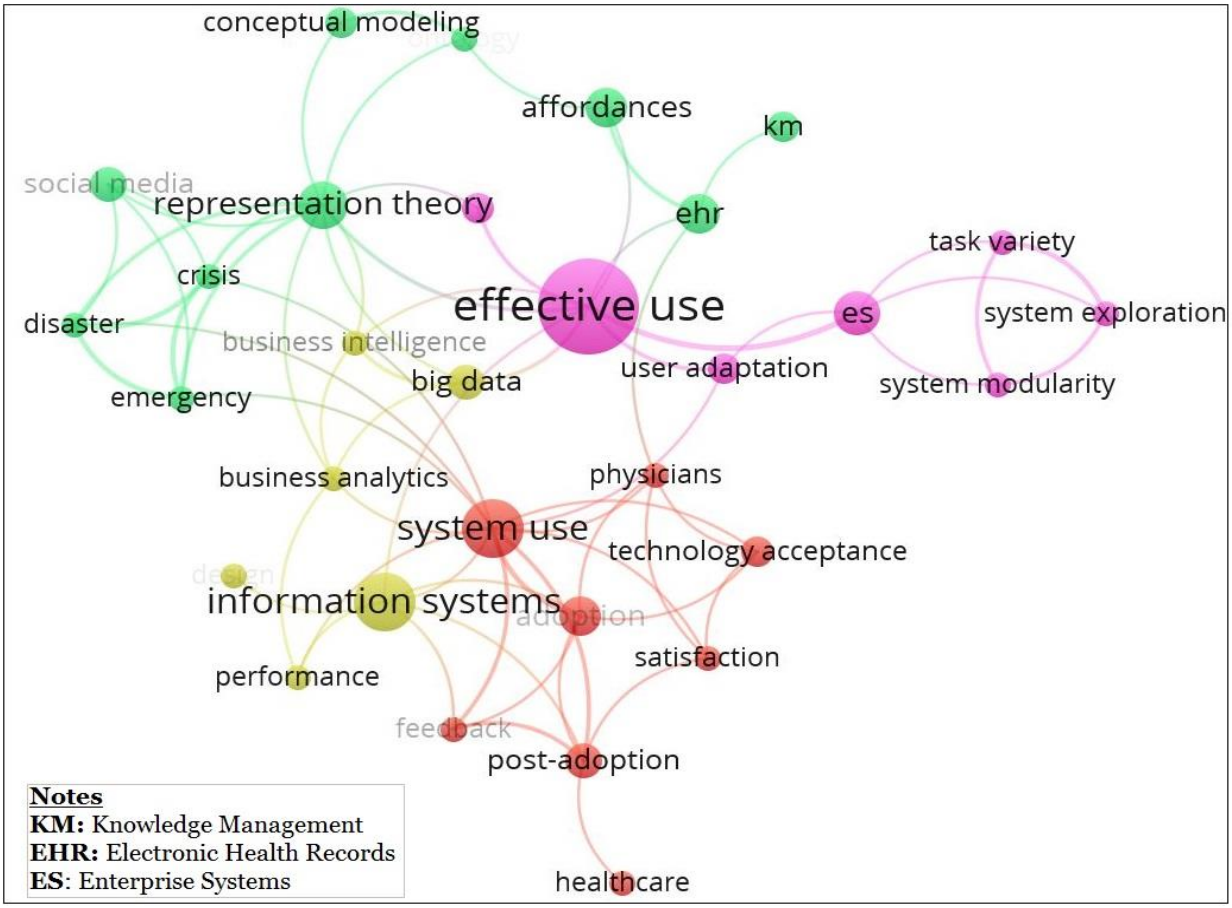

Figure 1: Network visualization of Effective Use related literature

As depicted in figure 2, a variety of theoretical concepts and contexts are used or informed by the effective use study such as affordance concept and social media context.

To go beyond the concept mapping, we reviewed the information systems literature limited to studies used and contextualized this theory. Table 1 summarizes and provided a picture of past research on effective use theory.

