THE MARKET EFFECT OF HEALTHCARE SECURITY: DO PATIENTS CARE ABOUT DATA BREACHES? [*]

Juhee Kwon[†] and M. Eric Johnson[‡]

Abstract

Data breach notification required by federal and state regulators has reduced information asymmetry on the effectiveness of information security programs. While pervasive media coverage of data breaches likely tarnishes an organization's reputation, there is little empirical evidence that shows how consumers react to such organizational failures. Focusing on the healthcare sector as one of the most information-intensive service industries, this paper investigates consumer reaction to data breaches by examining changes in patient visits consequent to breaches. Using a propensity score matching technique, we analyze a matched sample of 761 U.S. hospitals. We investigate how data breaches affect subsequent outpatient visits and admissions, accounting for the geographical-based competition within a Core Based Statistical Area (CBSA). We find that while data breaches do not affect patients' short-term choices, the cumulative effect of breach events over a three-year period significantly decreases the number of outpatient visits and admissions. Similarly, the cumulative number of breached records is negatively associated with outpatient visits and admissions. Further, the cumulative effects in competitive markets are significantly larger than those in non-competitive markets, which are insignificant. Our findings provide policy insights on effective security programs that induce providers to invest in security as they would for other market-based, brand-building initiatives.

Keywords: Security, Data Breaches, Healthcare, Economics, Propensity Score

[*] This research was partially supported by a collaborative award from the National Science Foundation (NSF award number CNS-1329686). The views and conclusions in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of NSF.

[†] Juhee Kwon, Assistant Professor of Information Systems in the College of Business at the City University of Hong Kong, juhee.kwon@cityu.edu.hk.

[‡] M. Eric Johnson, Ralph Owen Dean and Bruce D. Henderson Professor of Strategy in the Owen Graduate School of Management at Vanderbilt University, eric.johnson@owen.vanderbilt.edu.

Introduction

Information security failures have drawn significant media attention and consumer concern. In a few dramatic cases, like the recent Target breach, consumers have punished firms with reduced demand (McGrath 2014). Much of this impact appears to be somewhat short-lived and limited to the most egregious breaches. Many smaller breaches only receive moderate media coverage and consumers are often left with little real information concerning the trustworthiness of the firms where they do business. Security economics researchers have noted that investors also appear to shrug off breaches, with only limited stock price impact (Campbell et al. 2003; Cavusoglu et al. 2004; Kannan et al. 2007; Wang et al. 2013). This would lead one to conclude that securities markets do not see long-term revenue impact from breaches.

In past few years, the visibility of healthcare breaches has increased dramatically due to new breach reporting rules implemented under the HITECH Act. The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 encouraged healthcare providers to implement electronic healthcare records (EHRs) by channeling billions of dollars in financial incentives to adopters. Along with the rapid rise of EHRs adoption, more than 90% of healthcare providers also reported at least one data breach since 2011 (Ponemon 2013b) [1]. This recent breach epidemic was partially the result of stricter breach notification requirements that were tied to the HITECH Act. The requirements mandated that healthcare providers who discovered a data breach notify impacted individuals within 60 days after the discovery. Further, if the breach affected more than 500 people, it must be reported to media outlets and the U.S. Health and Human Services (HHS) (which posts such breaches on its website – sometimes

[1] The Ponemon survey (2013b) employed 80 healthcare organizations. Hospitals were asked to indicate if the experienced any type of breach, regardless of size or type of data lost. Our sample focuses on larger breaches involving PHI (HHS requires reporting for breaches involving more than 500 individuals). It is also likely that Ponemon's respondents would have more breach experience, and it might make the organizations actively participate in Ponemon's security survey due to security concerns. Our study employs a much large sample of 4,098 hospitals.

referred to as the Wall of Shame)[2] (HHS 2009). Such notification requirements have greatly contributed to the visibility of breaches of personally identifiable information, significantly adding to state breach notification laws already on the books.

Patient data breaches have often created strong public reactions, likely because of the private nature of medical information. However, the fear of security reputation loss does not appear to have induced appropriate security investment. Regulatory penalties under HITECH can force organizations to increase security efforts, yet few healthcare organizations have faced extensive regulatory action. With many data breaches and few geographic markets with significant competition, observers have noted that customers have little information to make informed hospital choices. Moreover, the imperfection of healthcare markets, which are characterized by provider consolidation and an insurance-induced wedge between patient and provider, may create moral hazards within the sector.

Certainly wide media coverage of massive data breaches, like the recent Community Health System hack (Munro 2014), has likely tarnished the reputations of some hospitals. This led us to consider consumer market reaction to increased breach reporting. Understanding the market reaction to data breaches has long attracted the attention of researchers in information security economics. Some researchers have investigated the market effect of data breaches by estimating the stock market reaction to data breaches (Kannan et al. 2007; Mulligan et al. 2007). Since few healthcare providers are publicly traded, focusing on equity markets has not been particularly fruitful in characterizing the business impact of data breaches. Thus, we examine how data breaches are linked to changes in subsequent outpatient visits and admissions, controlling for important local factors like market competition and other characteristics of healthcare providers.

[2] Breaches Affecting 500 or More Individuals, see https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Using a propensity score matching technique combined with a difference-in-differences approach, we find that data braches do not have any short-term impact on patient visits. However, the cumulative effects of breaches and affected records over a three-year period significantly decreases patient visits in competitive markets, but neither have any effect in non-competitive markets. Our findings indicate how patients respond to data breaches within different local markets. Understanding the market effect of data breaches enables policy makers to design programs that induce providers to invest in security as they would for other market-based, brand-building initiatives.

Background

Economic theory has suggested two ways to mitigate information asymmetry in an imperfect market (Greene 2003). First, information asymmetry can be mitigated by improving data transparency through regulatory requirements such as breach notification. Second, policy makers can offer certification programs that induce organizations to meet minimum standards. An organization's effort to meet such certification standards can help them learn and credibly improve security levels (Kwon et al. 2014). Later, if a data breach occurs, regulators and customers are more likely able to recognize whether the breach was the result of inadequate effort or bad luck (Kox 2013).

In healthcare, there have been some regulatory efforts to reduce information asymmetry. The recent U.S. HITECH Act provided various mechanisms (i.e., meaningful-use of EHR, breach notification, etc.) in order to resolve information asymmetry on a provider's security capability and performance. Through reputation formation, markets can curb moral hazards related to information asymmetry. The more reliable a provider's security reputation is, the more customers would trust the provider. Healthcare providers that show that they care about protecting patient information signal their trustworthiness.

From a market perspective, customers desiring better data protection would frequent high-security providers and potentially pay higher prices (Kox et al. 2014). However, it is often impossible or very costly for customers to observe an organization's security practices. Customers must simply assume that organizations work to ensure their best interest. Such information asymmetry induces a moral hazard problem that organizations do not make the needed investments to prevent security breaches. The impact of information asymmetry is exacerbated because it is sometimes difficult to verify whether a data breach has taken place. In this situation, organizations may keep data breaches silent for fear of reputation loss or monetary penalties.

Such moral hazards can be suppressed by reducing information asymmetry and punishing breached organizations (Greene 2003). The HITECH Act implements both breach notification requirements and penalties for unsecured data breaches. These mandated breach notifications and resulting media coverage have alerted customers to the security failures. Stronger data breach disclosure rules may reduce information asymmetry and signal security quality in way that actually changes customers' choices. Indeed, a recent Ponemon survey revealed that when medical records were lost or stolen, 57% of respondents said they would want to find another healthcare provider. Even without a breach, 56% said that if they believed their health provider was unable to safeguard medical records, they would seek another provider (Ponemon 2012). A drop in patient visits results in a decrease in revenue. Additionally, a breached provider may bear the cost of breach notification, remediation, litigation, and settlement.

