A Framework for Evaluating the Tension between Sharing and Protecting Health Information

Chad Anderson
Northern Kentucky University
andersonc16@nku.edu

Richard Baskerville
Georgia State University
Curtin University
baskerville@acm.org

Mala Kaul
University of Nevada, Reno
mkaul@unr.edu

Abstract

Health information exchange (HIE) is expected to improve the quality and cost of healthcare but sustained use of HIE by providers has been difficult to achieve. A number of factors play a role in that process including concern for the security and privacy of the exchanged information. This tension between the expected benefits of HIE resulting from collaboration and information sharing on the one hand, and the potential security risks inherent in the exchange process on the other hand, is not well understood. We propose an information security control theory to explain this tension. We evaluate this theory through a case study of the iterative development of the information security policy for an HIE in the western United States. We find that the theory offers a good framework through which to understand the information security policy development process.

1. Introduction

The digital transformation of healthcare is expected to improve care quality and reduce the costs of providing quality care [6]. 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 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" [1]. 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-1990's, community health information networks (CHINs) in the mid to late 1990's, and regional health information organizations (RHIOs) in the 2000's [34]. 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 the route to effective and sustained interoperability is multi-faceted and insufficiently understood [13].

One of the main challenges for interoperability is maintaining the security and privacy of the protected health information that is transmitted through the HIE [13, 37]. According to the Identity Theft Resource Center, in 2015, the healthcare sector experienced more than one third of all publicly reported data breaches [20]. Security breaches can have serious consequences, not only for patients, through identity theft or disclosure of private health records, but also for the healthcare organizations that stand to be impacted financially, through loss of reputation, trust, and potential legal and regulatory consequences. Threats to the security of health data are expected to remain high because of the value of medical records on the black market [2]. Unfortunately, the information systems in healthcare organizations are often not very robust when it comes to security. 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 [31].

A tension, therefore, 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 the 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 [36]. While an information security policy is prescribed by many as an essential component of an effective security program, there is little research on

URI: http://hdl.handle.net/10125/41598
ISBN: 978-0-9981331-0-2

the factors that go into developing that policy, and even less on the impact that the aforementioned tension plays in the policy development process. Therefore, an important research question for understanding and explaining what enables health information exchange is, *how does the essential tension between sharing and protecting health data impact the development of information security policies?*

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 data, in the development of their 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.

2. Theoretical background

Fundamental goals for information security include the confidentiality, availability, and integrity of data and the development of controls to support those goals [14, 3]. However, much of the published research on information security is limited in its consideration of the theoretical foundations that underpin it, and that which does typically makes use of theories that are applicable to a very limited range of the information security spectrum [30]. 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 [15]; while general deterrence theory (GDT) has been used to explain human behavior and the design of controls to combat computer crime and intentional abuse [33]. 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 papers [30]. This research aims to address these gaps in the literature by proposing a theoretical framework specific to information security, but one that is broadly applicable to a variety of security phenomena, and 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 [22], healthcare [16], education [28], etc. The purpose of this research is not to replicate prior research in multi-objective decision analysis, but rather, 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 healthcare 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 [23, 11]. 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 forego, because the controls are too difficult or expensive to acquire or operate.

2.1 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 external threat sources, or, insider threats. Exposure control reasoning aims to manage those risk exposures [8, 29] 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. Consequently, the addition of security requirements and controls into an information system can be expected to meaningfully 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 [17].

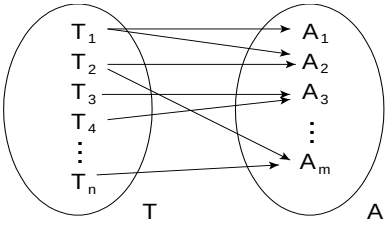

Figure 1. Threat-asset exposure edges (adapted from Hoffman et al [17])

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.

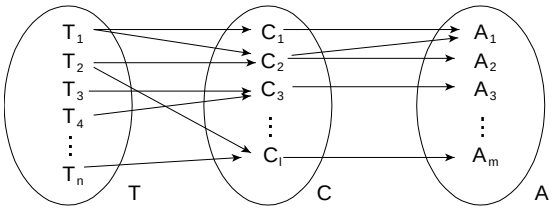

Figure 2. Threat-control-asset edges (adapted from Hoffman et al [17])

2.2 Ethical control reasoning

Ethical control reasoning arises in the need to make rational decisions about controls adoption. 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. Ethical controls 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 [10]. 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 [10]. 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 & Ashenden [21]. 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 different treatments than low frequency, high impact threats, etc. 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 high in frequency, but 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, while 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.

