9-16-2011

Why do Healthcare Organizations Choose to Violate Information Technology Privacy Regulations? Proposing the Selective Information Privacy Violations in Healthcare Organizations Model (SIPVHOM)

Paul Benjamin Lowry
City University of Hong Kong, paul.lowry.phd@gmail.com

Jeffrey D. Wall
University of North Carolina-Greensboro, jeffrey.d.wall@gmail.com

James Selfridge
Brigham Young University, jdselfridge@gmail.com

Recommended Citation

Lowry, Paul Benjamin; Wall, Jeffrey D.; and Selfridge, James, " Why do Healthcare Organizations Choose to Violate Information Technology Privacy Regulations? Proposing the Selective Information Privacy Violations in Healthcare Organizations Model (SIPVHOM)" (2011). *All Sprouts Content*. 453.
http://aisel.aisnet.org/sprouts_all/453

芽|Sprouts Working Papers on Information Systems ISSN 1535-6078

Why do Healthcare Organizations Choose to Violate Information Technology Privacy Regulations? Proposing the Selective Information Privacy Violations in Healthcare Organizations Model (SIPVHOM)

Paul Benjamin Lowry
City University of Hong Kong, China

Jeffrey D. Wall
University of North Carolina-Greensboro, USA

James Selfridge
Brigham Young University, USA

Abstract

Privacy concerns about protected healthcare information (PHI) are rampant because of the ease of access to PHI from the advent of Healthcare IT (HIT) and its exploding use. Continual negative cases in the popular attest to the fact that current privacy regulations are failing to keep PHI sufficiently secure in the climate of increate HIT use. To address these issues, this paper proposes a theoretical model with testable hypotheses to explain and predict organizational IT privacy violations in the healthcare industry. Our model, the Selective Information Privacy Violations in Healthcare Organizations Model (SIPVHOM), explains how organizational structures and processes and characteristics of regulatory environments alter perceptions of risk and thereby the likelihood of rule violations. Finally, based on SIPVHOM, we offer recommendations for the structuring of regulatory environments and organizational structures to decrease abuse of PHI.

Keywords: HIPPA, privacy violations, organizations, organizational violations, privacy regulations, privacy policies, healthcare, IT policies

Permanent URL: http://sprouts.aisnet.org/11-138

Reference: Lowry, P. B., Wall, J. D., Selfridge, J. (2011). "Why do Healthcare Organizations Choose to Violate Information Technology Privacy Regulations? Proposing the Selective Information Privacy Violations in Healthcare Organizations Model (SIPVHOM)," Proceedings > Proceedings of JAIS Theory Development Workshop . *Sprouts: Working Papers on Information Systems*, 11(138). http://sprouts.aisnet.org/11-138

Why do Healthcare Organizations Choose to Violate Information Technology Privacy Regulations? Proposing the Selective Information Privacy Violations in Healthcare Organizations Model (SIPVHOM)

ABSTRACT

Privacy concerns about protected healthcare information (PHI) are rampant because of the ease of access to PHI from the advent of Healthcare IT (HIT) and its exploding use. Continual negative cases in the popular attest to the fact that current privacy regulations are failing to keep PHI sufficiently secure in the climate of increate HIT use. To address these issues, this paper proposes a theoretical model with testable hypotheses to explain and predict organizational IT privacy violations in the healthcare industry. Our model, the Selective Information Privacy Violations in Healthcare Organizations Model (SIPVHOM), explains how organizational structures and processes and characteristics of regulatory environments alter perceptions of risk and thereby the likelihood of rule violations. Finally, based on SIPVHOM, we offer recommendations for the structuring of regulatory environments and organizational structures to decrease abuse of PHI.

INTRODUCTION

Since the 1970's, privacy laws have become increasingly prevalent in many areas of society. Beginning with the Fair Credit Reporting Act in 1971, other privacy laws such as the Family Education Rights and Privacy Act soon followed. With the advent of the Internet and the associated ease of distributing information, laws particular to protect privacy during the use of Information Systems (IS) have also emerged. Examples include the Children's Online Privacy Protection Act, and more recently, the Health Information Technology for Economic and Clinical Health (HITECH) Act. Our research concerns this latter act (and related acts worldwide), which is an extension of the Health Insurance Portability and Accountability Act (HIPAA). The US Congress enacted HIPAA in 1996 to protect patients' medical information—known as Protected Health Information (PHI)—from discrimination or other forms of damaging use. Subtitle D of the HITECH Act extended the enforcement rules of HIPAA to provide for stronger enforcement.

Despite the establishment of these medical privacy laws, data breaches cost the US healthcare industry $6 billion each year (Horowitz, 2010). Similarly, the Department of Health and Human Services (HHS)—the office in charge of monitoring compliance with HIPAA rules—receives nearly ten-thousand complaints about privacy violations each year. Not all of these complaints are IT-related and only 20 to 30 percent of the complaints require corrective action—with the majority of the remaining complaints being resolved before HHS begins an investigation (USDH&HS, 2011b). However, the cost of data breaches in the healthcare industry and the number of valid HIPAA complaints show a need for improvement in both technical and organizational compliance measures. The need for improvement is a particularly pressing problem considering the massive growth in the healthcare information technology (HIT) market.

Although the healthcare industry has been slow to adopt IS technology (Bhattacherjee et al., 2007; Connell & Young, 2007), in recent years, HIT has proven essential to the industry (Rivard et al., 2011). The 2010 Healthcare Information and Management Systems Society (HIMSS) Security Survey suggests that approximately 85 percent of healthcare organizations in the US now share PHI electronically (HIMSS, 2010). Similarly, growth in the adoption of HIT and the associated expenditures is explosive. Currently, $80 billion is spent annually in the US on HIT, and the HIT market in the US is expected to grow at a compound annual growth rate of 24 percent during 2012-2014

(RNCOS, 2011c). Similar growth is expected in other countries as well, with Russia's compound annual growth rate expected to be 17% during 2010-2014 (RNCOS, 2011b) and Australia's compound annual growth rate expected to be 5.2% during 2010-2012 (RNCOS, 2011a). With the proliferation of HIT worldwide, it will be ever more important to gain and maintain control over IT privacy violations.

To help control the growing problem of healthcare IT privacy violations, it is important to understand the many facets that contribute to the problem. The lens of this paper is organizational, as determined by people working in healthcare organization. We focus our attention on the selectivity in organizational rule violations—particularly IT privacy violations related to healthcare privacy laws such as HIPAA. *Organizational rule violations* are deviations from appropriate conduct, as prescribed by laws and regulations, by organizational members working individually or as groups acting in their organizational roles to accomplish organizational goals (Vaughan, 1996). As suggested by Selectivity Theory (Lehman & Ramanujam, 2009), organizations are selective in the rules that they violate. That is, different organizations violate different rules, and do so at different times while adhering to other rules. Selectivity Theory further suggests that attributes of the organization and regulatory environment affect perceptions of risk, and thereby the likelihood that a rule will be selected for violation. In this paper, we extend Selectivity Theory to explain and predict the selectivity in organizational violations of IT medical privacy laws.

A review on our phenomenon of interest in recent IS research shows that organizational violations—specifically those involving IT privacy regulations—are of increasing concern. Worldwide, many countries have implemented legislation similar to the Sarbanes-Oxley Act to prevent organizational violations such as financial reporting errors (Leon et al., 2010). In terms of organizational privacy violations, many employers keep personal health records of their employees (Burkhard et al., 2010) to share this information on a “national health information network” (Ozdemir et al., 2011), which increases potential for abuse of IT privacy regulations during information exchange. Personal health records are also stored on record systems owned by other agents independent of hospitals and clinics to facilitate the flow of records between hospitals, clinics, and other entities in the medical industry (Ozdemir et al., 2011). However, clinical staff may be prone to IS avoidance and choose not to use these systems (Kane & Labianca, 2011).

Recent studies show that although training of healthcare staff helps to reduce medical errors (Aron et al., 2011); problems still arise pertaining to patient records. Nevertheless, Warkentin et al. (2011) show that employee compliance with medical privacy laws can be improved through informal learning structures. They suggest that organizational support, feedback on privacy compliance, and opportunities to observe compliance activities built into informal learning structures can increase employee compliance with privacy rules such as HIPAA. Similarly, Johnston and Warkentin (2008) show that organizational support affects both an employee’s behavioral intent to comply with medical privacy laws and the employee’s self-efficacy in complying with the laws. They also show that employees of publicly owned medical institutions are more likely to perceive that the organization is supporting compliance efforts and experience self-efficacy to comply. Research has also shown how willing, or unwilling, patients are to disclose personal information for use in their digital records because of their concern for privacy (Anderson & Agarwal, 2011). We address this concern of organizational IT privacy violations.

This paper adds several important contributions to the literature on medical privacy laws, privacy violations, and organizational rule violations in general. Much research has been done in terms of individuals violating regulations (e.g., Atwater et al., 2001; D'Arcy et al., 2009; Gerlach et al., 2009; Siponen & Vance, 2010). However, organization-level studies in this context are rare. This gap in the literature has led to calls for more organizational-level and multilevel research in IS security and privacy topics {Belanger, 2012 #263}. Our goal thus is to start to fill the knowledge gap what causes organizations to violate regulations—specifically those relating to IT privacy. Our purpose is to extend Selectivity Theory (Lehman & Ramanujam, 2009) to explain and predict why organizations violate IT privacy regulations.

To address this goal, we proceed as follows. First, we outline Selectivity Theory and its several assumptions and constraints. Second, we demonstrate how healthcare organizations and HIPAA fit within the assumptions and constraints of Selectivity Theory. Third, we outline a theoretical model by adopting Selectivity Theory's propositions and further operationalize each proposition specific to the domain of IT privacy violations in the healthcare industry. Finally, we offer a discussion of our theoretical model and propose a series of measurement items that could be useful for future model testing.

REVIEWING FOUNDATIONAL THEORETICAL MODEL: SELECTIVITY THEORY

In this section, we propose a theoretical model that can explain and predict violations of medical privacy laws, particularly IT-related privacy violations. We name our model the *Selective Information Privacy Violations in Healthcare Organizations Model* (SIPVHOM). Although we use HIPAA as a proxy for purposes of consistency and clarity, SIPVHOM should also hold predictive power in determining compliance with other medical privacy laws and explain possible differences in compliance between privacy laws. Further, SIPVHOM has the potential to explain and predict differences in compliance between rules contained under the same law. Because HIPAA consists of multiple rules, researchers can use SIPVHOM to explain why some rules under HIPAA are more likely violated than others.

Ultimately, SIPVHOM should inform the creation of privacy laws, and the structuring of the associated regulatory environments and organizations that must abide by the laws.

We based SIPVHOM primarily on Selectivity Theory, proposed by Lehman and Ramanujam (2009). Selectivity Theory explains and predicts why organizations selectively violate some rules while complying with others. As will be shown in the following pages, Selectivity Theory is a natural fit to describe and predict IT privacy violations in the healthcare industry.

OVERVIEW OF SELECTIVITY IN RULE VIOLATIONS

Selectivity Theory posits that organizations are selective in the rules they violate (Lehman & Ramanujam, 2009). Selectivity Theory suggests that a series of contextual conditions and rule characteristics alter the likelihood of an organization selecting a rule for violation. When referring to *contextual conditions* in Selectivity Theory, we mean attributes of an organization—such as hierarchical structures or the complexity of business processes—that can influence rule violations. Likewise, *rule characteristics* refer to the attributes of a rule or the regulatory environment, such as the phrasing and framing of a rule or the power of regulatory agencies that have sway over organizational behaviors. The contextual conditions presented in Selectivity Theory include structural secrecy and the coupling between prior violations and the associated outcomes—referred to as *violation coupling*. Rule enforceability, procedural emphasis, and rule connectedness are the rule characteristics outlined in Selectivity Theory. In Selectivity Theory, *the likelihood of a rule violation* refers to the degree to which systemic factors within the organization and regulatory environment will prompt the possibility of a violation of some rule (Lehman & Ramanujam, 2009).

