Does Sharing Make My Data More Insecure?
An Empirical Study on Health Information Exchange and Data Breaches

Leting Zhang, Min-Seok Pang, Sunil Wattal
Fox School of Business, Temple University, Philadelphia, PA 19122
leting.zhang@temple.edu; minspang@temple.edu; swattal@temple.edu

PRELIMINARY DRAFT – MAY 2019

This paper examines the security implications of participation in inter-organizational systems (IOS) in the context of the healthcare industry. Specifically, we ask - how does joining in a Health Information Exchange (HIE) affect hospitals' data breach risks? On one hand, the hospitals in the HIE would be more attractive targets to intruders, and they may not have sufficient incentives to substantially invest in information security because of the inter-dependent risks. However, the HIE requires the participating hospitals to implement strong information technology (IT) governance to lower the participants' breach risks. We study this issue using a five-year (2010-2014) panel data from multiple sources on HIE participation and incidences of security breaches in hospitals. Our results show that joining in an HIE decreases a hospital's probability of a data breach. We also find that this mitigation effect is stronger for hospitals with a higher IT security capability. Surprisingly, a higher HIE participation rate also lowers the risks in hospitals that are not in the HIE in the same region. This paper contributes to the information systems literature by studying information security in IOS and the effectiveness of IT governance. We also provide security implications for policymakers and healthcare practitioners.

Keywords: Information security, Health Information Exchange (HIE), Inter-organizational system (IOS), IT governance

---

"Data on the move may be inherently less secure than data stored behind institutional firewalls."

-Commonwealth Fund President. David Blumenthal, MD, MPP

1. Introduction

Along with the value gained from information sharing, the challenge of protecting data privacy and security increase significantly. For one thing, the interconnected link adds another layer of risk; secondly, the participated entities could be a weak link in the systems and exposed others' data to risks (Kunreuther and Heal 2003; Ogut et al. 2004). Despite the practitioners' concerns toward the risks and researchers' appeals on this topic, there is a significant gap in literature on the information security in inter-organizational system (IOS). Particularly, there is no empirical study investigates whether connecting in an IOS affects a firm' information security performance. We examine the related questions by using IT governance in IOS context as a main theoretical framework to explain the mechanism of the mitigation effect on firms'

information security risks. Furthermore, how organizational characteristics lead to the heterogeneity in realizing the effect. Lastly, how the IOS participation rates affect risks in a region.

The high information security risks and requirements for interoperability makes healthcare sector a valid context to examine our research questions. In recent years, healthcare has topped the list of industries with a material risk of cyber intrusions and data breaches. According to research conducted by IBM and Ponemon Institute (2016), data breaches cost the U.S. healthcare sector $6.2 billion each year, also the healthcare data breaches cost the highest of any industry at $408 per record (Ponemon 2018). While electronic medical records, information sharing, cloud services, and the Internet of Things have become more prevalent in this sector, the ever-changing nature of security threats makes it more challenging for hospitals to sufficiently protect their information assets (Verizon 2016), given that security protection in many hospitals have not kept pace with growing security risks (Hoffman and Podgurski 2009; Sittig and Singh 2011).

In healthcare's digital transformation, Health Information Exchange (HIE) is one of the most important Health IT initiatives. It enables the sharing of patient information and diagnosis results between unaffiliated hospitals (Adler-Milstein and Jha 2014). In 2009, the HITECH Act was enacted to promote HIEs including providing incentives and subsidies for the exchange and education.[1] By 2014, more than 100 HIEs operated in the U.S. (Adler-Milstein et al. 2016). The main goal of HIEs is achieving better care coordination, greater efficiency, and improvement in the quality of care. However, along with those possible benefits, the challenge of protecting patients' information in such a context is increasing as well. The inter-dependent risks increase the uncertainty, complexity, and potential losses of the breach risks. First, in an interconnected system like an HIE, key components of risks, such as threats, vulnerabilities, potential losses and so on, are no longer isolated to any individual organization (Huang et al. 2014), which results in a higher uncertainty of data breach risks; Second, when hospitals join an HIE, the lack of IT standards, the presence of more or less compatible systems specific to the participating organizations, and the need for a centralized database introduce additional problems of system integration and increase the security risks (Pirnejad et al. 2008; Goroll et al. 2009); Third, one breach via HIE may involve many hospitals' patients, resulting in more severe consequences by way of a larger quantity of victims. For example, on July 13, 2016, Codman Square Health Center in Massachusetts was notified of a data breach incident.[2] An employee had

[1] https://journalofethics.ama-assn.org/article/hitech-act-overview/2011-03

[2] https://healthitsecurity.com/news/unauthorized-hie-access-leads-to-ma-data-security-incident

accessed the New England Healthcare Exchange Network (NEHEN) without authorization, leading a breach of approximately 140 Codman patients' information as well as that of around 4,000 others in the network.

These challenges make information security in the context of inter-organizationalsystem (IOS), especially in HIEs, critical concerns in practice that warrant scholarly attention (Appari et al. 2009). To the best of our knowledge, the connection between inter-organizational systems and information security has been scarcely established empirically, and even more so in the context of HIE and participants' information security risks. Therefore, in this study, we ask what roles that HIEs play in controlling participants' information security risks and what impact it has on hospitals' data breach risks.

This is by no means an intuitive question. On the one hand, participation in an HIE may lead to a higher data breach risk for both technical and economic reasons. First, joining the HIE increases data access points and expands the information flow, thus exacerbating potential information security risks. Second, the economic literature suggest that in the context of IOS where IT security risks are shared among different organizations, they may lack the incentives to implement strong security practices (Fang et al. 2014). On the other hand, joining an HIE may decrease security risks, because the HIEs play an active role in governing the information security of its participants by specifying policy and technology standards as part of IT governance mechanisms. In other words, as a member of an HIE, hospitals are required to comply with additional security protection and data standards imposed, policies by the HIE (Heath et al. 2017). However, HIEs also allow participants to maintain a certain degree of autonomy and independence from the HIE (McCarthy et al. 2014). The lack of a full control leads to heterogeneous realizations of IOS governance on information security. With these theoretical tensions, we aim to examine the following research questions: (i) What is the impact of joining in an HIE on hospitals' data breach risks? (ii) Is this impact heterogeneous on hospitals with different IT security capabilities? (iii) How HIE participation rates in a region affect the non-participants' data breach risks? We employ a five-year period (2010-2014) hospital-level panel dataset from the HIMSS database and conduct empirical analyses with several identification strategies including using instrumental variables. Our results offer some encouraging findings. Contrary to prevalent concerns on HIE security, becoming a member of an HIE lower the data breaches risk by 7%. We also find that the risk-mitigating effect of HIEs is magnified at hospitals with stronger security capabilities, the data breach risks for them decrease by 30%. In addition, non-participants in a region with a high participation rate also demonstrate better information security performance, 1% increase in HIE participation rates would drive the breach risks lower by 0.05% and 0.65% for non-participants and health referral regions respectively.

To the best of our knowledge, this is the first study to empirically examine the information security performance in IOS, or HIE in particular at the healthcare sector. This study not only contributes to the literature on security governance in IOS and HIEs but also provides meaningful insights for policymakers and practitioners in cybersecurity and healthcare.

2. Literature Review

2.1. IT Security Management and IT Governance

The management of information security has been extensively studied in IS literature. It is characterized as comprised of four activities: deterrence, prevention, detection, and remedies (Straub and Welke 1998). Previous studies examine both technologies (Cavusoglu et al. 2005) and human factors (D'Arcy et al. 2009) in controlling information security risks. In recent years, many research focused on IT security in the healthcare industry, they found that using encryption does not decrease the data breach (Miller and Tucker 2011); proactive security adoptions are more effective than reactive security adoptions (Kwon and Johnson 2014); furthermore, certain institutional characteristics of organizations lead to symbolic adoption of security protection rather than substantive adoption (Angst et al. 2017).

