Journal of Management Information Systems

ISSN: 0742-1222 (Print) 1557-928X (Online) Journal homepage: http://www.tandfonline.com/loi/mmis20

Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information

Chad Anderson, Richard L. Baskerville & Mala Kaul

To cite this article: Chad Anderson, Richard L. Baskerville & Mala Kaul (2017): Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information, Journal of Management Information Systems, DOI: 10.1080/07421222.2017.1394063

To link to this article: https://doi.org/10.1080/07421222.2017.1394063

Published online: 04 Dec 2017.

Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information

CHAD ANDERSON, RICHARD L. BASKERVILLE, AND MALA KAUL

Chad Anderson (andersonc16@nku.edu; corresponding author) is an assistant professor of business and health informatics at Northern Kentucky University. He received his Ph.D. in computer information systems from Georgia State University. His research focuses on the role of information systems in the delivery of health care, and his work has been published in *MIS Quarterly, Journal of the Association for Information Systems, Information and Organization, International Journal of Medical Informatics*, and others.

Richard L. Baskerville (baskerville@acm.org) is Regents' Professor and Board of Advisors Professor in the Department of Computer Information Systems, Robinson College of Business, Georgia State University and professor (partial appointment) in the School of Information Systems at Curtin University, Perth, Australia. A chartered engineer, he holds a Ph.D. in systems analysis from the University of London, and doctorates honoris causa from the University of Pretoria and Roskilde University. His research specializes in security of information systems, methods of information systems design and development, and the interaction of information systems and organizations. He is the author of *Designing Information Systems Security* (Wiley) and more than 300 articles in scholarly journals, professional magazines, and edited books. He serves on the editorial boards of several journals.

Mala Kaul (mkaul@unr.edu) is an assistant professor of information systems in the College of Business at the University of Nevada, Reno. She received her Ph.D. from the Robinson College of Business at Georgia State University. Her research focuses on information systems design, cyber security and privacy, and health information technology. She has extensive industry experience as an information systems professional. Her work has been published in *MIS Quarterly, Harvard Business Review, Journal of Database Management*, and other journals.

Abstract: Contemporary organizations operate in highly interconnected environments where they are frequently confronted by the challenge of balancing the protection of information resources with the need for sharing information. This tension between the expected benefits and the potential security risks inherent in the information sharing process, exists in many domains, including business, health care, law enforcement, and military—yet it is not well-understood. We propose an information security control theory to explain and manage this tension. We evaluate this theory through a longitudinal case study of the iterative development of the

Journal of Management Information Systems / 2017, Vol. 34, No. 4, pp. 1082–1112.

ISSN 0742–1222 (print) / ISSN 1557–928X (online)
DOI: https://doi.org/10.1080/07421222.2017.1394063

information security policies for a health information exchange in the western United States. Our study shows that the theory offers a good framework through which to understand the information security policy development process, and a way to reconcile the tension between information sharing and information protection. The theory has practical applicability to many business domains.

KEY WORDS AND PHRASES: ethical control, health care, health information exchange, information security, security control theory, security exposure control, security policy development.

Two opposing phenomena create an essential tension in information systems: the need to share information and the need to protect information. Technological advances have improved the ability to share and exchange information more efficiently while also increasing the burden of securing this information. The ability to share information between organizations is a broad, worldwide challenge today. In the public arena, government-to-government data sharing includes information about economic development, education, geography, health care, and law enforcement [20], while in the private arena, organizational data sharing includes the exchange of information between organizations, suppliers, and customers [45]. Traditional roadblocks to information sharing have included incompatibility of different systems and both organizational and legal authority to share information [14]. Such legal controls included the boundaries of Freedom of Information laws, privacy protection, trade secrets, and separation of powers between government agencies [69]. Incongruity in commercial objectives has also limited past information sharing (information integration) among firms [65].

However, the technical, organizational, and political benefits of shared information are growing; in fact, information sharing has become the new goal, enabled by technological advances that make information exchange easier [73]. Information sharing is also being driven by policy changes to promote efficiency and reduce waste so that the main challenge to information sharing has shifted to protecting information through cyber security [36]. Ironically, one of the most prominent areas feverishly demanding better information sharing is cyber security itself [62].

In this article, we focus on information sharing in health care because of the growth in the generation and sharing of extremely sensitive health data and the ethical and legal liability to protect the privacy of health information. The digital transformation of health care is expected to improve care quality and reduce the costs of providing quality care [8]. An important element of that process is interoperability (i.e., the ability of healthcare organizations to digitally exchange information). The National Coordinator for Health Information Technology (HIT) asserts that, "interoperability is necessary for a 'learning health system' in which health information flows seamlessly and is available to the right people, at the right place, at the right time" [52, p. iv]. The value of interoperability has been recognized for some time with the development of community health

management information systems (CHMISs) in the early to mid-1990s, community health information networks (CHINs) in the mid- to late 1990s, and regional health information organizations (RHIOs) in the 2000s [67]. More recently, the 2009 HITECH Act included nearly $550 million in federal funding for the development of health information exchanges (HIEs) in every state and U.S. territory. However, the limited success of these initiatives demonstrates that interoperability remains a challenge in the interorganizational knowledge exchange of health information [46], and that the route to effective and sustained interoperability is multifaceted and insufficiently understood [17].

While integration of information systems is crucial for improving clinical, operational, and managerial outcomes in health care, security and privacy concerns have been a significant barrier to adoption [41]. One of the main challenges for interoperability is maintaining the security and privacy of the protected health information that is transmitted [17, 74]. According to the Identity Theft Resource Center, in 2015, the health-care sector experienced more than one-third of all publicly reported data breaches [32]. Health-care data are attractive targets for cybercriminals since the data contain not only sensitive personal information but also financial information. Additionally, if credit card data are breached, credit cards can be canceled; unlike credit card numbers, medical data are less perishable and therefore more valuable. In 2016 alone, there were 325 large-scale breaches of health information, which compromised over 16 million patient records [55]. According to a recent report, one in every four U.S. consumers have had health-care data breached [1]. Since the risk of patient data disclosure is considered high, the medical industry is subject to stricter laws to protect patient information confidentiality [59]. Security breaches can have serious consequences, not only for patients, through identity theft or disclosure of private health records, but also for the health-care organizations that stand to be impacted financially, through loss of reputation, trust, and potential legal and regulatory consequences.

If we were to compare the cost of a health information breach with other data breaches, the average cost of a data breach is $4 million at $158 lost per record; the average cost of a health information breach of just 10,000 records is $7 million [54] and numerous providers have paid many times more. For example, the 2015 Anthem breach was settled at $115 million [4]. Hospitals, such as Hollywood Presbyterian and Kansas Heart proved highly vulnerable to a 2016 spate of ransomware attacks. In at least one case where a ransom was paid, the attackers only partly restored hospital data, demanding further ransom [61]. A recent review of security in health care found that the health-care industry is a major target for information theft because it lags well behind other industries in securing vital data [42]. Threats to the security of health information are expected to remain high because of the value of medical records on the black market [19]. This underscores the high stakes at play in the health-care context and the imperative need for protecting health information. Therefore, a tension exists between the expected value of facilitating interoperability and the potential threat of security breaches,

since the information exchange process could expose patients and providers to significant harm.

Security controls must be sufficient to protect data, but not restrictive to the point that they impede interoperability. Creating and sustaining an effective security program is essential to the achievement of the goal of balancing security and interoperability. A good security program starts with the development of an information security policy [15, 70]. Information security policies have been richly discussed in the literature. There are studies that focus on security policy development [22, 25, 37], implementation [39, 53], and effectiveness [23, 26, 29, 34]. However, none have focused on the impact that the aforementioned tension plays in the policy development process. Therefore, an important research question for understanding and explaining what enables effective information exchange is: *how is the development of information security policies implicated in balancing the essential tension between sharing and protecting information?*

This research answers that question by proposing a theoretical framework that provides a mechanism for balancing the tension between sharing and protecting information. We evaluate the framework by investigating how an HIE in the western United States addressed the tension between protecting and sharing health information in the development of its information security policies. We investigate the HIE's iterative policy development process through the theoretical lens of security controls reasoning and find that the framework is helpful in understanding and developing information security policies to support the HIE's goal of interoperability, while maintaining the privacy and security of the information managed by the exchange.

Theoretical Background

Fundamental goals for information security include the confidentiality, availability, and integrity of data and the development of controls to support those goals [3, 21]. However, much of the published research on information security is limited in its consideration of the theoretical foundations that underpin it, and where it does consider these, it typically makes use of theories that are applicable to a very limited range of the information security spectrum [60]. For example, economic theories (i.e., return on investment, internal rate of return, etc.) have been used to explain the financial value of controls and how that valuation is used to prioritize the decisions to implement those controls [24]; while general deterrence theory (GDT) has been used to explain human behavior and the design of controls to combat computer crime and intentional abuse [64]. Global theories that could broadly explain a wide range of phenomena in information security are lacking, either because they are not highly valued, or because information security scholars have tended to focus on very specific phenomena in their research. In addition, there is a general disconnect between information security research that engages in security theory development and empirical information security studies [60]. This research aims to address these

gaps in the literature by proposing a theoretical framework specific to information security, yet one that is broadly applicable to a variety of security phenomena, and then assessing that framework through an empirical investigation thus addressing both rigor and relevance.