Selectivity Theory further suggests that an organization’s perception of risk and focus of attention mediate the relationship between the contextual conditions and rule characteristics, and the likelihood of a rule violation. In Selectivity Theory, *perception of risk* refers to the extent to which a rule violation will be perceived as having negative outcomes that appear certain, severe, and uncontrollable (March & Shapira, 1987). Perception of risk has a negative relationship with the likelihood an organization will violate a rule. That is, as decision makers view a rule violation as riskier, they will be more likely to be deterred by fear of negative outcomes and the associated uncontrollability caused by the regulatory environment (Lehman & Ramanujam, 2009).

The other mediating variable, *focus of attention,* is based on the principle which suggests "that decision-makers will be selective in the issues and [solutions] they attend to at any one time and… that what decision-makers do depends on what issues and [solutions] they focus their attention on" (Ocasio, 1997). Lehman and Ramanujam (2009) offer little discussion on the focus of attention and its mediating role. Specifically, Selectivity Theory uses focus of attention differently for each of the constructs representing the contextual conditions and rule characteristics or only by implication. For this reason, we do not use focus of attention as a construct in SIPVHOM, as operationalizing focus of attention for each construct is outside our scope. Instead, we use focus of attention as a driving assumption of the model and bring up its role throughout the paper. The inconsistency in the use of focus of attention in Selectivity Theory also creates difficulty in offering a definite directional relationship. However, to be consistent with the visual model presented by Lehman and Ramanujam (2009), we present focus of attention as having a negative mediating relationship, as with perception of risk. Figure 1 depicts Selectivity Theory.

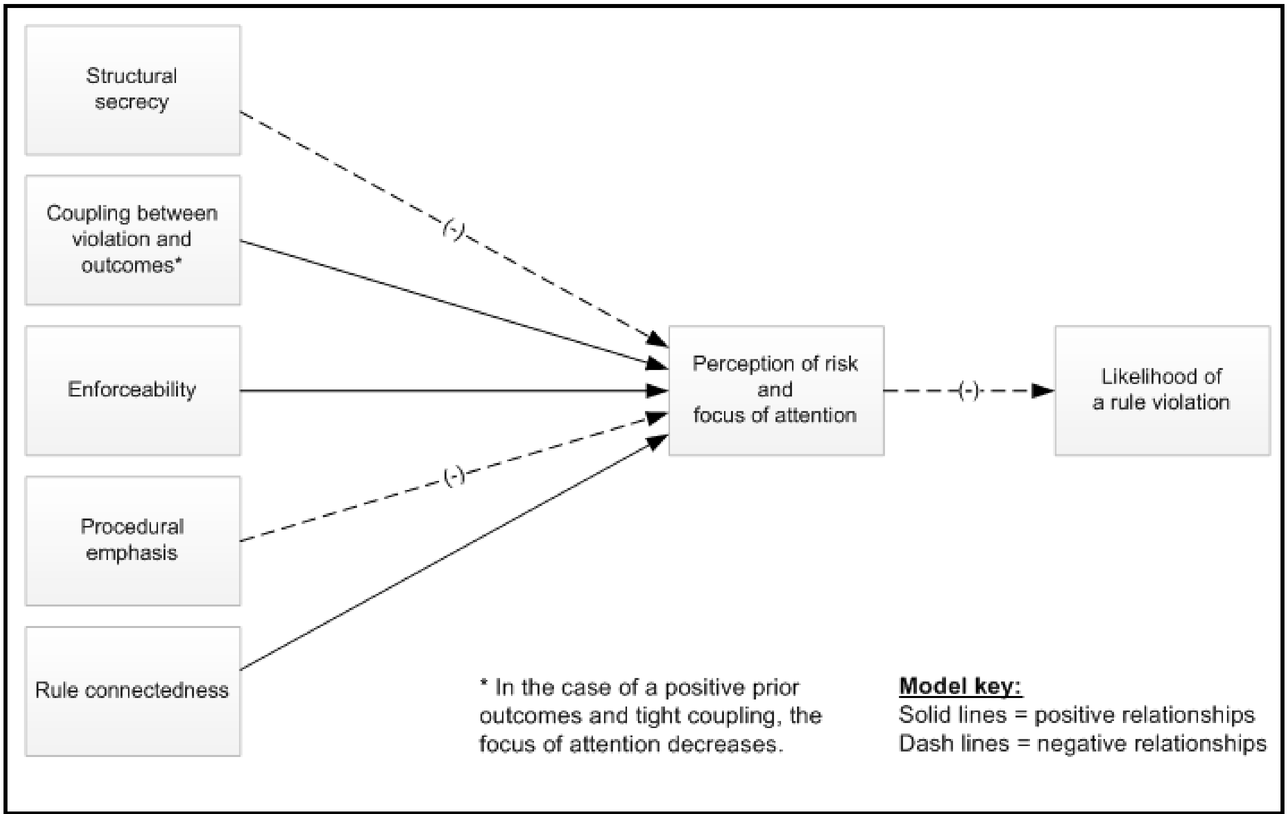

Structural secrecy
Coupling between violation and outcomes*
Enforceability
Procedural emphasis
Rule connectedness
(-)
(-)
Perception of risk and focus of attention
(-)
Likelihood of a rule violation
* In the case of a positive prior outcomes and tight coupling, the focus of attention decreases.
Model key:
Solid lines = positive relationships
Dash lines = negative relationships

Figure 1. Selectivity Theory, from (Lehman & Ramanujam, 2009)

Each of the contextual conditions and rule characteristics in Selectivity Theory alter the likelihood of a rule violation. Structural secrecy is one of the contextual conditions that affects the likelihood of a rule violation. According to Vaughan (1996), *structural secrecy* refers to “the way that patterns of information, organizational structures, processes, and transactions, and the structure of regulatory relations systematically undermine the attempt to know and interpret situations in organizations” (p. 647). Secrecy is created as the powers for regulating and complying with a rule are concentrated into a single organizational subunit (Kim et al., 2004). The concentration and isolation of rule related power into a single subunit minimizes potential conflicts related to and detection of a violation (Vaughan, 1996), which in turn decreases the perception of risk related to a rule violation. The decrease in the perception of risk thereby increases the likelihood of a rule violation (Lehman & Ramanujam, 2009).

Violation coupling is another contextual condition in Selectivity Theory. *Violation coupling* describes “the perceived likelihood that… violations will lead to known outcomes—either positive, such as a performance improvement, or negative, such as regulatory penalties” (Lehman & Ramanujam, 2009). When coupling is tight, outcomes of violations are well known and predictable, but when they are loose outcomes are unknown and unpredictable (Lehman & Ramanujam, 2009). The predictability caused by tight coupling allows organizational members to feel a sense of control over potential consequences (Shapira, 1997), which sense of control reduces the perception of risk and increases the likelihood of a rule violation (Lehman & Ramanujam, 2009).

However, when coupling is loose, outcomes of violations are not well known or predictable. The ambiguity associated with loose coupling leads organizational members to look to past actions to remedy organizational problems (Feldman & Pentland, 2003; March, 1997). If past solutions to a problem have resulted in rule violations, the ambiguity involved in loose coupling will leave organizational members unsure of the risk involved—prompting them to rely on the rule violating routines they have established previously (Lehman & Ramanujam, 2009).

Enforceability is a rule characteristic in Selectivity Theory that affects the likelihood of a rule violation. *Enforceability* is the extent to which organizations view regulatory agencies as able and likely to monitor compliance with a rule and seek justice for violations (Fuller et al., 2000). When opportunities to monitor an organization are high, organizational members perceive the risk of rule violation as high since the chances of detection are high. Similarly, the reduced control organizations have over the negative consequences that result from the regulatory intrusions increase the perception of risk and decrease the likelihood of a rule violation (Lehman & Ramanujam, 2009). Conversely, when opportunities to monitor an organization decrease, perceptions of risk decrease because organizations can more plausibly deny accusations (Gioia, 1992).

Procedural emphasis is another rule characteristic in Selectivity Theory. *Procedural emphasis* refers to whether the content of a rule emphasizes procedures over outcomes (Lange, 2008). When desired outcomes of a law are perceived as ambiguous, or procedural, organizational members seek to create interpretations of a rule, which interpretations over time become routine ways of responding to the rule (Lehman & Ramanujam, 2009). Once interpretations are routinized, organizational members feel a sense of predictability and control (March, 1997). This perceived predictability and controllability reduce perceptions of risk decrease, and thereby increase the likelihood of rule violations (Lehman & Ramanujam, 2009).

Rule connectedness is another rule characteristic presented in Selectivity Theory. *Rule connectedness* refers to the amount of interdependence or number of functional links a rule has with other rules (March et al., 2000). When rules are highly connected, coordination costs of violating a rule increase (Feldman & Pentland, 2003). Similarly, when multiple regulators exist or a rule system is complex, organizational members might feel less control over the domain of the rule (Lehman & Ramanujam, 2009). Multiple regulators also increases the likelihood of detection and sanctions (March & Shapira, 1987). The feeling of uncontrollability and the fear of sanctions increase the perception of risk involved in violating a rule and decrease the likelihood that a rule will be violated (Lehman & Ramanujam, 2009).

KEY ASSUMPTIONS OF SELECTIVITY THEORY

Lehman and Ramanujam (2009) explain that several key assumptions frame Selectivity Theory. We consider these assumptions carefully in adapting Selectivity Theory to our context. We categorize the assumptions and constraints into those dealing with rules, violations, and organizations. Table 1 summarizes the key assumptions that we leverage. The assumptions dealing with the rules themselves limit the direct extension of the model to other forms of social guidance or restraint, such as norms or standards. First, Selectivity Theory views rules as constraints on organizational members—not as moral principles that define social roles. Second, the scope of Selectivity Theory is on external formalized rules, such as laws; not on internal rules because they vary from organization to organization.

Table 1. Assumptions of Selectivity Theory that Pertain to SIPVHOM, from (Lehman & Ramanujam, 2009)

Category of Assumptions	Specific Assumption of the Model
Rules	Rules are viewed as constraints on organizational action and not as moral principles (p. 645)
	Rules must be external and formal, such as laws (p. 644).
	Rules must be low in ambiguity (p. 644).
Rule violations	Rule violations do not include individuals' violations for personal gain or sabotage (p. 644).
	Rule violations occur as the result of satisficing solutions, cause by limits to organizational attention, that presents themselves during the search for solutions to performance downfalls (p. 646).
	Rules violations will focus around critical organizational resources and the interests of powerful organizational coalitions (p. 647).
	Perceptions of the risk involved directly influences rule violations (p. 646).
Organizations	Dominant groups determine organizational actions predominantly (p. 646).
	Organizations are governed by an aspiration level (p. 646)
	The theoretical scope focuses only organizations that are vulnerable to committing violations, such as those experiencing organizational strain through performance downfalls or stiff competition (p. 646).

Third, Selectivity Theory is limited to rules that are reasonably low in ambiguity, which means that organizations will have similar interpretations of the rules (Lehman & Ramanujam, 2009). This does not mean that a rule must be completely clear; Selectivity

Theory accounts for some ambiguity in its procedural emphasis construct.