Another stream of literature is related to IT governance. Researchers consider it as one of the ways to achieve business performance goals from IT investment by making better IT-related decisions (Woodham 2002). Management control theory posits that effective IT governance mechanisms reduce IT-related risks (Simons 1991). A few studies examine how effective the mechanisms influence cybersecurity risks. For example, effective IT governance reduces security incidents in federal agencies (Pang and Tanriverdi 2017), the enactment of data breach disclosure laws by U.S. states reduces identity theft incidents (Romanosky et al. 2011), centralized IT governance, compared to the decentralized IT governance is more effective in lowering data breach risks (Liu et al. 2016), and the enforcement of Convention on Cybercrime deters distributed denial of service attacks (Hui et al. 2017). However, to the best of our knowledge, there is little research examining how IT governance affects information security risk in the IOS context.

2.2. Risks and Governance in Inter-organizational System

Inter-organizational systems (IOS) are information and communication technology-based systems that transcend legal enterprise boundaries (Bakos et al. 1991). Prior IOS literature shows IOS exchange enables efficient information sharing, making markets more attractive (Malone 1987; Wang and Seidmann 1995). However, the implementation and sustaining of IOS is a complex process involving different risks. The IT-enabled cooperation, if not nurtured, can degenerate into conflict. Some studies identified the potential risks in IOS from the perspectives of technical, economic, and socio-political (Kumar and Dissel1996). One of the

risks related to information security is that shared the resource could be fouled or contaminated. A typical example is the supply chain attack, it is a "cyber-attack that seeks to damage an organization by targeting less-secure elements in the supply network".[3] For instance, in 2013, Target was the victim of a supply chain attack. Because of the vendor's questionable security practices, hackers obtained the shared credential and gained entry into Target's system, it resulted in the breach of 70 million customers' personally identifiable information. Due to the prevalence of IOS, this attack increases significantly nowadays. According to Symantec's annual report (2018), there is a 200% increase in supply chain attacks accounts for breaches in 2017.

The root of the IOS security risks lies in two perspectives: technical and economic. They are not mutually exclusive and can also interact with one another. From a technical perspective, the increasing number of accesses point potentially increase the security risks. First, the attackers could be exposed to these points and strategically choose which one to exploited; Second, a point with low protection could be leveraged to spoil all the systems. Also, economic studies suggest organizations may have opportunistic behavior in the situation for mainly two reasons. First, it is difficult to control information security performance because it is a dynamic process. Though organizations could be required to install firewalls and anti-virus software, they can symbolically adopt those practices and decouple continuous related practices from their main activities (Angst et al. 2017), for example patching vulnerabilities in time. As a result, their risks are still high; Secondly, when facing inter-dependent risks, organizations cannot internalize other organization's breach cost, in another word, they have low incentive to invest enough to protecting the pooling resources. Previous studies use analytical models to examine the question, results show that the inter-dependency of risks reduces the organizations' incentive to invest in information security (Kunreuther and Heal 2003; Ogut et al. 2004). However, emphasizing member accountability would make them invest more in information security and lead to welfare gains (Fang et al. 2014).

Furthermore, IOS governance is critical in ensuring alignment in business among different organizations. The mechanisms of IOS governance can be classified as contractual or relational according to the IOS decision making processes and inter-organizational practices norms (Fischer and Huber 2012). The contractual governance mechanism relies on formalized, legal or contracts (Lee and Cavusgil 2006). Relational governance establishes the ability of social processes to enforce obligations, promises, and expectation (Poppo and Zenger 2002). Previous literature examines how IOS governances emerge, evolve and affect outcomes in different contexts such as large IT project development, outsourcing arrangement,

[3] https://en.wikipedia.org/wiki/Supply_chain_attack

open source software (Grant and Tan 2013; Kim 2013; Morgan et al. 2013). However, the impact of IOS governance on information security performance is still uninvestigated.

2.3. Health Information Exchange

Although information and privacy issues are highlighted in the establishment of HIEs in the real world (Adler-Milstein et al. 2009; Wong L.Y. 2010; Adjerid et al. 2016; Broyles et al. 2016), it has not been carefully examined. From some anecdotal evidence, most HIEs invest a lot in securing the data exchange. But the security levels of endpoints, hospitals, are also important in such a context. To the best of our understanding, no previous research examines the HIEs' role in controlling impact on hospitals' information security performance.

"Secure data" is one of the foremost priorities for all HIE. An HIE acts as a "quasi-governor" that oversees IT practices in all members hospitals (Adjerid et al.2018). Furthermore, the National Institute of Standards and Technology (NIST) establishes guidance on the security architecture and design processes for the HIE (Scholl et al. 2010). It states "An important core competency of the HIE is to maintain a trusting and supportive relationship with the organizations that provide data to, and retrieve data from, one another through the HIE. The trust requirement is met through a combination of legal agreements, advocacy, and technology for ensuring meaningful information interchange in a way that has appropriate protections". What's more, "To truly create a secure HIE environment, additional services are required to protect the data of the participating entities' organizational infrastructure (that is, the endpoints that house the data at rest)". Under the framework of contractual governance and relational governance, we identify three main practices that HIEs adopt in IOS governance, which are technology standardization, imposing policy and knowledge sharing. The first two practices are contractual governance, the last practice isrelational control.

First, technology standardization. More advanced systems, stringent authentication, and access controls are promoted in replace of the legacy system and loss access control. Specifically, HIEs provide standards and detailed guideline for technical controls. For example, they facilitate the promotion of using device password lock activated and used to gain local access to the given device, regular virus scan and other malware protection, file encryption and encryption of data at rest. An HIE's agreement says "Each participant shall be solely responsible for validating the accuracy of all output and security measures, including routine backup procedures."[4] Furthermore, it enforces access and audit controls which could decrease the probability of information security risks significantly. Also, it promotes technological choices

[4] https://gnohie.org/wp-content/uploads/2018/06/GNOHIE_TC_4.30.18.pdf

that limit the potential of abuse. For example, joining in HIEs involves the implementation of sharing tools (eg. Direct Messaging), it allows for the exchange of patient data between care providers while maintaining a high level of privacy and security or a tool. In the meantime, it would replace the traditional exchange techniques like fax, e-mail, and mobile messaging, all of which are less secure (Prochaska et al. 2015).

Second, HIEs design policies and stringent regulations about data exchange, including specifying data stewardship to establish trust between hospitals. When joining in an HIE, hospitals have to sign agreements with the HIE. The agreements impose accountability of security incidents to participants, which requires identification of the person or entity responsible for stewardship at each point in the flow of data from initial collection and use through the dissemination of any aggregation of the data, and its storage and ultimate destruction. In the participation agreement of North Coast Health Information Network HIE, there is an item about information security compliance. "...Such Policies and Standards will include administrative procedures, physical security measures, and technical security services that are reasonably necessary to secure the Data. HIE and Participant will comply with the security policies and Standards established by HIE". [5] Similarly, another HIE - HealtheConnection emphasizes it in the participation agreement: "HealtheConnections may terminate its Participation Agreement if a Breach of confidentiality or security ...occurs and the Participant does not promptly take measure either (i) to cure the breach, if cure is possible given the nature of the Breach, or (ii) to prevent subsequent similar Breaches, in either case in a manner reasonably satisfactory to HealtheConnection." All of these accountabilities increase the cost of data breach significantly. Therefore, it mitigates the inefficient underinvestment in security technologies by internalizing the externalities of security investments. Considering the total costs caused by malpractices and breach incidents, hospitals would substantially invest more in information security protection.

Third, inter-organizational learning could be helpful in improving security performance; especially when the security risks are dynamic. To implement the relational governance, the HIE provides a channel for knowledge sharing and additional support services, in such forms as webinars, training, or in-person meetings, which facilitate the spread of expertise and practices in information security across the HIE members. Through HIEs, hospitals could also keep up to date with data privacy and security regulations. A representative of an HIE participants says "It would help keep us informed with all the privacy and security things throughout the state and federal government" (Pevnick et al. 2012). As a result, hospitals will value security more and make efforts to decrease IT risks in an efficient way. Based on the effectiveness of the IOS governance, we propose our first hypothesis:

---

[5] http://www.ct.gov/hitect/lib/hitect/DOCS-_602151-v3-HITE-Production_Participation_Agr-7-11_BOD_approved.pdf

Hypothesis 1: Joining in the HIE decrease hospitals' data breach risks.