The essential tension identified in our study suggests forms of reasoning that are neither financial nor deterrent. Rather, it is a *tension between sharing and protecting data*. Sharing involves reasoning with an aim to expose sensitive data to *outsiders* (i.e., other individuals or organizations). On the other hand, protecting data is reasoning with an aim to seclude the data. Decision settings where there may be multiple, conflicting aims and multiple forms of reasoning have been noted in prior literature in decision analysis [40], health care [27], education [57], and so on. The purpose of this research is not to replicate prior research in multi-objective decision analysis, but to explore the two essential, conflicting objectives in the context of information sharing and information security. This is important because these conflicting objectives are unique to information security, especially in health-care settings, where sharing of information can provide enormous benefits, while also creating the burden of information protection.

This research proposes that these conflicting objectives incorporate two interrelated forms of security reasoning: exposure control reasoning and ethical control reasoning. The theory is based on the premise that the decision to enact controls to protect information systems is a fundamental and meaningful outcome of setting information security policies. Therefore, the decision to adopt an information security policy is an effective place to begin a search for explanations of otherwise unexplained information security behaviors. Exposure and ethics are chosen as the two anchors of controls policy reasoning because both concepts are prevalent and persistent in the information security literature [13, 47]. These two forms of control reasoning are often treated separately, although in most settings they combine to explain how decision makers decide between which controls to set into policy and which ones to forgo because the controls are too difficult or expensive to acquire or operate.

Exposure Control Reasoning

Exposure control reasoning is based on the fact that information assets (e.g., end-user devices, servers, networks, etc.) are inherently exposed to threats (e.g., human error, hackers, fires, etc.) Threat exposure includes threats of any potential exposure, disclosure, breach of confidentiality, or any form of risk exposures that may arise from inadvertent disclosure [33], external threat sources, or insider threats. Exposure control reasoning aims to manage those risk exposures [10, 58] through the identification and placement of controls between assets and threats. However, this process is complex and challenging because assets and threats may be linked to each other in a multitude of ways. For example, computer viruses are threats not only to desktop computing assets, but to computer-controlled

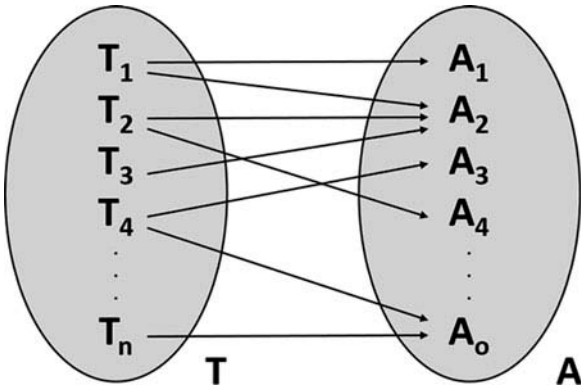

Figure 1. Threat-Asset Exposure Edges (Adapted from Hoffman et al. [28])

assets such as scanners, photocopiers, and so forth. Desktop computing assets are threatened not only by viruses but also by physical theft and network-based access penetration. Consequently, the addition of security requirements and controls into an information system can be expected to increase the cost and complexity of the system and its operation. This is why information security researchers and practitioners must focus on both, the analysis of assets, and the analysis of threats. Therefore, exposure control reasoning is an important component of many formalized approaches to information security.

One form of exposure control reasoning is represented in Figure 1. This figure represents an insecure system with the set of an organization's information assets (A) in relation to a set of information threats (T). The arrows represent edges between the members of each set. In this case, the edges (T-A) are exposures [28].

Exposure control reasoning aims to control such exposures by creating a set of controls (C) that protect organizational assets from security exposures. Each control is inserted to eliminate the edges between threats and assets. The aim is to replace each T-A edge with a T-C edge and a C-A edge (see Figure 2).

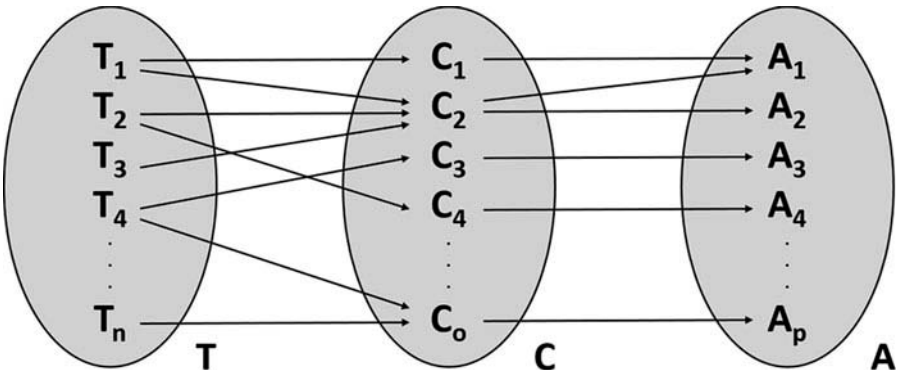

Figure 2. Threat-Control-Asset Edges (Adapted from Hoffman et al. [28])

Ethical Control Reasoning

Ethical reasoning is an area in psychology and management studies that deals with the process of determining the difference between right and wrong. It is related to information systems ethics, in our case, because decisions about adopting security and privacy controls are often made as a rational process of deciding what is the "right" thing to do: to invest in controls or risk the compromise [72].

Ethical control reasoning arises in the need to make rational decisions about the adoption of controls. These decisions rely on ethical reasoning because sometimes controls are unavailable or too costly in relationship to the likelihood of threats and the value of assets, or may even have perverse or unintended effects on the defense of systems [71]. Ethical control reasoning can take a number of forms, but the most common are utilitarian and deontological reasoning. Utilitarian reasoning focuses on achieving the greatest good and relies on risk analysis to determine the degree of hazard to important stakeholders [12]. Virtually all security design methodologies adopt some form of risk analysis as a central activity for determining whether a control is justified. Alternatively, deontological reasoning focuses on the moral duty of adherence to rules, and is used as the basis for compliance with laws and regulations [12]. For example, HIE privacy and security controls are currently governed by the 2013 HIPAA Final Rule.

One prevalent form of ethical control reasoning is the typical risk treatment framework, for example, Jones and Ashenden [35]. Such frameworks map risk treatments (controls) into categories suitable for different values of threat frequency and threat impact (see Figure 3). High frequency, low impact threats are given

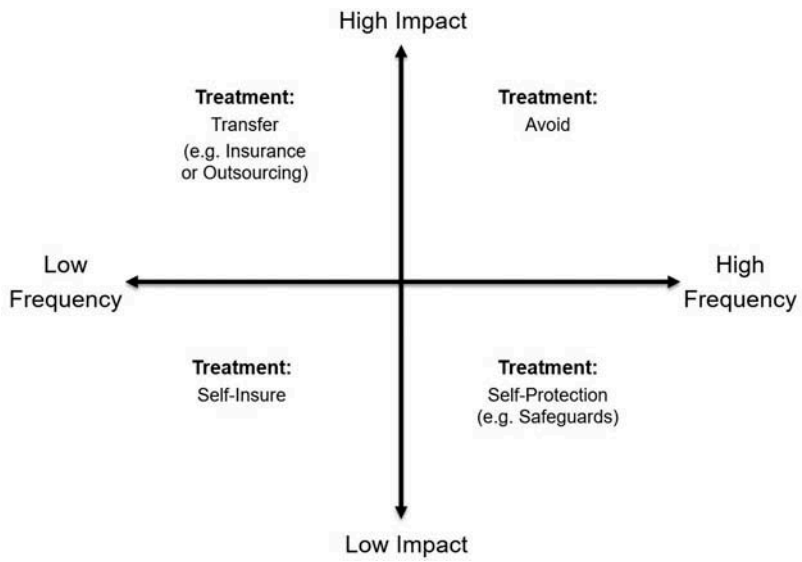

Figure 3. Risk Treatment Framework (Adapted from Jones and Ashenden [35])

different treatments than low frequency, high impact threats, and so on. Such treatment decisions are essentially a form of utilitarian ethical reasoning. Control treatments are enacted where they do the greatest good, and not where they do little good. For example, the risk of vandalism by an external hacker is a form of risk that can be relatively high in frequency, but relatively low in impact. The implementation of common self-protection mechanisms such as firewalls and VPN access for external users is an effective response to that threat, whereas cutting off all access from outside the organization will have little additional benefit, while significantly impeding legitimate work. The goal is not to eliminate risk, but rather to shift it down and to the left within the framework without enacting controls that are more impediment than benefit.

Formulating Policies

Exposure control reasoning and ethical control reasoning interact with each other in the formulation of information security policies. The creation of information security policies is a fundamental action in information security as it provides the basis for an organization's approach to information security. It is also the foundational document by which procedures and controls are selected and implemented [6, 16]. Therefore, the application of both exposure and ethical control reasoning in the development of an information security policy is essential to create a policy that enables both the sharing and protection of information. Both forms of reasoning span consideration for the assets and threats for which security controls must be implemented, the needs of relevant stakeholders, and the requirements of requisite laws and regulations.