Moreover, several assumptions describe the organizational factors assumed in Selectivity Theory. First, organizational members join organizational coalitions that may have differing goals and perceptions of organizational situations and circumstances (March & Simon, 1958). The coalition(s) with access to more critical organizational resources have greater influence over organizational actions (Pfeffer & Salancik, 1978). Second, organizational actions are guided by an *aspiration level,* which is an expected level of future performance or achievement (Cyert & March, 1963). Third, when performance falls below the aspiration level, organizations become more risk tolerant and are more likely to violate a rule as they search for a solution to the performance problem (Lehman & Ramanujam, 2009). This assumption follows the logic of Strain Theory (Merton, 1938), which theory suggests that entities that cannot attain culturally desirable goals through legitimate means will seek to achieve the goals through deviant behaviors. Selectivity Theory therefore is constrained to organizations experiencing strain caused by sources such as performance decline, high competition, or heavy regulation.

The assumptions dealing with violations constrain to which objects Selectivity Theory extends and how the likelihood of violations comes about. First, because Selectivity Theory is concerned with organizational rule violations, the model does not explain or predict individuals' violations committed for personal gain or sabotage. Some constructs and principles clearly apply to individuals committing violation, but explaining the underlying phenomena requires an individual-level theory.

Second, as organizations begin to look for solutions to performance issues, organizational attention is limited (March & Simon, 1958), thus limiting the number of alternatives they can consider (Ocasio, 2002). Although not all alternatives will lead to rule violations (Lehman & Ramanujam, 2009), recent studies show that often these limited alternatives do lead to violations (Alexander & Cohen, 1996; Harris & Bromiley, 2007). For example, Harris and Bromiley (2007) conducted a study of firms that misrepresented financial statements from 1997-2002. They compared data of firms that committed financial fraud or misrepresentation with data of average performing firms in the same industries at during the same period. The results showed firms that misrepresented financial statements were more likely to be low performers in comparison to average performers.

Third, because organizational attention is limited, organizations will mainly focus their attention on rules affecting critical resources or interests of powerful organizational coalitions (Lehman & Ramanujam, 2009). This occurs because organizations seeking relief to performance downfalls frame solutions in terms of regaining and maintaining critical resources (Pfeffer, 1992).

Fourth, solutions to performance downfalls are filtered by the perceived risk of implementing each alternative (Shapira, 1997; Slovic, 2000). As solutions are perceived as more risky, the likelihood of a rule violation will decrease, and vice versa for solutions that are perceived as less risky (Lehman & Ramanujam, 2009).

PROPOSING SIPVHOM TO EXPLAIN SELECTIVITY IN RULE VIOLATIONS EXTENDED TO A HIPAA IT PRIVACY REGULATION CONTEXT

As mentioned, in recent years, HIT has become essential in the healthcare industry (Rivard et al., 2011) and is now widely used (Feldman & Horan, 2011). Forecasts also suggest a boom in the HIT market over the next several years (RNCOS, 2011a; RNCOS, 2011b; RNCOS, 2011c). To combat privacy violations in all domains, governments worldwide have or are beginning to establish laws to protect individuals' privacy. In the United States, a series of laws guards privacy partially. HIPAA and the HITECH Act have taken the role of protecting PHI in the US. In other parts of the world, single laws protect PHI and other types of protected information. For example, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) establishes guidelines for protecting the electronic distribution of all types of private data, including PHI. The same is true for the European Union Directive on Data Privacy (EUDDP) by the European Union. Besides laws, international privacy standards like ISO 17799 are being developed to deal with the privacy of personal information in information systems (Thomas & Botha, 2007). ISO 17799 is not specifically for health records, but the standard covers all personal information, including personal health records.

Organizations can jeopardize the privacy of patients' PHI in many ways. IT privacy violations can occur from basic monitor positioning or not encrypting patient data sent to doctors' cell phones. As illustration, a healthcare organization can fail to keep their some of their transaction logs, which is a HIPAA breach. An example of an IT privacy violation is demonstrated by the resolution agreement between HHS and UCLA (USDH&HS, 2011d). In this case, numerous people accessed medical records over several years (2005-2008) without authority or a reason to do so. A contrasting violation is reflected in the resolution agreement between HHS and Cignet Health (USDH&HS, 2011d). This was the first civil resolution with a monetary penalty (valued at $4.3 million). Cignet Health was fined for refusing patient requests to access their own personal medical records.

Excepting ISO 17799, the mentioned privacy laws fit well into Selectivity Theory's constraints and driving assumptions—allowing our adaptation of Selectivity Theory to SIPVHOM. For a review of the key assumptions of Selectivity Theory and SIPVHOM, see Table 1. First, HIPAA, PIPEDA, and EUDDP are external formalized laws that govern multiple organizations. Second, these laws and directives are relatively stable, limiting unreasonable amounts of ambiguity in the purpose of the laws. Third, a regulatory agency governs the laws and directives. For example, HHS regulates HIPAA, and the office of the privacy commissioner regulates PIPEDA. The regulatory powers given to these agencies help to create a perception of risk, one of the important driving forces in Selectivity Theory and SIPVHOM. Fourth, as with most organizations, healthcare organizations worldwide have dominant coalitions that guide organizational actions. Finally, frequently healthcare organizations worldwide experience organizational strain, from financial difficulties, strains of growth, and burdensome regulations. Another potential stressor of healthcare organizations that exchange information with other organizations (e.g. PHI data warehouses) is incompatible internal IT privacy policies, along with incompatible data storage and handling. If the policies do not match well, organizations may find it is too costly to fully comply with the corresponding group, leaving violations as an opportunity cost (Feldman & Horan, 2011).

In proposing SIPVHOM, we use HIPAA as a proxy for other healthcare privacy laws, though some adaptation may be necessary to account for cultural factors when studying related laws in other countries. HIPAA gives the United States Office for Civil Rights the authority and guidelines to protect a person's PHI (USDH&HS, 2011e). HIPAA is monitored and regulated by HHS, and provides federal US protections for PHI held by covered entities, giving patients an array of rights with respect to that information (USDH&HS, 2007). Section D of the HITECH Act extends HIPAA rules, particularly those related to HIT. The HITECH Act has guidelines for safeguarding electronic storage and transmission of PHI and gives HHS power to issue heavy fines for violation of any of HIPAA's rules.

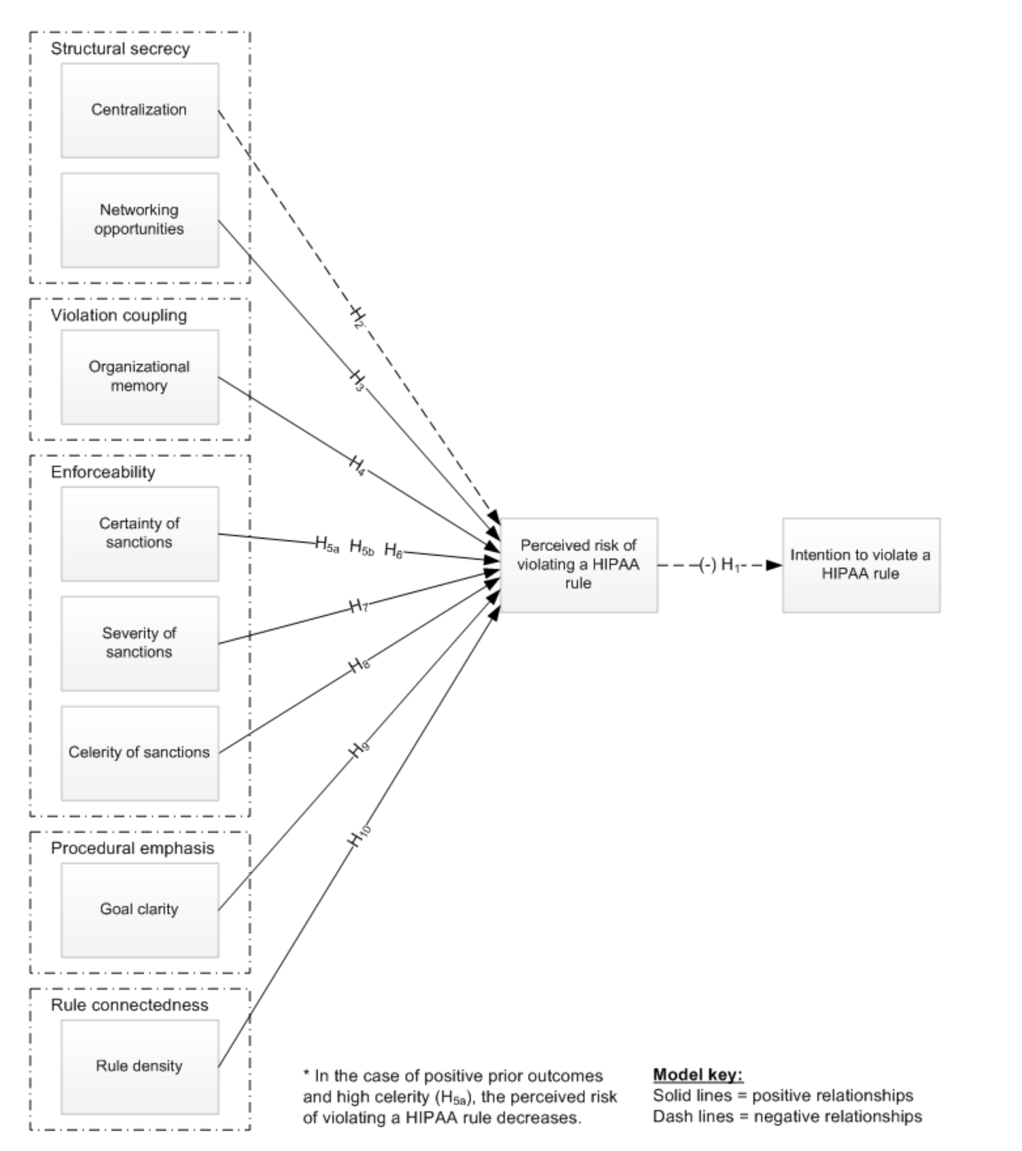
HIPAA is a useful surrogate for other privacy laws because it is standardized, formalized, used by a large population (Warkentin et al., 2011), and is quite expansive in its coverage. HIPAA consists of privacy rules, security rules, breach notification rules, and enforcement rules. The privacy rules outline appropriate uses and disclosures of PHI. The security rules establish appropriate administrative, physical, and technical measures to ensure the security of electronic PHI. The breach notification rules, an extension of HIPAA established by the HITECH Act, require healthcare organizations to provide timely notification of electronic breaches of unsecured PHI. The enforcement rules, also extended by the HITECH ACT, further establish provisions for conducting investigations of HIPAA violations and imposing fines. Importantly, HIPAA is also particular to healthcare, making it easier to isolate IT privacy violations by healthcare organizations.

EXTENDING PROPOSITIONS TO A HIPAA IT CONTEXT

SIPVHOM adopts the propositions proposed by Lehman & Ramanujam (2009) in Selectivity Theory, excepting the propositions which refer to focus of attention, to explain and predict IT privacy rule violations committed by healthcare organizations. SIPVHOM uses focus of attention as a driving axiom, but not as a construct. Beyond adopting Selectivity Theory’s propositions to a healthcare context, we further operationalize the propositions into a series of testable hypotheses. Appendix A provides several possible measures that might be useful in testing the hypotheses. We begin unfolding SIPVHOM by examining perceived risk as a predictor of the likelihood of IT privacy rule violations and offer testable hypotheses. We then discuss the contextual conditions and rule characteristics in SIPVHOM that affect the perceived risk of violating IT privacy rules. Figure 2 depicts SIPVHOM and its hypotheses.