Under the contractual governance, hospitals join in HIEs need to implement a series of security controls, which enables the right exchange. These controls could also, in turn, enhance hospitals information security performances. However, the effect could be heterogeneous on hospitals with different level of related capability. For one thing, according to path dependency in technology (Brian 1989; Cohen and Levinthal 1990), a firm's ability and incentive to adopt a newer technology are largely a function of its level of related experience with prior technologies. From the perspective of technology standard, hospitals with higher information security capabilities are more experienced in information security management. Furthermore, an established higher awareness in information security enable the hospital to better cope with the new technologies without violating the security practices, facilitating the realization of security enhancements under the IOS governance. From the perspective of the accountability, hospitals with higher information security capabilities would find it more cost-effectiveness to shift the potential penalty to substantially invest in information security, which is not the case for hospitals with very limited related resources and a high start cost. Therefore, we propose our second hypothesis:

Hypothesis 2: The mitigation effect of joining in HIEs is greater on hospitals with higher information security capabilities.

To further investigate the relational governance mechanism, we examine the spillover effect of knowledge sharing. Specifically, we propose that there is a spillover effect in a region where an HIE participation rate is high. Because the HIE is an initiative at the health referral region level, the communication and security practices promoted by the HIE not only have an impact on the participants but also should affect the other hospitals which are not participants. Also, the data breach risks would be lower in the region. Thus, the third and fourth hypotheses are as follow:

Hypothesis 3: Non-participating hospitals in a region with a higher HIE participation rate have lower data breach risks.

Hypothesis 4: A Health referral region with a higher HIE participation rate have lower data breach risks.

3. Data and Methods

3.1. Data

Our empirical approach aims to examine the impact of joining in an HIE on information security risks for individual hospitals by leveraging a five-year (2010-2014) panel dataset of more than 4,500 hospitals. We classify the data into three types:(1) Data on hospital characteristics and IT practice, (2) data on health

referral region characteristics, and (3) data on security breaches. The explanations for each type are as follow.

3.1.1. Hospital Characteristics and IT Practice

We collect hospital-level data from the Healthcare Information and Management Systems Society (HIMSS) Analytics database. It is widely used in prior healthcare IT research (Angst et al. 2017; Kwon and Johnson 2014; Amalia R. Miller and Tucker 2009). From the HIMSS dataset, we can identify whether hospitals join in HIEs as our primary variable of interest. To eliminate the confounding effects, we incorporate a battery of hospitals' characteristics including the number of beds as a measure for hospital size, their memberships in health systems, the number of beds in the health system as the size of the health system, academic type, and profitability. We also consider their IT adoptions including the number of IT security practices and the number of operational IT applications as a measure of IT capability. Furthermore, we use a common approach (Burke et al. 2002; Burke and Menachemi 2004) to categorize healthcare applications into different types based on their functionalities - clinical applications, administrative applications, and strategic applications. We account for different types of IT applications in our model because they can indicate the inherent information risks of the hospital (Miller and Tucker 2014).

Based on the number of adopted IT security practices, we classify hospitals into two types – high IT security capability type and low IT security capability type. Specifically, in HIMSS database, there are ten recorded IT security applications including firewall, encryption, antivirus, intrusion detection system and so on. The mean number of adopted applications is 4.77, and the standard deviation is 1.9. Therefore, we define a hospital which has less than five IT security applications as a low IT security capability type; otherwise, it is a high IT security capability type.

Additionally, over the time period we study, the Centers for Medicare and Medicaid Services (CMS) introduced meaningful-use (MU) attestation to facilitate EHR assimilation into clinical workflows. The attestation requires healthcare providers to establish systematic procedures to address quality and security (Kwon and Johnson 2018) and it promotes the data sharing capability. Hospitals have an incentive to reach the MU standard because they can get a monetary reward after passing the attestation. Considering that the attestation may affect HIEs' impact on data breach, we collect data on hospitals' meaningful-use status and use them as control variables in our model.

3.1.2. Health Referral Region and Market Characteristics

Health Information Exchanges have emerged as regionally focused efforts. Thus, we also leverage several variables at health referral region (HRRs) level. HRRs are precisely defined to capture the geographic region

where a patient is likely to receive the majority of their care, therefore requiring the sharing of medical information enabled by an HIE among providers in an HRR (Adjerid et al. 2018). We obtain data on HRRs from Dartmouth Health Atlas (DHA) and identify 306 HRRs across the U.S.

Next, we derive market concentration at the regional level. Market concentration is a factor that could influence hospitals' decisions in regards to joining HIE. Hospitals in more competitive markets are less likely to engage in HIE because they are more sensitive about the potential gains in quality (Adler-Milstein and Jha 2014). In the meantime, the level of competition also influences hospitals' investment strategy. Therefore, hospitals in a competitive market would shift resources to more consumer-visible activities and have more data breaches (Gaynor et al. 2012). In order to reduce the bias, we incorporate the HRR-level Herfindahl-Hirschman Index (HHI) as the competition index of a market. In this study, we follow the practices in previous studies (Gaynor et al. 2012) by using the number of hospital beds as the size of hospitals and calculating the market share of each hospital and the sum of squared for all hospitals in the same HHR as HHI in a market.

Furthermore, we incorporate a set of demographic variables including personal income, unemployment rate, and population. To obtain the demographic characteristics of health referral regions, we follow the practice similar to previous research (Atasoy et al. 2017). First, we collect county-level data from the Bureau of Labor Statistics and match them to zip-codes level. Then we use Crosswalk Files provided by DHA to match zip-codes to health referral regions (HRR) and calculated the average statistics for each HRR.

Lastly, we also consider the regional level healthcare measurements including outpatient costs, test costs, the number of emergency department visit, the number of readmission and case mix index. Those data are also provided by DHA.

3.1.3. Data Breach

We collect hospitals' security breach incidents from two sources – the Privacy Rights Clearing House and the U.S. Department of Health and Human Service (HHS) – which were commonly used in previous research (Angst et al. 2017; Kwon and Johnson 2014, 2018). From the dataset, we can find information on each incident, such as hospital information, breach date, breach types (hacking, unintended disclosure, malicious insider etc.) and the number of affected records. After merging the hospital and breach incident data manually, we construct a 5-year panel dataset. There are more than 800 data breach incidents that can be attributed to entities in HIMSS. Summary statistics are presented in Table 1.

Table 1. Summary Statistics					
Name	**Description**	**Mean**	**SD**	**Min**	**Max**
Dependent variable					
Data breach	An indicator variable for whether the hospital has data breaches	0.04	0.20	0.00	1.00
Independent variable					
Join in HIEs	An indicator variable for whether the hospital join in HIEs	0.41	0.49	0.00	1.00
Moderating variable					
High IT security capability	An indicator variable for whether the hospital is a high IT security capability type	0.79	0.41	0.00	1.00
Instrument variables for joining in HIEs					
HIE participation rate (HRR)	The percentage of hospitals join in HIEs in the HRR	0.30	0.20	0.00	1.00
Outpatient cost (HRR)	Outpatient Dialysis Facility actual Medicare costs in the HRR	2.15e+08	1.68e+08	1.69e+07	1.11e+09
Hospital level control variables					
Size	ln (The number of beds a hospital has)	4.49	1.14	0.69	7.53
IT capability	ln (The number of apps a hospital has)	4.01	0.46	0.00	4.91
Admin IT	The number of administration applications a hospital adopts	14.09	4.04	0.00	32.00
Strategic IT	The number of strategic applications a hospital adopts	5.27	2.59	0.00	19.00
Clinical IT	The number of clinical applications a hospital adopts	37.55	15.02	0.00	84.00
Member	An indicator variable for whether the hospital is a member of a health system	0.65	0.48	0.00	1.00
MU1	An indicator variable for whether the hospital is in stage 1 of Meaningful Use Attestation	0.35	0.48	0.00	1.00
MU2	An indicator variable for whether the hospital is in stage 2 of Meaningful Use Attestation	0.07	0.25	0.00	1.00
HRR (Health Referral Region) level control variables					
Income	ln (Personal income)	10.61	0.19	9.98	11.57
Population	ln (Population)	11.99	0.89	9.82	17.56