Research has considered the role [30], importance [68], structure [6], and content [16] of the information security policy, as well as the relationship between information security and compliance [43]. However, none have directly addressed the essential tension between the need to both share and protect information that is fundamental to organizations like an HIE. Our theoretical model addresses that tension and we apply the model to an HIE to understand how the tension is managed through the information security policy development process in such an organization.

The Essential Tension

In formulating and applying security policies for an HIE, the policy developers have to balance the requirements of ensuring interoperability and availability of information to authorized parties, while at the same time ensuring confidentiality, integrity, and overall security. Policy makers can adopt exposure control reasoning for controlling the threat of any kind of malicious or accidental exposure of information that may result in a security breach, including breach of confidentiality. Similarly, they can use ethical control reasoning to

rationalize decisions on the appropriate level of controls. However, these two forms of reasoning must be balanced to both enable the sharing of information and protecting that information. Thus, exposure and ethical control reasoning, correspond to the tension between the aims of "sharing" and "protection" in creating an HIE security policy. *Exposure control reasoning* aims to develop complete security and privacy, creating a path to ensure that we *protect everything*. It offers a mathematical frame that is verifiably complete and secure. *Ethical control reasoning*, in contrast, aims to make rational decisions about *what not to protect*. It assumes that a fully protected system is expensive and morally unreasonable. It accepts that there are trade-offs in security, such as the trade-off between complete security and complete interoperability. It guides the reasoning across a threshold where some exposures are acceptable. The occurrence of these risks is acceptable because such events can be insured, or they are inexpensive, or they are avoidable in operation, or safeguards are sufficiently effective.

Our identification of this theoretical tension is not intended as a normative substitute for existing theories and methods of multicriteria decision making. Rather, this tension helps explicate the knowledge and preferences of the decision maker [31] that is a necessary input to multicriteria decisions. It offers a clear frame for illuminating the contradictory inputs to the decision process. Normatively, multicriteria decision theories, such as multiple attribute utility theory [7, 40] or the analytical hierarchy process, can then be employed for the decision-making process itself [56].

Case Study

A qualitative case study was conducted to evaluate an HIE's information security policy development. The HIE in this study, henceforth to be known as WesternHIE, is located in the western United States and includes participating health-care organizations across the entire state in which it operates. The HIE was initially formed in 2011 and continues to operate successfully with 129 health-care organizations currently participating in the exchange, representing a sizable portion of the state's health-care community.

Method

This was a longitudinal study that began as an exploration of the role that security policy development plays in the success of an HIE. Therefore, a qualitative research approach was employed because it provided the flexibility necessary to pursue emergent avenues of inquiry as data collection progressed [48, 49]. Following the first round of data collection, our analysis identified the tension between sharing and protecting health information and a pattern of shifting focus in policy development related to that tension. We conducted a second round of data collection almost two

years after the first, in order to confirm the patterns identified in our initial analysis. We based our research process on Eisenhardt's guidelines for building theory through case study research [18].

Arrangements for data collection were coordinated through the HIE's executive director, who was known to the first author. Pursuant to the goals of the study, the executive director arranged meetings or provided contact information for everyone still with the organization, or still available for contact, who had participated or was participating in the HIE's information security policy development process. Within that scope of access, semi-structured interviews were conducted, either in person or over the phone, with HIE staff members and one external consultant.

In qualitative research, semi-structured interviews help guide the participants in sharing their accounts of events and processes that are relevant to the research focus, while enabling the researcher to follow new lines of inquiry as the incoming data suggests. Therefore, while the initial questions (see Appendixes A and B) were structured to the extent that they focused the conversation on the security policy development process, subsequent questions were adapted to pursue emerging ideas both within specific interviews and in subsequent interviews [48].

Interviews were conducted in two phases. The first phase took place in early 2015 and included interviews with six staff members and an external consultant. The second phase took place at the end of 2016 where five staff members were interviewed, only two of whom had been interviewed in the first phase, the executive director and the project coordinator who had been an HIT intern in 2015 (see Table 1). All interviews were audio-recorded with the exception of one, in which the participant asked not to be recorded. For that interview, the researchers made handwritten notes, as was also done for all recorded interviews. In addition to the interviews, documentation was collected and analyzed, including the different versions of the security policies, policy development timelines, and the document deliverables at each stage of the policy development process.

Analysis of the data started immediately after the initial interview and continued throughout the data collection processes in both phases. Interview

Table 1. Study Participants

Phase 1 participants	Phase 2 participants
Executive director	Executive director
HIT director	HIE director
Outreach director	Assistant HIE director
QIO information security officer	New QIO information security officer
Support specialist	Project coordinator
HIT intern	
External consultant	

transcripts and document data were analyzed by all the authors in an iterative process of data reduction and conclusion drawing [49] with the initial goal of identifying elements of the information security development process that explained how the HIE had been successful in developing and growing the exchange. Each author would analyze the available data individually looking for themes and then the group would come together to discuss those themes, iterating the process until we collectively identified the tension between sharing and protecting data that the HIE was addressing through controls reasoning that shaped the development, implementation, and revision of their information security policies. The second round of data collection served as an evaluation of the security controls framework and a confirmation that the controls reasoning we were seeing in the first phase of interviews continued to hold over time. The following account details the iterative process that WesternHIE took with the development and revisions of its information security policies.

HIE Security Policy Development

WesternHIE has gone through four distinct iterations of information security policy development since the organization was created in 2011. Two of those iterations had already occurred and the third was in process at the time of the first round of interviews in early 2015. The fourth iteration was in process at the time of the second round of interviews in late 2016 (see Figure 4).

Before delving into the details of the case study, we preface those details with a summary of our findings (see Table 2 and Figure 5). Table 2 provides an overview of the four iterations of policy development in the case, with quotes that exemplify the emphasis on exposure control and ethical control reasoning that occurred in each iteration.

Figure 5 illustrates that the tension between sharing and protecting information was always present, but that the emphasis on exposure and ethical controls reasoning shifted through the iterations.

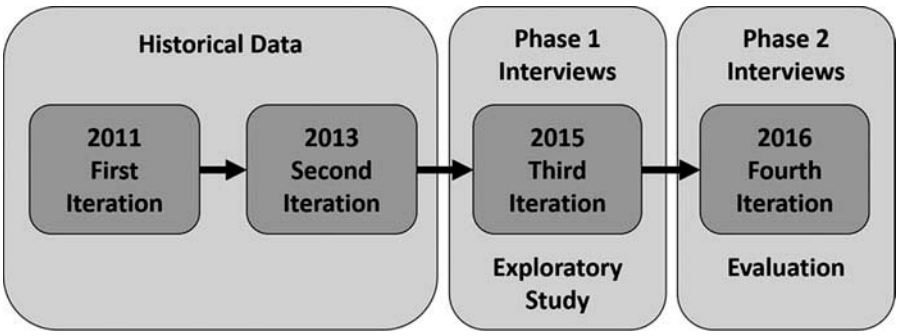

Figure 4. Timeline of Information Security Policy Development Iterations and Study Phases

Table 2. Summary of Study Findings

Iteration	Exposure control	Ethical control
1st	Bringing together community members to identify threats.	Focusing on compliance with HIPAA and state law to establish policies.
	We're taking down what you the community member think. (Executive director)	*What I always go back to is, what is the Rule? What is the Privacy Rule? What is the Security Rule? (External Consultant)*
2nd	Expanding policies to account for more threats.	Focusing on NIST guidelines to evaluate current policies.
	Someone could hack into [WesternHIE] and use it as a backdoor into the QIO. (QIO ISO)	*I assessed [WesternHIE's] security posture based on NIST standards. (QIO ISO)*
3rd	Implementing a policy template for more effective policy articulation.	Reducing policies to ease the burden on participants to comply.
	The first step was developing a standard template, because there was lots of variation [in how the policies were written]. (Support specialist)	*We look for feedback [on the policies]. Is there anything we overlooked or that would be a concern to them as participants? (Policy intern)*
4th	Implementing an LMS to enable more control over policy training and compliance.	Further reducing policies to ease burden on HIE staff to audit policy compliance.
	Now we have a way of enforcing it, because we don't give access [to the HIE] until they complete these particular training courses. (Assistant HIE director)	*We're going through these motions having to monitor this and it's not even a functionality that we support. (HIE director)*

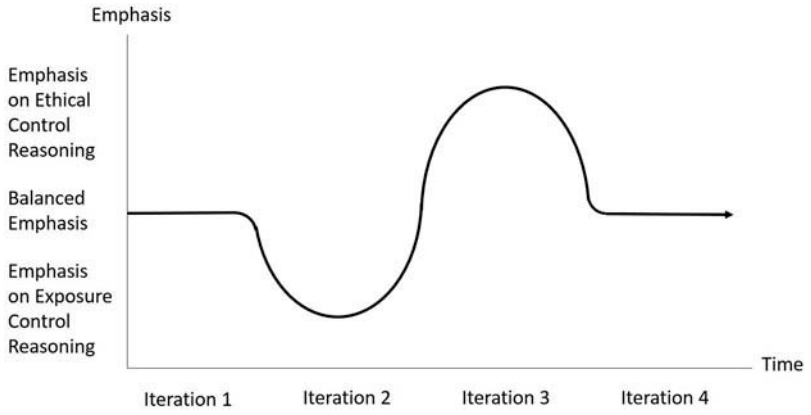

Figure 5. Shifting Emphasis on Forms of Reasoning Across the Iterations

First Iteration

WesternHIE was created by the state's Quality Improvement Organization (QIO). The QIO had been approached by several individuals from the state's health-care community to take the lead in setting up an HIE for the state. They agreed, but quickly decided to spin off the HIE both to avoid a conflict of interest and to generate buy-in from the community because it required them to ask the community for board members for the HIE. "What better way to get buy-in than to reach out to our community and say, look, we need board members. You're going to help shape and move technology within the state" (HIT director).