Conversely, other recent surveys have highlighted breach fatigue, indicating that customers may be growing weary of the epidemic of data breaches (Ponemon 2013a; Ponemon 2014). These results indicated that while data breaches are still compounding the public fears of identity theft, 71% of respondents said they rarely discontinued their relationship with a breached healthcare provider. Indeed 61% of them said they believed that data breaches affect most providers and they think it is unavoidable, while 67% explained that it is too difficult to find another provider with comparable services. A full 45% chose to maintain the relationship despite a breach, because they believed that their healthcare providers resolved the security failure to their satisfaction. These responses show that data breach fatigue could result in continued relationships with breached organizations—likely due to the post-HITECH epidemic of data breach disclosures and low market competition in some geographies.

Consolidation within U.S. healthcare markets has further reduced competition in already imperfect markets characterized by an insurance-induced wedge between patient and provider. Although patients may want to avoid breached providers, they may not be able to find other suitable alternatives within their geographic area that are also covered by their insurance. On the other hand, in competitive healthcare markets, data breaches could impact patient visits to hospitals with visible security failures. In this project, we empirically examine how data breach disclosures affect patient visits to breached healthcare providers and how market competition influences the effect of breaches on patient visits.

Data

Sample

Our data were collected from several sources. Hospital data came from the Healthcare Information and Management Systems Society (HIMSS) Analytics™ Database, which has been widely used in previous studies to examine the impact of healthcare information systems (Angst et al. 2009; Hillestad et al. 2005; Miller et al. 2009). The database provides information about the number of admissions, the number of outpatient visits, the numbers of adopted healthcare and security applications, and organizational characteristics (i.e., operating expense, organizational type, bed size, academic, etc.). We focus on acute-care hospitals that provide short-term medical and/or surgical treatment and care. The total longitudinal sample includes 4,098 hospitals reporting annual status for more than consecutive 3 years to acquire pre-breach information.

Healthcare data breaches were obtained from two data sources: HHS (from 2009 to 2013) and Privacy Clearinghouse (from 2006 to 2013)[3]. Data breaches were matched with the hospitals from the HIMSS database. Over the period from 2007 to 2013 (see Appendix B1), our sources reported 735 unique data breaches. Among them, 500 breaches occurred in our sample of acute-care hospitals. The remaining 235 breaches were dropped because they occurred in other healthcare-related businesses.

Finally, we employed hospital location-specific demographic information such as the population eligible for Medicare, total population, and the number of hospitals in the area. This data were supplied via the Core Based Statistical Area (CBSA) level in the Area Health Resources Files (AHRF)[4]. A CBSA is a U.S. geographic area defined as an urban center of at least 10,000 people and adjacent areas that are socioeconomically tied to the urban center by commuting. CBSA can be categorized as metropolitan statistical areas having over 50,000 people and micropolitan areas fewer than 50,000.

[3] Chronology of Data Breaches Security Breaches 2005 – Present. See http://www.privacyrights.org/data-breach

[4] The AHRF provides an extensive county-level database assembled annually from over 50 sources including extensive demographic and training information on over 50 health professions. See http://ahrf.hrsa.gov/download.htm

Measures

We compare hospitals that experienced data breaches to those that did not, but match on other key factors including prior breaches, prior patient visits and admissions, adopted EHRs, full-time employees, operating expense, and academic type. Table 1 includes the definitions of the variables employed in this study. *Breach* was measured as a binary variable reflecting whether a hospital experienced any breach in year t, while *prebreach* is the number of data breaches that a hospital experienced in the prior 36 months. *Affected records* denotes the number of records compromised by data breaches within 36 months. In order to examine the changes in patient visits due to a data breach, two variables were employed: *outpatient visits* and *admissions. Outpatient visits* denotes the number of outpatient visits, and *admissions* were measured as the number of patient admissions, which include the number of adult and pediatric admissions (excluding births). For these variables, a logarithmic transformation was used because, from an econometric perspective, the probability of a data breach is a concave function of the number of the prior patient visits, operating expense, and healthcare applications. For instance, when a healthcare provider has a very large number of patient visits, the marginal effect of an additional patient visit (e.g., operating expense and healthcare applications) should not be as big as that for a healthcare provider who has very few patient visits (Greene 2003). Using the same reasoning, the number of patient visits in a period subsequent to a breach is a convex function of the number of breached records. When a breach affects more than one million records, the marginal effect of additional affected records should not be the same as that of a breach that affects only hundreds or fewer records.

Based on the numbers of *outpatient visits* and *admissions*, we estimated each hospital's *market share*. A hospital's outpatients and admissions were divided by the total number of outpatient visits and admissions within a CBSA, respectively. *Marketshare* was measured by a hospital's portion of total outpatient visits and admissions within a CBSA[5]. In order to consider a hospital's effort for regulatory compliance, our model includes *MUyears*, which was measured by counting the years since a hospital had attested to Meaningful Use (MU) of EHRs.

We further considered other organizational characteristics, including *the numbers of healthcare applications* (*i.e., EHR systems, security*, and *healthcare clinic applications*), *operating expense, no of beds,* and *academic type.* Additionally, *Security* represents the number of adopted security applications such as anti-virus, encryption, firewall, intrusion detection, user authentication, and spam/spyware filter. Likewise, *EHRs* denote the number of adopted EHRs applications (e.g., Clinical Decision Support System, Computerized Practitioner Order Entry, Medical Vocabulary, Order Entry, Patient/Physician Portal, EMR, etc.). *Health IT* includes all adopted applications used in clinical workflows (e.g., Nursing system, Ambulatory system, Cardiology, Clinical System, Scheduling, etc.). *OpExp* represents hospital fiscal-year spending on operations such as staffing, property expenses, etc. *Beds and FTE were* measured as the numbers of licensed bed and full-time employees, respectively.

Academic describes whether the hospital is an academic organization or not. Many healthcare providers are affiliated with a group that consists of a main organization named *parent* and other sub-organizations affiliated with the "*parent*". Given this structure, the size of the group with which a hospital is affiliated is also important. *Affiliation* denotes the number of affiliated members in a group. *Metro* indicates whether a hospital is in a metropolitan area or a micropolitan area. *Population* and the number of hospitals (*NofHospitals*) were included as CBSA-level control variables. Table 2 shows descriptive statistics for all variables.

[5] $Marketshare = (\frac{A\ hospital's\ outpatient\ visits}{A\ CBSA' soutpaient\ visits} + \frac{A\ hospital's\ admissions}{A\ CBSA' admissions})/2$

Empirical Analysis and Results

Our study aims to empirically identify changes in patient visits consequent to data breaches, controlling for hospital market share and other factors. In this research context, it is important to account for causality related to self-selection bias. For instance, hospitals that have more patient visits may likely be larger and have more resources and subsequently have better security performance. If this causality issue is significant, we anticipate that hospitals would have fewer patient visits both prior to a data breach as well as afterward. To control for selection bias, we employed a propensity score matching technique.

Selection Analysis

Propensity score matching has been used to select treatment and control groups that resemble each other in all relevant characteristics before an event (in our case, a data breach) to create a statistical equivalence between two groups (Rishika et al. 2013; Rosenbaum et al. 1983). Following an approach outlined in earlier studies (Heckman et al. 1997; Levine et al. 2010; Smith et al. 2005), our selection analysis seeks to discern whether the two groups (those who experienced a breach and those who did not) were similar in outpatient visits, admissions, MU attestation, operating expense, healthcare applications, and others (i.e., metropolitan area, academic type, the size of an affiliated group, etc.) prior to a data breach. After dropping bed size, which is highly correlated to admissions, most of the correlations among the variables show low values (see Table 3 and Appendix B2). The tolerances and variance inflations indicate that multicollinearity is not a concern in our selection model.[6]

[6] The variance inflations of all variables are less than four. A usual threshold of variance inflations is 10.0, which corresponds to a tolerance cutoff of 0.1.

