2021

Socio-technical Challenges to the Effective Use of Health Information Systems (IS) and Data Protection: A Contextual Theorization of the Dark Side of IS Use

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

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

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

Follow this and additional works at: [https://aisel.aisnet.org/acis2021](https://aisel.aisnet.org/acis2021)

**Recommended Citation**  
[https://aisel.aisnet.org/acis2021/49](https://aisel.aisnet.org/acis2021/49)

This material is brought to you by the Australasian (ACIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ACIS 2021 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Socio-technical Challenges to the Effective Use of Health Information Systems (IS) and Data Protection: A Contextual Theorization of the Dark Side of IS Use

Full 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

Information Systems (IS) research on health IS use has suffered from a positivity bias – largely focusing on upside gains rather than the potential dark side of usage practices. Exploring the dark side and failures in health IS use, such as shortcomings in data privacy and cybersecurity, can provide useful insights for research, practice, and policy. Through qualitative analyses of three datasets collected between 2015 and 2021, we theorize challenges to the effective use of IS and data protection in Australian health services. We propose a contextualized theory of ‘health records misuse’ with two overarching dimensions: data misfit and improper data processing. We explain sub-categories of data misfit: availability misfit, meaning misfit, and place misfit, as well as sub-categories of improper data processing: improper interaction and improper data recording and use. Our findings demonstrate how health records misuse arises from socio-technical systems, and impacts health service delivery and patient safety.

Keywords Digital health, effective use theory, health records misuse, data privacy, cybersecurity.
1 Introduction

Digital health has been recognized as a strategic capability to help healthcare services to improve service delivery and reduce cost (Karahanna et al. 2019; Strong et al. 2014). But digital health and use alone is not sufficient to actualize benefits (Burton-Jones and Grange 2013). It is the effective use of digital health information systems (IS) across the healthcare ecosystem that can help in achieving intended outcomes (Agarwal et al. 2010; Burton-Jones and Volkoff 2017). Effective use can also be complex (Burton-Jones and Grange 2013) and significant challenges exist at individual and organizational levels that can prevent the achievement of desired outcomes (Agarwal et al. 2010; Burton-Jones and Volkoff 2017) and lead to unintended consequences (Parks et al. 2017).

The health IS literature has increasingly focused on the bright side of digital health, such as digital advantages (Karahanna et al. 2019), activity improvements (Abouzahra and Ghasemaghaei 2021), and the enhancement of patient self-management (Savoli et al. 2020). Insights from the dark side are limited. The dark side refers to “negative phenomena that are associated with the use of IT, and that have the potential to infringe the well-being of individuals, organizations and societies” (Taraftar et al. 2015, p. 161). Multiple calls for investigating the dark side of IS have highlighted the importance of research regarding the negative’ phenomena (Myers 2021; Rossi et al. 2021). Understanding the dark side of IS use (e.g., data privacy and cybersecurity) in healthcare services is critical. This is especially important in healthcare because it is an extreme context where IS use can have an effect on human life.

Our goal in this paper is to outline socio-technical factors challenging the effective use of Health IS, especially from a data protection perspective. In particular, we examine the dark side of health data protection use in which digital health technologies along with behavioral, managerial, and organizational aspects play a substantive role (Sarker et al. 2019). We situate our work in the emerging program of research on effective use theory (Burton-Jones and Grange 2013; Burton-Jones and Volkoff 2017; Trieu et al. Forthcoming) which has focused on upside gains to date but has much to gain by adding a dark side perspective, such as understanding how effective use could involve mitigating threats to data privacy. We address our aim by developing a contextualized theory of how electronic health record systems can be misused, leading to failures in protecting health data.

Our theory of misuse can be viewed as a ‘theory for understanding’ (Gregor 2006) as it offers explanations on how ‘health records misuse’ occurs in healthcare services. Understanding how technology is used is an important factor for practice and policy (Schneier 2020). Thus through explaining the dark side of health IS use, we aim to inform not just researchers but also health service practitioners as well as policy makers responsible for data protection policies in digital health.

The paper is structured as follows. We first review the health IS use literature to highlight the dominant concepts and theories, and how this literature can be enriched with a new insight linking health IS use and data protection. We then present our approach for qualitative analysis. This section is followed by reporting our findings: data structure and explanations of ‘health records misuse.’ We then conclude.