The WesternHIE board contracts with the QIO to operationalize the exchange that includes a management contract, which means that WesternHIE has no employees; they are instead employees of the QIO. One result of this arrangement is that WesternHIE does not have a dedicated information security officer (ISO), but instead makes use of the QIO's ISO as necessary. This had implications for the information security policy development process at WesternHIE.

WesternHIE's HIT director said that most HIEs would set up their governance structure first, and then select a vendor to provide the hardware and software for the exchange.

> Most HIEs would establish their governance structure and organizational structure and then go through a vendor selection. . . . We did not do that. We made a conscious decision to run two parallel paths. One is governance and how do we set up the infrastructure. The second was . . . we wanted to put the vendor in place and start getting out to show physicians that this could actually work. (HIT director)

This created a crossover in WesternHIE's startup processes because they needed certain things in place to operationalize the HIE (e.g., privacy and security policies). Therefore, in the summer of 2011, eight task forces were established by the WesternHIE board of directors to develop a plan for the major components of the HIE (e.g., Privacy and Security and Data Use Agreement Task Force, Financial Sustainability Task Force, Governance and Outreach Task Force, etc.).

The task-force development process was co-facilitated by the WesternHIE executive director, and an external consultant who served as the expert on HHS Federal Policy. The task forces comprised WesternHIE staff as well as members of the community (e.g., the privacy and security task force comprised 13 members that included a hospital privacy officer who was also an attorney, the director of health information management at another hospital, the general counsel for a third hospital, a state Medicaid administrator, the corporate compliance manager for a large physician's group, etc.). The diversity of participants was both a benefit and a challenge because, while multiple perspectives produced a greater range of ideas, each participant also had to consider others' perspectives and think more broadly [9, 11].

The task forces met once in July 2011 and twice in August 2011 to discuss their area of focus and develop a recommendation for how WesternHIE should proceed.

The privacy and security policy recommendations were driven by the HIPAA Privacy Rule, Security Rule, and Breach and Notification Rule. There were 42 HIPAA standards that needed to be examined and addressed in the developed policies. For example, the preamble to the HIPAA Final Rule specifically defines an HIE as a Business Associate of a Covered Entity. Therefore, the policies had to be developed keeping that structure in mind. "What I always go back to is, what is the Rule? What is the Privacy Rule? What is the Security Rule? … and we mapped standard by standard" (External consultant).

There were also state laws regarding security and privacy that the HIE would have to follow, but those laws were not clear and well-developed at the time the HIE was being set up. "We had bad statutes and zero regulations on any statutes" (HIE director).

> There was one interpretation of the statute that existed at the time that if you took the literal language and tried to apply it you would have shut down electronic exchange of any health data in the state. . . . Everything would have had to revert to paper if you had taken it with that interpretation and there were folks who looked at it that way and refused to participate in the HIE until that got resolved. That, I think, was the one thing that stood out as the biggest challenge for us in the early days. (HIE director)

In this early stage of the HIE, the tension between protecting and sharing data was evident. One of the goals was to get the technology up and running, to quickly generate buy-in from physicians that an exchange could work. At the same time, the privacy and security task force recognized the need to create security policies based on HIPAA regulations and state laws to protect the data that would be exchanged. Both exposure and ethical control reasoning were employed in the parallel paths of setting up the governance structure for the HIE and getting the exchange running as a proof of concept for providers.

However, the consultant worried that the ethical reasoning over-excluded both utilitarian reasoning and exposure reasoning. In other words, the aim to seclude data was unnecessarily eclipsing the (more strategic) aim to expose or share data. For example, she noted that with regard to HIPAA compliance by HIE participants,

> Many of the hospitals in particular may have developed policies that are more strict than HIPAA … and that can often become a problem because the point of the HIE is to share the information and share the data in a secure way, but also you don't want to put up roadblocks to having providers and others being able to access information when they need it. (External consultant)

She was not only conditioning the ethical reasoning, that is, filtering a dominant deontological reasoning with a utilitarian lens. She was also reasoning about acceptable levels of exposure. For example, there was a recognition that all participants in an HIE together comprised a collective "weak-link phenomenon." When one participant suffers a data breach, all participants would suffer [51].

> I initially put together several examples of data use agreements, because, especially in an HIE, it's very important to have an agreement that goes beyond a business associate agreement so the HIE has clear written relationships with their providers that are part of the HIE [so] each of those providers is meeting their obligations to the HIE. (External consultant)

Each task force generated a report for its focus area. These were provided to the external consultant in September 2011, for aggregation into a full report to the WesternHIE board of directors. The final report generated by the external consultant was completed and submitted to the board in October 2011, and represented a roadmap for how to proceed in building out the HIE. WesternHIE then took that roadmap and began developing the organizational structures to achieve the goals of the roadmap. For privacy and security, that meant constructing the actual policies and procedures.

There was a defined end-date for the initial task forces, but WesternHIE subsequently set up two new task forces, one for patient consent, which has since been twilighted, and policies were written out of it, and one for compliance and audit, which is an ongoing group. The compliance and audit group is an advisory group set up by the board to make sure WesternHIE is doing audits appropriately and to provide advice on what to do in regard to actionable items. The compliance and audit group is the only community group still in place, but WesternHIE also has an internal policy committee that meets a couple of times each month.

The initial set of privacy and security policies were written by WesternHIE staff based on the roadmap constructed by the Privacy and Security and Data Use Agreement Task Force. At this point, the reasoning shifted from predominantly one of seclusion, which was deontological in nature, to a more utilitarian focus. The HIT director noted that writing a policy is easy, but getting staff buy-in is difficult. "Inevitably you get the GM nod from a lot of staff and then they go back to doing what they have typically done in the past. . . . How do you take a policy and make it part of the culture?" (HIT director).

Certain policies also had a more utilitarian focus with regard to the participant's needs because the participants would be most impacted by those particular policies. The consent policy was one in which the participants would be responsible for gaining consent from patients and therefore the policy development process took more input from participants.

> We met once a month for six months to bring the community back together to say, okay, you're going to be the ones getting the consents. Where would this fit in the doctor's office? How would you go about this? What would the flow be? Developing the policy for that, developing the form, developing the fact sheet that you give to somebody. (Executive director)

At this point, the information security officer, because of the relationship noted earlier, had not been directly involved in the development of the information security policies for WesternHIE.

Second Iteration

In 2013 WesternHIE decided it needed some expert help to evaluate its existing policies and the information security officer (ISO) offered to take charge of that process, which kicked off on September 9, 2013. "We needed more [policies], we needed to make sure what we had was correct … we wanted some confirmation, some validation about what we had done because he's the expert" (Executive director).

In addition to the ISO, two other WesternHIE staff members were on the core evaluation team along with a four-member project steering committee that included the ISO. The ISO's plan was to assess WesternHIE's security posture using National Institute of Standards and Technology (NIST) guidelines [63] for the evaluation, but he also looked to outside sources to see what other HIEs around the country were doing. He felt the evaluation process at WesternHIE was not as well-defined and structured as he had experienced in other contexts and that the participants were often distracted with other tasks and did not put enough importance on the evaluation process. He also felt there was a limited awareness by the staff on how to carry out the process, so he had to spend time educating the other participants on how to properly conduct the evaluation.

There is a growing presence of exposure control reasoning as the need for evaluation rises. There is also an introduction of NIST guidelines as a driver of deontological reasoning to balance the early focus on HIPAA rules. Concerns that reflect exposure control reasoning include worries that someone could hack a partner organization in the HIE and use it as a backdoor to compromise other partners. To overcome this risk exposure, all partners will need to be strong, and their relationships need to be good enough to maintain a high level of security for the HIE.

The evaluation included a gap assessment where HIPAA-required best practice privacy and security policies were compared with WesternHIE's existing policies. For example, the policy on permitted use and disclosure existed, but it was considered "thin" and therefore the team concluded that it should be updated to reflect the HIPAA Final Rule of 2013, while the policy on receiving and resolving complaints and or concerns did not exist, and therefore the team concluded that a policy and procedures should be developed using the best practice example. The evaluation process lasted four weeks and was completed on October 3, 2013, which then led to a period of policy writing and revising.