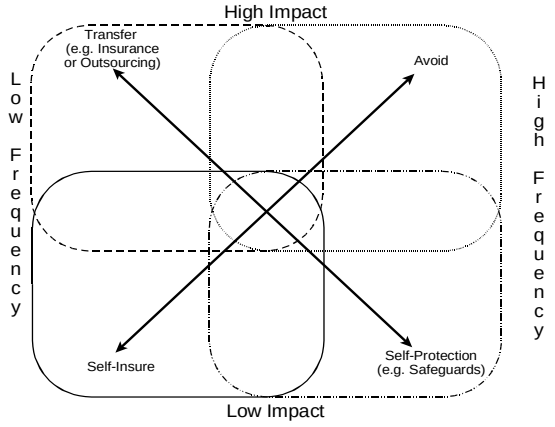

Figure 3. Risk treatment framework (adapted from Jones & Ashenden [21])

2.3 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 and is the foundational document by which procedures and controls are selected and implemented [4, 12]. Therefore, the application of both exposure and ethical controls reasoning in the development of an information security policy is essential to create a policy that takes into account, the assets and threats for which security controls must be implemented, the needs of relevant stakeholders, and the requirements of requisite laws and regulations, to enable both the sharing and protection of information.

Research has considered the role [18], importance [35], structure [4], and content [12] of the information security policy, but 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.

2.4 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. 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, policy makers can adopt exposure control reasoning. Similarly, they can use ethical control reasoning to rationalize the 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 controls 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 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 there are trade-offs in security, such as the tradeoff 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 multi-criteria decision making. Rather, this tension helps explicate the knowledge and preferences of the decision maker [19] that is a necessary input to multi-criteria decisions. It offers a clear frame for illuminating the contradictory inputs to the decision process. Normatively, multi-criteria decision theories, such as Multiple Attribute Utility Theory [5, 22] or the Analytical Hierarchy Process, can then be employed for the decision-making process itself [27].

3. Case study

A qualitative case study was utilized to evaluate an HIE's information security policy development process. The HIE in this study, which shall henceforth be known as WesternHIE, is located in the western United States and includes participating healthcare organizations across the entire state in which it operates. The HIE was initially formed in 2011 and continues to operate successfully experiencing growth with 89 healthcare organizations currently participating in the exchange, representing a sizeable portion of the state's healthcare community.

3.1. Method

This was not an a priori study of the tension between sharing and protecting data. Rather it was an exploratory study to understand the role of security policy development 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 [24].

Arrangements for data collection were coordinated through the HIE's executive director, who was known to one of the authors. 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 in the HIE's information security policy development process at one point or another. Within that scope of access, semi-structured interviews were

conducted, either in person or over the phone, with the executive director, five other HIE staff members and an 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 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 [24]. Interviews took place over a four month period in 2015 and were conducted by one or more of the authors. All interviews were audio-recorded with the exception of one in which the participant asked not to be recorded. Documentation was also collected and analyzed including the different versions of the security policy, policy development timelines, and the document deliverables at each stage of the policy development process.

Analysis of the data started after the initial interview and continued through the completion of data collection. Interview transcripts and document data were analyzed at different points by all of the authors in an iterative process of data reduction and conclusion drawing [25] with the goal of identifying elements of the information security development process that explained how the HIE had been successful in developing and growing the exchange. Through this process we identified the tension between sharing and protecting data that the HIE had to address through the development, implementation, and revision of their information security policies. The following account details that iterative process.

3.2. HIE security policy development

WesternHIE has gone through three distinct iterations of information security policy development since the organization was created in 2011.

3.2.1. 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 healthcare 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 then 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 WestermHIE 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 HIE's 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)*

That created 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 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, ...) 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 other perspectives and think more broadly [7, 9].