Next, we used a logit model to evaluate which factors affect a hospital's breach occurrence and calculate the probability of breach occurrence based on the characteristics. The dependent variable, *Breach* is a dummy, coded as one in year *t*, if a hospital experienced a breach in that year:

$$\begin{aligned} Breach_{it} = F(\, & Prebreaches_{it-1\sim-3}, lnAddimissions_{it-1}, lnOutpatientVisits_{it-1}, \\ & lnOpExp_{it-1}, lnEHRs_{it-1},\ lnHealthIT_{it-1}, lnSecurity_{it-1}, \\ & Affiliation_{it-1},\ MUYears_{it-1}, Academic_{it-1}, lnFTE_{it-1}, \\ & Metro_{it-1}, Year_{i}, u_{it}\,) \end{aligned} \qquad (1)$$

where $F(\cdot)$ is the logit function.

Table 4 presents the results from the selection model (1). The results suggest that hospitals that experienced data breaches in last three years were more likely to have a subsequent breach (0.709 at $p < 0.01$). Data breaches were more likely in hospitals having more admissions (0.287 at $p < 0.01$) and academic hospitals (0.729 at p < 0.01). While more healthcare applications lead to a higher probability of breach occurrence (2.791 at $p < 0.01$), EHRs were negatively associated with breach occurrence (-0.578 at $p < 0.01$). This implies EHR adoption improves information security, but the complexity of many added healthcare applications adds risk—likely related to integration weaknesses and the challenges of holistic security across applications. Hospitals in metropolitan areas were more likely to experience breach occurrences (0.796 at $p < 0.01$) than in micropolitan areas, and hospitals affiliated with a larger group were less likely to have a breach (-0.003 at $p <0.01$).

Matching on a propensity score estimated by the logit model (1) allows us to identify a control group of non-breached hospitals with similar pre-period patient visits and other breach determinants (e.g., EHRs, healthcare applications, security software, MU attestation, etc.) to those who experienced a data breach. Single nearest neighbor matching was employed with a caliper approach. Each breached hospital was matched to a hospital having the most similar propensity score without a data breach. We refer to the absolute difference between the two propensity scores in a matched pair of hospitals as the “match distance”. Best matches were first made and next-best matches were chosen within 0.003, until no further matches could be made. Of the 500 breach incidents for which we estimated propensity scores, we successfully matched 406 treatments with meaningful use to 355 controls. The number of control hospitals was smaller than treatment hospitals because some hospitals experienced more than one breach.

To further ensure the quality of our propensity score matching, we examined how the independent variables were positioned between the treatment and control groups in the post matching condition by using *t*-tests within the matched groups. As described in Table 5, the differences between the two groups of post-matching hospitals on admissions and outpatient visits are substantially smaller, implying better statistical balance on their performance. Further, we compared the difference of propensity scores to check if there was substantial overlap in the characteristics of the hospitals that experienced a breach and those who did not. The total sample (before matching) shows a significant difference in the propensity scores between the two groups (-14.21 at $p < 0.01$). After matching, the two groups have nearly identical propensity scores (-0.25 at $p > 0.1$).

Treatment Analysis

While propensity score matching can resolve the selection bias on observable variables, our analysis could still be complicated by bias from unobservable factors (Heckman et al. 1997). Hospital-specific unobservable factors may jointly affect security failure and healthcare performance. For instance, hospitals with well-integrate EHRs (that information was not included in our data) might achieve both better data protection and more patient visits. Thus, data breaches could be correlated with patient visits, but not affect it.

In order to eliminate the bias of such unobservable factors between treatment and control hospitals, we utilized a difference-in-differences approach along with propensity score matching. Estimating treatment effects with a difference-in-differences specification using panel data is a robust technique recently used by researchers (Amore et al. 2014; Gopal et al. 2013; Levine et al. 2010; Rishika et al. 2013). In our study, a difference-in-differences estimator generally represents the difference of patient visits (i.e., the number of admissions and outpatient visits) between pre and post period for the treatment and control groups. A difference-in-differences technique allows each hospital to have its own (unique) baseline level for each outcome. Since the control group has very similar characteristics to the treatment group, except for breach experience, the difference in the trends of patient visits before and after a breach can be better attributed to the breach. If there were important unobservable factors that affected patient visits to a hospital and that differed between breached and non-breached hospitals, the effect of a breach on the changes in breached hospitals' patient visits between two periods would have been indistinguishable from that of the changes in non-breached hospitals.

Our treatment model evaluates how data breaches affect the differences of the two groups' patient visits between the periods. The differences are measured as the changes in outpatient visits and admissions ($\mathit{\Delta} lnpatientVisits_{it,Diff(t_{+1}-t)}$) for the period 12 months before and 12 months after a breach ($\Delta lnOutPatientVisits_{it,(t_{+1}-t)}$ and $\Delta lnAdmisisons_{it,(t_{+1}-t)}$).

$$\begin{aligned} &\mathit{\Delta} lnPatientVisits_{it,Diff(t_{+1}-t)} = \qquad (2) \\ &\quad \beta_{0i} + \beta_1 Breach_{it} + \beta_2 lnPatientVisits_{it} + \beta_3 lnOpExp_{it} + \beta_4 lnEHRs_{it} \\ &\quad + \beta_5 lnHealthIT_{it} + \beta_6 lnSecurity_{it} + \beta_7 Affiliation_{it} + \beta_8 Academic_{it} \\ &\quad + \beta_9 MUyears_{it}, + \beta_{10} MarketShare_{it} + lnFTE_{it-1} + \beta_{11} lnNofHospitals_{it} + \epsilon_{it} \end{aligned}$$

$$\Delta lnPatientVisits_{it,Diff(t_{+1}-t)} = \tag{3}$$
$$\beta_{0i} + \beta_1 PreBreach_{it} + \beta_2 lnPatientVisits_{it} + \beta_3 lnOpExp_{it} + \beta_4 lnEHRs_{it}$$
$$+ \beta_5 lnHealthIT_{it} + \beta_6 lnSecurity_{it} + \beta_7 Affiliation_{it} + \beta_8 Academic_{it}$$
$$+ \beta_9 MUyears_{it}, + \beta_{10} MarketShare_{it} + lnFTE_{it-1} + \beta_{11} lnNofHospitals_{it} + \epsilon_{it}$$

$$\Delta lnPatientVisits_{it,Diff(t_{+1}-t)} = \tag{4}$$
$$\beta_{0i} + \beta_1 lnAffectedRecords_{it} + \beta_2 lnPatientVisits_{it} + \beta_3 lnOpExp_{it}$$
$$+\beta_4 lnEHRs_{it} + \beta_5 lnHealthIT_{it} + \beta_6 lnSecurity_{it} + \beta_7 Affiliation_{it}$$
$$+\beta_8 Academic_{it} + \beta_9 MUyears_{it}, + \beta_{10} MarketShare_{it} + lnFTE_{it-1}$$
$$+ \beta_{11} lnNofHospitals_{it} + \epsilon_{it}$$

Only breached hospitals in each pair of the matched sample have a positive value for the binary variable ($Breach_{it}$), which was coded as 1 if a data breach occurred within 12 months, and 0 otherwise (Model (2)). We further analyzed the effects of cumulative breaches ($PreBreach_{it}$) , which was measured as the number of data breaches that occurred in last 36 months and the affected records ($lnAffectedRecords_{it}$), which denote the number of records compromised by data breaches within 36 months (Model (3) and (4)). Our primary interest is the coefficient, β_1, which represents the estimated effect of data breaches on patient visits.