Unemployment Rate	Unemployment rate	7.90	2.22	2.82	16.75
Competition	Competition index (HHI)	6.81	0.78	5.00	9.11
Test cost	ln (Total test cost)	17.25	1.03	14.18	19.42
No. ED visit	ln (Number of emergency department visit)	11.39	0.83	9.20	13.07
No. Readmission	ln (Number of readmission)	8.79	0.93	6.21	10.66
CMI	Case Mix Index	1.46	0.12	1.10	2.15
Observation	27038				

3.2. Empirical Models

3.2.1 Linear Probability Model

First, in order to test H1, we estimate a panel linear probability model (LPM) with heteroskedasticity-robust standard errors. Specifically, the model is as follow:

$$Breach_{it} = f(joinHIE_{it}, X_{it}, \theta_{jt}, \gamma_i, \mu_t, \epsilon_{it})$$

In the specification, the outcome variable is $Breach_{it}$. It indicates whether a hospital i has security breaches in year t. Our primary variable of interest is $JoinHIE_{it}$, which captures whether a hospital i joins in an HIE in year t. Other variables are control variables. X_{it} and θ_{jt} are vectors of time-varying characteristics of hospitals and health referral regions respectively, γ_i and μ_t are hospital and year fixed-effects, respectively, and ϵ_i is independently and identically distributed errors. Furthermore, we use robust standard errors in all estimations. Although the LPM has the limitation that the predict values may not in the range of 0 to 1, but it enables us to avoid the incidental parameters problem in a non-linear model with fixed effect (Miller and Tucker 2009) .

In order to examine the moderating effect of hospitals' security capabilities, we incorporate an interaction term and estimate the following model:

$$Breach_{it} = f(joinHIE_{it}, joinHIE_{it} * SecurityIT_{it}, X_{it}, \theta_{jt}, \gamma_i, \mu_t, \epsilon_{it})$$

Finally, we evaluate the spillover effect of the HIE participations. The primary variable of interest is the number of HIE participants in the health referral region, the outcome variable indicates whether a non-participant has security breaches. In this model, we account for health referral regions' characteristics including average income, population and unemployment rate to control for the confounding effects. Also, we choose hospitals not join in HIEs in our sample.

$$Breach_{it} = f(ParticipantionRate_{jt}, X_{it}, \theta_{jt}, \gamma_i, \mu_t, \epsilon_{it} | NotJoinHIE)$$

3.2.2. Instrument Variables Model

One challenge in identification is the endogeneity of joining in HIEs. Although we use control variables and fixed effects to control for observable and time-invariant heterogeneities, it is still possible that there are omitted variables. It's more reasonable that the hospitals care less about the information security are more likely to join in HIEs. To identify the causal relationship, we use instrumental variables in the linear probability model, which has similar performance with probit IV model (Angrist 2002; Miller and Tucker 2009). Specifically, we instrument for the endogenous indicator of whether the hospital join HIE with two regional level variables: the percentage of hospitals join in HIEs, outpatient costs. These two instruments affect hospitals' decisions in HIE adoption but are plausibly uncorrelated with hospitals' data breach risks.

Our first IV is the percentage of hospitals join in HIEs in the same HRR. Based on the network effect theory, the benefits that adopters from a network technology are positively associated with the size of the network (Katz and Shapiro 1986), especially in IOS setting, as more peers adopt IOS, the network effect would arise, which accelerate the adoption (Zhu et al. 2006). For one thing, the positive impact of the number of IOS adopters on the benefits that an individual adopter can achieve by enabling the sharing of information with a larger number of partners over the IOS. Also, it is possible that the adoption increases the number of compatible softwares and hardware solutions as the standard diffuses. In the context of health IT, network effects are proved to be important when hospitals decided whether to adopt EMRs when they can electronically exchange patients' information (Miller and Tucker 2009). Similarly, the more hospitals decide to join in an HIE, the more valuable the HIE remains, reinforcing the smaller the likelihood that a hospital would want to join that HIE to be interoperable with others. However, the percentage of participants in the health referral region would not affect the focal hospitals' data breach risks through other channels. Therefore, we argue that it is a valid instrument variable.

The second IV is outpatient costs in the health referral region. It indicates the degree of necessity of information sharing in the region to an extent. The higher the outpatient costs are in the health referral region, the more valuable for hospitals in the region to join in HIEs considering the marginal improvement in qualities of treatments and decreases in costs. Also, the regional outpatient costs would not impact a single hospital's data breach risk.

4. Results

4.1. Baseline Estimations

The results of our baseline model are presented in Table 2. We find strong support for H1, which proposes HIEs' governance does lower the hospitals' data breach risks. In Column 1 of Table 2, we control for a set of hospital and HRR characteristics. In Column 2 and Column 3, we use hospital fixed effect to eliminate the bias caused by omitted time-invariant hospitals variable. Results in Column 1 and 2 show that the coefficients of joining in HIEs are significantly negative. In Column 2, the FE model suggests joining in HIEs is associated with a reduction in the probability of a data breach by 2.7%.

Next, we turn to examine the moderating effect of hospitals' security IT capabilities on the relationship between joining in HIEs and data breaches. We also find strong support for H2, specifically, when a hospital has higher security IT capability, joining in HIE would be more effective in reducing data breach risks. Column 3 reports the significantly negative coefficient of the interaction term, $JoinHIE_{it} * High\text{SecurityIT}$. For high IT security capability hospitals, joining in HIEs lower their data breach risks by 3.6%, while there is no significant mitigation effect on hospitals with low IT security capabilities.

4.2. Instrumental Variables Model

To address the endogeneity issue of joining in HIEs, we use instrumental variables methods with fixed effects panel data models. Results are presented in Table 3. First, we perform a two-stage least square (2SLS) analysis with fixed effects to examine the main effect of Joining HIEs. In the first stage, as we predict, in column (1) both IVs are positively associated with hospitals decisions in joining in HIE. The F-statistics of excluded instruments in the first stage has a value of 247.795, which is much greater than the conventional threshold value of 10 (Staiger and Stock 1997), proving our IVs are not weak. In addition, the Hansen J statistic has a value of 0.010 and cannot reject the null (p=0.919), which ensures that the overidentification restrictions are satisfied and our IVs are valid. In this model, the coefficient of $JoinHIE_{it}$ is -0.07, which means the hospital's data breach risk decrease by 7 % after they join HIEs. Interestingly, the magnitude is larger than the one in the baseline model. One explanation could be that the higher the hospital's information security risk is, the more likely it would join in HIE. It is reasonable because privacy and security are major concerns for hospitals to join (Adjerid et al. 2016; Adler-Milstein et al. 2009; Broyles et al. 2016; Wong L.Y. 2010), the fewer hospitals care about the issue, the more likely they will join in HIEs.

Then, we instrument for both the main effect of Joining in HIEs and its interaction with IT security capability by using the interactions of IT security capability and two IVs as additional instruments. We

provide the results in column 3,4,5 in Table 3. The significantly negative coefficient of the interaction terms provides strong support for Hypothesis 2. Here again, we find the IVs does not suffer from weak identification, as suggested by the F-statistic of excluded instruments (247.559). Additionally, the Hansen J statistic suggests that the overidentification restrictions are not rejected (Hansen J=0.273, p=0.873). The coefficient of the interaction term is -0.317, which means, after joining in HIEs, the probability of data breach on hospitals with higher security IT capabilities would decrease by 13.6% (-0.317+0.182=0.135). Overall, the results of IV regression provide strong support for our Hypothesis 1 and Hypothesis 2.