The task forces met once in July 2011 and twice in August 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 which 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)*

In this early stage of the HIE, the tension between protecting and sharing data was evident. There was the goal of getting the technology up and running to quickly generate buy-in from physicians that an exchange could work, while at the same time the privacy and security task force recognized the need to create security policies based on HIPAA regulations 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 was unnecessarily eclipsing the (more strategic) aim to expose or share. 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 [26].

> *"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 their focus area. These were provided to the external consultant in September 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 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 have 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.

3.2.2. Second iteration. In 2013 WesternHIE decided they needed some expert help to evaluate their 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, there were two other WesternHIE staff members 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 NIST guidelines [32] for the evaluation, but he also looked to outside sources to see what other HIE's 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 value 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. In order 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.

3.2.3. 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 that there was 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 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 controls 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 2-3 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 organization's continued to grow and currently includes 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 contends that the general perception and engagement with the process and the resulting policies has been very positive both from active participants and the community at large.

4. Discussion

In order to evaluate our theoretical framework, we analyzed the tension between sharing and protecting health data on WesternHIE's information security policy development process. For this, we considered the ways in which exposure and ethical control reasoning were utilized 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 healthcare 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 non-standard formats would not be effective as a mechanism for securing information assets because the policies would be less likely to be read and applied. In other words, reasoning 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.

Ethical control reasoning is concerned with the rational 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 healthcare community and taskforces were created that included a diversity of members from the healthcare community. This represents a focus on utilitarian reasoning in which the goal was to form a group that would be best positions 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.

For WesternHIE the tension between sharing and protection in the development of information security policies was always present, but the reasoning applied to manage that tension shifted from one iteration to the next. 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 non-standardized structure as impediments to the use of those policies by staff and participants and a hindrance to participants in the use of the HIE.

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.

5. Conclusion

The exchange of health information between providers is considered critical to the improvement of healthcare both in better care quality and cost reduction. To increase participation in health information exchange and sustain that participation over time, healthcare 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 that brings together stakeholders, experts, and prior codified knowledge, can provide an important foundation for a successful HIE.

6. References

[1] *Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap*, The Office of the National Coordinator for Health Information Technology, 2015.

[2] *Experian Third Annual 2016 Data Breach Industry Forecast*, 2016.

[3] S. Alsalamah, H. Alsalamah, A. W. Gray and J. Hilton, *Information Security Threats in Patient-Centered Healthcare*, in A. Moumtzoglou, ed., *M-Health Innovations for Patient-Centered Care*, IGI Global, Hershey, PA, 2016.

[4] R. Baskerville and M. Siponen, "An information security meta-policy for emergent organizations", Logistics Information Management, 15 (2002), pp. 337-346.

[5] V. Belton and T. Stewart, *Multiple Criteria Decision Analysis: An Integrated Approach*, Kluwer Academic Publishers, Dorchester, The Netherlands, 2002.

[6] D. J. Brailer, *Decade of health information technology: Delivering consumer-centric and information-rich health care*, US Department of Health and Human Services, 2004.

[7] V. Brown, M. Tumeo, T. S. Larey and P. B. Paulus, "Modeling Cognitive Interactions During Group Brainstorming", Smal Group Research, 29 (1998), pp. 495-526.

[8] A. Conklin and A. McLeod, "Information security foundations for the interoperability of electronic health records", International Journal of Healthcare Technology and Management, 11 (2010), pp. 104-112.