2 Background

IS use is among the key building block of IS literature and has been examined in various contexts (Baird and Maruping 2021; Burton-Jones et al. 2017b). Understanding the use of IS in healthcare, as an extreme context (Hällgren et al. 2018), has received significant attention in both IS and organization science (Bhattacherjee et al. 2018; Lapointe and Rivard 2007; Oborn et al. 2011; Savoli et al. 2020).

To illustrate the important concepts in Health IS use, we conducted a bibliometric analysis via VOSviewer (Van Eck and Waltman 2010). This analysis focuses on research on health IS use published in the top 10 IS journals (basket of eight journals, ‘Information & Management’, and ‘Information & Organization’). To identify relevant literature we used the Scopus database which covers these targeted journals. We used a broad set of search terms that reflect the concept of IS use and healthcare context in the title/abstract/keywords of papers. Our search terms were: (“system use” OR “system usage” OR “technology use” OR “continuous use” OR "IT use" OR "IS Use" OR “effective use” OR “deep structure use” OR “enhanced use” OR “meaningful Use” OR “use of IT” OR “use of the system” OR “use of information” OR “use of system” OR “feature Use” OR “portal Use” OR “use of e-mail” OR “use of mobile” OR “use of portal” OR “IT service use” OR “use of social media” OR “social media use” OR “use of electronic” OR “record* use” OR “data use” OR “use of data” OR “use of digital” OR misuse OR abuse OR “improper use”) AND (“health care” OR healthcare OR “home care” OR “community care” OR “aged care” OR “primary care” OR hospital OR hospitals OR patient* OR “disease” OR “chronic conditions” OR clinic* OR medic* OR telehealth OR telemedicine OR
"health data" OR "health information" OR "health professional*" OR physician OR surgeon OR paramedic). This search strategy led to the identification of 54 papers related to health IS use.

Figure 1 represents the keyword co-occurrence network of health IS use studies. A shorter distance between two nodes (e.g., IT use and adoption) generally reflects a close relationship. The line between two nodes represents that they have appeared together (e.g., privacy and security). A greater co-occurrence of keywords results in a thicker line. The same color in the diagram represents a cluster. VOSviewer divided the health IS Use literature into six clusters and one item (implementation).

Figure 1: Network visualization of Health IS Use Related Literature

The network visualization illustrates health IS use-related concepts including multimodal networks, adoption, implementation, use mediation, resistance to use, effective use, affordance, privacy, and security. This visualization also shows the links between some concepts such as privacy and effective use has not been studied.

Beyond the concept-centric approach, we also reviewed the seminal papers in the health IS use literature. These papers are based on network visualization depicted by VosViewer and have more than 50 citations in the Scopus. The type and unit of analysis in this visualization are citations and documents (articles). Figure 2 shows this citation-centric visualization. The size of nodes in Figure 2 illustrates the impact (number of citations) of the scholars on literature. For example, the study by Agarwal et al. (2010) on digital transformation is cited by 439 research indexed in Scopus. Whereas the research by Liang et al. (2010) on physicians’ IT use is cited by 54.
**Figure 2: Network Visualization of Seminal Papers on the Health IS Use Related Literature (only showing the first author and year)**

Figure 1 and Figure 2 are the outcomes of our bibliometric networks analysis via VOSviewer. Based on the network visualization (two close clusters of research: colored by red and green) and seven unlinked research), in Table 1 we summarized past research on health IS use.