Author(s)	Level of analysis	Context/setting	Method	Theory
Lauterbach et al. (2020)	Multi-level	Banking	Mixed	Effective use, representation theory
Bonaretti et al. (2020)	Individual	Hospitality	Quantitative	Effective use
Savoli et al. (2020)	Individual	Healthcare	Mixed	Effective use, attribution theory, learned helplessness theory
Bao et al. (2020)	Individual	Healthcare	Quantitative	Effective use
Torres and Sidorova (2019)	Individual	Business intelligence and analytics	Quantitative	Effective use, IS success model
Marchand and Raymond (2018)	Multi-level	SMEs	Mixed	Effective use
Burton-Jones and Volkoff (2017)	Multi-level	Healthcare	Qualitative	Effective use

Table 1. Illustrative Examples of Past Research on Effective Use Theory

As the network visualization (Figure 1) illustrates, concepts including system use, adaptation, post-adoption, and affordance, and contexts such as big data, electronic health records, and social media have been investigated using Effective Use as a theoretical lens. However, by applying an integrative approach from table 1 and figure 1, we can see that concepts such as privacy and security have not been explored as a component of effective use. This is a missed opportunity because an effective use lens could provide more direct insights for organizations regarding whether they are using their systems in a way that is addressing users' security and privacy needs, and would prevent adverse events such as health data breaches. This theory development study aims to address this theoretically and practically important knowledge gap and expand the current explanatory power of effective use theory. Figure 2 demonstrates the scope of our study and expected contributions to the effective use theory and data protection.

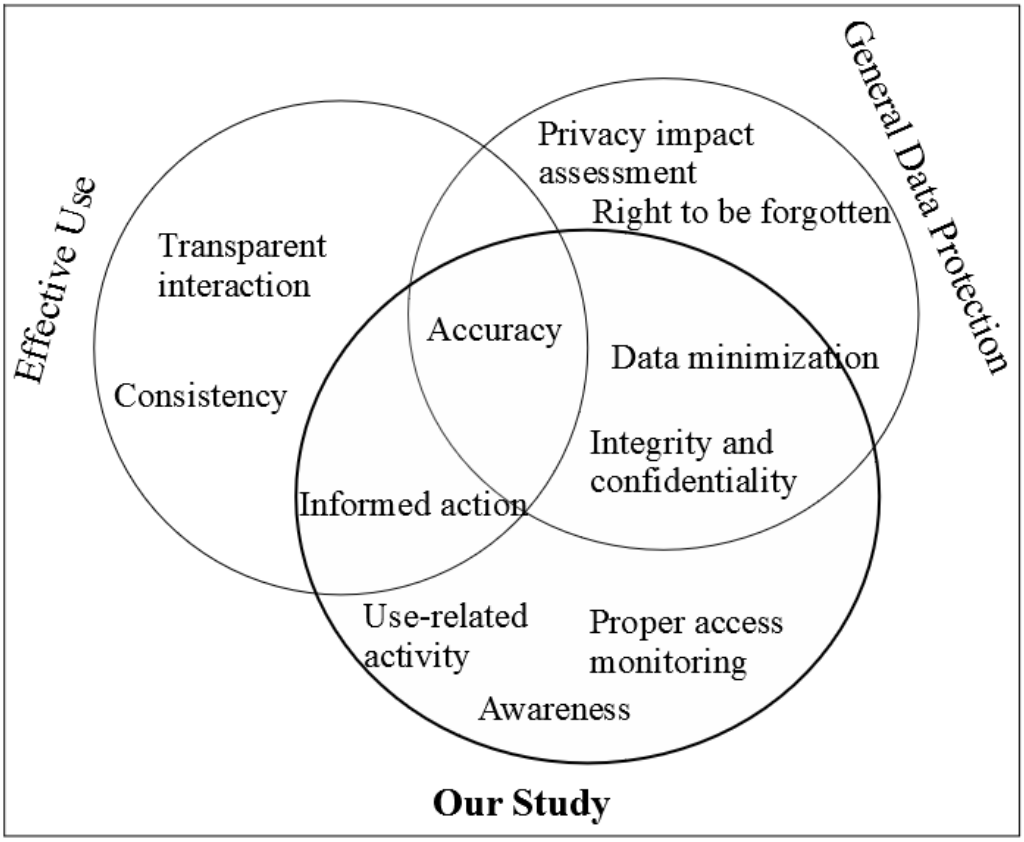

Figure 2: The Scope of Our Study

3 Method

This study builds upon data from a longitudinal qualitative study of a state-wide digital health transformation mega project in Australia. From 2015 to 2019, our team conducted over 100 interviews with individuals in different roles including clinicians (allied health, physicians, nurses, and pharmacists) and managers (hospital administration and health executives). While we initially sampled participants and asked questions based on an interest in effective use in general, we noticed that a small but significant subset of the interviewees raised issues related to data privacy and security. Upon further analysis, we identified 19 that discussed the issue in some depth. Further details of the research context are available in Burton-Jones et al. (2020). Effective use of information systems was the main theme in this longitudinal research. In this article, we focus only on privacy- and security-related themes emerged from that data. Table 2 summarizes our research study procedures.