The results of the treatment models (2) ~ (4) are presented in Table 6. Model (2) evaluates the effect of breach occurrence within a year. The results of Model (2) show that a recent breach occurrence does not have any influence on either outpatient visits or admissions. On the other hand, the cumulative effect of data breaches in Model (3) was associated with a significant decrease in outpatient visits (-0.226 at $p < 0.05$) and admissions (-0.621 at $p < 0.01$). This implies that patients do not immediately react to a breach, but rather over time, and with multiple breaches, patients are more likely to switch healthcare providers. The results of Model (4) demonstrate that breach size, in terms of number of patients effected, also matters. Larger breaches are associated with larger decreases (-0.036 at p <0.05 for outpatient visits and -0.083 at p <0.01 for admissions). Note that MU attestation does not appear to have any effect on patient visits. This implies that the HITECH instituted MU certification program does not contribute to reducing patient information asymmetry (thus impacting demand), although it should be linked to developing better procedures on the supply (provider) side.

Market share

Healthcare markets exhibit geographical-based competition within each local area. When more than one hospital exists in a local area, they compete for market share. However, there may be few healthcare markets with enough competition to allow patients to make choices based on security issues (Gaynor et al. 2012). Thus, we further analyzed whether a hospital's market share influenced the effect of data breaches on patient visits.

We categorized hospitals into three groups based on the competition in each local market (i.e., CBSAs) in terms of the distribution of market share. The categorization based on the distribution makes it possible to balance the sample sizes among the groups. In group one, 380 hospitals reside between the 25th and 75th percentile of market share (174 and 206 in the control and treatment groups, respectively). These hospitals have enough competitors with comparable services to ensure a competitive marketplace (the 25th and 75th percentile represent hospitals with market shares between 1.42% and 17.55%). The remaining 190 small hospitals with insignificant market power and 191 large hospitals with significant market power are assigned into the other two groups (91 and 90 in the controls, 99 and 101 in treatments, respectively) (see Figure 1). Large providers have few comparable competitors and significant market power. At the other end of the spectrum, very small providers may draw little media coverage from a breach and serve small populations thus making their impact negligible. Appendix A1 provides the details on the distribution of market share.

For the three groups, we separately analyzed the effect of data breaches on patient visits. As described in Table 7 and 8, we found that hospitals in the competitive market group had results that were consistent with the aggregate analysis, but with higher R-squared. While there was little short-term impact in the competitive markets, the cumulative impact of data breaches and affected records was associated with significantly decreased outpatient visits and admissions (-0.427 and -0.057 at $p < 0.05$ in outpatients visit, -0.987 and -0.124 at $p < 0.01$ in admissions). For the hospitals groups with very large or very small market share, we found no significant effect between breaches and patient visits. In order to ensure robustness, we further conducted our analysis with two groups (thus creating the same sample size): the competitive group (hospitals between the 25th and 75th percentile of market share) and non-competitive group (very large and small hospitals combined). As described in Appendix A2 and A3, the effects of breaches were consistent with the three group analysis.

Discussion and Conclusions

Healthcare is one of the most regulated sectors in the U.S. economy. With increasing concerns over the security and privacy of patient healthcare data, regulators at both the state and federal levels have deployed legislation to encourage better information security. Researchers have examined the impact of the incentives and penalties related to security and data breaches. Far less attention has been paid to market mechanisms that might impact security investment. Breach notification and media coverage of data breaches has improved consumer awareness of provider security performance. We examined market reaction to hospital data breaches by analyzing both the short-term and cumulative impact of breaches on subsequent outpatient visits and admissions, accounting for geographically based competition.

We found that data breaches do not affect patients' short-term choices, but the cumulative effect of breach events over a three-year period significantly decreased the number of outpatient visits and admissions. The cumulative number of breached records was also negatively associated with outpatient visits and admissions. Overall, the breaches had the most impact in competitive markets where consumers had significant provider choice. Our results suggest that consumers react to cumulative data breaches, but their reaction is restricted in markets with limited competition.

This paper builds on the practical and theoretical foundations of security signals in healthcare markets with information asymmetry. While prior security research focused on studying the supply-side effect, such as security investment and regulatory compliance, our study investigated the demand-side effect such as consumer reaction to information security under various market conditions. From the theoretical perspective, our study extends prior research in moral hazards arising from information asymmetry by applying the theory to information security in healthcare markets. Although the market impact of quality and security in healthcare is clouded by the U.S. third-party payment system and government intervention, healthcare markets remain subject to the fundamental rules of economics, and economic analysis is essential in appraising public policy.

Our study also provides an empirical understanding of market reactions in the security context. We identify how cumulative data breaches influence subsequent demand, accounting for market structure. The results provide policy insights on effective security guidelines aligned with the complex healthcare markets. Policy-makers should focus on providing differentiated security programs which work differently based on a hospital’s market power and also considering the heterogeneity of competition in a marketplace. For instance, in terms of regulatory interventions, a carrot approach can be used for hospitals with insignificant market power, while a stick approach could be useful for those with significant market power. Competition and information transparency can drive hospitals within competitive markets to actively develop and maintain security programs.

References

Amore, M. D., Garofalo, O., and Minichilli, A. "Gender Interactions Within the Family Firm," *Management Science* (60:5), May 2014, pp 1083-1097.

Angst, C. M., and Agarwal, R. "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuation," *MIS Quarterly* (33:2) 2009, pp 339-370.

Campbell, K., Gordon, L., Loeb, M., and Zhou, L. "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," *Journal of Computer Security* (11:3) 2003, p 431.

Cavusoglu, H., Mishra, B., and Raghunathan, S. "The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers," *International Journal of Electronic Commerce* (9:1), Fal 2004, pp 69-104.

Gaynor, M. S., Hydri, M. Z., and Telang, R. "Is Patient Data Better Protected in Competitive Healthcare Markets? ," in: *Workshop on the Economics of Information Security (WEIS), Berlin, Germany*, 2012.

Gopal, A., Goyal, M., Netessine, S., and Reindorp, M. "The Impact of New Product Introduction on Plant Productivity in the North American Automotive Industry," *Management Science* (59:10), Oct 2013, pp 2217-2236.

Greene, W. H. *Econometric Analysis*, (5th ed.) Prentice Hall, 2003.

Heckman, J. J., Ichimura, H., and Todd, P. E. "Matching as an econometric evaluation estimator: Evidence from evaluating a job training programme," *Review of Economic Studies* (64:4), Oct 1997, pp 605-654.

HHS "Breach Notification for Unsecured Protected Health Information; Interim final Rule," D.o.H.a.H. Services (ed.), 2009, pp. 42740-42770.

Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville, R., and Taylor, R. "Can electronic medical record systems transform health care? Potential health benefits, savings, and costs," *Health Affairs* (24:5), Sep-Oct 2005, pp 1103-1117.

Kannan, K., Rees, J., and Sridhar, S. "Market reactions to information security breach announcements: An empirical analysis," *International Journal of Electronic Commerce* (12:1), Fal 2007, pp 69-91.

Kox, H., and Straathof, B. "Economic aspects of Internet Security," in: *CPB Background Document*, 2014.

Kox, H. S., Bas "Economic aspects of Internet security," C.N.B.f.E.P. Analysis (ed.), 2013.

Kwon, J., and Johnson, M. E. "Meaningful Healthcare Security: Does “Meaningful-Use” Attestation Improve Information Security Performance?," in: *Workshop on the Economics of Information Security (WEIS), Penn State University*, 2014.

Levine, D. I., and Toffel, M. W. "Quality Management and Job Quality: How the ISO 9001 Standard for Quality Management Systems Affects Employees and Employers," *Management Science* (56:6), Jun 2010, pp 978-996.

McGrath, M. "Target Profit Falls 46% On Credit Card Breach And The Hits Could Keep On Coming," in: *Forbes* http://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/, 2014.

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

Mulligan, D. K., and Bamberger, K. A. "Security Breach Notification Laws:Views from Chief Security Officers," University of California-Berkeley School of Law, 2007.