Third Iteration

In late 2014, another round of policy evaluation took place, but this time the ISO was not involved in the process and it was primarily carried out by a new set of staff members who were not involved in the 2013 evaluation. "Here's an area where we could use some extra eyes and ears. We need to update, we need to review these [privacy and security policies]" (Executive director).

At that point, WesternHIE had 60+ privacy and security policies, many of which had been added as a result of the 2013 evaluation. The evaluation team started by prioritizing the policies and removing those that were specific to certain procedures, which helped to reduce the scope of their work. They also found that many were written from the perspective of a covered entity. The HIE is not a covered entity, but is instead a business associate of participating covered entities. Therefore, policies that focused on the HIE as a covered entity could also be eliminated. Finally, because of their relationship to the QIO, they found that many of the policies were part of the QIO's policies that WesternHIE could use indirectly. Therefore, the ISO had indirect involvement in the process because he had authored many of the QIO policies that were used in whole or in part by WesternHIE. In addition, they found significant variation in how the policies were structured, so they developed a standard template with clear instructions and examples for future policy writers. The template was based on the experience that some of the team members had with policy writing in other organizations.

The decision to develop and implement a policy template reflected ethical control reasoning with a utilitarian focus because the goal was not to reanalyze the policies from the perspective of threats and assets but to make the policies easier to read and use by participants. Policy drafting started with the assignment of a policy owner who could be the person who had identified the need, or another person in that functional area. The owner of a policy was responsible for writing the policy and the template made that responsibility much less daunting. The revised policies were then sent out to the HIE participants for review. Participants had 45 days to review the policy and submit questions. "We do send these policies out after they are approved [by the compliance and audit committee]. We look for feedback, is there anything we overlooked or that would be a concern to them as participants?" (Policy intern).

This also reflects a focus on ethical control reasoning with a utilitarian goal of understanding the needs of participants and incorporating those needs, as appropriate, into the policies. They originally anticipated that the process would take two to three months but it ended up taking a year to complete. In the end, the policies were reduced from 60+ to 14.

Through this process of developing, implementing, and revising the HIE's information security policies the list of participant organizations continued to grow and by early 2015 included as active members of the HIE: 62 physician offices, 9 acute care hospitals, 7 diagnostic services, and 1 health plan. With that many participants, each of which is ultimately responsible for the health information they share through the exchange, agreement and compliance with the HIE's information security policies has not been homogeneous, but the HIE contended that the general perception and engagement with the process and the resulting policies have been very positive from the perspective of active participants and the community at large.

Fourth Iteration

In 2016, WesternHIE again initiated an evaluation of their information security policies. The QIO also replaced its information security officer in early 2016 and the new ISO participated in this latest iteration of revisions. In this iteration, the focus for policy development was to further clean and refine the existing policies. The thought was that, while the policies had been significantly revised in the previous iteration, they still retained significant verbiage from the second iteration that could be a problem for the organization. "The verboseness of the security policies, in my estimation, exposed the organization to unintended consequences" (New ISO).

Specifically, the new ISO felt that the existing policies contained details that should be reserved for procedures. He explained that the policies should be more general in their wording because any litigation would focus on what the policies say and the policies are what regulators would look at when auditing the organization. "It took us about six months to wade through the policies, to weed out all of the extraneous words, and to make it very concise and reflective of what we did" (New ISO).

The views of the new ISO reflect a focus on exposure control reasoning, but in the opposite way that the first ISO had been focused on exposure control. The first ISO had worried that the organization faced exposures from policies that were not sufficiently comprehensive, while the new ISO worried that the verboseness of the existing policies would expose the organization to litigation and audit penalties because they would not able to follow everything included in those policies.

The level of detail in the policies was also adversely impacting the operationalization of the HIE, because those details were requiring unnecessary work that drew resources away from other parts of the exchange. For example, the audit and compliance policy contained requirements to perform audits on elements of the HIE that were not being used.

> Our audit and compliance policy spelled out this list; you have to audit all of these things, and some of them simply weren't relevant. It doesn't apply, nobody does it, we're going through these motions having to monitor this and it's not even a functionality that we support. Why are we explicitly having to monitor and report on this month after month and quarter after quarter when it's never going to change? (HIE director)

In addition to reducing unnecessary work, streamlining the policies enabled the HIE to take a more flexible approach to accomplishing their goals with regard to security and privacy.

> As we've started changing that model it gives us greater flexibility. Here's the goal, here's what we're trying to mitigate, here's what we're trying to monitor for, here's what we're trying to accomplish. And then we have the flexibility at that point to deploy a greater range of tools or skills sets amongst the team to accomplish that. (HIT director)

Those views reflect an ethical controls reasoning with a focus on utilitarian reasoning where the goal was to reduce the resource requirements for complying with the written policies and to enable greater flexibility in achieving the goals of privacy and security that were critical to the success of the HIE.

In 2016, the HIE had also decided to implement a learning management system (LMS) to better document and control the training that was required by all participant users. Prior to 2016, the HIE privacy and security policies were given to each participating organization as a paper or digital document and the organization was asked to have each of its users read through the policies and acknowledge their understanding of those policies as part of their HIE training. The organization would inform WesternHIE when its users had completed the privacy and security policy training and WesternHIE would then grant access to the HIE for all those users.

Because of that structure, WesternHIE could not confirm that each individual user had read and sufficiently understood the policies, and they felt it would benefit the security of the HIE if they could do so. The LMS became the way to enable that ability because the training had to be completed by each user in the organization through individual account-based access, which meant that WesternHIE could enforce individual compliance with the training requirement. Specifically, WesternHIE would send each user his or her individual HIE access credentials, but those credentials would not be provided until the user had completed the required training modules in the LMS, at which point the system would send the user's unique HIE credentials. "I think it will improve the end-users' understanding of the HIE's policies, the HIE's procedures, and our attention to privacy and security issues and patient consent issues and I think it will bring those topics more into light for the end-user than they are right now" (HIE director).

The LMS was implemented in February 2016 and WesternHIE began using it to conduct compliance training as participating organizations added new users or came up for their annual compliance renewal, although it was still being refined at the end of 2016.

> I think one of our biggest challenges will be, not the enforcement of the policy course that we're going to ask our HIE end users to take, but how is it going to affect their use of the HIE? It is a challenge for us to make it informative, but not daunting, and that we need to roll it out and maintain and insist that they do this, without asking them to give up a whole chunk of their day going through these policies and procedures and training courses. (Assistant HIE director)

There was general agreement among the WesternHIE staff that the LMS was going to be beneficial to HIE security. For example, the WesternHIE staff member in charge of conducting audits explained that the LMS generated detailed data on training completion whereas, before the LMS was implemented, that information was only available from the people conducting the training. There was, however,

some concern about pushback from the participants if the training became too burdensome.

> A year from now we may be discussing, what were the challenges and how did we overcome the insistence on having thousands of people go through these policy and procedure trainings, and were we successful? It's walking that thin line where we need them to do it, but we don't want to put them into a position where they say, forget it, I don't have time for it so I won't use it. (Assistant HIE director)

The LMS represented a focus on exposure control reasoning as WesternHIE realized that its existing methods for confirming that HIE participants had read and understood the privacy and security policies left it exposed to the potential for many participant users to be using the HIE without being sufficiently aware of important privacy and security behaviors and expectations. There was recognition that implementing the LMS and forcing participants to complete the required training in a more regimented fashion could possibly drive some participants out of the exchange; however, the benefits of exposure control outweighed the cost of losing some participants.

In looking forward, as privacy and security become increasingly important to the viability of an organization like WesternHIE, they are considering some organizational restructuring to improve their capabilities in this regard. "Because of all the threats and the worries and, when is the breach going to come for us? Because it just seems inevitable" (Executive director).

One planned change will be to hire an ISO for the HIE instead of continuing to borrow time from the QIO's information security officer. That will provide them with a dedicated staff member with appropriate credentials and experience to manage the security of the HIE. "For what the HIE needs to do is more than what I can do part time" (New ISO).

They are also considering the need for a higher-level manager of privacy and security and additional staff support for privacy and security tasks. For example, the WesternHIE staff member currently in charge of conducting audits noted the need for additional staff to support the audit process. "I'm doing all of these audits on my own and it's only a small portion of my time. I have a million other things to do as well" (Project coordinator).

These considerations also reflect a focus on exposure control reasoning as the organization realizes that not having the right personnel could increase its exposure to the growing number of threats in the environment.

One other change in progress was a shift from being a directed exchange to becoming a more query-based exchange. Directed exchange is when a participant connects his or her electronic health record (EHR) to the exchange so that relevant information can be automatically pulled into the exchange from the EHR or pushed to the EHR from the exchange. Query-based exchange, in contrast, involves individual searches for patient information on the exchange that simply requires a browser

and a patient identifier to conduct the search. That shift in focus requires changes in the privacy and security policies.