Stage	**Tasks**
Stage 1: Conducting the overarching digital health evaluation research project (2015-2019)	Conducting and transcribing interviews as the main data source
Stage2: Identification, screening, and including	Searching in the data source to identify concept related to privacy and security and screening the transcripts for data protection practices and

Stage	Tasks
	including relevant interview transcriptions for analysis
Stage 3: Coding and conceptualizing	Open coding of interview texts for identifying data protection concepts, and consequently developing themes and the overarching theoretical dimension
Stage 4: Contextual theorization	Providing explanations on how users practice Personal Data Protection (PDP)-aware use in the healthcare context

Table 2. Research Study Procedures

After conducting stage 1 and 2, we included 19 interview transcripts for our data analysis and theorization. Table 3 provides an overview of the participants of these included transcripts.

Participant characteristics		Number
Role*	IT	4
	Admin	6
	Physician	6
	Nursing	1
	Allied Health	7
Level	Front-line	11
	Manager	8
Total number of participants		19
Notes: *some participates have multiple roles (e.g., admin and physician)		

Table 3. Overview of Research Participants

Stage 3 and 4 were informed by guidelines recommended by Gioia et al. (2013) for theoretical advancement.

4 Results

4.1 Data Structure

In this study, we attempted to theorize the complexity of health data protection-in-practices via users' activities involved in different levels and contexts of healthcare organizations. Data protection was central concepts in our understanding of medical and managerial practices (i.e., accuracy, appropriate access management). Table 4 illustrates the data structure and how our study progressed from concept to emergent themes, and the overarching dimension.

Level	***1st Order Concepts***	***2nd Order Themes***	***Aggregate dimensions***
Individual (Health professionals)	Not recording data beyond the scope of practice and considering legal requirements	Data minimization	PDP-aware frontline use
	Careful documentation of data (i.e., related to mental health) in the general chart		
	Writing sensitive information with the guidance from the hospital solicitor		
	Proper record keeping (i.e., not having parallel files)		
	Considering customers' rights/requests for not including sensitive personal data in their medical records (i.e., domestic violence)		
	Documenting sensitive data in a way that is meaningful for an authorized person	Informal encoding	
	An accurate reflection of what's going on and has happened	Accuracy	

Level	***1st Order Concepts***	***2nd Order Themes***	***Aggregate dimensions***
	An accurate reflection on patients' conditions (both positive and negative)		
	Correct and accurate inputs, and documentation		
	A holistic picture on the patients by real-time information and data		
	Ensuring the truth of patients' history and changes		
Organization	Understanding the clinical environment and increasing cyber-awareness regarding the use of connected health systems	Improving cyber-awareness	PDP-aware organizational use
	Getting appropriate training for proper access		
	Managing auditable information	Appropriate access management	
	Monitoring who accessed what, when and how, and from where		
	Informing about inappropriate access		
	Questioning about user access and data processing		
	Doing weekly/monthly report and monitoring closely for inappropriate access and taking aware actions		
	Better control of data access		
	Getting involved in privacy complaints		
	Granting and revoking permission for access		
	Putting constraints and warnings in the system and demanding reasons for extracting data		
	Appropriate monitoring of VIP patients		

Table 4. Data Structure

4.2 From Data Structure to Theoretical Explanations

Building upon our empirical data from the use of health IT, we contextually explained the phenomenon of health data protection-in-practice. We labeled our theoretical concept as *Personal Data Protection (PDP)- Aware Use*. *This concept captures practices and use activities for facilitating effective data protection*. The overarching dimension, *PDP- Aware Use,* emerged in multi-levels of individual (frontline users) and organizational PDP- Aware Use.

From an individual level of analysis, we identified three themes: 'data minimization', 'informal encoding', and 'accuracy' whereas from an organizational level of analysis, the themes were 'improving cyber-awareness' and 'appropriate access management.