Proposition 1: An increased perception of risk decreases the likelihood that a privacy rule will be selected for violation

An increase in the perceived risk associated with a rule violation will decrease the



* In the case of positive prior outcomes and high celerity (H_{5a}), the perceived risk of violating a HIPAA rule decreases.

Model key:
Solid lines = positive relationships
Dash lines = negative relationships

Figure 2. Selective Information Privacy Violations in Healthcare Organizations Model (SIPVHOM)

likelihood that the rule will be violated (Lehman & Ramanujam, 2009). Perceptions of risk "will vary across organizations, depending on their histories, structures, and cultures" (Lehman & Ramanujam, 2009). As organizations' members search for solutions to organizational strain, alternatives will be selected based on their perceived risk (Shapira, 1997; Slovic, 2000). Alternatives that involve a rule violation will be perceived as riskier to the extent that negative outcomes appear more certain, severe, and uncontrollable (March & Shapira, 1987). The more that a negative outcome is potentially threatening to the organization's legitimacy, the more risky it will seem (Zucker, 1977). As decision makers perceive an alternative resulting in a rule violation as riskier, they will be less likely to select the alternative and violate the rule (Lehman & Ramanujam, 2009).

To operationalize perceptions of risk and the likelihood of rule violations, we leverage research by Dinev & Hart (2006) and D’Arcy et al. (2009). Although most of the conceptualizations of risk in IS literature have focused on economic loss (Jarvenpaa et al., 2000; Pavlou, 2003; Pavlou & Geffen, 2004), Dinev and Hart (2006) show that risk can be conceptualized in other ways that may be more salient to situational factors. For example, they focus their study on *privacy risk* (the perceived uncertainty related to disclosing personal information) relative to individuals’ e-commerce purchasing behaviors. Importantly, for e-commerce purchasing behavior, conceptualizing risk as privacy risk “might be… more influential… than economic risk in dissuading individuals from conducting e-commerce transactions” (Dinev & Hart, 2006). Although this paper is not interested in privacy risk, nor e-commerce, the flexibility in selecting non-economic risk factors that are salient to healthcare organizations makes Dinev and Hart’s (2006) conceptualization of risk useful to the economically neutral description of risk proposed in SIPVHOM.

Dinev and Hart’s (2006) conceptualization of risk is also compelling because it links risk to behavioral intention. We suggest that the behavioral intention to violate a HIPAA rule is an appropriate operationalization for the likelihood of a HIPAA rule violation. The logical jump from the behavioral intention to violate a rule to the likelihood of a rule violation is not a big leap, because behavioral intention is often measured on a continuum (e.g., weak intention to strong intention) (e.g., D'Arcy et al., 2009; Johnston & Warkentin, 2010). This is the essence of the Theory of Reasoned Action (TRA) (Ajzen & Fishbein, 1980) and the Theory of Planned Behavior (TPB) (Ajzen, 1988). Thus, as intentions to violate weaken so does the likelihood of a rule violation. Importantly, behavioral intention has been widely used as a construct in IS research and—important to our study—in IS security research. For example, D'Arcy et al. (2009) use behavioral intention to account for individual's misuse of an organization's IS, such as privacy breaches or property damage. Like their study, we are interested in the misuse of privacy, but unlike their study, we are only interested in privacy violations. Since our study ultimately focuses on IT privacy rule violations, we make use of D'Arcy et al. (2009) IS misuse intention as a representation of the likelihood of a rule violation.

Similar to Lehman and Ramanujam (2009), Dinev and Hart (2006) suggest that perceptions of risk result from fear and uncertainty about negative consequences of actions. They further posit that concern about the perceived risk—an internalization of the potential negative consequences associated with an action—will lead to further uncertainty and thereby strengthen the effect of risk on behavioral intention. Lastly, they suggest that people will try to avoid perceived negative consequences. The desire to avoid negative consequences is consistent with expectancy theory (Van Eerde & Thierry, 1996; Vroom, 1964), which predicts that individuals act in ways that will minimize negative outcomes and maximize positive outcomes. Following this logic, decision makers in charge of HIPAA compliance will avoid alternatives to performance downfalls that result in a HIPAA rule violation to the extent that the consequences of violating the rule are perceived negatively. In summary,

> *H_1: An increase in the perceived risk of violating a HIPAA rule will decrease the intention of violating the rule.*

Proposition 2: Structural secrecy decreases perception of risk

Structural secrecy is a contextual condition that affects the likelihood of a privacy-rule violation. An increase in structural secrecy decreases the perception of risk and subsequently increases the likelihood that a rule will be violated (Lehman & Ramanujam, 2009). High secrecy occurs when roles and responsibilities for monitoring and complying with a rule are concentrated into a single subunit (Kim et al., 2004). This concentration of rule-related power into a single subunit can occur with the division of labor, organizational hierarchy, and job specialization that isolate knowledge of rule-related tasks (Vaughan, 1996). Furthermore, secrecy increases when the activities of the subunit are dissociated from other subunits (March & Simon, 1958). Informal relationships between members of subunits have been shown to have more influence on communication structures than formal relationships (Ghoshal et al., 1994). The increase in secrecy caused by the dissociation of subunits therefore could increase if the members of the subunit in charge of rule compliance are removed from informal networking structures as well as from formal structures. When secrecy is high, the isolation of rule-related power and knowledge helps to minimize potential conflicts related to and detection of a violation (Vaughan, 1996), which decreases the perception of risk related to a rule violation (Lehman & Ramanujam, 2009). Sharing the roles and responsibilities for monitoring and complying with a rule amongst organizational subunits can help to reduce secrecy (Lehman & Ramanujam, 2009).

Management or other dominant coalitions can foster structural secrecy to guard managerial interests and to protect critical resources that are vulnerable to external rules (Lehman & Ramanujam, 2009). In the practice of medicine, some of the most important organizational values and interests of dominant coalitions (e.g., doctors, nurses, hospital administrators) include the quality and efficiency of the care provided to patients (Grol, 2001; Schade et al., 2006; Teasdale, 2008), and a strong valuation of autonomy and status by physicians and other healthcare professionals (Rivard et al., 2011). Where HIPAA infringes on the quality or efficiency of care, or the autonomy or status of healthcare professionals, secrecy is likely to be high. HIPAA mandates that organizations must establish a system for monitoring and complying with HIPAA rules, but offers flexibility in the design of the regulatory system (USDH&HS, 2011d). Similarly, HHS does not actively monitor compliance (Administration, 2011). Together, these factors make designing an organizational regulatory system high in secrecy less detectable and more feasible for organizations governed by HIPAA.

In general, the healthcare industry—especially hospitals and clinics—are likely to be high in structural secrecy. Again, physicians value and seek for a high degree of autonomy in their work. In essence, a physician’s autonomy is parallel to isolating power into a single subunit. The extent to which physicians are granted full autonomy to make decisions regarding their patients and patient data fosters structural secrecy. The “clan” mentality shared by physicians also fosters secrecy. That is, physicians tend to rely heavily on the opinions of other physicians while ignoring opinions of external groups (Agarwal et al., 2007). Because physicians tend to ignore external influence, the “clan” mentality is parallel to being removed from informal communication structures, which further increases secrecy.

Similarly, private-sector medical organizations are more likely to hoard organizational resources than public sector organizations—leading to an increase in structural secrecy in private sector organizations. This notion receives support from the findings of Johnston and Warkentin (2008). They show that employees of public sector medical organizations are more likely to feel efficacy and support in their privacy compliance efforts than employees in private-sector medical organizations. This could be the case if public-sector medical organizations receive more resources (and oversight) to comply with rules like HIPAA. If true, private-sector medical organizations, would be more likely to engage in activities to protect critical organizational resources, and may therefore, intentionally create structural secrecy.

Organizations in the healthcare industry can reduce structural secrecy in several ways. For example, hospitals can establish inter-unit teams of administrators, doctors, and nurses dedicated to interpreting and monitoring HIPAA regulations. To take advantage of the “clan” mentality of physicians, hospital or clinic administrators might also seek to gain approval of highly regarded physicians, allowing these physicians to influence other physicians. Similarly, Nicholson and Smith (2007) looked at the impact of HIPAA and other policies that protect personal health information. They found that government policies such as HIPAA merely highlight the deficiencies inherent in medical record privacy systems. They suggest that the best approach to compliance is to emphasize education about the key issues within HIPAA: confidentiality and sensitivity. Organization-wide HIPAA training would likely reduce secrecy by creating a sense that HIPAA-related violations can be easily exposed to the entire organization.

Because no valid measure currently exists for structural secrecy, to operationalize the relationship between structural secrecy and perception of risk, we focus on operationalizations of communication structures. Communication structures have been shown to affect intra-organizational knowledge sharing (Tsai, 2002). *Communication structures* refer to the formal and informal structures that direct and regulate communication within an organization (Ghoshal et al., 1994; Tsai, 2002). Formal communication structures are those created by organizational hierarchy. Formal structures consist of centralization, formalization, and specialization (Miller & Droge, 1986; Van de Ven, 1976). Centralization, for example, is an important element in organizational structure and has been shown to be a parsimonious representation of formal structure (Ghoshal et al., 1994). According to Tsai (2002), centralization can create inefficiencies in the transfer of knowledge, and can also create an inactive role for subunits that do not hold decision-making authority. This inactive role may "reduce the initiatives that a [subunit] takes in" exchanging information with other subunits (Tsai, 2002, p. 181). These findings about centralization are consistent with the findings of (Kim et al., 2004) on secrecy. By obscuring information, centralization acts to create secrecy, and as predicted by Lehman and Ramanujam (2009), this will decrease perceptions of detection and the risk involved in violating a rule. Accordingly, healthcare organizations that centralize the power of monitoring and complying with HIPAA regulations will likely experience increased secrecy and decreased perceptions of risk. In summary,

> *H_2: An increase in the centralization of power related to HIPAA compliance will decrease the perceived risk associated with a HIPAA rule violation.*

Informal communication structures have also been shown to affect the transfer of knowledge (Tsai, 2002). In fact, informal structures can have more influence on communication than formal structures (Ghoshal et al., 1994). Informal communication structures are relationships that develop laterally or horizontally, rather than vertically as occurs in organizations with high centralization. Unlike centralization, informal relationships help to improve the exchange of information between organizational subunits (Homans, 1950), and can even give subunits access to other subunits and their resources (Gupta & Govindarajan, 1986). This exchange and access facilitates knowledge sharing (Tsai, 2002) and therefore decreases the likelihood of high structural secrecy. Hence, healthcare organizations that encourage lateral communication through informal relations with members of other subunits will experience an increase in knowledge sharing, thereby decreasing the chance of structural secrecy. In summary,

> *H_3: An increase in informal networking opportunities between a subunit in charge of HIPAA compliance and other subunits will increase the perceived risk associated with a HIPAA rule violation.*

Proposition 3: Violation coupling affects perception of risk

Violation coupling is another contextual condition that affects the violation likelihood of a privacy rule. When organizational members detect a tightly coupled connection between prior rule violations and the associated outcomes, perceptions of risk increase when the outcome is negative and decrease when the outcome is positive (Lehman & Ramanujam, 2009). When coupling is tight, organizational members perceive the outcome of a violation as predictable. Whereas, when coupling is loose, outcomes of a violation are ambiguous and not easily predicted (Lehman & Ramanujam, 2009). When coupling is tight and prior outcomes are positive, organizational members feel a sense of control over potential consequences (Shapira, 1997). Violations tightly coupled to positive outcomes, therefore, are less likely to be perceived as risky and are more likely to be repeated (Lehman & Ramanujam, 2009). However, when violations are tightly coupled to negative outcomes, the perception of risk increases (Holland, 1975) and the rule is less likely to be selected for violation (Lehman & Ramanujam, 2009).