<table>
<thead>
<tr>
<th>Cluster/concept</th>
<th>Approach to study health IS use</th>
<th>Theory</th>
<th>Data protection (including privacy &amp; security)</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Models of IS use</td>
<td>Focus on direct and indirect use, and IS use avoidance</td>
<td>Social network perspective</td>
<td>A call for more research in health information security (Agarwal et al. 2010)</td>
<td>Kane and Alavi (2008), Agarwal et al. (2010), Kane and Labianca (2011)</td>
</tr>
<tr>
<td>IS Use intention</td>
<td>Focus on behavioral intention towards use and continue to use</td>
<td>Innovation diffusion theory, Theory of Planned Behavior (TPB), Unified Theory of Acceptance and Use of Technology (UTAUT)</td>
<td>NI</td>
<td>Jackson et al. (2013)</td>
</tr>
<tr>
<td>Cluster/concept</td>
<td>Approach to study health IS use</td>
<td>Theory</td>
<td>Data protection (including privacy &amp; security)</td>
<td>Authors</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Contextual explanations of effective use of IS</td>
<td>Focus on affordance actualization and explanations of effective use in the context of community care electronic healthcare record (EHR)</td>
<td>Effective use</td>
<td>Partially consider data protection by investigating constructs such as accuracy</td>
<td>Burton-Jones and Volkoff (2017)</td>
</tr>
<tr>
<td>Emergent use of IS in practice</td>
<td>Focus on the context of use in practice, and the role of negotiations (power and politics)</td>
<td>Practice lens</td>
<td>NI</td>
<td>Constantinides and Barrett (2006)</td>
</tr>
<tr>
<td>Diversity of IS use</td>
<td>Focus on electronic patient record use in a multidisciplinary practice</td>
<td>Practice theory</td>
<td>NI</td>
<td>Oborn et al. (2011)</td>
</tr>
<tr>
<td>Institutionalization of IS use</td>
<td>Focus on improving understandings of IS use with concepts such as theorization, translation, practical use, &amp; legitimization</td>
<td>Institutional theory</td>
<td>NI</td>
<td>Nielsen et al. (2014)</td>
</tr>
<tr>
<td>IS use attitudes</td>
<td>Focus on the use in departmental contexts and its association with attitudes toward IS</td>
<td>NI, problem driven</td>
<td>NI</td>
<td>Aydin and Rice (1991)</td>
</tr>
<tr>
<td>IS use</td>
<td>Focus on IS use as a consequence of team climate</td>
<td>UTAUT, Social influence theories</td>
<td>NI</td>
<td>Liang et al. (2010)</td>
</tr>
</tbody>
</table>

Table 1. Illustrative Examples of Seminal Research on Health IS Use

As evident in Table 1, a wide range of theories from IS discipline (e.g., TAM, UTAUT, and effective use) and adjacent disciplines in the organization and social sciences (e.g., practice theory, institutional theory, TPB) have been contextualized in healthcare. Our review of the literature, however, clearly demonstrates that the IS use literature inadequately addresses data protection concepts. Only the study by Burton-Jones and Volkoff (2017) investigated concepts related to data protection such as accuracy, and even that study only did so indirectly and from a positive angle (focusing on how clinicians strove to enter more accurate data for better decision-making). The only other study mentioning data protection only did so briefly in a call for more research on health data security (Agarwal et al. 2010).

Beyond our selected review on seminal research that drives literature on health IS use, our literature review did find a small but notable connection between meaningful use and privacy (see figure 1, gold cluster on right-hand side). However, upon inspection of these studies, we found that this link had only been investigated from a nominal and proxy view. In other words, the focus of these studies on meaningful use is still not on how IS use can contribute to privacy and security. For example, Kwon and Johnson (2018) found that meaningful use attestation is associated with the reduction of accidental internal data breaches in the long term. In a similar study, Kim and Kwon (2019) indicated that meaningful use initiatives can increase the risk of data breaches. Although these two studies provide useful information on IS use, the measures of meaningful use in these studies was binary, without
adequate contextual explanations. These shortcomings can lead to incomplete conclusions about IS use in healthcare.

Our study addresses this missed opportunity in the literature on the dark side of health IS use, especially with regard to data privacy. Between the two native theories in IS use (see Table 1), UTAUT and effective use, our contextual explanations and contribution are inspired by effective use. We select this theory for two reasons. Our study is beyond intention to use and focuses more on actual (mis)use, and (mis)practices that constrain appropriate informed actions. Also, among the contextualized IS use theories in healthcare, effective use theory provides better insight for data protection (accuracy). Thus, this theory, as an overarching lens, is a suitable candidate for further exploration and theorization. Another reason for using this theory is that it provides an opportunity for improving the theory by giving greater attention to the dark side of IS use. Overall, therefore, we seek to improve theory and practice by overcoming the aforementioned lack of attention to, and inadequate coverage of, the dark side of health IT use, especially risks to data privacy and security. Figure 3 demonstrates our interdisciplinary approach, context, and expected contributions to the IS use literature and privacy principles (e.g., the Australian Privacy Principles (APPs)). APPs are ‘principles-based law’. A breach of an APP can lead to regulatory action and penalties (OAIC n.d.).