4.2.1 Data Minimization

Data minimization refers to the extent to which data is "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (Article 5 of the General Data Protection Regulation (GDPR)). In our study, data minimization was manifested in how users (e.g., allied health professionals) mindfully record health data limited to their scope of practice. This recording of data should be essential and relevant to care delivery (e.g., patient mental health and relevant medical risks) or legal actions (e.g., in case of domestic violence).

To illustrate the value of recording relevant and necessary health data, a psychologist worked at the outpatient's clinic explained that:

> *"There is information relating to a patient's mental health care, which is what I am doing, that is* ***not necessarily appropriate to be visible*** *in a general chart. Either, because it is very delicate information and one needs to be* ***careful about documenting*** *that in the general chart, or because perhaps it contains raw data from some tests, for example, and the tests have copyright constraints, so obviously we cannot put those into the chart."*

As healthcare service is a complex context, data minimization practices, and defining what should be included in health records is challenging. Thus, for practicing data minimization, users should consider the type and sensitivity of data. This complexity is especially highlighted in an area where social workers providing services regarding domestic violence, sexual assault, and child protection:

> *"Because we get privilege to such sensitive information, it is a fine line between what is recordable and what should be left out of the medical chart."* (Social worker).

In such a context that users are involved in healthcare delivery face complexity in safeguarding the confidentiality of data, they can seek to receive advice from lawyers (e.g., hospital solicitor). A social worker gave an example in such a context:

> *"I have a notebook that I write notes in. If it is really that sensitive, no, I would not be writing it down. I would be – it is just something that I have. There has been on occasion that I have, with the guidance from the hospital solicitor, put in my assessment just for confidentiality reasons."*

Considering the scope of practice is a relevant concept to data minimization. Healthcare professionals must not input unnecessary data in the medical records that are beyond their roles. A psychologist noted:

> *"There's the **scope of practice**, so what I write has to **relate**. I wouldn't comment on blood pressure, for example. I do need to provide information on the person's mental state to support their care and I am ethically and possibly legally required to report on risk factors, especially with children. ... There was an example of a patient wanting to keep confidential some elements about her private life that we agreed didn't affect her medical plan, so I didn't put it on her chart."*

4.2.2 Informal Encoding

Informal encoding is an emerging theme in our study which refers to recoding data in a way that understandable for authorized users. This theme is distinct and goes well beyond privacy regulation compliance. In this practice users consider the context (systems and users) they are providing healthcare services. For example, there might be a large healthcare organization with an opportunity of wide access to medical records (because of a lack of data access controls based on role or because of a need for an integrative health system). In this case, to minimize the risk of improper access, health professionals can use an informal encoding:

> *"We find ways to capture that information and we might have **a certain sentence** that we use in an assessment that alludes to the fact that there is some sensitive information. But we do not actually write down what is going on.*
>
> [INTERVIEWER: So, it is a code between you and your colleagues].
>
> *Yes. It might be – for example, it is probably prejudicial childhood. If you read that it could mean anything but social workers reading that, you would be saying that there is some form of child abuse of some sort, dysfunctional family.*
>
> [INTERVIEWER: Is this because other clinicians basically access, from other departments access the information, or is it also because the patient as well somehow?]
>
> *Yes. It is both. It is both. Because, I always write my assessments – in the back of my mind I normally **think well**, at some point the patient can access, you know, can ask to access their records. So, I write it in a way, or I try and write it in a way that if they do read that, then ..." (Social worker)*

4.2.3 Accuracy

Accuracy is the linking theme in our study that provides a connection between the data protection regulations (e.g., GDPR) and native information system theories (e.g., Effective Use Theory). Informed by GDPR and Effective Use Theory, we refer accuracy as the extent to which health data is "accurate and, where necessary, kept up to date" and how well health data is "faithfully reflects the domain being represented" (Article 5 of GDPR; Burton-Jones and Grange (2013, p. 642)).