> As we've taken the strategy for the HIE into more query-based exchange, as opposed to directed exchange, that query-based exchange now requires a different level of auditing at the patient level. Who's accessing who? When are they accessing? What's the appropriateness of access? What's the reason for access? Had we stayed very heavily in a directed exchange, had we chosen a strategy that took us down a robust directed exchange methodology, that would have impacted those policy requirements. (HIE director)

Here, ethical control reasoning with a utilitarian focus is driving the growth in query-based exchange as WesternHIE recognizes the value of offering both directed and query-based exchange to participants. However, exposure control reasoning is again at play, as WesternHIE realizes that query-based exchange offers greater opportunities for inappropriate search activity that could compromise the privacy of patients. Therefore, additional auditing of participant activity will be necessary going forward.

Discussion

Information sharing is bringing new rewards to many fields, such as commerce, education, health care, law enforcement, and so on. But perhaps nowhere other than health care is the tension between sharing information and securing information as prominent. Having immediate and complete information about a patient is critical for the success of the health-care provider. But this critical availability can stand in direct opposition to the need to protect the confidentiality of this information from the prying eyes of an unauthorized intruder, or from accidental disclosure. A theoretical framework for managing this tension, one that operates well in health care, could be a valuable model for managing security of information sharing in many other kinds of settings.

In order to evaluate our theoretical framework, we analyzed the tension between sharing and protecting health information in WesternHIE's information security policy development process. For this, we considered the ways in which exposure and ethical control reasoning were used by the members of the HIE to develop their information security policies and assessed how those two forms of reasoning interacted in the policy development process.

Exposure control reasoning is concerned with the implementation of controls to separate assets from their associated threats. For WesternHIE this started with an analysis of the assets and threats that would be relevant to an HIE. In creating the initial task force for privacy and security, WesternHIE's decision to include participants from the health-care and legal domains was predicated on the belief that diversity would produce a range of perspectives to better identify the relevant assets

and threats for which controls would need to be defined in the information security policies.

The second iteration of WesternHIE's information security policies was initiated on the belief that the expertise of the information security officer could help identify gaps in the assets and threats for which the policies were written. Here the tension between sharing and protecting was most pronounced as the ISO was focused on protection, while the other members of the HIE were more focused on enabling their participants to exchange data with fewer restrictions. The result of that assessment and revision was the expansion of the information security policies to include controls for additional assets and threats identified by the ISO.

The third iteration, which did not involve the ISO directly, was focused on refining and consolidating the organization's policies by applying a uniform template to all policies and eliminating those that were focused too narrowly on specific procedures or roles. The belief was that a high number of policies in nonstandard formats would not be an effective mechanism for securing information assets, because the policies would be less likely to be read and applied. In other words, reasoning that is focused too heavily on exposure control can lead to a set of policies that appear to provide comprehensive guidance on the implementation of controls to protect organizational assets from security threats, but run the risk of being rarely consulted and therefore ineffective.

In the fourth iteration, further refinement of the policies took place as the new ISO recognized the threats associated with including too much detail in the policies. Here, exposure control reasoning was focused on the threats of litigation and regulatory audits that verbose policies would produce. The LMS implementation also represented a focus on exposure control reasoning where the HIE was looking for a mechanism to better document and control the training required for participant users to be in compliance with HIE policies for privacy and security. There was some concern with how the LMS and the training it was designed to enforce would impact the use of the HIE by participants, but the expected value of improved compliance and control of user training was substantial enough to not make that concern a deterrent to implementing the LMS. Exposure control reasoning was also part of the decision to bolster the security focus of the HIE by hiring a dedicated ISO and other security-oriented staff members and the need for additional auditing as the exchanged moved toward greater use of query-based exchange.

Ethical control reasoning is concerned with the rationale for how decisions are made regarding information security controls. When WesternHIE was created, the organization was deliberately set up to include board members from the health-care community and taskforces were created that included a diversity of members from the health-care community. This represents a focus on utilitarian reasoning in which the goal was to form a group that would be best positioned to determine how the HIE should be built to facilitate the greatest good for the community in which it would operate. In addition, an external consultant was brought in to serve as an expert on the legal requirements for HIE, which represents a focus on deontological

reasoning to make sure the HIE was going to be compliant with federal law, specifically HIPAA and state law.

In the second iteration, the information security officer chose to assess the information security policies using NIST guidelines for evaluation and followed a structured approach that would produce a more rigorous and complete set of policies. He was concerned that the system connections between the HIE and the QIO would allow someone to hack into the HIE and use it as a backdoor into the QIO. Therefore, a weak HIE was a vulnerability for the QIO for which he was responsible. Consequently, the ethical control reasoning of the ISO was focused primarily on a utilitarian perspective of what was best for the QIO.

The third iteration relied more heavily on deontological reasoning as the HIE staff strove to work with participants to formulate policies that would work for them. The consent policy was an example of this where the participants would be the ones engaging in consent activities so they were consulted more directly on the consent policy and forms. The goal was to produce a set of policies that were more accessible to both HIE staff and participants.

In the fourth iteration, ethical control reasoning with a utilitarian focus was seen in the efforts to remove unnecessary requirements from the policies that would reduce the workload on HIE staff to be in compliance with those policies and enable the HIE to have greater flexibility in how it operationalized the policies. Ethical control reasoning was also driving the growth in query-based exchange as WesternHIE realized the potential value of increasing its ability to offer access to the exchange that did not require a full connection to a participant's EHR.

For WesternHIE, the tension between sharing and protection in the development of its information security policies was always present, but the reasoning applied to manage that tension shifted from one iteration to the next. Figure 5, presented at the beginning of the case study, illustrates how the emphasis on one or both forms of reasoning shifted through the iterations. The first iteration was probably the most balanced in terms of how exposure and ethical control reasoning was applied to the policy development process as the privacy and security task force constructed a roadmap for the HIE's initial round of policy development. The second iteration was much more focused on exposure control reasoning as the ISO attempted to bring more rigor and a stronger security focus to the policy development process. The third iteration shifted to ethical control reasoning as the HIE staff saw the number of policies and their nonstandardized structure as impediments to the use of those policies by staff and participants and a hindrance to participants in the use of the HIE. The fourth iteration, like the first, was more balanced in the use of exposure and ethical control reasoning. Exposure control reasoning drove the new ISO's goal of removing the verboseness in the policies to reduce exposure to not complying with everything in the policies while at the same time that process invoked ethical control reasoning as the staff recognized the need to reduce the workload-associated policy compliance. The LMS was implemented to increase compliance and control over participant training that was a source of exposure to the HIE. This aligns with the literature that suggests that increased accountability reduces policy violations

[66]. The HIE was looking to hire additional security staff to better manage security threats, but it were also increasing the use of query-based exchange to further drive adoption of the HIE and increase the sharing of data. Thus the LMS was an additional way for the HIE, beyond traditional security controls, to manage or control exposure through compliance.

This framework therefore suggests that as organizations develop their information security policies and more generally consider their information security program, both exposure and ethical control reasoning are necessary to balance the tension between protecting and sharing information. This means that focusing on one type of reasoning over the other, while not necessarily a problem, will shift the focus of the tension to either sharing or protection. While the tension may not be perfectly balanced, leaning too far in one direction will often be detrimental to the organization as either the ability to share information is weakened or the organization becomes too exposed to potential threats. In the case of WesternHIE, an early balance between protection and sharing gave way to an emphasis on protection (i.e., exposure control reasoning dominates). This emphasis was followed by a counterbalancing swing to an emphasis on sharing (i.e., ethical control reasoning dominates). After these two points of emphasis, the balance was restored between information protection and information sharing. These swings may occur because too great a focus on protection could drive participants away from the exchange. Overprotection becomes too much of a burden to participants. Too great a focus on sharing could also drive participants away if that focus enabled the exchange to be breached. These findings are important because, while the literature says that ISO and NIST frameworks are mature, the findings in this study indicate that users cycle between ISO and NIST frameworks and utilitarian reasoning.

Two additional things stood out as important factors across these four iterations of policy development and organizational change at WesternHIE. First was the ongoing process of evaluating and revising the privacy and security policies. The organization has never been satisfied with what they have developed and implemented. They recognize that as time progresses, there is a continual need to revisit and renew what has been done in the past to make sure that what they have is still relevant, and to make changes, as necessary, to address new circumstances and opportunities. This need for ongoing evaluation of security policies and practices is evidenced in the literature [2].

A second factor was that the executive director was a constant through all four iterations. She was, in fact, the only person who had been involved through the entire life cycle of policy development and revisions at WesternHIE. She was a driver of change and supported the work of her staff in shaping and reshaping the privacy and security policies, to maintain the balance between protecting the exchange's data and enabling the exchange to grow and provide access to that data to an increasing number of participant organizations. The executive director recognized the value in bringing together people with a diversity of ideas along with useful skill sets to develop the exchange and to continue to revise and renew it.

The literature offers evidence for the value of effective leadership in IT adoption and assimilation in general [5, 38, 50], but little has been studied on leadership in information security in particular. This study provides evidence that leadership is an important characteristic of effective privacy and security policy development. The stability of leadership in the top position at WesternHIE, and their championing of this effort, has provided balance in the organization's ability to both protect and share information as evidenced by continued growth in participation in the exchange while maintaining a strong track record of security with no breaches to date. The role of leadership in driving sustained and successful information security efforts offers an important avenue for further research.