Figure 3: The Overlapping Research Area

3 Methods

This research is based on three sources of qualitative data from 2015-2021. Our first and main data set was originated from a longitudinal project of studying digital health (implementation, use, and evaluation) conducted from 2015 to 2019 in Australia. Digital Alpha project (a pseudonym) is a diversified and unique context in health services including allied health services to surgery and emergency services. Our research team interviewed over 100 healthcare staff involved in the use and management of electronic medical records (EMR). This includes frontline clinicians, IT professionals, and service managers. To evaluate the Digital Alpha project and improve effective use, the research team interviewed participants to gain insights into the state and actual use of digital health systems. As the research evolved, we noticed that other concepts which were indirectly related to effective use (from the dark side) emerged. Especially, experienced health service managers and IT professionals expressed their concerns about the complexity of healthcare data use and issues about data protection such as data privacy, accuracy, and security. In our first data source, 16 participants (7 at the managerial level and 9 at the front line level (including health professionals and IT staff)) had discussed the data protection issues in some depth. Inspired by the result of the Digital Alpha project, our second data source came from interviews with subject matter experts in privacy and cybersecurity. In 2020, we conducted interviews with 15 experts to further explore the dark side of health IS use that can result in health data breaches such as unauthorized access. The third data source used in this study was news articles about recent privacy and cybersecurity incidents in Australian health services. To collect this data, we searched the Factiva database, which aggregates content from a large number of media sources (such as...
newspapers, journals, magazines, television, and radio transcripts). In our search strategy, we used relevant keywords that represent the dark side of health data use ("privacy breach" OR "data privacy" OR "data breach" OR "cyber attack" OR cybersecurity OR "cyber security" OR ransomware OR "improper use" OR "unauthorized access" OR "unauthorized access" OR "unauthorized disclosure" OR "unauthorized disclosure") AND (healthcare OR Health OR Hospital OR clinic OR patient OR "aged care")), limited to Region (Australia) and timestamp (1 January-7 July 2021). All news articles were reviewed for their relevance to the dark side of health IS use (data protection failures) and consequent outcomes. On this basis, 14 articles were included in our analysis. Table 2 provides an overview of privacy and security incident that received media coverage.

<table>
<thead>
<tr>
<th>Health Service/event</th>
<th>State</th>
<th>Incident</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>UnitingCare facilities, including the Wesley and St Andrews War Memorial hospitals, and several aged care facilities</td>
<td>Queensland, (including Brisbane, and Sunshine Coast)</td>
<td>Cybersecurity</td>
<td>The Australian, BrisbaneTimes, CSO Online, Fraser Coast Chronicle, ABC News, The Courier Mail, Mail Online</td>
</tr>
<tr>
<td>Eastern Health, including Box Hill Hospital and Maroondah Hospital</td>
<td>Melbourne</td>
<td>Cybersecurity</td>
<td>The Australian, Yedioth Ahronoth</td>
</tr>
<tr>
<td>Not indicated (general), Use of personal devive by Physicians</td>
<td>Queensland</td>
<td>Privacy</td>
<td>Courier Mail</td>
</tr>
<tr>
<td>NSW Health, Accellion</td>
<td>New South Wales</td>
<td>Cybersecurity</td>
<td>The Australian Financial Review</td>
</tr>
<tr>
<td>Ambulance data breach</td>
<td>Tasmania</td>
<td>Privacy and cybersecurity</td>
<td>The Advocate, ABC News, The Examiner</td>
</tr>
</tbody>
</table>

Table 2. Overview of included news

To provide a contextual theorization of the dark side of health IS use, we followed the approach recommenced by Gioia et al. (2013). We, first, inductively advanced our data analysis without any theoretical lens. But as the themes emerged, we also transitioned from induction to abduction upon consulting the relevant literature (Alvesson and Kärreman 2007; Sætre and Van de Ven 2021). This consultation of IS use and theories (e.g., Burton-Jones et al. 2017a; Burton-Jones and Grange 2013; Burton-Jones and Volkoff 2017; Eden et al. 2018; Strong and Volkoff 2010) was helpful in our contextual theorization.

4 Findings

Guided by the Gioia et al. (2013) methodology, Table 3 illustrates the result of data analysis. The concepts were originated from the two sets of interview data and data protection incidents highlighted in our secondary data. We provided a data structure overview first, to provide a preview of the major findings. Our findings are structured around the two aggregated dimensions that emerged from the analysis (along with consultations with relevant IS use literature): data misfit and improper data processing. In our study, we refer to this dark side of usage patterns as 'health records misuse'.