An accurate reflection of caregiver reality (i.e., what's going on and has happened) depends upon users' practices, i.e., putting accurate and update data in medical record systems. For example, an emergency specialist noted:

> *"... because you want to know that what you're reading is a reflection of what's actually been going on. A lot of the information gets pulled, such as results, so that will be accurate. The actual entry of the notes, such as the problem lists, keeping that up to date is relying on a person to enter it."*

To illustrate accurate data, clinicians should consider reflection on patients' conditions, recording both positive and equally important, negative conditions of patients. A physician and director of clinical services explained the rationale for recording important negatives to ensuring accuracy:

> *"Well, there's a saying that we still use, but I've heard this, a thousand times, good notes, good protection, poor notes, poor protection, no notes, no protection. ... I think that notes that include important negatives, such as things that are not wrong with the patient and are stated as such, contribute strongly to the accuracy of the record. ... because when I'm handing over verbally to one of my staff, a complex patient, I might say, "There has been no fever. There has been no cough. There are abdominal signs. There is nothing new in the skin and the joints." All of these can be omitted and assumed that they're negative, or they can be explicitly stated to be negative."*

Beyond data protection, accuracy also helps users to perform informed actions, which in turn, contribute to patient health. A dietitian manager explained the role of real-time data and completeness as follows:

> *"... you're getting a lot more real-time data and I suppose it's created a better picture. Overall holistic picture for the patient. Also not repeating things that have already been done*. Not thinking, "Do I need to request a blood test for this patient?"

4.2.4 Improving cyber-awareness

Improving cyber-awareness refers to organizational practices that provides appropriate training to users on how to effectively use systems in an authorized way and understand cybersecurity issues (e.g., beyond password sharing and downloading). Training and awareness are two concepts that are related to this theme and also can be mapped to the second function of the National Institute of Standards and Technology (NIST) cybersecurity framework (protection).

Training not only is an important concept for the effective use of health systems but also facilitates data protection practices as they provide an opportunity for users on how to properly access health data. A gap in training can lead to failure in data protection and also hinder the materialization of benefit from digital health investment. A clinical benefit manager noted on getting appropriate training:

> *"... benefit's always a combination of the functionality but then how you use it and how well you use it. So if you've got appropriate training in it, then great. If there's a gap in training and you don't know what you're meant to be doing, then if you don't have the proper access to the system, your functionality is restricted because it's based on your security role and your privileges, then that's going to hinder the realisation of that benefit because you don't have the appropriate permissions to sign off or to do what you need to do."*

Cybersecurity awareness, as an organization-wide activity, should also be considered in health data practices. This first-order concept is related to users' proper understanding of cyber-threats and unauthorized activities. As healthcare systems are becoming connected and integrated, cybersecurity awareness is critical for protecting health data. A Chief Information Officer (CIO) explained:

> "*So, when I'm in my area, I worry about my password, I don't share that. But what we're trying to do now is get people to understand that cyber security is a much broader, much greater thing and you don't need to just worry about sharing your password and not downloading something, it's about changing behaviour and attitude and understanding, cause and effects are two things that are not just within your environment, but with all the things contributing to your environment, because your environment might be where you work, but because you're totally connected now, it's everything. It doesn't matter what you do.*"

4.2.5 Appropriate Access Management

The final theme of PDP-aware use is appropriate access management. In our study, we defined appropriate access management as using the system in a way that an organization effectively monitors users' access to health data (user and system), evaluates the appropriateness of access (user and task) and takes informed action (reactive and proactive). This theme also aligns with the *protection* function of the NIST cybersecurity framework, and especially the category of *identity management and access control.*

Transforming from traditional health systems to digital health systems providing benefits and challenges for appropriate access management. For example, digital health can increase the ability of organizations to manage auditable data to monitor user access to data. This benefit is noted by a Deputy Medical Director:

> *"We will get a bucket load of auditable information which again needs governance. So it's all very well having thousands of CCTV's around, but who's looking at them. So we can go back and find out who accessed what, when and how, and from where".*

Similarly, on the affordance of Health information systems for appropriate access management (abilities for actions), a health information manager explained:

> *"There's a functionality in the system that allows a smart time auto player so if there's an inappropriate access you can actually have the video of you strolling around so that's very good for a HR management process."*

Another perspective regarding appropriate access management is that the managers in their practice of data access monitoring should always question why a certain user accesses and uses health data. A Nurse Unit Manager noted:

"… it's flagged and then if somebody opens that chart it's like 'okay […]'s opened, you know, […]'s chart over there' and 'why is she doing that, there's no relationship and no reason she should be doing that' and then I'd be questioned into that."