Table 2: Linear Probability Model -Main Effect and Moderating Effect

VARIABLES	(1) Data Breach	(2) Data Breach	(3) Data Breach
Join in HIEs	**-0.007****	**-0.027*****	**0.013**
	(0.004)	**(0.007)**	**(0.012)**
JoinHIEs* High IT			-0.049***
Security Capability			(0.012)
High IT Security	-0.011***	-0.025***	-0.010
Capability	(0.004)	(0.007)	(0.008)
IS Plan	-0.039***	-0.101***	-0.101***
	(0.004)	(0.012)	(0.012)
Size	0.017***	-0.035**	-0.034**
	(0.002)	(0.015)	(0.015)
IT Capability	0.019***	-0.002	-0.007
	(0.007)	(0.012)	(0.012)
Administration IT	-0.002**	0.000	0.000
	(0.001)	(0.001)	(0.001)
Strategic IT	0.001	0.005**	0.005**
	(0.001)	(0.002)	(0.002)
Clinical IT	0.000	-0.001**	-0.001*
	(0.000)	(0.000)	(0.000)
Member of a system	0.045***	0.037***	0.037***
	(0.003)	(0.013)	(0.013)
MU1	0.011***	0.007	0.008
	(0.004)	(0.005)	(0.005)
MU2	0.009	0.003	0.004
	(0.008)	(0.010)	(0.010)
Income	0.028**	0.100	0.103
	(0.013)	(0.065)	(0.065)
Population	0.020***	0.078	0.078
	(0.005)	(0.056)	(0.056)
Unemployment rate	0.002**	0.003	0.003
	(0.001)	(0.003)	(0.003)
Competition	0.022***	0.055*	0.056*
	(0.005)	(0.028)	(0.028)
Constant	-0.765***	-2.072**	-2.114**
	(0.143)	(1.051)	(1.054)

Hospital FE	NO	YES	YES
Time FE	YES	YES	YES
R-squared	0.037	0.323	0.324
Observations	19955	19955	19955
No. Hospitals	4793	4793	4793

Notes. Robust standard errors are reported in parentheses
*** p<0.01, ** p<0.05, * p<0.1

Table 3: Instrumental Variable Model – Main Effect and Moderating Effect

	Main Effect		Moderating Effect		
VARIABLES	(1) Stage 1 Join in HIEs	(2) Stage 2 Data Breach	(3) Stage 1 Join in HIEs	(4) Stage 1 joinHIE* High IT Security	(5) Stage 2 Data Breach
Join in HIEs		**-0.070***			0.182***
		(0.042)			(0.061)
JoinHIEs *					**-0.317*** **
High IT Security					**(0.049)**
HIE participation rate	0.463***		0.419***	-0.159***	
	(0.029)		(0.042)	(0.031)	
Outpatient cost	0.000***		0.000	0.000	
	(0.000)		(0.000)	(0.000)	
HIE Participation rate*			0.056	0.673***	
High IT Security			(0.040)	(0.033)	
Outpatient cost *			0.000	0.000***	
High IT Security			(0.000)	(0.000)	
High IT Security	0.008	-0.025***	-0.027	0.102***	0.074***
	(0.010)	(0.007)	(0.018)	(0.018)	(0.017)
IS Plan	0.035***	-0.099***	0.016	0.024	-0.030**
	(0.013)	(0.012)	(0.020)	(0.019)	(0.015)
Size	0.017	-0.034**	-0.119***	-0.174***	-0.039***
	(0.020)	(0.015)	(0.022)	(0.022)	(0.014)
IT Capability	-0.121***	-0.008	-0.002	-0.002	0.000
	(0.022)	(0.013)	(0.002)	(0.002)	(0.001)
Administration IT	-0.001	0.000	0.035***	0.034***	-0.098***
	(0.002)	(0.001)	(0.013)	(0.012)	(0.012)
Strategic IT	-0.007***	0.005**	-0.007***	-0.007***	0.004*
	(0.002)	(0.002)	(0.002)	(0.002)	(0.002)
Clinical IT	0.007***	-0.001	0.007***	0.009***	0.001
	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)
Member of a system	-0.019	0.036***	-0.019	-0.015	0.037***
	(0.016)	(0.013)	(0.016)	(0.015)	(0.014)
MU1	0.007	0.008	0.008	0.017***	0.011**
	(0.006)	(0.005)	(0.006)	(0.005)	(0.005)
MU2	0.001	0.003	0.001	0.015	0.007
	(0.012)	(0.010)	(0.012)	(0.012)	(0.010)

Income	-0.155*	0.093	-0.157*	-0.088	0.109
	(0.081)	(0.065)	(0.081)	(0.074)	(0.067)
Population	0.064	0.085	0.062	0.013	0.089
	(0.068)	(0.055)	(0.068)	(0.065)	(0.057)
Unemployment rate	-0.005	0.002	-0.005	-0.003	0.004
	(0.004)	(0.003)	(0.004)	(0.004)	(0.003)
Competition	-0.028	0.053*	-0.030	-0.026	0.057**
	(0.037)	(0.028)	(0.037)	(0.036)	(0.029)
Hospital FE	YES			YES	
Time FE	YES			YES	
Observations	19553			19553	
No. Hospitals	4793			4793	
Weak identification	133.528			66.598	
Significance of Stage 1 regressions	247.795			247.559	
Significance of Stage 1 regressions (p -value)	0.000			0.000	
Hansen J statistics	0.010			0.273	
Hansen J p-value	0.919			0.873	

Notes. Robust standard errors are reported in parentheses

* p<0.10, ** p<0.05, *** p<0.01

4.3. Spillover Effect

To investigate the spillover effect, we focus on how the number of HIE participators in a region affects a non-participant's data breach risk. The sample includes hospitals not join HIE in each year. Then we use the Linear Probability Model to estimate the effect. According to Column 1 in Table 4, the coefficient of the number of participants is significantly negative. Specifically, a 1% increase in HIE participation rate would lower the data breach risks of non-participants by 0.05%. We argue that there are two pathways lead to the results: Firstly, the institutional theory suggests organizations' behavior could be driven by social structure (Boxenbaum and Jonsson 2008), in our context, hospitals in a region with higher HIE participation rate are more likely to value information security and more easily to acquire related practices; Secondly, hospitals plan to join HIE also starts to follow HIEs' requirements including improving their information security performance. Because the independent variable is a dummy variable, we also use alternative models to prove the robustness of our results, these models include the Probit model, the Logit model, the Logit model with hospital fixed effect. The results are consistent and they provide strong support for Hypothesis 3.

Then, we examine how HIE participant rates in the health referral region affect the regional information security performance. In this analysis, we use health referral regions, instead of hospitals, as the unit of analysis. The dependent variable is the number of data breach incidents in a health referral region.

We also calculate the average number of adopted IT security applications, the average number of live IT applications to proxy the IT security capability and IT capability of the health referral region respectively. The OLS model estimation suggests that a 1% increase in HIE participation rate lead to 0.65% derease in the number of data breach incidents in the region. Considering the dependent variable is a count variable, we use Poisson model and Negative binomial model. The results are consistent. Again, Hypothesis 4 is supported.