<table>
<thead>
<tr>
<th>1st Order Concepts</th>
<th>2nd Order Themes</th>
<th>Aggregate dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unavailability of data entry system to authorized users (e.g., nurses)</td>
<td>Availability misfit</td>
<td>Data misfit</td>
</tr>
<tr>
<td>Bidirectional unavailability (order and result) in the laboratory system</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unavailability of medical notes to clinicians</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inaccessibility of digital systems and patient data as a result of cybersecurity incidents (e.g., ransomware)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A mismatch between the information (e.g., doctors' notes)</td>
<td>Meaning misfit</td>
<td></td>
</tr>
<tr>
<td>Different understanding of the sensitivity of data (e.g., HIV data)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Using an improper word or wrong language for describing patients  
Placing patient data in a different chart  
Putting the problems in the free text fields (instead of using the structured problem list)  
Not putting critical data in a specific section (e.g., allergy section)  
Seemingly-innocent interactions with health systems (i.e., trying to find out which ward his/her mother was)
Accessing data for unauthorized monitoring  
Widespread and seamless access to health data-creating potentials for unauthorized access  
Improper documentation of patient data (i.e., printing out a piece of paper to write on it)  
Using personal devices and tools (including third-party apps and email) for data recording and communications  
Using legacy information systems

<table>
<thead>
<tr>
<th>1st Order Concepts</th>
<th>2nd Order Themes</th>
<th>Aggregate dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improper interaction</td>
<td>Improper data processing</td>
<td></td>
</tr>
</tbody>
</table>

Table 3. Data Structure

4.1 Data misfit

The first dimension of health records misuse is data misfit. Data misfit refers to situations where health data is not accessible to an authorized person or data used in a way that triggers data quality issues (i.e., meaning misfit and place misfit). These issues can adversely influence the effective use of health IS, especially informed clinical action.

In the privacy literature, availability is among the key components of data security (Oetzel and Spiekermann 2014). In the healthcare context, availability misfit occurs when data is not available for health professionals and staff involved in health services (including admins) for the delivery of care to patients. A typical type of availability misfit, which is on the rise in the healthcare industry, is caused by cybersecurity incidents, especially ransomware attacks. This type of misfit can result in significant disruption to healthcare delivery. For example, as a result of ransomware in March 2021, Victoria’s Eastern Health experienced significant impacts, including shutting down critical health systems and postponement of some categories of surgery. Following is an example of availability misfit impact:

“[…] hospital staff treating him [a patient] were unable to access his medical history and, due to his complex needs, he was unable to verbally communicate to the doctor and nurses treating him that he had a history of diabetes and was experiencing extreme pain from a sore toe.” (Cunningham 2021)

We also identified another type of availability misfit that arises from the socio-technical aspects of use. This misfit moves from individual misuse to collective misuse, as explained by a clinical nurse.

“[…] they have their own records and system called [ABC: a pseudonym] and it’s a statewide data entry system, and they don’t generally write much on our [DEF] screen or in patients’ charts because they write everything on [ABC] and our nurses don’t have access to [ABC]. So it’s very difficult for our nurses to get the information off them when the communication is quite hostile sometimes. […] “What’s supposed to happen is when they finish a patient assessment they print off their [ABC] notes and give them to us so they’re available but not a lot of them do that, they seem to leave us out of the step.”

Meaning misfit and place misfit are associated with data quality issues. In the healthcare context, these types of failure-use can compromise the APPs 10 (quality of personal information). Even in some medical cases, these misfits influence patient safety, especially in emergency care and cases related to patients who suffer from allergies. For example, in emergency care knowing patient allergies is critical to clinical decisions. If a patient has a life-threatening penicillin allergy, it is critical that data is recorded accurately for informed medical action (Rochford 2021). The following quotes illustrate meaning misfit and place misfit respectively:

“There was a recent example where a medical record that I can say was reviewed because there had been a complaint that was obvious that the person was using a form of words that they shouldn’t have used for that particular person. It wasn’t derogatory or anything it just wasn’t relevant. I think they
inserted a template and it was the wrong language or wrong words just wrong probably from another record.” (an executive director)