However, it should be noted that in some contexts, appropriate access management can be complex. As an example of this complexity, A Deputy Medical Director indicated:

> *"… we don't know what happened to that information usually, I mean if they took a photocopy of it, or printed it or took a photo."*

To provide the general overview of our theory development we summarized the key components of PDP-aware use in Table 5.

Theory overview	
In our study, we developed a theory of data protection and provided a new concept, PDP-aware use, which made contributions to 'systems use' and 'information privacy and security' literature.	
Theory component	**Instantiation**
Type of theory	Theory for explaining PDP-aware use (type II theory)
Primary constructs	Data minimization, informal encoding, accuracy, improving cyber-awareness, and appropriate access management
Level	Multi-level (individual and organizational)
Context	Healthcare, users (health professionals (e.g., physicians, psychologists, social workers) and IT staff, managers), health information system (e.g., EHR), tasks (e.g., medical practices, access management), regulation (e.g., privacy), timeline (2015-2019)
Overarching proposition	The extent to which users mindfully interact with health systems (secure and proper access) and awarely use health data in their practices can facilitate (or hamper) effective health data protection
Theoretical advancements	Introducing new constructs (e.g., data minimization, informal encoding) and contextual explanations which go well beyond the current boundary of Effective Use Theory

Table 5. An Overview PDP-Aware Use

5 Conclusion

This research investigated the complexity of health data protection-in-practices with the purpose to develop a theory for explaining PDP-aware use in the context of healthcare. We conducted an inductive analysis of qualitative data from 2015 to 2019, and followed the Gioia Methodology for constructing grounded theory, and using an interpretative approach for explanations. Our analysis revealed PDP-aware use in five areas of practice: data minimization, informal encoding, accuracy, proper use-related activity, and appropriate access management. These practices go beyond the practices or activities previously reported in the system use, privacy, and health informatics literature.

PDP-aware use constructs, especially, the emerging concepts related to data minimization and informal coding are novel and important for health data protection. These concepts can be further explored and theorized in future research. Furthermore, we proposed a theory for contextual explanations of PDP-aware use. This type II theory, in line with Gregor (2006)'s typology on information systems theories, can be used by researchers as a platform for future theory elaboration and theory development (e.g., theory type IV: theory for explaining and predicting). Also, our study provides opportunities for future consideration as an input to further opening the black box of data protection-in-practice by developing theories for design and action (type V), e.g., designing cyber-awareness training tools or privacy-protective add-ons for EMR systems.

References

Agarwal, R., Gao, G., DesRoches, C., and Jha, A. K. 2010. "Research Commentary—the Digital Transformation of Healthcare: Current Status and the Road Ahead," *Information Systems Research* (21:4), pp. 796-809.

Alshehri, S., Mishra, S., and Raj, R. K. 2016. "Using Access Control to Mitigate Insider Threats to Healthcare Systems," *2016 IEEE International Conference on Healthcare Informatics (ICHI)*: IEEE, pp. 55-60.

Bao, C., Bardhan, I. R., Singh, H., Meyer, B. A., and Kirksey, K. 2020. "Patient–Provider Engagement and Its Impact on Health Outcomes: A Longitudinal Study of Patient Portal Use," *MIS Quarterly* (44:2), pp. 699-723.

Bernardi, R., and Exworthy, M. 2020. "Clinical Managers' Identity at the Crossroad of Multiple Institutional Logics in It Innovation: The Case Study of a Health Care Organization in England," *Information Systems Journal* (30:3), pp. 566-595.

Bernardi, R., Sarker, S., and Sahay, S. 2019. "The Role of Affordances in the Deinstitutionalization of a Dysfunctional Health Management Information System in Kenya: An Identity Work Perspective," *MIS Quarterly* (43:4), pp. 1177-1200.

Bonaretti, D., Bartosiak, M., Lui, T.-W., Piccoli, G., and Marchesani, D. 2020. "“What Can I(S) Do for You?”: How Technology Enables Service Providers to Elicit Customers' Preferences and Deliver Personalized Service," *Information & Management* (57:6), pp. 1-13.

Burton-Jones, A., Akhlaghpour, S., Ayre, S., Barde, P., Staib, A., and Sullivan, C. 2020. "Changing the Conversation on Evaluating Digital Transformation in Healthcare: Insights from an Institutional Analysis," *Information and Organization* (30:1), p. 100255.