Munro, D. "Cyber Attack Nets 4.5 Million Records From Large Hospital System," in: *Forbes*, http://www.forbes.com/sites/danmunro/2014/08/18/cyber-attack-nets-4-5-million-records-from-large-hospital-system/, 2014.

Ponemon "2013 Survey on Medical Identity Theft," Ponemon Institute, https://clearwatercompliance.com/wp-content/uploads/2013/10/2013-Medical-Identity-Theft-Report-FINAL.pdf.

Ponemon "2013 Third Annual Benchmark Study on Patient Privacy & Data Security," Ponemon Institute, http://www.ponemon.org/news-2/45.

Ponemon "2014 Fourth Annual Benchmark Study on Patient Privacy and Data Security," Ponemon Institute, http://www.ponemon.org/blog/fourth-annual-benchmark-study-on-patient-privacy-and-data-security.

Rishika, R., Kumar, A., Janakiraman, R., and Bezawada, R. "The Effect of Customers' Social Media Participation on Customer Visit Frequency and Profitability: An Empirical Investigation," *Information Systems Research* (24:1), Mar 2013, pp 108-127.

Rosenbaum, P. R., and Rubin, D. B. "The central role of the propensity score in observational studies for causal effects," *Biometrika* (70:1) 1983, pp 41-55.

Smith, J. A., and Todd, P. E. "Does matching overcome LaLonde's critique of nonexperimental estimators?," *Journal of Econometrics* (125:1-2), Mar-Apr 2005, pp 305-353.

Wang, T. W., Kannan, K. N., and Ulmer, J. R. "The Association Between the Disclosure and the Realization of Information Security Risk Factors," *Information Systems Research* (24:2), Jun 2013, pp 201-218.

Table 1. Definitions of variables

Variable	Definition
Breach	1 if a hospital has any breach at year t, 0 otherwise
PreBreach	Number of breaches in last 36 months
Affected Records	the number of records compromised by data breaches within 36 months
Admissions	Number of admissions, which include the number of adult and pediatric admissions (excluding births).
OutpatientVisits	Number of outpatient visits
MUYears	Number of years after MU attestation
OpExp	Hospital spending on operations such as staffing, property expenses, etc.
EHRs	Number of adopted Electronic Healthcare Records (e.g., Clinical Decision Support System, Computerized Practitioner Order Entry, Medical Vocabulary, Order Entry, Patient/Physician Portal, etc.)
HealthIT	Number of adopted healthcare operating applications (e.g., Nursing system, Ambulatory system, Cardiology, Clinical System, Scheduling, etc.)
Security	Number of adopted security software (e.g., Anti-Virus, Encryption, Firewall, Spam/Spyware Filter, etc.)
Affiliation	Number of affiliated members
FTE	Number of full-time employees
Beds	Number of licensed beds
Academic	1 if a hospital is an academic institute, 0 otherwise.
Population	Total population in a CBSA
NofHospitals	Number of hospitals in a CBSA
Metro	1 if a hospital is in a metro area, 0 otherwise
MarketShare	Hospital market share (hospital's outpatients and admissions divided by the total outpatient visits and admissions of its CBSA, respectively)

Table 2. Descriptive statistics

Variable	Mean	StdDev	Min	Max
Breach	0.03	0.17	0.00	1.00
PreBreach	0.07	0.28	0.00	3.00
Affected Records *	21.78	292.53	0.00	413,717.13
Admissions *	9.20	10.44	0.01	303.51
OutpatientVisits *	150.98	212.48	0.00	4,310.00
OpExp †	183.24	266.75	0.07	9,502.98
EHRs	4.53	2.47	0.00	22.00
HealthIT	66.22	25.43	1.00	285.00
Security	6.63	4.47	0.00	34.00
Affiliation	24.67	41.96	1.00	162.00
FTE *	1.16	1.77	0.01	103.04
Beds *	0.21	0.20	0.00	1.87
Academic	0.06	0.24	0.00	1.00
MUyears	0.19	0.56	0.00	3.00
Metro	0.77	0.42	0.00	1.00
Population(CBSA) †	2.26	3.40	0.01	13.24
NofHospitals(CBSA)	29.57	37.91	0.00	140.00

Notes. *1,000 unit , † 1,000,000 unit. The total observations are 19,186

Table 3. Correlations

	(1)	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**	**(8)**	**(9)**	**(10)**	**(11)**	**(12)**	**(13)**	Tol	VIF
(1) Breach	1.000														
(2) PreBreach	**0.187**	1.000												0.83	1.21
(3) lnAffectedRecords	**-0.074**	**0.180**	1.000											0.88	1.14
(4) lnAdmissions	**0.141**	**0.191**	**-0.142**	1.000										0.26	3.81
(5) lnOutpatientVisits	**0.056**	**0.100**	**-0.120**	**0.620**	1.000									0.51	1.96
(6) lnOpExp	**0.035**	**0.071**	-0.034	**0.526**	**0.522**	1.000								0.53	1.88
(7) lnEHRs	**0.071**	**0.066**	**-0.144**	**0.272**	**0.149**	**0.116**	1.000							0.48	2.09
(8) lnHealthIT	**0.158**	**0.186**	-0.060	**0.553**	**0.333**	**0.223**	**0.688**	1.000						0.34	2.92
(9) lnSecurity	**0.075**	**0.118**	0.027	**0.229**	**0.087**	**0.102**	**0.286**	**0.435**	1.000					0.63	1.60
(10) Affiliation	**-0.041**	**-0.055**	-0.036	**-0.061**	**-0.244**	**-0.048**	**0.065**	**-0.020**	**0.165**	1.000				0.89	1.12
(11) Academic	**0.152**	**0.195**	-0.024	**0.298**	**0.165**	**0.177**	**0.119**	**0.186**	**0.057**	**-0.105**	1.000			0.72	1.40
(12) MUyears	**0.018**	**0.056**	0.028	**0.136**	**0.103**	**0.080**	**0.269**	**0.217**	**0.178**	**0.117**	**0.016**	1.000		0.90	1.11
(13) lnFTE	**0.120**	**0.177**	**-0.090**	**0.842**	**0.627**	**0.686**	**0.232**	**0.452**	**0.180**	**-0.135**	**0.336**	**0.101**	1.000	0.23	4.39
(14) Metro	**0.069**	**0.086**	0.053	**0.210**	-0.009	**0.081**	**0.066**	**0.097**	**0.094**	**0.077**	**0.096**	**0.020**	**0.173**	0.90	1.11

Note. Bold represents statistically significant correlation coefficients with p<0.05

Table 4. The effect of organizational factors on breach occurrence: Estimating the propensity scores for breach occurrence

DV: Breach Occurrence (0 or 1) at year, *t*				
Parameter	Estimate		StdErr	Odd Ratio Estimate
Intercept	-16.998	***	0.924	
PreBreach	0.709	***	0.095	2.032
lnAdmissions	0.287	***	0.080	1.333
lnOutpatientVisits	-0.076	**	0.033	0.926
lnOpExp	-0.036	*	0.022	0.964
lnEHRs	-0.578	***	0.102	0.561
lnHealthIT	2.791	***	0.229	16.309
lnSecurity	-0.030		0.075	0.97
Affiliation	-0.003	**	0.001	0.997
Academic	0.729	***	0.135	2.073
MUyears	0.049		0.092	1.05
lnFTE	0.051		0.073	1.053
Metro	0.796	***	0.186	2.217
Years dummies				
R-Square	0.054			
Max-rescaled R-Square	0.216			
Likelihood Ratio	852.46	***		
Observations	15,098			

Note. P-values: * Significant at p <0.1, ** Significant at p<0.05, *** Significant at <0.01