Table 4: The impact of HIE participation rates on non-participants' data breach risks

	(1) LPM	(2) Probit	(3) Logit	(4) Logit
VARIABLES	Data Breach	Data Breach	Data Breach	Data Breach
HIE participation rate	-0.058**	-0.503**	-0.969**	-2.164**
	(0.028)	(0.236)	(0.460)	(1.091)
No. hospital in HRR	-0.005***	-0.005	-0.009	-0.232***
	(0.002)	(0.003)	(0.006)	(0.064)
Member of a system	-0.045**	0.238***	0.551***	0.040
	(0.018)	(0.092)	(0.191)	(0.543)
System Size	0.000***	0.000***	0.000***	0.000***
	(0.000)	(0.000)	(0.000)	(0.000)
IT Security Capability	0.001	-0.013	-0.011	0.157
(HRR)	(0.005)	(0.039)	(0.075)	(0.174)
IT Capability (HRR)	-0.001	0.001	-0.001	-0.026
	(0.001)	(0.006)	(0.011)	(0.026)
ln(Outpatient cost)	-0.075	-0.401*	-0.851*	-4.884**
	(0.047)	(0.244)	(0.484)	(1.969)
ln (Test cost)	0.045	-0.238*	-0.531**	-1.789
	(0.032)	(0.129)	(0.252)	(1.731)
No. ED visit	0.136	0.592	1.198	2.886
	(0.094)	(0.378)	(0.749)	(3.821)
No. Readmission	0.095**	0.066	0.194	5.366**
	(0.047)	(0.222)	(0.434)	(2.289)
CMI	-0.101*	-0.066	-0.231	-5.507*
	(0.054)	(0.374)	(0.737)	(3.001)
Population	-0.031	0.641***	1.248***	5.080
	(0.111)	(0.176)	(0.345)	(3.991)
Competition	0.010	0.539***	1.031***	1.087
	(0.038)	(0.155)	(0.303)	(1.679)
Income	0.136	1.076***	2.210***	3.506
	(0.083)	(0.247)	(0.478)	(4.022)
Unemployment rate	0.004	0.062***	0.144***	-0.020
	(0.004)	(0.023)	(0.046)	(0.153)
Hospital FE	YES	NO	NO	YES
Time FE	YES	YES	YES	YES
R-squared	0.441	-	-	-
Log- likelihood		-1727.376	-1719.876	-366.651
Observations	11826	11826	11826	1721

No. Hospitals	3213	3213	3213	399

Notes. Robust standard errors are reported in parentheses (Column (1)); Standard errors are reported in parentheses (Column (2), (3), (4))
* p<0.10, ** p<0.05, *** p<0.01

Table 5. The Impact of HIE participation rates on data breach risks in HRR

VARIABLES	(1)OLS No. breach in the HRR	(2) Poisson No. breach in the HRR	(3) Negative Binomial No. breach in the HRR
HIE participation rate	-0.658**	-1.513**	-1.078**
	(0.261)	(0.607)	(0.465)
No. hospital in HRR	0.002	-0.078*	0.008
	(0.084)	(0.045)	(0.011)
Average (No. IT security in the HRR)	-0.007	0.040	0.059
	(0.059)	(0.101)	(0.084)
Average (No. live app in the HRR)	-0.004	-0.028	-0.015
	(0.008)	(0.020)	(0.011)
ln (Outpatient cost)	-1.107*	-2.993**	-1.218*
	(0.635)	(1.410)	(0.681)
ln (Test cost)	1.182*	1.431	0.239
	(0.659)	(1.033)	(0.389)
No. ED visit	1.778	4.514*	-0.561
	(1.435)	(2.537)	(1.056)
No. Readmission	-0.640	0.445	1.409**
	(0.671)	(1.090)	(0.635)
CMI	0.339	-0.338	0.369
	(0.759)	(1.564)	(1.059)
Competition	0.345	0.746	0.289
	(0.776)	(0.963)	(0.452)
ln (HRR Personal income)	1.045	-0.162	1.087
	(1.516)	(2.599)	(0.798)
HRR Unemployment rate	-0.016	0.057	0.096
	(0.060)	(0.085)	(0.062)
R-squared	0.450	-	-
$\chi 2$	-	85.319	123.364
Log likelihood		-990.051	-872.183
Observations	1530	1150	1150
No. HRR	306	306	230

Notes. Robust standard errors are reported in parentheses (Column (1), (2)); Standard errors are reported in parentheses
* p<0.10, ** p<0.05, *** p<0.01

5. Additional Analyses

5.1 Exogenous Shock - HIPAA Omnibus Rule of 2013

The HIPAA Omnibus rule aims to enhance a patient's privacy protection, providing individuals new rights to their personal health information and strengthens the government's ability to enforce the law. A major aspect of the Omnibus Rule was the change stating that to determine whether an organization is a business associate or a conduit depends on the access they have to PHI provided to them by a covered entity. "This is important because as HIEs and other health information organizations are considered business associates, they must also understand their role in notifying individuals affected by a health data breach." The rule was published in the Federal Register on January 25, 2013, and went into effect on March 26, 2013. We argue that Omnibus rule would enhance the responsibility of HIEs, therefore enhancing the HIE's mitigation effect on participated hospitals' data breach risks.

We use *AfterOmnibus* to indicate the period after the rule becomes effective in our sample, which is from 2013 to 2014. Then we incorporate $JoinHIEs * AfterOmnibus$ in the linear probability model. As we can see in Table 6, the coefficient of the interaction term is significantly negative, it suggests that enactment of the Omnibus Rule enhances the HIE's governance effect, leading to a 2.9% decrease in data breach risks for HIE participants.

Table 6. Omnibus Rule's Impact

	(1) Data Breach
Join in HIEs	-0.010
	(0.008)
JoinHIEs* AfterOmnibus	-0.029***
	(0.007)
AfterOmnibus	0.049***
	(0.009)
Hospital Control Variable	YES
HRR Control Variable	YES
Hospital FE	YES
HRR FE	YES
R-squared	0.324
Observations	19955
No. Hospitals	4793

Notes. Robust standard errors are reported in parentheses
* p<0.10, ** p<0.05, *** p<0.01

6. Robustness Checks

We argue that HIEs play a role in governing the data sharing and improving the information security performance of hospitals join HIE. In addition, the HIE participation rates, which indicate the level of penetration of inter-organizational system (IOS), affect the information security performance of non-participants and health referral regions. Specifically, a higher participation rate in the region would lead to lower data breach risks for both participants and non-participants. We leverage a comprehensive set of control variables, use instrument variables and estimate alternative models to prove the results are consistent. However, the policies in states may become a confounding factor and bias the results. As previous research suggests, policies on privacy have a significant impact on the diffusion of health IT (Amalia R. Miller and Tucker 2009; Adjerid et al. 2016). To address the concern, we leverage the interaction of two dummies, state fixed effect and time fixed effect, to control for the possible enactment of certain legislations. The interaction term is incorporated in all the OLS specifications which are estimated before. The consistency suggests our results are robust.

Table 7. Robustness checks

	(1) Data Breach	(2) Data Breach	(3) Data Breach	(3) Data Breach (Non-participant)	(4) Data Breach (HRR level)
Join in HIEs	**-0.026*** **	0.016	-0.009		
	(0.007)	(0.012)	(0.008)		
joinHIE* High IT Security Capability		**-0.052*** **			
		(0.013)			
HIE participation rate				**-0.070** **	**-0.565***
				(0.030)	**(0.319)**
joinHIE* AfterOmnibus			**-0.030*** **		
			(0.007)		
Hospital Controls	YES	YES	YES	YES	NO
HRR Controls	YES	YES	YES	YES	YES
Group FE	Hospital FE	Hospital FE	Hospital FE	Hospital FE	HRR FE
Time FE	YES	YES	YES	YES	YES
State FE * Time FE	YES	YES	YES	YES	YES
R-squared	0.359	0.360	0.360	0.484	0.593
Observations	19955	19955	19955	11826	1530
No. Group	4793	4793	4793	3213	306

Notes. Robust standard error are reported in parentheses
* p<0.10, ** p<0.05, *** p<0.01

7. Conclusion

This research empirically evaluates how a Health Information Exchange (HIE) influences information security risks in the healthcare sector. Our results suggest that becoming part of an HIE decreases the likelihood of data breaches at a hospital. Furthermore, this improvement effect is more salient hospitals with stronger security capabilities, also, non-participants' data breach risks would be lower in a region with a higher HIE participation rate. Although the context in this study is the healthcare sector, we believe that these findings are generalizable to other sectors with IOS.