“So if you’re taking a history, Johnny is allergic to penicillin has been for years blah, blah, blah and the doctor writes it as he’s writing his normal note like he used to in hard copy he does it in type and doesn’t stick it up in the allergy section.” (a medical director)

4.2 Improper data processing

The second dimension of health records misuse is improper data processing. Improper data processing occurs when the data-related actions (including logging, collection, use, and disclosure) and interactions with a health IS performed by users violate patients’ data privacy and goes against Australian privacy principles such as APP 6 (use or disclosure of personal information) and APP 11 (security of personal information). Two second-order themes of improper data processing that emerged from our data analysis were: ‘improper interaction’, and ‘improper data recording and use’.

In health services, widespread access to Health IS by individuals, without role-based access controls in place, can facilitate improper interaction. In this type of misuse, the social dimension may be more critical than the technical components. The following quotes demonstrate examples of improper interactions in health services.

“The other misuse I know that hospital health service can be very hot on is inappropriate access to records. I don’t know if you’ve heard that before but the tracking is just so easy now particularly if you have the same surname as the person. It can be whether you’re in [Hospital X] or elsewhere so there are people who potentially have accessed records for their children who might have been in another facility.” (a director of allied health)

“So my colleagues who had been senior nurses report all the time about ambulance and other emergency staff reading patient files. Wally during transfer. Because they’ve got nothing else to do. They just hanging around during the transfer.” (a privacy and digital health expert)

“There’s one today about a doctor who’s gone and looked, been seen in the ward looking at a record, said she was a registrar, had a lanyard on and claimed to be looking how a friend was getting on, possibly innocent, possibly not, but I’m trying to investigate that one. There’s going to be an awful lot of issues around that, just cybersecurity tag stuff.” (a deputy medical director)

The second misuse related to data processing is improper data recording and use. This pattern of improper use occurs when health professionals fail to properly document patient data (i.e., printing out a piece of paper to write on it) or using personal devices for recording and communicating health data. Such improper data recording and use by health professionals were expressed by several participants:

“I was looking at their daily lists and what they do, they still print out a piece of paper and write on it. We often find them on the floor and that’s a worry, because that’s patient information.” (a deputy medical director); “[…] there’s the same concerns would’ve existed with paper notes. They’re left around all the time. Patients don’t go looking in them. So, I think that’s a bit excessive, that sort of concern.” (a surgeon)

“Some GPs would use their personal Gmail account to request for photographs of people when they do telehealth. For example, nowadays in the COVID-19 era, you would see a lot of like something gp@gmail.com and then they ask the person to send. This means that somebody working in Google can also look at it, and if the email is not really secure along the way, you can actually do many text to look at all this information.” (a cybersecurity expert)

Similarly, at an organizational level, the use of outdated legacy systems that are vulnerable to cybersecurity incidents emerged as a serious component of health records misuse in our analysis. For example, a global cyber-attack on Accellion, a legacy file-sharing system, impacted organizations around the world including NSW Health (Roddan and Mason 2021).

5 Conclusion

Reflecting on the dark side of health IS use through qualitative analysis in Australian health services, we contextually theorized health records misuse. Our theorization provides explanations on two patterns of health IS use: data misfit and improper data processing. These two types of health records misuse are key challenges to effective use as they work against the very purpose for which the health services invest in the systems (Burton-Jones and Grange 2013; Burton-Jones and Volkoff 2017). We demonstrated a contextualization approach for studying the darks side of IS use in healthcare where data protection
failures are consequential for organization service delivery, clinical decision making, patient trust, and safety. By combining data from in-depth data collection in one health service as well as interviews with experts, and news reports from the health sector as a whole, we believe the contextualized theory has potentially wide relevance within the health sector. By highlighting key dimensions of health records misuse, the study offers insights for improving data governance and devising relevant data protection policies in the healthcare context, which should help health service executives and digital health policy makers. More generally, the study also demonstrates how the theory of effective use as a whole can be extended to examine dark-side concepts. This idea could be extended further in other sectors within and beyond health care.

6 References


**Copyright © 2021 Pool, Akhlaghpour & Burton-Jones. This is an open-access article licensed under a Creative Commons Attribution-NonCommercial 3.0 Australia License, which permits non-commercial use, distribution, and reproduction in any medium, provided the original author and ACIS are credited.**