Table 5. t-tests before and after matching

Variables	Total Sample (n=19,186)					Matched Sample (n=761)				
	Breach =0 (n=18,622)		Breach =1 (n=564)		*t* Value	Breach =0 (n=355)		Breach =1 (n=406)		*t* Value
	Mean	StdDev	Mean	StdDev		Mean	StdDev	Mean	StdDev	
PreBreach	0.06	0.26	0.37	0.62	-11.95***	0.25	0.54	0.27	0.45	-0.92
lnAdmissions	8.40	1.37	9.48	1.02	-22.96***	9.39	1.09	9.31	1.02	1.11
lnOutpatientVisits	10.72	2.74	11.63	2.74	-7.80***	11.67	2.04	11.88	1.27	-1.62
lnOpExp	17.99	2.63	18.55	4.38	-2.98***	18.78	3.21	19.06	2.18	-1.38
lnEHRs	1.36	0.61	1.62	0.79	-7.77***	1.40	0.69	1.45	0.81	-0.92
lnHealthIT	4.10	0.42	4.50	0.43	-21.09***	4.36	0.33	4.41	0.38	-1.83*
lnSecurity	1.60	0.89	1.99	0.86	-10.38***	1.88	0.81	1.99	0.74	-2.08**
Affiliation	25.05	42.32	15.01	27.02	8.51***	14.11	29.33	12.71	19.45	0.76
Academic	0.06	0.23	0.28	0.45	-11.59***	0.23	0.42	0.23	0.42	0.34
MUyears	0.19	0.56	0.25	0.60	-2.40**	0.12	0.42	0.07	0.28	1.57
lnFTE	6.34	1.32	7.28	1.54	-14.43***	7.09	1.52	7.16	1.21	-0.64
Metro	0.76	0.42	0.93	0.25	-15.65***	0.90	0.29	0.91	0.28	-0.46
Propensity	0.03	0.05	0.15	0.18	-14.42***	0.09	0.11	0.10	0.10	-0.25

Note. P-values: * Significant at p <0.1, ** Significant at p<0.05, *** Significant at <0.01

Table 6. The effects of data breaches on out-patient visits

	$\Delta lnOutPativentVisit_{it,Diff(t_{+1}-t)}$			$\Delta lnAdmissions_{it,Diff(t_{+1}-t)}$		
	Model(2)	**Model(3)**	**Model(4)**	**Model(2)**	**Model(3)**	**Model(4)**
	Breach	**Breach# (3years)**	**Breach Size (3years)**	**Breach**	**Breach# (3years)**	**Breach Size (3years)**
Intercept	4.909 *** (1.221)	5.024 *** (1.216)	5.015 *** (1.233)	-0.177 (1.082)	-0.048 (1.052)	-0.264 (1.062)
Breach	0.128 (0.117)			-0.017 (0.099)		
PreBreach		-0.266 ** (0.121)			-0.621 *** (0.1)	
lnAffectedRecords			-0.035 ** (0.016)			-0.083 *** (0.013)
lnAdmissions				-0.046 (0.074)	-0.043 (0.072)	-0.06 (0.074)
lnOutpatientVisits	-0.313 *** (0.050)	-0.302 *** (0.050)	-0.305 *** (0.050)			
lnOpExp	-0.107 *** (0.035)	-0.103 *** (0.035)	-0.101 *** (0.035)	-0.005 (0.030)	0.001 (0.030)	0.006 (0.030)
lnEHRs	0.056 ** (0.027)	0.054 ** (0.027)	0.049 * (0.028)	0.051 ** (0.023)	0.04 * (0.022)	0.024 (0.023)
lnHealthIT	-0.513 * (0.301)	-0.564 * (0.301)	-0.551 * (0.305)	-0.236 (0.256)	-0.307 (0.249)	-0.244 (0.252)
lnSecurity	0.024 (0.017)	0.033 * (0.017)	0.035 * (0.018)	0.004 (0.015)	0.021 (0.015)	0.024 (0.015)
Affiliation	-0.004 * (0.002)	-0.004 * (0.002)	-0.004 * (0.002)	-0.003 (0.002)	-0.003 (0.002)	-0.003 (0.002)
Academic	-0.567 *** (0.157)	-0.535 *** (0.157)	-0.549 *** (0.162)	-0.664 *** (0.134)	-0.585 *** (0.131)	-0.634 *** (0.135)
MUyears	0.121 (0.107)	0.123 (0.169)	0.12 (0.172)	0.108 (0.143)	0.152 (0.14)	0.137 (0.142)
MarketShare	0.329 *** (0.096)	0.320 *** (0.096)	0.323 *** (0.099)	0.218 *** (0.079)	0.207 *** (0.077)	0.274 *** (0.091)
lnFTE	0.233 *** (0.084)	0.229 *** (0.084)	0.222 *** (0.085)	0.096 (0.081)	0.104 (0.079)	0.075 (0.08)
lnNofHospitals	0.153 ** (0.077)	0.161 ** (0.077)	0.163 ** (0.078)	0.135 ** (0.067)	0.153 ** (0.065)	0.213 *** (0.074)
R-Square	0.113 ***	0.117 ***	0.119 ***	0.054 ***	0.101 ***	0.107 ***
Adj R-Sq	0.099	0.103	0.105	0.038	0.086	0.092
Obs	761	761	745	761	761	745

Notes. Standard errors are in parentheses. P-values: * Significant at p <0.1, ** Significant at p<0.05, *** Significant at <0.01

Table 7. Comparison of the effects of data breaches on outpatient visits in three groups

	Insignificant Market Power			Competitive Market			Significant Market Power		
	Model(2)	Model(3)	Model(4)	Model(2)	Model(3)	Model(4)	Model(2)	Model(3)	Model(4)
	Breach	Breach# (3years)	Breach Size (3years)	Breach	Breach# (3years)	Breach Size (3years)	Breach	Breach# (3years)	Breach Size (3years)
Intercept	7.946 **	8.291 ***	8.367 ***	6.389 ***	6.903 ***	6.972 ***	0.057	0.071	0.236
	(3.089)	(3.072)	(3.075)	(2.088)	(2.085)	(2.113)	(0.544)	(0.541)	(0.562)
Breach	0.308			0.061			-0.018		
	(0.32)			(0.173)			(0.042)		
PreBreach		0.129			**-0.427 ****			-0.073	
		(0.333)			**(0.187)**			(0.048)	
lnAffectedRecords			0.016			**-0.057 ****			-0.011
			(0.042)			**(0.023)**			(0.007)
lnOutpatientVisits	-0.309 ***	-0.299 ***	-0.298 ***	-0.393 ***	-0.375 ***	-0.374 ***	-0.111 ***	-0.116 ***	-0.128 ***
	(0.107)	(0.107)	(0.107)	(0.098)	(0.097)	(0.099)	(0.035)	(0.035)	(0.036)
lnOpExp	-0.219 ***	-0.223 ***	-0.224 ***	-0.261 ***	-0.238 **	-0.230 **	0.007	0.007	0.006
	(0.085)	(0.085)	(0.085)	(0.097)	(0.095)	(0.096)	(0.009)	(0.009)	(0.009)
lnEHRs	0.012	0.015	0.021	0.092 **	0.085 **	0.085 **	0.000	-0.001	0.003
	(0.063)	(0.063)	(0.063)	(0.042)	(0.042)	(0.043)	(0.012)	(0.012)	(0.013)
lnHealthIT	-0.847	-0.852	-0.880	-0.697	-0.851 *	-0.868 *	0.127	0.130	0.121
	(0.755)	(0.762)	(0.756)	(0.497)	(0.498)	(0.505)	(0.108)	(0.107)	(0.110)
lnSecurity	0.040	0.033	0.033	0.011	0.021	0.023	0.008	0.008	0.012 *
	(0.049)	(0.052)	(0.052)	(0.025)	(0.025)	(0.026)	(0.006)	(0.006)	(0.007)
Affiliation	-0.006	-0.006	-0.006	-0.004	-0.004	-0.004	0.000	0.000	0.000
	(0.008)	(0.008)	(0.008)	(0.003)	(0.003)	(0.003)	(0.001)	(0.001)	(0.001)
Academic	-0.720	-0.744	-0.744	-1.046 ***	-0.956 ***	-0.988 ***	-0.012	0.005	0.029
	(0.559)	(0.567)	(0.567)	(0.229)	(0.230)	(0.233)	(0.059)	(0.059)	(0.062)
MUyears	0.619	0.633	0.617	0.047	0.075	0.068	-0.098	-0.073	-0.103
	(0.594)	(0.600)	(0.596)	(0.218)	(0.216)	(0.217)	(0.068)	(0.069)	(0.071)
MarketShare	62.03	58.773	58.567	0.172	0.092	0.101	-0.005	-0.009	0.004
	(52.75)	(52.86)	(52.82)	(0.218)	(0.218)	(0.222)	(0.110)	(0.109)	(0.111)
lnFTE	0.256	0.240	0.243	0.776 ***	0.722 ***	0.697 ***	0.104 ***	0.108 ***	0.105 **
	(0.173)	(0.175)	(0.174)	(0.212)	(0.210)	(0.213)	(0.040)	(0.040)	(0.041)
lnNofHospitals	0.131	0.119	0.119	0.029	0.063	0.062	-0.058	-0.057	-0.046
	(0.264)	(0.265)	(0.265)	(0.136)	(0.136)	(0.138)	(0.041)	(0.041)	(0.042)
R-Square	0.168 ***	0.165 ***	0.165 ***	0.149 ***	0.161 ***	0.166 ***	0.144 ***	0.154 ***	0.174 ***
Adj R-Sq	0.112	0.108	0.108	0.121	0.133	0.138	0.086	0.097	0.116
Obs	190	190	190	380	380	372	191	191	183