This study makes several important contributions to the literature on information security. First, it examines the effectiveness of IT governance in the IOS setting. Although IOS has been associated with various benefits within technical, organizational and political spheres (Dawes 1996; Ramon Gil-Garcia et al. 2007), a major challenge to further development of IOS is information security. The risks lie in both outside and inside. To mitigate these risks, prior research proposes that IT governance mechanisms are crucial in mitigating the security risks (Pang and Tanriverdi 2017), but to the best of our knowledge, few studies have empirically examined the mechanisms. Our research fills this gap. Second, we offer an important finding that the characteristics of individual hospitals also play a key role in moderating HIE's governance role in information security. Specifically, the underinvestment manifested when a hospital faces a higher cost in security investment. In the context of implementing the HIE, hospitals with lower security capabilities are more likely to suffer from data breaches. Thirdly, we examine the spillover effect of governance conducted by HIEs, it is important to realize the effect when evaluating the value of IOS governance in information security.

This study also provides some practical implications. First, although many stakeholders express concerns that an HIE may escalate privacy and security problems in the healthcare sector, contrary to their concerns, our results show that hospitals are less likely to suffer from data breaches after they join in an HIE. By promoting secure technologies, posing stringent regulations, and facilitating communication, hospitals data breach risks decrease after joining HIEs. Second, our findings suggest that carefully designed IT frameworks are necessary to protect valuable information exchanged over the IOS. It is necessary for the HIEs to provide sufficient support to the member hospitals for security infrastructures, policies, and training, particularly for hospitals without sufficient security capabilities. Thirdly, for policymakers, it is important to realize the regional effect of mitigating information security risks when evaluating the value of IOS governance in HIEs.

This study is subject to a few limitations. Firstly, a lack of HIE-level data makes it difficult for us to examine the governance mechanisms in a finer grain. Because we cannot capture the variations in HIEs' organizational, technical structure, we can only use IT governance theory and anecdotal evidence to explain the mechanism. Secondly, the measurement of IT security capability is coarse. We define two types of hospitals – high type and low type by comparing the number of adopted IT security applications to the average adopted number. Previous studies use the number of adopted IT security applications to proxy hospitals' investment in information security (Angst et al. 2017; Kwon and Johnson 2017). But in our study, for the purpose of interpretation, it is better to use binary variable to indicate a hospital's IT security capability. Thirdly, we don't know whether breach incidents in our dataset involve the health records from multiple hospitals. It would be interesting to use this information to measure the cost and benefit of joining in HIEs in a more precise way. These could be directions for future research.

Reference

Adjerid, I., Acquisti, A., Telang, R., Padman, R., and Adler-Milstein, J. 2016. "The Impact of Privacy Regulation and Technology Incentives: The Case of Health Information Exchanges," *Management Science* (62:4), pp. 1042–1063.

Adjerid, I., Adler-Milstein, J., and Angst, C. M. 2018. "Reducing Medicare Spending Through Electronic Information Exchange: The Role of Incentives and Exchange Maturity," *Information Systems Research* (Feb).

Adler-Milstein, J., Bates, D. W., and Jha, A. K. 2009. "U.S. Regional Health Information Organizations: Progress and Challenges," *Health Affairs* (28:2), pp. 483–492.

Adler-Milstein, J., and Jha, A. K. 2014. "Health Information Exchange among U.S. Hospitals: Who's in, Who's out, and Why?," *Healthcare* (2:1), pp. 26–32.

Adler-Milstein, J., Lin, S. C., and Jha, A. K. 2016. "The Number of Health Information Exchange Efforts Is Declining, Leaving the Viability of Broad Clinical Data Exchange Uncertain," *Health Affairs*.

Angrist, J. D. 2002. "Estimation of Limited Dependent Variable Models With Dummy Endogenous Regressors," *Journal of Business & Economic Statistics* (19:1), pp. 2–28.

Angst, C. M., Block, E. S., Arcy, J. D., and Kelley, K. 2017. "When Do IT Security Investments Matter? Accounting For The Influence of Institutional Factors In The Context of Healthcare Data Breaches," *MIS Quartely* (41:3), pp. 893–916.

Appari, A., Anthony, D. L., and Johnson, M. E. 2009. "HIPAA Compliance: An Examination of Institutional and Market Forces," *Proceedings of the 8th Workshop on Economics of Information Security* (2006), pp. 1–23.

Atasoy, H., Chen, P., and Ganju, K. 2017. "The Spillover Effects of Health IT Investments on Regional Healthcare Costs," *Management Science*.

Ayabakan, S., Bardhan, I., Zheng, Z., and Kirksey, K. 2017. "The Impact of Health Information Sharing on Duplicate Testing," *MIS Quartely* (41:4), pp. 1083–1103.

Bakos, J. Y., Journal, S., Systems, I., Fall, N., and Taylor, P. 1991. *Information Links and Electronic Marketplaces : The Role of Interorganizational Information Systems in Vertical Markets Linked References Are Available on JSTOR for This Article : Information Links and Electronic Marketplaces : The Role of Interorganizati*, (8:2), pp. 31–52.

Brian, A. 1989. *Competing Technologies , Increasing Returns , and Lock-In by Historical Events*, (99:394), pp. 116–131.

Broyles, D., Crichton, R., Jolliffe, B., and Sæbø, J. I. 2016. "Health Information Exchange," *Health Information Exchange* (170:7), pp. 149–162.

Burke, D. E., and Menachemi, N. 2004. "Opening the Black Box: Measuring Hospital Information Technology Capability," *Health Care Management Review* (29:September), pp. 207–217.

Burke, D. E., Wang, B. B. L., Wan, T. T. H., and Diana, M. L. 2002. "Exploring Hospitals' Adoption of Information Technology," *Journal of Medical Systems* (26:4), pp. 349–355.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2005. "The Value of Intrusion Detection Systems in Information Technology Security Architecture," *Information Systems Research*.

Cohen, W. M., and Levinthal, D. A. 1990. "Absorptive Capacity : A New Perspective on Learning and Innovation Authors (s): Wesley M . Cohen and Daniel A . Levinthal Source : Administrative Science Quarterly , Vol . 35 , No . 1 , Special Issue : Technology , Organizations , and Innovation (Mar .," *Administrative Science Quarterly* (35:1), pp. 128–152.

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.

Dawes, S. S. 1996. *Interagency Information Shoring : Expected Benefits , Monogeoble Risks*, (15:3), pp. 377–394.

Fang, F., Parameswaran, M., Zhao, X., and Whinston, A. B. 2014. "An Economic Mechanism to Manage Operational Security Risks for Inter-Organizational Information Systems," *Information Systems Frontiers* (16:3), pp. 399–416.

Fischer, T., and Huber, T. 2012. The Evolution of Contractual and Relational Governance in Outsourcing (242).

Gaynor, M. S., Hydari, M. Z., and Telang, R. 2012. "Is Patient Data Better Protected in Competitive Healthcare Markets?," *WEIS* (Weis), pp. 1–27.

Goroll, A. H., Simon, S. R., Tripathi, M., Ascenzo, C., and Bates, D. W. 2009. "Community-Wide Implementation of Health Information Technology: The Massachusetts EHealth Collaborative Experience," *Journal of the American Medical Informatics Association* (16:1), pp. 132–139.

Gowrisankaran, G., and Stavins, J. 2004. "Network Externalities and Technology Adoption: Lessons from Electronic Payments," *RAND Journal of Economics* (35:2), pp. 260–276.

Grant, G., and Tan, F. B. 2013. "Governing IT in Inter-Organizational Relationships: Issues and Future Research," *European Journal of Information Systems*.

Heath, M., Appan, R., and Gudigantala, N. 2017. "Exploring Health Information Exchange (HIE) Through Collaboration Framework: Normative Guidelines for IT Leadership of Healthcare Organizations," *Information Systems Management* (34:2), Taylor & Francis, pp. 137–156.

Hoffman, S., and Podgurski, A. 2009. "Scholarly Commons E-Health Hazards: Provider Liability and Electronic Health Record Systems E-HEALTH HAZARDS: PROVIDER LIABILITY AND ELECTRONIC HEALTH RECORD SYSTEMS," *Scholarly Commons*.

Huang, C. D., Behara, R. S., and Goo, J. 2014. "Optimal Information Security Investment in a Healthcare Information Exchange: An Economic Analysis," *Decision Support Systems*.