[9] T. Connolly, R. L. Routhieaux and S. K. Schneider, "On the Effectiveness of Group Brainstorming: Test of One Underlying Cognitive Mechanism", Smal Group Research, 24 (1993), pp. 490-503.
[10] P. Conway and B. Gawronski, "Deontological and Utilitarian Inclinations in Moral Decision Making: A Process Dissociation Approach", Journal of Personality and Social Psychology, 104 (2013), pp. 216-235.
[11] R. Courtney, *Security risk assessment in electronic data processing*, *AFIPS Conference NCC*, 1977, pp. 97-104.
[12] N. F. Doherty, L. Anastaskis and H. Fulford, "The information security policy unpacked: A critical study of the content of university policies", International Journal of Information Management, 29 (2009), pp. 449-457.
[13] K. B. Eden, A. M. Totten, S. Z. Kassakian, P. N. Gorman, M. S. McDonagh, B. Devine, M. Pappas, M. Daeges, S. Woods and W. R. Hersh, "Barriers and facilitators to exchanging health information: a systematic review", International Journal of Medical Informatics, 88 (2016), pp. 44-51.
[14] J. L. Fernández-Alemán, I. C. Señor, P. Á. O. Lozoya and A. Toval, "Security and privacy in electronic health records: A systematic literature review", Journal of Biomedical Informatics, 46 (2013), pp. 541-562.
[15] L. Gordon and M. Loeb, "Return on Information Security Investments: Myths vs. Realities", Strategic Finance, 84 (2002), pp. 26-31.
[16] J. Higgs and M. A. Jones, *Clinical decision making and multiple problem spaces*, in J. Higgs, M. Jones, S. Loftus and N. Christensen, eds., *Clincial Reasoing in the Health Professions*, Focal Press, Amsterdam, 2008.
[17] L. Hoffman, E. Michelman and D. Clements, *SECURATE - Security evaluationand analysis using fuzzy metrics*, *AFIPS National Computer Conference*, 1978, pp. 531-540.
[18] K. S. Hong, Y. P. Chi, L. R. Chao and J. H. Tang, "An empirical study of information security policy on information security elevation in Taiwan", Information Management & Computer Security, 14 (2006), pp. 104-115.
[19] C.-L. Hwang and A. S. M. Masud, *Multipe Objective Decision Making - Methods and Applications: A State-of-the-Art Survey*, Springer-Verlag, Berlin, Heidelberg, 1979.
[20] ITRC, *Do You Need Help with an Identity Theft Problem?*, 2015.
[21] A. Jones and D. Ashenden, *Risk Management for Computer Security: Protecting Your Network & Information Assets*, Butterworth-Heinermann, Oxford, 2005.
[22] R. L. Keeney and H. Raiffa, *Decisions with Multiple Objectives: Peferences and Value Tradeoffs*, Cambridge University Press, Cambridge, 1993.
[23] J. Martin, *Security, Accuracy and Privacy in Computer Systems*, Prentice Hall, Englewood Cliffs, 1973.
[24] J. Mason, *Qualitative Researching*, Sage Publications, London, 2002.
[25] M. B. Miles and A. M. Huberman, *Qualitative Data Analysis*, SAGE Publications, Thousand Oaks, CA, 1994.
[26] P. G. Neumann, "Risks in Digital Commerce", Communications of the ACM, 39 (1996), pp. 154.
[27] T. L. Saaty, "Decision making with the analytic hierarchy process", International Journal of Services Sciences, 1 (2008), pp. 83-98.
[28] T. D. Sadler and D. L. Zeidler, "Patterns of informal reasoning in the context of socioscientific decision making", Journal of Research in Science Teaching, 42 (2005), pp. 112-138.
[29] E. J. Schweitzer, "Reconciliation of the cloud computing model with US federal electronic health record regulations", Journal of the American Medical Informatics Association, 19 (2012), pp. 161-165.
[30] M. Siponen, R. Willison and R. Baskerville, *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.
[31] B. Siwicki, *Ransomware attackers collect ransom from Kansas hospital, don't unlock all the data, then demand more money*, *Healthcare IT News*, 2016.
[32] R. D. Sriram, *Health Information Technology (IT)*, The National Institute of Standards and Technology (NIST), 2016.
[33] D. Straub and R. Welke, "Coping with Systems Risk: Security Planning Models for Management Decision-making", MIS Quarterly, 22 (1998), pp. 441-469.
[34] J. R. Vest and L. D. Gamm, "Health Information Exchange: Persistent Challenges and New Strategies", Journal of the American Medical Informatics Assocation, 17 (2010), pp. 288-294.
[35] B. von Solms and R. von Solms, "The 10 deadly sins of information security management", Computers & Security, 23 (2004), pp. 371-376.
[36] M. E. Whitman, "In defense of the realm: understanding the threats to information security", International Journal of Information Management, 24 (2004), pp. 43-57.
[37] V. A. Yeager, D. Walker, E. Cole, A. M. Mora and M. L. Diana, "Factors Related to Health Information Exchange Participation and Use", Journal of Medical Systems, 38 (2014), pp. 1-9.