Due to the complexity of organizations, however, loose coupling is far more prevalent than tight coupling (Lehman & Ramanujam, 2009). Some of the reasons for the pervasiveness of loose coupling include dissociation between the violators of a rule and those who experience the outcomes; the occurrence of violations and outcomes at different points in time; one violation leading to multiple outcomes; one outcome stemming from multiple causes; and a lack of organizational memory (Lehman & Ramanujam, 2009).

This situation may be particularly true with regard to HIPAA rules. First, the healthcare industry is very complex. The industry is highly fragmented with multiple players (Bentley et al., 2008). Second, HIPAA regulations allow organizations to outsource their data storage and other HIPAA regulated tasks (USDH&HS, 2003). By outsourcing, violations made by the outsourcer could be dissociated from the outcomes experienced by the organization or create a lack of organizational memory. Lastly, HHS does not monitor compliance of HIPAA, but asks that victims report abuses (Administration, 2011). If a delay occurs between a HIPAA privacy violation and the time that a patient reports the abuse or HHS commences an investigation, loose coupling is possible.

When an organization cannot detect a tightly coupled connection between prior rule violations and the associated outcomes, perceptions of risk decrease (Lehman & Ramanujam, 2009). The ambiguity resulting from loose coupling drives an organization to identify agreeable interpretations of an outcome, which interpretations are not necessarily correct (Weick, 1995). Organizations often fulfill this need by looking to past actions and rely on previous alternatives to remedy problems (Feldman & Pentland, 2003; March, 1997). Similarly, to validate prior decisions, organizational members may construe outcomes in a self-justifying manner (March, 1997). If an organization has previously violated a rule, due to the ambiguity caused by loose coupling and the ease of relying on past alternatives, the risk of violating the rule again may not be easily discernible (Lehman & Ramanujam, 2009). Healthcare organizations may be more likely to experience loose coupling. For example, HIPAA has a self-reporting and patient-reporting mechanism (Administration, 2011), and if neither is activated, then a violation may never be detected and lead to bad habits or policy work around.

To operationalize violation coupling, we focus on one of the conditions that creates loose coupling—lack of organizational memory. *Organizational memory* refers to the "collective beliefs, behavioral routines, or physical artifacts that vary in their content, level, dispersion, and accessibility" (Moorman & Miner, 1997). As suggested in this definition, multiple forms of organizational memory exist, including beliefs, behavioral routines and procedures, and physical artifacts such as organizational structure. In healthcare organizations, organizational memory might manifest itself through beliefs and values such as quality of care. Concerning IT privacy violations, organizational memory might manifest itself in policies and procedures on using computer systems to minimize HIPAA violations. As suggested above, perceptions of risk decrease as the organizational memory on violation outcomes diminishes. Since violations are primarily actions, we focus our study of organization memory primarily on behavioral routines and procedures rather than on beliefs and values or physical artifacts.

Organizational memory can affect violation coupling in several ways. First, the dispersion of organizational memory may not be widely accepted (Moorman & Miner, 1997). Certain organizational subcultures, for example, might be slow to adopt organizational memory (Cohen & Levinthal, 1990; Deshpande & Frederick E. Webster, 1989; Martin & Siehl, 1983; Smircich, 1983). In hospitals, three main groups exist with separate values—nurses, doctors, and administrators (Rivard et al., 2011). Each group has different views on the organization and on violations of HIPAA. In general, administrators feel the greatest need to comply with HIPAA rules, whereas doctors and nurses may see the rules as hindrances to the quality or efficiency of providing care to patients. Similarly, administrators feel a greater self-efficacy to comply than do medical staff (Johnston & Warkentin, 2008).

Nurses and doctors thus might have less organizational memory of HIPAA compliance procedures and are more likely to violate them. This may be particularly true for physicians if the "clan" mentality held amongst physicians is opposed to HIPAA or HITECH

Act regulations. Venkatesh et al. (2011) show that a physician's professional network has a negative effect on the use of e-healthcare systems. Physicians, therefore, may be opposed to the goals of the HITECH Act. However, if the "clan" mentality is leveraged to promote compliance with privacy laws, HIPAA- and HITECH-related organizational memory may improve. When organizational memory of HIPAA related procedures and outcomes are widely dispersed, the salience of HIPAA violations and the associated outcomes are likely to rise. This is turn will create the outcome-based risk perceptions predicted by Lehman and Ramanujam (2009). In summary,

> *H_{4a}: When the dispersion of organizational memory of HIPAA related information is low, prior HIPAA violations will decrease the perception of risk despite the prior outcomes associated with a HIPAA rule violation.*
>
> *H_{4b}: When the dispersion of organizational memory is high, prior HIPAA violations with positive outcomes will decrease the perception of risk associated with a HIPAA rule violation.*
>
> *H_{4c}: When the dispersion of organizational memory is high, prior HIPAA violations with negative outcomes will increase the perception of risk associated with a HIPAA rule violation.*

Third, the accessibility to organizational memory may be restricted (Moorman & Miner, 1997). Lehman and Ramanujam (2009) suggest that organizations may seek to increase structural secrecy by isolating information about monitoring of and compliance with a rule in order to create opportunities for violation. They explain that this may be particularly true for rules that inhibit the pursuit or maintenance of critical organizational resources (Lehman & Ramanujam, 2009). Similarly, they suggest that organizational structures can create secrecy by isolating compliance and monitoring responsibilities into a single organizational subunit. Ultimately, structural secrecy minimizes the amount of organizational knowledge about a given subject distributed to other parts of the organization. When organizations isolate information—on purpose or unintentionally through the design of organizational structures—the accessibility to organizational memory is likely to decrease. In summary,

> *H_{5a}: When structural secrecy is high, prior HIPAA violations will decrease the perception of risk despite the prior outcomes associated with a HIPAA rule violation.*
>
> *H_{5b}: When structural secrecy is low, prior HIPAA violations with positive outcomes will decrease the perception of risk associated with a HIPAA rule violation.*
>
> *H_{5c}: When structural secrecy is low, prior HIPAA violations with negative outcomes will increase the perception of risk associated with a HIPAA rule violation.*

Proposition 4: Enforceability increases perception of risk

The enforceability of a privacy rule is a rule characteristic that affects the likelihood of rule violation. An increase in the enforceability of a rule increases the perception of risk, making a rule less likely to be violated (Lehman & Ramanujam, 2009). Enforceability is high when regulatory agencies are able to frequently monitor the actions of an organization, which is most likely to occur when the regulatory agency and the organization are highly interdependent (Edelman, 1992). Enforceability also increases when the social consequences for seeking justice for violations are low (Fuller et al., 2000). This is likely to occur when a regulatory agency "exert[s] strong influence on [an] organization" (Lehman & Ramanujam, 2009). However, to avoid alienating powerful constituencies, regulatory agencies do not always exert their full influence (Edelman & Suchman, 1997). When chances to monitor an organization are high, enforceability increases the perceived risk of violating a rule by increasing the chances of detection and reducing the control organizations have over the negative consequences that can result from a rule violation (Lehman & Ramanujam, 2009). In contrast, when chances to monitor an organization decrease, perceptions of risk decrease because organizations are better able to deny accusations plausibly (Gioia, 1992) and increase control by creating symbolic compliance (Edelman, 1992).

To operationalize enforceability, we rely on deterrence theory. Deterrence theory comes from criminology research, but IS security research has also recently applied this theory to information security policy compliance research (e.g., D'Arcy et al., 2009; Qing et al., 2011; Siponen & Vance, 2010). Deterrence theory states that perceptions of sanctions designed to punish violators deters individuals from deviant behavior. Research has looked at multiple characteristics of sanctions in inducing deterrence, including the severity of sanctions, the certainty of sanctions, and the celerity of sanctions. *Severity of sanctions* refers to “the perceived degree of punishment for [an] intended act” (Qing et al., 2011, p. 57). *Certainty of sanctions* refers to “the perceived probability of being punished for [an] intended act” (Qing et al., 2011, p. 57). *Celerity of sanctions* refers to “the perceived swiftness of being punished for [an] intended act (Qing et al., 2011, p. 57). Much debate exists about the strength and importance of each of these characteristics, and some contradictory findings exist with regard to deterrence theory in general. For example, D’Arcy et al. (2009) found evidence that severity of sanctions is more effective in deterring deviant behavior than the certainty of sanctions, whereas Nagin and Pogarsky (2001) did not. Qing et al. (2011) also found no evidence of deterrence effects. We do not take issue with these findings, but instead rely on the theoretical basis of deterrence theory to explain how sanctions might affect risk perceptions in decision makers.

The certainty of sanctions and the severity of sanctions create a sense of fear, which acts to deter IS violations (D'Arcy et al., 2009). Both enforceability as proposed in Selectivity Theory and the certainty and severity of sanctions, as proposed in deterrence theory, suggest that fear of negative outcomes reduces the likelihood of deviant behaviors. Again, the desire to avoid negative consequences is consistent with expectancy theory (Van Eerde & Thierry, 1996; Vroom, 1964).

Currently, HIPAA does not directly monitor organizational actions, but relies instead on victims to report violations (Administration, 2011). According to Miller and Sarat (1981), when victims are left to report abuses, laws are more likely to be abused than when the rules are monitored by third-party agencies. Additionally, few documented cases of regulatory sanctions for HIPAA violations exist. In fact, as of 2008, the HHS reported that it had received over 33,000 complaints pertaining to privacy violations but no fines had been levied (Insider, 2008). The lack of previous negative outcomes makes HIPAA penalties appear to be unlikely and uncertain. In summary,

> *H_6: An increase in the certainty of sanctions for a HIPAA rule violation will increase the perceived risk associated with the HIPAA rule violation.*

However, despite the uncertainty of sanctions related to HIPAA violations, some financial settlements exist, including a $2.25 million settlement by CVS for not disposing of records correctly and a $1 million settlement made by RiteAid for improperly disposing of pill bottles and labels (USDH&HS, 2011a; USDH&HS, 2011e). Similarly, with the advent of the HITECH Act, stiff penalties are increasingly common—such as a $1 million fine assessed to Massachusetts General Hospital and a $4.3 million fine to Cignet Healthcare. For these organizations, repeat offenses would be less likely due to an increase in the perceived risk created by severe fines and settlements. In summary,

> *H_7: An increase in the severity of sanctions for a HIPAA rule violation will increase the perceived risk associated with the HIPAA rule violation.*

Lastly, the celerity of sanctions decreases deviance. However, celerity has been shown to be the weakest characteristic of sanctions (Nagin & Pogarsky, 2001). Pavlovian conditioning is the basis of celerity—particularly the conditioning of responses by timely negative reinforcement. This conditioning was predicted for animals, and humans “possess a far greater cognitive capacity than do animals for connecting acts with temporally remote consequences" (Nagin & Pogarsky, 2001, p. 867). Nonetheless, to be consistent with deterrence theory in its entirety we present celerity in the model. In comparison to other government sanctions, HIPAA sanctions may be particularly slow to occur. As suggested above, HIPAA violations are self-reported and any delay in a patient reporting violations will decrease celerity. Similarly, many reported abuses are resolved before HHS can even find the time to start an investigation. Given this information, we offer the following hypothesis:

> *H_8: An increase in the celerity of sanctions for a HIPAA rule violation will increase the perceived risk associated with the HIPAA rule violation.*

Proposition 5: Procedural emphasis decreases perception of risk

Procedural emphasis is another rule characteristic that affects the likelihood of a privacy rule violation. An increase in procedural emphasis decreases the perception of risk, and subsequently increases the likelihood of a rule violation (Lehman & Ramanujam, 2009). When procedural emphasis is high, the desired outcomes of a rule are ambiguous. Whereas, when it is low, a rule is unambiguous and desired outcomes are clearly defined (Edelman, 1992). According to Lehman and Ramanujam (2009), organizational interpretations of a rule in situations where procedural emphasis is high can lead to a routinized interpretation of the rule that holds true even in unambiguous situations. This occurs through the managerialization of law "wherein legal ideas are refigured by managerial ways of thinking as they flow across the boundaries of legal fields and into managerial and organizational fields" (Edelman et al., 2001, p. 1589). Interpretations of rules tend to be guided by the pursuit of critical, organizational resources (Lehman & Ramanujam, 2009). Power struggles about the interpretations of a rule create emerging meaning (Pfeffer, 1992). The meaning is legitimized by powerful organizational members to favor their particular interpretations (Johnson et al., 2006), which interpretations become stabilized methods for maintaining and acquiring critical resources (Lehman & Ramanujam, 2009). As interpretations of rules stabilize and become routinized, organizational members view them as predictable and controllable (March, 1997). The routinized interpretations cause perceptions of risk to decrease, even in unambiguous situations (Lehman & Ramanujam, 2009).