This research has focused on the tension between sharing and protecting health information. Although interoperability is important for sharing information, our examination regarded the security policies rather than the technical aspects of the interoperability. A future study could examine the specific effect of system interoperability on security.

While this research was based on a single case, it was a longitudinal study with multiple iterations that acted as new instances of organizational reflection and change. Extending the study to additional sites would enable confirmation of the theory in those additional settings, but the generalizability of this research is no less valuable for its focus on one case [44].

Conclusion

The exchange of health information between providers is considered critical to the improvement of health care both in better care quality and cost reduction. To increase participation in health information exchange and sustain that participation over time, health-care organizations and individual consumers must feel confident that the information shared and accessed through the exchange is secure and private. The inherent tension in this process between the need to share and desire to protect health information has impacted the achievement of greater interoperability.

We introduce a theory of information security control that considers the development of an information security policy, as a foundational and fundamental process in information security, through the relationship between exposure control reasoning and ethical control reasoning. We find that these two forms of reasoning can be used to balance the tension between sharing and protecting information and that an effective information security policy development process brings together stakeholders, experts, and prior codified knowledge. This approach can provide an important foundation for a successful HIE and help enable more secure information sharing in other arenas that similarly bear the tension between sharing and protecting critical data.

Our investigation provides several novel contributions. First, we address a gap in the information security field by offering a theoretically and empirically grounded policy-making framework for addressing the tension between information sharing and information protection. Second, our information sharing security theory bears special

significance to other industry domains where information sharing is governed by strict laws due to the specifically sensitive nature of the information. Third, our findings provide a way forward for promoting the notion of information exchanges that have traditionally floundered due to the security concerns associated with information sharing. Finally, our theory has strong practical implications for practitioners, both in health care and other domains, who may use the learning from the iterative security policy development process to aid their security policy development decisions. They can also apply the theoretical framework to find a balance between openness and protection that best aligns with their specific, local, information goals.

References

1. Accenture. Digital trust: Are you one breach away from losing a healthcare consumer? 2017. Available at www.accenture.com/t20170411T012518__w__/us-en/_acnmedia/PDF-43/Accenture-Health-Are-You-One-Breach-Away-From-Losing-a-Healthcare-Consumer.pdf (accessed on September 4, 2017)
2. Alberts, C.J., and Dorofee, A. *Managing Information Security Risks: The OCTAVE Approach*. Boston, MA: Addison-Wesley Longman, 2002.
3. Alsalamah, S.; Alsalamah, H.; Gray, A.W.; and Hilton, J. Information security threats in patient-centered healthcare. In A. Moumtzoglou (ed.), *M-Health Innovations for Patient-Centered Care*. Hershey, PA: IGI Global, 2016, pp. 298–318.
4. Anthem. 2015 cyber attack settlement agreement reached, 2016. Available at www.anthemfacts.com/cyber-attack (accessed on September 4, 2017)
5. Armstrong, C.P., and Sambamurthy, V. Information technology assimilation in firms: The influence of senior leadership and IT infrastructures. *Information Systems Research*, *10*, 4 (1999), 304–327.
6. Baskerville, R., and Siponen, M. An information security meta-policy for emergent organizations. *Logistics Information Management, 15*, 5/6 (2002), 337–346.
7. Belton, V., and Stewart, T. *Multiple Criteria Decision Analysis: An Integrated Approach*. Dorchester, The Netherlands: Kluwer Academic, 2002.
8. Brailer, D.J. Decade of health information technology: Delivering consumer-centric and information-rich health care. US Department of Health and Human Services, 2004. Available at http://www.providersedge.com/ehdocs/ehr_articles/the_decade_of_hit-delivering_customer-centric_and_info-rich_hc.pdf (accessed on March 19, 2017).
9. Brown, V.; Tumeo, M.; Larey, T.S.; and Paulus, P.B. Modeling cognitive interactions during group brainstorming. *Small Group Research*, *29*, 4 (1998), 495–526.
10. Conklin, A., and McLeod, A. Information security foundations for the interoperability of electronic health records. *International Journal of Healthcare Technology and Management, 11*, 1–2 (2010), 104–112.
11. Connolly, T.; Routhieaux, R.L.; and Schneider, S.K. On the effectiveness of group brainstorming: Test of one underlying cognitive mechanism. *Small Group Research*, *24*, 4 (1993), 490–503.
12. Conway, P., and Gawronski, B. Deontological and utilitarian inclinations in moral decision making: A process dissociation approach. *Journal of Personality and Social Psychology*, *104*, 2 (2013), 216–235.
13. Courtney, R. Security risk assessment in electronic data processing. In *AFIPS Conference NCC*, Dallas, TX, 1977, pp. 97–104.
14. Dawes, S.S. Interagency information sharing: Expected benefits, manageable risks. *Journal of Policy Analysis and Management*, *15*, 3 (1996), 377–394.
15. Doherty, N.F., and Fulford, H. Aligning the information security policy with the strategic information systems plan. *Computers and Security*, *25*, 1 (2006), 55–63.

16. Doherty, N.F.; Anastaskis, L.; and Fulford, H. The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management, 29* (2009), 449–457.

17. Eden, K.B.; Totten, A.M.; Kassakian, S.Z.; Gorman, P.N.; McDonagh, M.S.; Devine, B.; Pappas, M.; Daeges, M.; Woods, S.; and Hersh, W.R. Barriers and facilitators to exchanging health information: A systematic review. *International Journal of Medical Informatics, 88* (2016), 44–51.

18. Eisenhardt, K.M. Building theories from case study research. *Academy of Management Review*, *14*, 4 (1989), 532–550.

19. Experian. Experian third annual 2016 Data Breach Industry Forecast, 2016. Available at https://www.experian.com/assets/data-breach/white-papers/2016-experian-data-breach-industry-forecast.pdf (accessed on May 24, 2017)

20. Fan, J.; Zhang, P.; and Yen, D.C. G2G information sharing among government agencies. *Information and Management, 51*, 1 (2014), 120–128.

21. Fernández-Alemán, J.L.; Señor, I.C.; Lozoya, P.Á.O.; and Toval, A. Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, *46*, 3 (2013), 541–562.

22. Flowerday, S.V., and Tuyikeze, T. Information security policy development and implementation: The what, how and who. *Computers and Security*, *61* (2016), 169–183.

23. Goel, S., and Chengalur-Smith, I.N. Metrics for characterizing the form of security policies. *Journal of Strategic Information Systems*, *19*, 4 (2010), 281–295.

24. Gordon, L., and Loeb, M. Return on information security investments: Myths vs. realities. *Strategic Finance*, *84* (2002), 26–31.

25. Gritzalis, D. A baseline security policy for distributed healthcare information systems. *Computers and Security*, *16*, 8 (1997), 709–719.

26. Herath, T., and Rao, H.R. Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*, 2 (2009), 106–125.

27. Higgs, J., and Jones, M.A. Clinical decision making and multiple problem spaces. In J. Higgs, M. Jones, S. Loftus, and N. Christensen (eds.), *Clincial Reasoning in the Health Professions*. Amsterdam, The Netherlands: Focal Press, 2008, pp. 3–18.

28. Hoffman, L., Michelman, E., and Clements, D. SECURATE - Security evaluation and analysis using fuzzy metrics. In *AFIPS National Computer Conference*, 1978, pp. 531–540.

29. Höne, K., and Eloff, J. What makes an effective information security policy? *Network Security, 6* (2002), 14–16.

30. Hong, K.S.; Chi, Y.P.; Chao, L.R.; and Tang, J.H. An empirical study of information security policy on information security elevation in Taiwan. *Information Management and Computer Security*, *14*, 2 (2006), 104–115.

31. Hwang, C.-L., and Masud, A.S.M. *Multipe Objective Decision Making—Methods and Applications: A State-of-the-Art Survey*. Berlin, Germany: Springer-Verlag, 1979.

32. Identity Theft Resource Center (ITRC). Medical data breaches come with high risks, 2016, Available at http://www.idtheftcenter.org/Data-Breaches/medical-data-breaches-come-with-high-risks.html (accessed on May 24, 2017)

33. Johnson, M.E. Information risk of inadvertent disclosure: An analysis of file-sharing risk in the financial supply chain. *Journal of Management Information Systems*, *25*, 2 (2008), 97–124.

34. Johnston, A.C.; Warkentin, M.; McBride, M.; and Carter, L. Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems*, *25*, 3 (2016), 231–251.

35. Jones, A., and Ashenden, D. *Risk Management for Computer Security: Protecting Your Network and Information Assets*. Oxford, UK: Butterworth-Heinermann, 2005.

36. Kache, F., and Seuring, S. Challenges and opportunities of digital information at the intersection of Big Data Analytics and supply chain management. *International Journal of Operations and Production Management*, *37*, 1 (2017), 10–36.

37. Kadam, A.W. Information security policy development and implementation. *Information Systems Security*, *16*, 5 (2007), 246–256.