Hui, K.-L., Kim, S. H., and Wang, Q.-H. 2017. "Cybercrime Deterrence and International Legislation: Evidence From Distributed Denial of Service Attacks.," *MIS Quarterly* (41:2), pp. 497-A11.

Katz, M. L., and Shapiro, C. 1986. "Technology Adoption in the Presence of Network Externaliteis," *Journal of Political Economy* (94:4), pp. 822–841.

Kern, L. M., Barron, Y., Abramson, E. L., Patel, V., and Kaushal, R. 2009. "HEAL NY: Promoting Interoperable Health Information Technology in New York State," *Health Affairs* (28:2), pp. 493–504.

Kim, B. 2013. "Competitive Priorities and Supply Chain Strategy in the Fashion Industry Bowon," *Qualitative Market Research: An International Journal,* (16:2), pp. 214–242.

Kumar, K., and Dissel, H. G. Van. 1996. "Managing Conflict and Cooperation in Interorganizational Systems," *Management Information Systems Quarterly* (20:3), pp. 279–300.

Kunreuther, H., and Heal, G. 2003. "Interdependent Security," *Journal of Risk and Uncertainty* (26:2–3), pp. 231–249.

Kwon, J., and Johnson, M. E. 2014. "Proactive Versus Reactive Security Investments in the Healthcare Sector," *MIS Quarterly* (38:2), pp. 451-+.

Kwon, J., and Johnson, M. E. 2017. "Meaningful Healthcare Security : Does ' Meaningful - Use ' Attestation Improve Information Security Performance ?," *MIS Quarterly (Forthcoming)* (2:4), pp. 1–5.

Kwon, J., and Johnson, M. E. 2018. "Meaningful Healthcare Security: Does Meaningful-Use Attestation Improve Information Security Performance?," *MIS Ouarterly* (42:4), pp. 1043–1067.

Lee, Y., and Cavusgil, S. T. 2006. "Enhancing Alliance Performance: The Effects of Contractual-Based versus Relational-Based Governance," *Journal of Business Research* (59:8), pp. 896–905.

Liu, C.-W., Smith, R. H., Huang, P., and Lucas, H. C. 2016. *IT Governance, Security Outsourcing, and Cybersecurity Breaches: Evidence from the U.S. Higher Education*.

Malone, T. W. . 1987. "Modeling Coordination in Organizations and Markets," *Management Science* (33:10), pp. 1317–1332.

McCarthy, D. B., Propp, K., Cohen, A., Sabharwal, R., Schachter, A. A., and Rein, A. L. 2014. "Learning from Health Information Exchange Technical Architecture and Implementation in Seven Beacon Communities," *EGEMs (Generating Evidence & Methods to Improve Patient Outcomes)* (2:1).

Miller, Amalia R., and Tucker, C. 2009. "Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records," *Management Science* (55:7), pp. 1077–1093.

Miller, Amalia R, and Tucker, C. 2009. "Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records (Electronic Companion)," *Management Science* (55:7).

Miller, A. R., and Tucker, C. E. 2011. "Encryption and the Loss of Patient Data," *Journal of Policy Analysis and Management : [The Journal of the Association for Public Policy Analysis and Management]* (30:3), pp. 534–556.

Miller, A. R., and Tucker, C. E. 2014. "Electronic Discovery and the Adoption of Information Technology," *Journal of Law, Economics, and Organization* (30:2), pp. 217–243.

Morgan, L., Feller, J., and Finnegan, P. 2013. "Exploring Value Networks: Theorising the Creation and Capture of Value with Open Source Software," *European Journal of Information Systems* (22:5), pp. 569–588.

Ogut, H. U., Menon, N., and Raghnathan, S. 2004. "Cyber Insurance and IT Security Investment: Impact of Interdependent Risk," *Infosecon.Net*, pp. 1–30.

Overhage, J. M., Evans, L., and Marchibroda, J. 2005. "Communities' Readiness for Health Information Exchange: The National Landscape in 2004," *Journal of the American Medical Informatics Association* (12:2), pp. 107–113.

Pang, M., and Tanriverdi, H. 2017. "Security Breaches in the U . S . Federal Government."

Pevnick, J. M., Claver, M., Dobalian, A., Asch, S. M., Stutman, H. R., Tomines, A., and Fu, P. 2012. "Provider Stakeholders' Perceived Benefit from a Nascent Health Information Exchange: A Qualitative Analysis," *Journal of Medical Systems* (36:2), pp. 601–613.

Pirnejad, H., Bal, R., and Berg, M. 2008. "Building an Inter-Organizational Communication Network and Challenges for Preserving Interoperability," *International Journal of Medical Informatics*.

Ponemon. 2016. "Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data," *Annual Benchmark Study on Privacy & Security of Healthcare Data* (5:May), pp. 1–42.

Ponemon Institute LLC. 2018. "2017 Cost of Data Breach Study, Global Overview," *IBM Security*.

Poppo, L., and Zenger, T. 2002. "Do Formal Contracts and Relational Governance Function as Substitutes or Complements?," *Strategic Management Journal* (23:8), pp. 707–725.

Prochaska, M. T., Bird, A.-N., Chadaga, A., and Arora, V. M. 2015. "Resident Use of Text Messaging for Patient Care: Ease of Use or Breach of Privacy?," *JMIR Medical Informatics* (3:4), p. e37.

Ramon Gil-Garcia, J., Chengalur-Smith, I. S., and Duchessi, P. 2007. "Collaborative E-Government: Impediments and Benefits of Information-Sharing Projects in the Public Sector," *European Journal of*

Information Systems (16:2), pp. 121–133.

Riggins, F. J., Kriebel, C. H., and Mukhopadhyay, T. 1994. "The Growth of Interorganizational Systems in the Presence of Network Externalities," *Management Science* (40:8), pp. 984–998.

Romanosky, S., Telang, R., and Acquisti, A. 2011. "Do Data Breach Disclosure Laws Reduce Identity Theft," *Journal of Policy Analysis and Management* (32:2), pp. 296–322.

Scholl, M., Stine, K., Lin, K., and Steinberg, D. 2010. *Security Architecture Design Process for Health Information Exchanges (HIEs)*.

Simons, R. 1991. *Strategic Orientation and Top Management Attention to Control Systems*, (12:December 1988), pp. 49–62.

Sittig, D. F., and Singh, H. 2011. "Legal, Ethical, and Financial Dilemmas in Electronic Health Record Adoption and Use," *Pediatrics* (127:4), pp. e1042–e1047.

Staiger, D., and Stock, J. 1997. "Instrumental Variables Regression with Weak Instruments Author," *Econometrica* (65:3), pp. 557–586.

Straub, D. W., and Welke, R. J. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), p. 441.

Symantec. 2018. "2018 Internet Security Threat Rerpot - Executive Summary."

Verizon. 2016. "2016 Data Breach Investigations Report," *Verizon Business Journal* (1), pp. 1–65.

Walker, J., Pan, E., Johnston, D. S., Adler-Milstein, J., Bates, D. W., and Middleton, B. 2005. "The Value of Health Care Information Exchange and Interoperability.," *Health Affairs* (Suppl Web), pp. W5-10-W5-18.

Wang, E. T. G., and Seidmann, A. 1995. "Electronic Data Interchange: Competitive Externalities and Strategic Implementation Policies," *Management Science* (41:3), pp. 401–418.

Wong L.Y., T. M. P. H. S. 2010. "Barriers to Cross-Institutional Health Information Exchange ---A Literature Review," *Complementary Therapies in Medicine* (24:3), pp. 22–34.

Woodham, P. W. and R. 2002. "Don ' t Just Lead , Govern : Implementing Effective IT Governance," *MIT Sloan School of Management Working Ppaer*, p. 17.

Zhu, K., Kraemer, K. L., Gurbaxani, V., and Xu, S. X. 2006. "Migration to Open Standard Interorganizational Systems: Network Effects, Switching Costs and Path Dependency," *MIS Quarterly* (30:August), pp. 515–539.