In the healthcare industry, one power struggle for interpreting HIPAA rules manifests as a struggle between administrators and physicians over the degree of physician autonomy in complying with HIPAA. Due to the physician “clan” mentality, physicians are likely to interpret HIPAA rules in a self-interested manner that minimizes encroachments on physician autonomy and maximizes the efficiency and quality of care they can provide to patients.

We propose goal clarity as a useful surrogate to procedural emphasis. *Goal clarity* refers to the extent to which a goal designates a clear course of action and provides information about how to achieve the goal (Tziner et al., 1993). When the goal clarity of a rule is high, the rule’s expected outcomes are defined clearly. As predicted by Lehman and Ramanujam (2009), when outcomes are clearly defined ambiguity will be low—making plausible deniability less likely and perceived risk high. Currently, many of HIPAA’s rules are flexible and allow for interpretations, calling for “reasonable” actions (USDH&HS, 2008). Similarly, the interpretations of HIPAA rules are continually evolving (Wipke-Tevis & Pickett, 2008). These circumstances make certain HIPAA rules lower in goal clarity and higher in procedural emphasis—increasing violation likelihood. In summary,

> *H_9: An increase in the goal clarity of a HIPAA rule will decrease the perception of risk associated with the rule.*

Proposition 6: Rule connectedness increases perception of risk

Rule connectedness is another rule characteristic that affects the likelihood of a privacy rule violation. An increase in rule connectedness will increase perceptions of risk and thereby decrease the likelihood of a rule violation (Lehman & Ramanujam, 2009). When connectedness is high, a rule has many interdependent rules. Whereas, when connectedness is low, a rule has no interdependent rules, or only a few (Lehman & Ramanujam, 2009). Connectedness increases perceived risk in two ways. First, coordination costs increase when rules are highly connected (Feldman & Pentland, 2003). Second, when multiple regulators exist or the rule system is complex, organizational members may feel less control (Lehman & Ramanujam, 2009), which increases the likelihood of detection and sanctions (March & Shapira, 1987). The increase in coordination costs and likelihood of detection increase the perception of risk involved in violating a rule.

Several factors can establish high rule connectedness. First, complex work may require more interdependencies between rules to help govern the complexity (Scott, 2002). Similarly, multiple governing bodies may issue interdependent rules in a complex environment where each agency participates in regulation (Landau, 1969). Additionally, large-scale crises may induce the creation of interdependent rules (Collins et al., 2005; March et al., 2000). Rule connectedness can also increase purposefully when rules or governing agencies are strategically created to ensure conformity (Lehman & Ramanujam, 2009).

Furthermore, we argue that in an IT context, the advent of new technology can lead to the creation of new rules. For example, the ubiquity of HIT in the healthcare industry prompted legislators to create the HITECH Act. The act was created to encourage the meaningful use and adoption of HIT (USDH&HS, 2011c). Subtitle D of the HITECH Act micromanages the details surrounding the electronic transmission of PHI and now adds civil and criminal penalties for violations (USDH&HS, 2011c). The introduction of HITECH Act will likely reduce the likelihood of future HIPAA violations relative to the growth of HIT.

Lastly, we argue that global connections between physicians may increase rule connectedness. For example, European nations are attributed with being more concerned with patient privacy than nations like the US. To the extent that highly respected physicians in Europe with pro-privacy ideals associate with physicians in other parts of the world, the influence of European privacy ideals may spread to other parts of the world, thereby increasing perceptions of rule connectedness.

To operationalize rule connectedness we rely on Sullivan's (2010) measure of rule density. Like Lehman and Ramanujam (2009), Sullivan (2010) shows how organizational attention can affect rules. Selectivity Theory uses organizational attention to describe how rules that are highly connected draw attention. Conversely, Sullivan (2010) uses organizational attention to describe how regulating bodies focus attention on certain problems to create new rules in a rule domain. In essence, both authors are investigating the number of related rules. Therefore, rule density serves as an excellent measure for rule connectedness. In summary,

> *H_{10}: An increase in the rule density of a HIPAA rule will increase the perceived risk of violating the rule.*

DISCUSSION

Given the many problems that healthcare institutions face in regard to compliance with IT medical privacy laws, this paper proposed SIPVHOM (see Figure 2), which is a model developed to explain and predict violations of IT privacy rules. In particular, we use HIPAA as a proxy for IT privacy violations. IT privacy violations are of particular importance because of the ubiquity of the electronic transfer and display of protected medical information (HIMSS, 2010). Although we selected HIPAA as a surrogate privacy law to create a seamless story for SIPVHOM, the model can also help to predict organizational compliance with similar privacy laws—such as PIPEDA in Canada or EUDDP.

SIPVHOM is based primarily on Selectivity Theory (Lehman & Ramanujam, 2009), a model proposed to predict selectivity in organizational rule violations. Like Selectivity Theory, SIPVHOM suggests that a series of contextual conditions and rule characteristics affect the perception of risk involved in violating a rule, and thereby, the likelihood that a rule will be selected for violation. We offer testable hypotheses of the propositions of Selectivity Theory contextualized to HIPPA. With the recent adoption of the HITECH Act in the US and its role in allowing the first significant fines for HIPAA violations starting in 2011, we offer a timely investigation of the topic of medical privacy laws. In the future, SIPVHOM can help explain the likely changes in compliance due to the advent of the HITECH Act. Ultimately, we believe SIPVHOM can help to inform the creation and reform of privacy laws and the structuring of the regulatory environments that govern them and the organizations that must follow them.

Although the focus of this paper has been on healthcare organizations, researchers can likely extend SIPVHOM to other related domains. As illustration, credit card fraud is a colossal issue for consumers, credit-card companies, and credit-card issuing banks. Few formalized, external rules exist to mandate how organizations should deal with the electronic transfer of credit card data; however, a sort of private ordering has emerged in the credit card industry. The industry has created a form of external control through the Payment Card Industry Data Security Standard (PCI DSS). Although not a traditional law, PCI DSS contains many of the same qualities of a formalized law that make Selectivity

Theory and SIPVHOM ideal models to explain and predict violations of PCI DSS. The listed core assumptions of SIPVHOM are the primarily constraints that researchers should consider for such an extension. Nonetheless, further theoretical development could neutralize many of the limiting assumptions. For example, researchers could likely apply many of the concepts of SIPVHOM to an individual context by substituting organizational theories with individual-level psychological theories.

LIMITATIONS AND FUTURE RESEARCH

The primary limitation of SIPVHOM is that it has not been empirically tested (neither has Selectivity Theory). To help facilitate the future testing of SIPVHOM, we thus briefly address ways researchers might operationalize and test its constructs. In doing so, it is important to note that multiple measures exist for some of the constructs; thus, using discretion is pivotal in selecting the most appropriate and representative measures to maximize construct validity. Some of the constructs also do not have closely associated measures from the literature, which makes opertionalization more challenging. For these constructs, we suggest possible measurement surrogates. Appendix A summarizes these possibilities.

In terms of testing, preliminary studies could test the hypotheses through scenarios-based approach where working professionals receive hypothetical vignettes to test the underlying theory. This approach has several advantages when dealing with topics with which participants do not want to disclose their individual involvement in and knowledge of the organization's violations, and has been effectively used in IS compliance research (e.g., Hu et al., 2011; Siponen & Vance, 2010). Testing can then evolve to more challenging field studies of actual organizations that are required to follow HIPAA. More complex testing could also potentially use large samples of randomly selected organizations and randomly selected individuals within these organizations. Finally, organizations from different cultures and with different HIPAA-like regulations would be useful to study. A study of SIPVHOM focused on organizational culture could also be useful because the interplay between doctors, nurses, and administrators has been shown to be important in daily hospital life (Rivard et al., 2011).

Another limitation of SIPVHOM includes the lack of predictive and explanative power with regard to organizations performing at or above their aspiration levels, and internal rules and regulations. Again, part of SIPVHOM's foundation is Merton's Strain Theory (1938), which is leveraged to suggest that organizations that cannot obtain socially desirable goals through legitimate means might seek to fulfill their goals through deviant behavior. This theoretical foundation limits the predictive power of our model to those organizations that cannot attain their aspiration level. SIPVHOM is also restricted to predicting external formalized rules, and does not extend to social norms related to privacy, or internal regulations of organizations. Because social norms are unregulated in the same manner as formalized rules, they do not fit SIPVHOM well, and the nuances in the differences between internal rules and regulations would likely pose a problem in showing selectivity of rule violations at an organizational level.

Similarly, Selectivity Theory suggests that organizational attention is an important mediating construct in explaining violations, but the evidence and discussion of focus of attention is scant in Lehman and Ramanujam's (2009) article. For this reason, SIPVHOM does not apply focus of attention as a construct, but instead uses the concept as an axiom to describe certain aspects of the model. Future research can revisit and further build the link to organizational attention.

Finally, it could be beneficial to study SIPVHOM in the context of multiple privacy laws. For example, HIPAA, PIPEDA, or EUDDP could be examined together to determine if the rule characteristics or contextual conditions related to the laws cause differences in the frequency or severity of violations. Importantly, future studies could also look at HIPAA violations and mobile technology, since many current uses of mobile technology used by doctors and nurses are breaches of HIPAA rules. Lastly, future studies might further explore the role of organizational attention on IT privacy rule violations.

CONCLUSION

The explosive growth of HIT in the healthcare industry and the number of HIPAA violations reported each year demonstrate a need for healthcare organizations to improve HIPAA-regulation compliance. Unless changes in regulatory environments and organizational structures change dramatically for the better, HIPAA violations are likely to worsen. Fortunately, SIPVHOM offers a way to explain and predict organizational violations of IT privacy rules, including HIPAA. The model and recommendations presented in this paper could help to improve regulatory environments and organizational structures by showing where the deficiencies and vulnerabilities in the current healthcare delivery system lie.