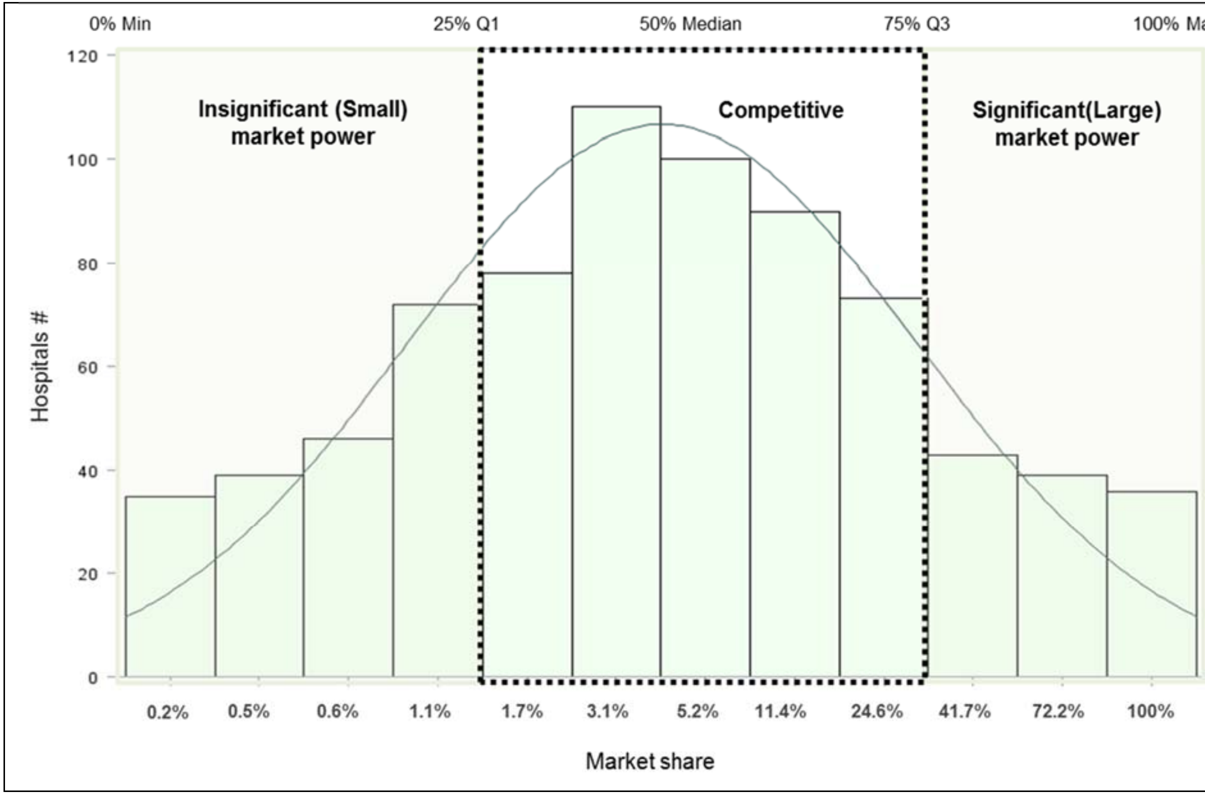
Notes. Standard errors are in parentheses. P-values: * Significant at p <0.1, ** Significant at p<0.05, *** Significant at <0.01

Table 8. Comparison of the effects of data breaches on admissions in three groups

	Insignificant Market Power			Competitive Market			Significant Market Power		
	Model(2)	**Model(3)**	**Model(4)**	**Model(2)**	**Model(3)**	**Model(4)**	**Model(2)**	**Model(3)**	**Model(4)**
	Breach	**Breach# (3years)**	**Breach Size (3years)**	**Breach**	**Breach# (3years)**	**Breach Size (3years)**	**Breach**	**Breach# (3years)**	**Breach Size (3years)**
Intercept	-3.64 **	-3.399 *	-3.465 **	3.386	3.66	3.191	0.109	0.104	0.065
	(1.774)	(1.745)	(1.747)	(2.659)	(2.562)	(2.611)	(0.282)	(0.284)	(0.291)
Breach	0.135			-0.02			-0.028		
	(0.178)			(0.176)			(0.025)		
PreBreach		-0.041			**-0.987 *****			0.006	
		(0.187)			**(0.185)**			(0.029)	
lnAffectedRecords			-0.015			**-0.124 *****			-0.001
			(0.023)			**(0.023)**			(0.004)
lnAdmissions	-0.022	-0.034	-0.030	-0.341 *	-0.223	-0.151	-0.057	-0.055	-0.051
	(0.109)	(0.110)	(0.108)	(0.194)	(0.188)	(0.194)	(0.037)	(0.038)	(0.039)
lnOpExp	0.018	0.016	0.017	-0.25 *	-0.137	-0.093	0.001	0.000	0.000
	(0.047)	(0.047)	(0.047)	(0.139)	(0.135)	(0.139)	(0.005)	(0.005)	(0.005)
lnEHRs	-0.057	-0.054	-0.058 *	0.117 ***	0.098 **	0.101 **	0.011	0.011	0.006
	(0.035)	(0.035)	(0.035)	(0.043)	(0.041)	(0.042)	(0.007)	(0.007)	(0.008)
lnHealthIT	0.478	0.448	0.448	-0.655	-1.010 **	-1.038 **	-0.020	-0.020	-0.018
	(0.417)	(0.421)	(0.417)	(0.505)	(0.491)	(0.498)	(0.064)	(0.065)	(0.067)
lnSecurity	-0.030	-0.028	-0.024	0.022	0.041 *	0.040	-0.004	-0.005	-0.005
	(0.027)	(0.029)	(0.029)	(0.026)	(0.025)	(0.025)	(0.004)	(0.004)	(0.004)
Affiliation	0.006	0.006	0.006	-0.004	-0.004	-0.004	0.000	0.000	0.000
	(0.004)	(0.004)	(0.004)	(0.003)	(0.003)	(0.003)	(0.001)	(0.001)	(0.001)
Academic	-0.012	-0.043	-0.071	-1.108 ***	-0.889 ***	-0.933 ***	-0.029	-0.029	-0.032
	(0.314)	(0.323)	(0.322)	(0.233)	(0.228)	(0.231)	(0.036)	(0.036)	(0.038)
MUyears	0.134	0.116	0.112	0.064	0.147	0.109	0.006	0.008	0.003
	(0.327)	(0.331)	(0.328)	(0.221)	(0.212)	(0.214)	(0.041)	(0.042)	(0.043)
MarketShare	-8.470	-8.295	-9.306	0.449 **	0.327	0.348 *	-0.023	-0.019	-0.019
	(26.11)	(26.39)	(26.25)	(0.210)	(0.203)	(0.206)	(0.064)	(0.064)	(0.066)
lnFTE	-0.021	-0.013	-0.010	0.817 **	0.542	0.412	0.064 *	0.062	0.066 *
	(0.103)	(0.103)	(0.103)	(0.356)	(0.346)	(0.357)	(0.038)	(0.039)	(0.039)
lnNofHospitals	0.449 ***	0.457 ***	0.460 ***	0.044	0.137	0.134	0.020	0.020	0.013
	(0.152)	(0.152)	(0.152)	(0.123)	(0.120)	(0.122)	(0.024)	(0.024)	(0.025)
R-Square	0.088	0.085	0.087	0.134 ***	0.197 ***	0.201 ***	0.060	0.054	0.038
Adj R-Sq	0.026	0.023	0.025	0.106	0.170	0.174	0.003	0.010	0.030
Obs	190	190	190	380	380	372	191	191	183