38. Karimi, J.; Bhattacherjee, A.; Gupta, Y.P.; and Somers, T.M. The effects of MIS steering committees on information technology management sophistication. *Journal of Management Information Systems*, *17*, 2 (2000), 207–230.

39. Karyda, M.; Kiountouzis, E.; and Kokolakis, S. Information systems security policies: A contextual perspective. *Computers and Security*, *24*, 3 (2005), 246–260.

40. Keeney, R.L., and Raiffa, H. *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*. Cambridge, UK: Cambridge University Press, 1993.

41. Khoumbati, K.; Themistocleous, M.; and Irani, Z. Evaluating the adoption of enterprise application integration in health-care organizations. *Journal of Management Information Systems*, *22*, 4 (2006), 69–108.

42. Kruse, C.S.; Frederick, B.; Jacobson, T.; and Monticone, D.K. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*, 1 (2017), 1–10.

43. Kwon, J., and Johnson, M.E. Health-care security strategies for data protection and regulatory compliance. *Journal of Management Information Systems*, *30*, 2 (2013), 41–66.

44. Lee, A.S., and Baskerville, R.L. Generalizing generalizability in information systems research. *Information Systems Research*, *14*, 3 (2003), 221–243.

45. Li, Y.-C.; Kuo, H.-S.; Jian, W.-S.; Tang, D.-D.; Liu, C.-T.; Liu, L.; Hsu, C.-Y.; Tan, Y.-K.; and Hu, C.-H. Building a generic architecture for medical information exchange among healthcare providers. *International Journal of Medical Informatics*, *61*, 2 (2001), 241–246.

46. Lim, S.Y.; Jarvenpaa, S.L.; and Lanham, H.J. Barriers to interorganizational knowledge transfer in post-hospital care transitions: Review and directions for information systems research. *Journal of Management Information Systems*, *32*, 3 (2015), 48–74.

47. Martin, J. *Security, Accuracy and Privacy in Computer Systems*. Englewood Cliffs, NJ: Prentice Hall, 1973.

48. Mason, J. *Qualitative Researching*. London, UK: Sage, 2002.

49. Miles, M.B., and Huberman, A.M. *Qualitative Data Analysis*. Thousand Oaks, CA: Sage, 1994.

50. Neufeld, D.J.; Dong, L.; and Higgins, C. Charismatic leadership and user acceptance of information technology. *European Journal of Information Systems*, *16*, 4 (2007), 494–510.

51. Neumann, P.G. Risks in Digital Commerce. *Communications of the ACM*, *39*, 1 (1996), 154.

52. Office of the National Coordinator (ONC). Connecting health and care for the nation: A shared nationwide interoperability roadmap, 2015. Available at https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf (accessed on March 19, 2017)

53. Pathari, V., and Sonar, R. Identifying linkages between statements in information security policy, procedures and controls. *Information Management and Computer Security*, *20*, 4 (2012), 264–280.

54. Ponemon, L. 2017 Ponemon Institute Cost of a Data Breach Study, 2017. Available at https://securityintelligence.com/media/2017-ponemon-institute-cost-of-a-data-breach-study/ (accessed on September 4, 2017)

55. Redspin. Breach Report 2016: Protected Health Information (PHI). Cynergis Teki, 2017. Available at https://www.redspin.com/resources/download/breach-report-2016-protected-health-information-phi/.

56. Saaty, T.L. Decision making with the analytic hierarchy process. *International Journal of Services Sciences, 1* (2008), 83–98.

57. Sadler, T.D., and Zeidler, D.L. Patterns of informal reasoning in the context of socioscientific decision making. *Journal of Research in Science Teaching*, *42*, 1 (2005), 112–138.

58. Schweitzer, E.J. Reconciliation of the cloud computing model with US federal electronic health record regulations. *Journal of the American Medical Informatics Association*, *19*, 2 (2012), 161–165.

59. Sen, R., and Borle, S. Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, *32*, 2 (2015), 314–341.

60. Siponen, M.; Willison, R.; and Baskerville, R. Power and practice in information systems security research. In R. Boland, M. Limayem, and B. Pentland (eds.), *International Conference on Information Systems*. Paris, France, 2008, pp. 1–12.

61. Siwicki, B. Ransomware attackers collect ransom from Kansas hospital, don't unlock all the data, then demand more money. *Healthcare IT News*, 2016. Available at http://www.healthcareitnews.com/news/kansas-hospital-hit-ransomware-pays-then-attackers-demand-second-ransom (accessed on March 19, 2017)

62. Skopik, F.; Settanni, G.; and Fiedler, R. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers and Security, 60* (2016), 154–176.

63. Sriram, R.D. Health Information Technology (IT). The National Institute of Standards and Technology (NIST), 2016. Available at https://www.nist.gov/healthcare (accessed on September 4, 2017)

64. Straub, D., and Welke, R. Coping with systems risk: Security planning models for management decision-making. *MIS Quarterly, 22* (1998), 441–469.

65. Titah, R.; Shuraida, S.; and Rekik, Y. Integration breach: Investigating the effect of internal and external information sharing and coordination on firm profit. *International Journal of Production Economics, 181*, Part A (2016), 34–47.

66. Vance, A.; Lowry, P.B.; and Eggett, D. Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, *29*, 4 (2013), 263–290.

67. Vest, J.R., and Gamm, L.D. Health information exchange: Persistent challenges and new strategies. *Journal of the American Medical Informatics Assocation, 17* (2010), 288–294.

68. von Solms, B., and von Solms, R. The 10 deadly sins of information security management. *Computers and Security, 23*, 5 (2004), 371–376.

69. Wenjing, L. Government information sharing: Principles, practice, and problems—An international perspective. *Government Information Quarterly*, *28*, 3 (2011), 363–373.

70. Whitman, M.E. In defense of the realm: Understanding the threats to information security. *International Journal of Information Management*, *24*, 1 (2004), 43–57.

71. Wolff, J. Perverse effects in defense of computer systems: When more is less. *Journal of Management Information Systems*, *33*, 2 (2016), 597–620.

72. Woodward, B.; Davis, D.C.; and Hodis, F.A. The relationship between ethical decision making and ethical reasoning in information technology students. *Journal of Information Systems Education*, *18*, 2 (2007), 193–202.

73. Yang, T.-M., and Maxwell, T.A. Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government Information Quarterly*, *28*, 2 (2011), 164–175.

74. Yeager, V.A.; Walker, D.; Cole, E.; Mora, A.M.; and Diana, M.L. Factors related to health information exchange participation and use. *Journal of Medical Systems, 38*, 8 (2014), 1–9.

Appendix A: Phase 1 Interview Guide

Timeline

When did you join the QIO?

When did you take on the work with WesternHIE and why did you assume that role?

What is your current role with WesternHIE?

Historical Account

What do you recall about the environment at WesternHIE when you first got started with regard to information security and privacy?

What stood out for you with regard to WesternHIE's privacy and security policies?

How would you describe the organizational structures that were in place to facilitate change?

Please describe the process that occurred with regard to making changes to the organization's privacy and security policies.

Who was involved in the process and who were the primary drivers of change at that time?

Current View

What do you see as the current strengths and weaknesses of WesternHIE for implementing and maintaining a good privacy and security policy?

How is the organization continuing to evaluate and change its policies and procedures and what mechanisms are in place to ensure that process continues effectively?

Who is currently involved in the process of evaluating and updating the organization's privacy and security policies?

What mechanisms are in place to ensure that existing policies are being met in practice?

Who is responsible for enforcement and compliance?

Future Thoughts

Where do you see the organization going with regard to privacy and security?

What changes to the health-care environment might be the most critical for WesternHIE to look for with regard to maintaining good privacy and security?

Current Policies and Procedures

What responsibilities does the Policy Owner have? Operational oversight?

How is compliance with permitted use and disclosure handled? How do you ensure that the workforce is only accessing PHI [protected health information] on an as needed basis?

Who is on the Crisis Communication Team?

Who is on the security incident response team?

What is included in the WesternHIE training program for their workforce and for participants?

What is a Provider Address Book?

What is the status of partial record consent? Will your vendor offer that or not and is the state still considering it as a requirement for HIE?

What's included in the Business Associate Agreement?

How is auditing of the vendor handled?

Appendix B: Phase 2 Interview Guide

Describe your role at WesternHIE and how that role has changed during your time with the organization.

Describe your prior experiences that prepared you for your work at WesternHIE.

Explain your involvement in the development and implementation of WesternHIE's information security policies since spring of 2015.

How did the process of developing and implementing WesternHIE's information security policies relate to your expectations for how that process should occur?

How have WesternHIE's information security policies changed since spring of 2015 and why were those changes necessary?

Describe any key issues that you encountered in developing the information security policies for WesternHIE.

Do you feel that WesternHIE's information security policies are effective in their current form?

Describe any key issues that you encountered in implementing the information security policies for WesternHIE.

Explain how WesternHIE's information security policies are enforced and audited.

How successful has WesternHIE been in achieving its goals as a health information exchange?

From your perspective, what are some of the primary challenges that WesternHIE has experienced in achieving its goals.