BIBLIOGRAPHY

Administration, N. A. R. (2011, 10 FEB 2011). *Electronic Code of Federal Regulations - Title 45*. Retrieved FEB 13, 2011, from http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=78dff1c5c9198f68cadfc53895bb373d&rgn=div6&view=text&node=45:1.0.1.3.75.4&idno=45

Agarwal, R., Mishra, A., Angst, C., and Anderson, C. L. (2007, December 9-12), "*Digitizing healthcare: The ability and motivation of physician practices and their adoption of electronic health record systems,"* 2007 International Conference on Information Systems, Montreal, Canada, pp. 1-17.

Ajzen, I. (1988). *Attitudes, Personality and Behavior*. Chicago, Illinois, USA: Dorsey Press.

Ajzen, I. and Fishbein, m. (1980). *Understanding Attitudes and Predicting Social Behavior* (Vol. 278). Englewood Cliffs, New Jersey, USA: Prentice-hall.

Alexander, C. R. and Cohen, M. A. (1996), "New evidence on the origins of corporate crime," *Working Papers, U.S. Department of Justice-Antitrust Division* 17(4), pp. 421-435.

Anderson, C. L. and Agarwal, R. (2011), "The digitalization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information," *Information Systems Research* 22(3), pp. 469-490.

Aron, R., Dutta, S., Janakiraman, R., and Pathak, P. A. (2011), "The impact of automation of systems on medical errors: Evidence from field research," *Information Systems Research* 22(3), pp. 419-428.

Atwater, L. E., Waldman, D. A., Carey, J. A., and Cartier, P. (2001), "Recipient and observer reactions to discipline: Are managers experiencing wishful thinking?," *Journal of Organizational Behavior* 22(3), pp. 249-270.

Bentley, T. G. K., Effros, R. M., Palar, K., and Keeler, E. B. (2008), "Waste in the U.S. healthcare system: A conceptual framework," *The Milbank Quarterly* 86(4), pp. 629-659.

Bhattacherjee, A., Menachemi, N., Kayhan, V., and Brooks, R. (2007), "The differential performance effects of healthcare information technology adoption," *Information Systems Management* 24(1), pp. 5-14.

Burkhard, R., Schooley, B., Dawson, J., and Horan, T. (2010), "Information systems and healthcare XXXVII: when your employer provides your personal health record--exploring employee perceptions of an employer-sponsored PHR system," *Communications of the Association for Information Systems* 27(19), pp. 323-338.

Cohen, W. M. and Levinthal, D. A. (1990), "Absorptive capacity: A new perspective on learning and innovation," *Administrative Science Quarterly* 35(September), pp. 128-152.

Collins, D. W., Gong, G., and Li, H. (Eds.). (2005), "*The Effect of the Sarbanes-Oxley Act on the Timing Manipulation of CEO Stock Option Awards."* Iowa City, Iowa, USA: University of Iowa.

Connell, N. A. D. and Young, T. P. (2007), "Evaluating healthcare information systems through an enterprise perspective," *Information & Management* 44(4), pp. 433-440.

Cyert, R. M. and March, J. G. (1963). *A Behavioral Theory of the Firm*. Englewood Cliffs, New Jersey, USA: Prentice Hall.

D'Arcy, J., Hovav, A., and Galletta, D. (2009), "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," *Information Systems Research* 20(1), pp. 79-98.

Deshpande, R. and Frederick E. Webster, J. (1989), "Organizational culture and marketing: Defining the research agenda," *Journal of Marketing* 53(January), pp. 3-15.

Dinev, T. and Hart, P. (2006), "An extended privacy calculus model for e-commerce transactions," *Information Systems Research* 17(1), pp. 61-80.

Edelman, L. B. (1992), "Legal ambiguity and symbolic structures: Organizational mediation of civil rights law," *American Journal of Sociology* 97(6), pp. 1531-1576.

Edelman, L. B., Fuller, S. R., and Mara-Drita, I. (2001), "Diversity rhetoric and the managerialization of law," *American Journal of Sociology* 106(6), pp. 1589-1641.

Edelman, L. B. and Suchman, M. C. (1997), "The legal environments of organizations," *Annual Review of Sociology* 23(1997), pp. 479-515.

Feldman, M. S. and Pentland, B. T. (2003), "Reconceptualizing organizational routines as a source of flexibility and change," *Administrative Science Quarterly* 48(1), pp. 94-118.

Feldman, S. S. and Horan, T. A. (2011), "The dynamics of information collaboration: A case study of blended IT value propositions for health information exchange in disability determination," *Journal of the Association for Information Systems* 12(February), pp. 189-207.

Fuller, S. R., Edelman, L. B., and Matusik, S. F. (2000), "Legal readings: Employee interpretation and mobilization of law," *Academy of Management Review* 25(1), pp. 200-216.

Gerlach, J. H., Kuo, F. B., and Lin, C. S. (2009), "Self sanction and regulative sanction against copyright infringement: a comparison between U.S. and China college students," *Journal of the American Society for Information Science & Technology* 60(8), pp. 1687-1701.

Ghoshal, S., Korine, H., and Szulanski, G. (1994), "Interunit communication in multinational corporations," *Management Science* 40(1), pp. 96-110.

Gioia, D. A. (1992), "Pinto fires and personal ethics: A script analysis of missed opportunities," *Journal of Business Ethics* 11(5-6), pp. 379-389.

Grol, R. (2001), "Improving the quality of medical care: Building bridges among professional pride, payer profit, and patient satisfaction," *Journal of the American Medical Association* 286(20), pp. 2578-2585.

Gupta, A. K. and Govindarajan, V. (1986), "Resource sharing among SBUs: Strategic antecedents and administrative implications," *Academy of Management Journal* 29(4), pp. 695-714.

Harris, J. and Bromiley, P. (2007), "Incentives to cheat: The influence of executive compensation and firm performance on financial misrepresentation," *Organizational Science* 18(3), pp. 350-367.

HIMSS. (2010, Last update date: November 3). *2010 HIMSS Security Survey Sponsored by Intel*. Retrieved August 31, 2011, from http://software.intel.com/en-us/articles/HIMSS-Security-Survey/, pp. 1-22.

Holland, J. H. (1975). *Adaptation in Natural and Artificial Systems*. Cambridge, Massachusetts, USA: MIT Press.

Homans, G. C. (1950). *The Human Group*. New York, NY, USA: Harcourt, Brace, and World.

Horowitz, B. T. (2010, Last update date: Nov. 18, 2010). *Data breaches cost health care industry $6 billion annually*: CMS Wire. Retrieved August 31, 2011, from http://www.cmswire.com/cms/information-management/data-breaches-cost-the-healthcare-industry-up-to-us6-billion-annually-009305.php, pp. 1-4.

Hu, Q., Xu, Z., Dinev, T., and Ling, H. (2011), "Does deterrence work in reducing information security policy abuse by employees?," *Communications of the ACM* 54(6), pp. 54-60.

Insider, E. (2008), "Related to: HIPAA Privacy Rule: 33,000 complaints, no fines," *Optometry* 79(7), pp. 405-407.

Jarvenpaa, S. L., Tractinsky, N., and Vitale, M. (2000), "Consumer trust in an internet store," *Information Technology and Management* 1(12), pp. 45-71.

Johnson, C., Dowd Timothy, J., and Ridgeway Cecilia, L. (2006), "Legitimacy as a social process," *Annual Review of Sociology* 32(2006), pp. 53-78.

Johnston, A. C. and Warkentin, M. (2008), "Information privacy compliance in the healthcare industry," *Information Management & Computer Security* 16(1), pp. 5-19.

Johnston, A. C. and Warkentin, M. (2010), "Fear appeals and information security behaviors: An empirical study," *MIS Quarterly* 34(3), pp. 549-566.

Kane, G. C. and Labianca, G. (2011), "IS avoidance in health-care groups: a multilevel investigation," *Information Systems Research* 22(3), pp. 504-522.

Kim, H., Hoskisson, R. E., and Wan, W. P. (2004), "Power dependence, diversification strategy, and performance in keiretsu member firms," *Strategic Management Journal* 25(7), pp. 613-636.

Landau, M. (1969), "Redundancy, rationality, and the problem of duplication and overlap," 29(4), pp. 346-358.

Lange, D. (2008), "A multidimensional conceptualization of organizational corruption control," *Academy of Management Review* 33(3), pp. 710-729.

Lehman, D. W. and Ramanujam, R. (2009), "Selectivity in organizational rule violations," *Academy of Management Review* 34(4), pp. 643-657.

Leon, L., Abraham, D., and Kalbers, L. (2010), "Beyond regulatory compliance for spreadsheet controls: A tutorial to assist practitioners and a call for research," *Communications of the Association for Information Systems* 27(28), pp. 541-560.

March, J. G. (1997), "Understanding how decisions happen in organizations," In Z. Shapira (Ed.), *Organizational decision making* (pp. 9-32). New York, NY, USA: Cambridge University Press.

March, J. G., Schulz, M., and Zhou, X. (2000). *The Dynamics of Rules: Change in Written Organizational Codes*. Stanford, CA, USA: Stanford University Press.

March, J. G. and Shapira, Z. (1987), "Managerial perspectives on risk and risk taking," *Management Science* 33(11), pp. 1404-1418.

March, J. G. and Simon, H. A. (1958). *Organizations*. Oxford, UK: Wiley.

Martin, J. and Siehl, C. (1983), "Organizational culture and counter culture: An uneasy symbiosis," *Organizational Dynamics* 12(Autumn), pp. 52-64.

Merton, R. K. (1938), "Social Structure and Anomie," *American Sociological Review* 3(5), pp. 672-682.

Miller, D. and Droge, C. (1986), "Psychological and traditional detriments of structure," *Administrative Science Quarterly* 31(4), pp. 539-560.

Miller, R. E. and Sarat, A. (1981), "Grievances, claims, and disputes: Assessing the adversary culture," *Law and Society Review* 15(3/4), pp. 525-566.

Moorman, C. and Miner, A. S. (1997), "The impact of organizational memory on new product performance and creativity," *Journal of Marketing Research* 34(February), pp. 91-106.

Nagin, D. S. and Pogarsky, G. (2001), "Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: Theory and evidence," *Criminology* 39(4), pp. 865-892.

Nicholson, S. and Smith, C. A. (2007), "Using lessons from health care to protect the privacy of library users: Guidelines for the de-identification of library data based on HIPAA," *Journal of the American Society for Information Science and Technology* 58(8), pp. 1198-1206.

Ocasio, W. (1997), "Towards an attention-based view of the firm," *Strategic Management Journal* 18(Summer Special Issue), pp. 187-206.

Ocasio, W. (2002), "Organizational power and dependence," In J. C. Baum (Ed.), *Companion to organizations* (pp. 263-285). Oxford, UK: Blackwell.

Ozdemir, Z., Barron, J., and Bandyopadhyay, S. (2011), "An analysis of the adoption of digital health records under switching costs," *Information Systems Research* 22(3), pp. 491-503.

Pavlou, P. A. (2003), "Consumer Acceptance of electronic commerce: Integrating trust and risk with the Technology Acceptance Model," *International Journal of Electronic Commerce* 7(3), pp. 101-134.

Pavlou, P. A. and Geffen, D. (2004), "Building effective online marketplaces with institution-based trust," *Information Systems Research* 15(1), pp. 37-59.

Pfeffer, J. (1992). *Managing with Power: Politics and Influence in Organizations*. Boston, Massachusetts, USA: Harvard Business School Press.

Pfeffer, J. and Salancik, G. R. (1978). *The external control of organizations*. New York, NY, USA: Harper & Row.