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 Volkoff, O. 2017. "How Can We Develop Contextualized Theories of Effective Use? A Demonstration in the Context of Community-Care Electronic Health Records," *Information Systems Research* (28:3), pp. 468-489.

Choi, S. J., Johnson, M. E., and Lehmann, C. U. 2019. "Data Breach Remediation Efforts and Their Implications for Hospital Quality," *Health services research* (54:5), pp. 971-980.

Davison, R. M., and Martinsons, M. G. 2016. "Context Is King! Considering Particularism in Research Design and Reporting," *Journal of Information Technology* (31:3), pp. 241-249.

Findikoglu, M., and Watson-Manheim, M. B. 2016. "Linking Macro-Level Goals to Micro-Level Routines: Ehr-Enabled Transformation of Primary Care Services," *Journal of Information Technology* (31:4), pp. 382-400.

Gioia, D. A., Corley, K. G., and Hamilton, A. L. 2013. "Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology," *Organizational research methods* (16:1), pp. 15-31.

Gregor, S. 2006. "The Nature of Theory in Information Systems," *MIS quarterly*), pp. 611-642.

Grewal, D., Hulland, J., Kopalle, P. K., and Karahanna, E. 2020. "The Future of Technology and Marketing: A Multidisciplinary Perspective," *Journal of the Academy of Marketing Science* (48), pp. 1-8.

Hempel, G., Janosek, D. B., and Raziano, D. B. 2020. "Hacking Humans: A Case Study and Analysis of Vulnerabilities in the Advancing Medical Device Landscape," *Cyber Security: A Peer-Reviewed Journal* (3:4), pp. 351-362.

Kim, S. H., and Kwon, J. 2019. "How Do Ehrs and a Meaningful Use Initiative Affect Breaches of Patient Information?," *Information Systems Research* (30:4), pp. 1184-1202.

Lauterbach, J., Mueller, B., Kahrau, F., and Maedche, A. 2020. "Achieving Effective Use When Digitalizing Work: The Role of Representational Complexity," *MIS Quarterly* (44:3), pp. 1023-1048.

Marchand, M., and Raymond, L. 2018. "Performance Measurement and Management Systems as It Artefacts," *International Journal of Productivity and Performance Management* (67:7), pp. 1214-1233.

Pool, J., Akhlaghpour, S., and Fatehi, F. 2020. "Towards a Contextual Theory of Mobile Health Data Protection (MHDP): A Realist Perspective," *International Journal of Medical Informatics* (141), p. 104229.

Pool, J., Akhlaghpour, S., Fatehi, F., and Burton-Jones, A. 2019. "Causes and Impacts of Personal Health Information (PHI) Breaches: A Scoping Review and Thematic Analysis," *Proceedings of the 23rd Pacific Asia Conference on Information Systems: Secure ICT Platform for the 4th Industrial Revolution, PACIS 2019*, X'ian, China.

Savoli, A., Barki, H., and Paré, G. 2020. "Examining How Chronically Ill Patients' Reactions to and Effective Use of Information Technology Can Influence How Well They Self-Manage Their Illness," *MIS Quarterly* (44:1), pp. 351-389.

Tidy, J. 2020. "Police Launch Homicide Inquiry after German Hospital Hack." *BBC News* Retrieved 20/09/2020, from https://www.bbc.com/news/technology-54204356

Torres, R., and Sidorova, A. 2019. "Reconceptualizing Information Quality as Effective Use in the Context of Business Intelligence and Analytics," *International Journal of Information Management* (49), pp. 316-329.

Van Eck, N. J., and Waltman, L. 2010. "Software Survey: Vosviewer, a Computer Program for Bibliometric Mapping," *scientometrics* (84:2), pp. 523-538.

Venkatesh, V., Rai, A., Sykes, T. A., and Aljafari, R. 2016. "Combating Infant Mortality in Rural India: Evidence from a Field Study of Ehealth Kiosk Imlementations," *MIS Quarterly* (40:2), pp. 353-380.

Wosik, J., Fudim, M., Cameron, B., Gellad, Z. F., Cho, A., Phinney, D., Curtis, S., Roman, M., Poon, E. G., and Ferranti, J. 2020. "Telehealth Transformation: Covid-19 and the Rise of Virtual Care," *Journal of the American Medical Informatics Association* (27:6), pp. 957-962.