Qing, H., Xu, Z., Dinev, T., and Ling, H. (2011), "Does deterrence work in reducing information security policy abuse by employees?," *Communications of the ACM* 54(6), pp. 54-60.

Rivard, S., Lapointe, L., and Kappos, A. (2011), "An Organizational Culture-Based Theory of Clinical Information Systems Implementation in Hospitals," *Journal of the Association for Information Systems* 12(Special Issue), pp. 123-162.

RNCOS. (2011a, Last update date: May 1, 2011). *Australian healthcare IT analysis*. Retrieved August 31, 2011, from http://www.marketresearch.com/RNCOS-v3175/Australian-Healthcare-2683966/, pp. 1-35.

RNCOS. (2011b, Last update date: Feb, 2011). *Russia IT industry analysis*. Retrieved August 31, 2011, from http://www.marketresearch.com/RNCOS-v3175/Russia-6083721/, pp. 1-65.

RNCOS. (2011c, Last update date: May 1, 2011). *US healthcare IT market analysis*. Retrieved August 31, 2011, from http://www.marketresearch.com/RNCOS-v3175/Healthcare-6285506/, pp. 1-75.

Schade, C. P., Sullivan, F. M., de Lusignan, S., and Madeley, J. (2006), "e-Prescribing, efficiency, quality: Lessons from the computerization of UK family practice," *Journal of the American Medical Informatics Association* 13(5), pp. 470-475.

Scott, W. R. (2002). *Organization: Rational, Natural, and Open System*. Englewood Cliffs, New Jersey, USA: Prentice-Hall.

Shapira, Z. (1997). *Organizational Decision Making*. New York, NY, USA: Cambridge University Press.

Siponen, M. and Vance, A. (2010), "Neutralization: New insights into the problem of employee information systems security policy violations," *MIS Quarterly* 34(3), pp. 487-A412.

Slovic, P. (2000). *The Perception of Risk*. London, UK: Earthscan.

Smircich, L. (1983), "Concepts of Culture and Organizational Analysis," *Administrative Science* 28(September), pp. 339-358.

Sullivan, B. N. (2010), "Competition and beyond: Problems and attention in the organizational rulemaking process," *Organization Science* 21(2), pp. 432-450.

Teasdale, G. (2008), "Quality in healthcare and the quest for improvement," *Scottish Medical Journal* 53(2), pp. 3-6.

Thomas, G. and Botha, R. A. (2007), "Secure mobile device use in healthcare guidance from HIPAA and ISO17799," *Information Systems Management* 24(4), pp. 333-342.

Tsai, W. (2002), "Social structure of "coopetition" within a multiunit organization: Coordination, competition, and intraorganizational knowledge sharing," *Organization Science* 13(2), pp. 179-190.

Tziner, A., Kopelman, R. E., and Livneh, N. (1993), "Effects of performance appraisal format on perceived goal characteristics, appraisal process satisfaction, and changes in rated job performance: A field experiment," *The Journal of Psychology* 127(3), pp. 281-291.

USDH&HS. (2003, Last update date). *Summary of the HIPAA Privacy Rule*: U.S. Department of Health & Human Services. Retrieved November 7, 2011, from http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf, pp. 1-19.

USDH&HS. (2007, Last update date). *HIPAA Security Series*: U.S. Department of Health & Human Services. Retrieved February 21, 2011, from http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf, pp. 1-29.

USDH&HS. (2008, Last update date). *Resolution Agreement* (Web page): U.S. Department of Health & Human Services. Retrieved February 11, 2011, from http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/providenceresolutionagreement.html, pp.

USDH&HS. (2011a). *Case Examples and Resolution Agreements*. Retrieved February 21, 2011, from http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html

USDH&HS. (2011b). *Enforcement Data*. Retrieved August 11, 2011, from http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/historicalnumbers.html

USDH&HS. (2011c). *HITECH Act Enforcement Interim Final Rule*. Retrieved February 13, 2011, from http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html

USDH&HS. (2011d). *Resolution Agreement*. Retrieved August 19, 2011, from http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/uclaagreement.html

USDH&HS. (2011e). *Understanding Health Information Privacy*. Retrieved February 13, 2011, from http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

Van de Ven. (1976), "A framework for organizational assessment," *Academy of Management Review* 1976(1), pp. 64-78.

Van Eerde, W. and Thierry, H. (1996), "Vroom's expectancy models and work-related criteria: A meta-analysis," *Journal of Applied Psychology* 81(5), pp. 575-586.

Vaughan, D. (1996). *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*. Chicago, Illinois, USA: University of Chicago Press.

Venkatesh, V., Zhang, X., and Sykes, T. A. (2011), ""Doctors do too little technology": A longitudinal field study of an electronic healthcare system implementation," *Information Systems Research* 22(3), pp. 523-546.

Vroom, V. H. (1964). *Work and Motivation*. Oxford, UK: Wiley.

Warkentin, M., Johnston, A. C., and Shropshire, J. (2011), "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention," *European Journal of Information Systems* 20(January), pp. 267-284.

Weick, K. (1995). *Sensemaking in Organizations*. Thousand Oaks, CA, USA: Sage.

Wipke-Tevis, D. D. and Pickett, M. A. (2008), "Impact of the health insurance portability and accountability act on participant recruitment and retention," *Western Journal of Nursing Research* 30(1), pp. 39.

Zucker, L. G. (1977), "The role of institutionalization in cultural persistence," *American Sociological Review* 42(5), pp. 726-743.

APPENDIX A. POTENTIONAL OPERATIONALIZATIONS OF SIPVHOM CONSTRUCTS

Table of Operationalizations for SIPVHOM Constructs

Construct	Subconstruct	Code	Items	Description
Structural secrecy	Centralization	CEN-1	Our business transactions with other units should be approved by upper management?	Borrowed from (Tsai, 2002). Rated 1 to 7 (strongly disagree – strongly agree).
		CEN-2	Any agreement or dispute over interunit activities should be reported to upper management and we should let them settle the issue?	
		CEN-3	Upper management has the ultimate power to decide whether or not we collaborate with other units in the orgnaization?	
	Networking opportunities	NET-1	On average, how many days per year do you spend in interdepartmental committees, teams, and task forces?	Borrowed from (Ghoshal et al., 1994).
		NET-2	On average, how many days per year do you spend in interdepartmental meetings and conferences?	
		NET-3	On average, how many days per year do you spend in meetings with upper management?	
Violation coupling	Organizational memory level	OML-1	Compared to other healthcare organizations, my organization has: A great deal of knowledge about [insert a particular HIPAA IT rule here or ask about HIPAA in general]	Borrowed from (Moorman & Miner, 1997). Rated 1 to 7 (strongly disagree – strongly agree).
		OML-2	Compared to other healthcare organizations, my organization has: A great deal of experience with [insert a particular HIPAA IT rule here or ask about HIPAA in general]	
		OML-3	Compared to other healthcare organizations, my organization has: A great deal of familiarity with [insert a particular HIPAA IT rule here or ask about HIPAA in general]	
		OML-4	Compared to other healthcare organizations, my organization has: Invested a great deal in measure to prevent [insert a particular HIPAA IT rule here or ask about HIPAA in general]	
	Organizational memory dispersion	OMD-1	Rate the degree of consensus among administrators with regard to procedures for [insert a particular HIPAA IT rule]:	Borrowed from (Moorman & Miner, 1997). Rated 1 to 7 (low – high).
		OMD-2	Rate the degree of consensus among doctors with regard to procedures for	

			[insert a particular HIPAA IT rule]:	
		OMD-3	Rate the degree of consensus among nurses with regard to procedures for [insert a particular HIPAA IT rule]:	
Enforceability	Certainty of sanctions	CER-1	It is routine for our organizations to be audited by Health and Human Services to identify HIPAA computer violations.	Borrowed from (Qing et al., 2011). Rated 1 to 7 (strongly disagree – strongly agree).
		CER-2	Organizations that [insert a particular HIPAA IT rule here] will be caught.	
		CER-3	It is likely that [insert a particular HIPAA IT rule here] can be traced back to the violating organization.	
	Severity of sanctions	SEV-1	Organizations caught [insert a particular HIPAA IT rule here] will be severely punished.	Borrowed from (Qing et al., 2011). Rated 1 to 7 (strongly disagree – strongly agree).
		SEV-2	Organizations caught [insert a particular HIPAA IT rule here] will be reprimanded.	
		SEV-3	Organizations caught [insert a particular HIPAA IT rule here] will face serious consequences.	
	Celerity of sanctions	CEL-1	For our organization, actions against [insert a particular HIPAA IT rule here] are immediate.	Borrowed from (Qing et al., 2011). Rated 1 to 7 (strongly disagree – strongly agree).
		CEL-2	For our organization, actions against [insert a particular HIPAA IT rule here] are instantaneous.	
		CEL-3	For our organization, actions against [insert a particular HIPAA IT rule here] are timely.	
Procedural emphasis	Goal clarity	GC-1	Procedural emphasis measures could be It is clear what outcomes are expected in the HIPAA rule that states [insert a particular HIPAA IT rule here].	Borrowed from (Tziner et al., 1993). Rated 1 to 7 (strongly disagree – strongly agree).
		GC-2	The information provided on the HHS website about [insert a particular HIPAA IT rule here] will help you protect patient’s medical information.	
		GC-3	The information provided on the HHS website about [insert a particular HIPAA IT rule here] was sufficiently unambiguous.	
		GC-4	The information provided to you by HHS about [insert a particular HIPAA IT rule here] was sufficiently detailed.	

Rule connectedness	Rule density	RD-1	As a researcher, select the HIPAA IT violation of interest and follow the instructions to the right. It should be the same rule that you select for the scenario above.	Borrowed from (Sullivan, 2010). Calculate the “density” of rules by tracking, coding, and aggregating the following statistics for a specific time period: • Gather all rule proposals and finalization dates • Code all rules into distinct categories • Code all rules to indicate whether they influence human or nonhuman factors • Record finalized rules as an event, non-finalized rules as a non-event • Code all rule violation reports (incident reports) to identify them as having either human or non-human causes.
Perception of risk	Perceived risk of violations	PRV-1	What do you believe is the risk for your organization due to the possibility that: My organization could be issued severe sanctions for violations of [insert a particular HIPAA IT rule here]	Borrowed from (Dinev & Hart, 2006). Rated 1 to 7 (very low risk – very high risk). Fill in with the rule selected for the scenario.
		PRV-2	possibility that: The media could damage my organization’s image by sharing information about violations of [insert a particular HIPAA IT rule here] committed by my organization	
		PRV-3	possibility that: My organization will be caught if it violates [insert a particular HIPAA IT rule here]	
Likelihood of a rule violation	Misuse intent	MI-1	If you were Sam, what is the likelihood that you would have [insert a particular HIPAA IT rule here]?	Borrowed from (D'Arcy et al., 2009). Rated 1 to 7 (very unlikely – very likely) If multiple scenarios are used: MI-1 = MI-1(scenario$_1$) + …MI-1(scenario$_n$).
		MI-2	I could see myself [insert a particular HIPAA IT rule here] if I were in Sam’s situation.	

	Moral commitment	MC-1	It was morally acceptable for Sam to [insert a particular HIPAA IT rule here].	Fill in with the rule selected for the scenario.

芽|Sprouts

Working Papers on Information Systems | ISSN 1535-6078

Office:
Sprouts
University of Amsterdam
Roetersstraat 11, Room E 2.74
1018 WB Amsterdam, Netherlands
Email: admin@sprouts.aisnet.org