Notes. Standard errors are in parentheses. P-values: * Significant at p <0.1, ** Significant at p<0.05, *** Significant at <0.01

Figure 1. Histogram of market share



Appendix A1. Distribution of market share

Quantile	Market Shares					Hospitals#	Market Type
	Mean	StdDev	Median	Min	Max		
100% Max	99.7%	1.1%	100.0%	95.8%	100.0%	36	Large market power
90.0%	72.4%	7.9%	72.2%	60.7%	90.1%	39	Large market power
85.0%	43.9%	6.0%	41.7%	36.1%	57.6%	43	Large market power
75% Q3	25.1%	5.1%	24.6%	17.5%	34.9%	73	Competitive
65.0%	11.9%	3.1%	11.4%	7.6%	17.4%	90	Competitive
50% Median	5.3%	1.0%	5.2%	3.9%	7.5%	100	Competitive
35.0%	3.0%	0.5%	3.1%	2.2%	3.9%	110	Competitive
25% Q1	1.8%	0.2%	1.7%	1.4%	2.2%	78	Competitive
15.0%	1.1%	0.2%	1.1%	0.8%	1.4%	72	Small market power
10.0%	0.6%	0.1%	0.6%	0.5%	0.8%	46	Small market power
5.0%	0.4%	0.1%	0.5%	0.3%	0.5%	39	Small market power
0% Min	0.2%	0.1%	0.2%	0.0%	0.3%	35	Small market power

Appendix A2. Comparison of the effects of data breaches on out-patient visits in two groups

Market Share	Competitive market			Noncompetitive market		
	Model(2)	Model(3)	Model(4)	Model(2)	Model(3)	Model(4)
Variables	Breach	Breach# (3years)	Breach Size (3years)	Breach	Breach# (3years)	Breach Size (3years)
Intercept	6.389 ***	6.903 ***	6.972 ***	4.907 ***	5.054 ***	5.109 ***
	(2.088)	(2.085)	(2.113)	(1.589)	(1.589)	(1.615)
Breach	0.061			0.203		
	(0.173)			(0.161)		
PreBreach		**-0.427 ****			0.025	
		(0.187)			(0.169)	
lnAffectedRecords			**-0.057 ****			0.006
			(0.023)			(0.023)
lnOutpatientVisits	-0.393 ***	-0.375 ***	-0.374 ***	-0.255 ***	-0.251 ***	-0.253 ***
	(0.098)	(0.097)	(0.099)	(0.059)	(0.059)	(0.06)
lnOpExp	-0.261 ***	-0.238 **	-0.23 **	-0.095 **	-0.094 **	-0.094 **
	(0.097)	(0.095)	(0.096)	(0.037)	(0.037)	(0.038)
lnEHRs	0.092 **	0.085 **	0.085 **	0.008	0.011	0.016
	(0.042)	(0.042)	(0.043)	(0.036)	(0.036)	(0.038)
lnHealthIT	-0.697	-0.851 *	-0.868 *	-0.438	-0.463	-0.484
	(0.497)	(0.498)	(0.505)	(0.389)	(0.39)	(0.396)
lnSecurity	0.011	0.021	0.023	0.028	0.029	0.029
	(0.025)	(0.025)	(0.026)	(0.024)	(0.025)	(0.025)
Affiliation	-0.004	-0.004	-0.004	-0.002	-0.002	-0.002
	(0.003)	(0.003)	(0.003)	(0.004)	(0.004)	(0.004)
Academic	-1.046 ***	-0.956 ***	-0.988 ***	-0.169	-0.178	-0.161
	(0.229)	(0.23)	(0.233)	(0.241)	(0.241)	(0.248)
MUyears	0.047	0.075	0.068	0.26	0.233	0.242
	(0.218)	(0.216)	(0.217)	(0.277)	(0.276)	(0.288)
MarketShare	0.172	0.092	0.101	0.324 ***	0.334 ***	0.344 ***
	(0.218)	(0.218)	(0.222)	(0.12)	(0.12)	(0.124)
lnFTE	0.776 ***	0.722 ***	0.697 ***	0.068	0.061	0.059
	(0.212)	(0.21)	(0.213)	(0.094)	(0.095)	(0.096)
lnNofHospitals	0.029	0.063	0.062	0.156	0.166	0.172
	(0.136)	(0.136)	(0.138)	(0.108)	(0.108)	(0.11)
R-Square	0.149 ***	0.161 ***	0.166 ***	0.117 ***	0.113 ***	0.114 ***
Adj R-Sq	0.121	0.133	0.138	0.088	0.084	0.084
Obs	380	380	372	381	381	373

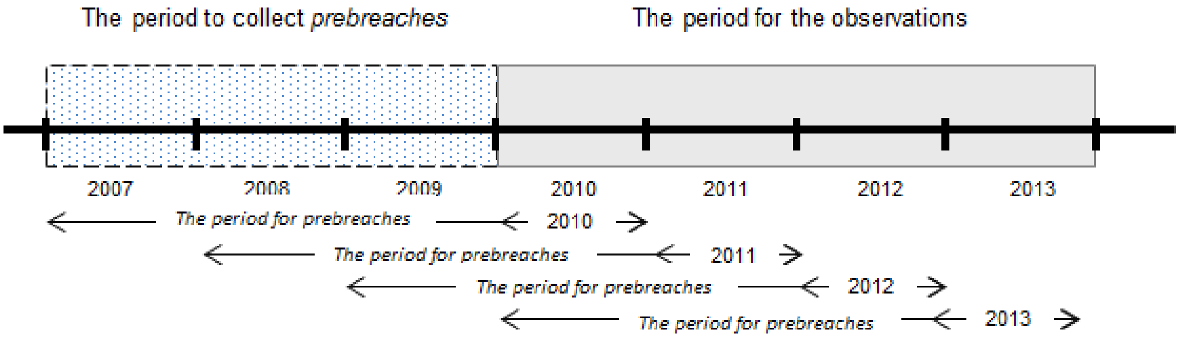
Notes. Standard errors are in parentheses. P-values: * Significant at p <0.1, ** Significant at p<0.05, *** Significant at <0.01

Appendix A3. Comparison of the effects of data breaches on admissions in two groups

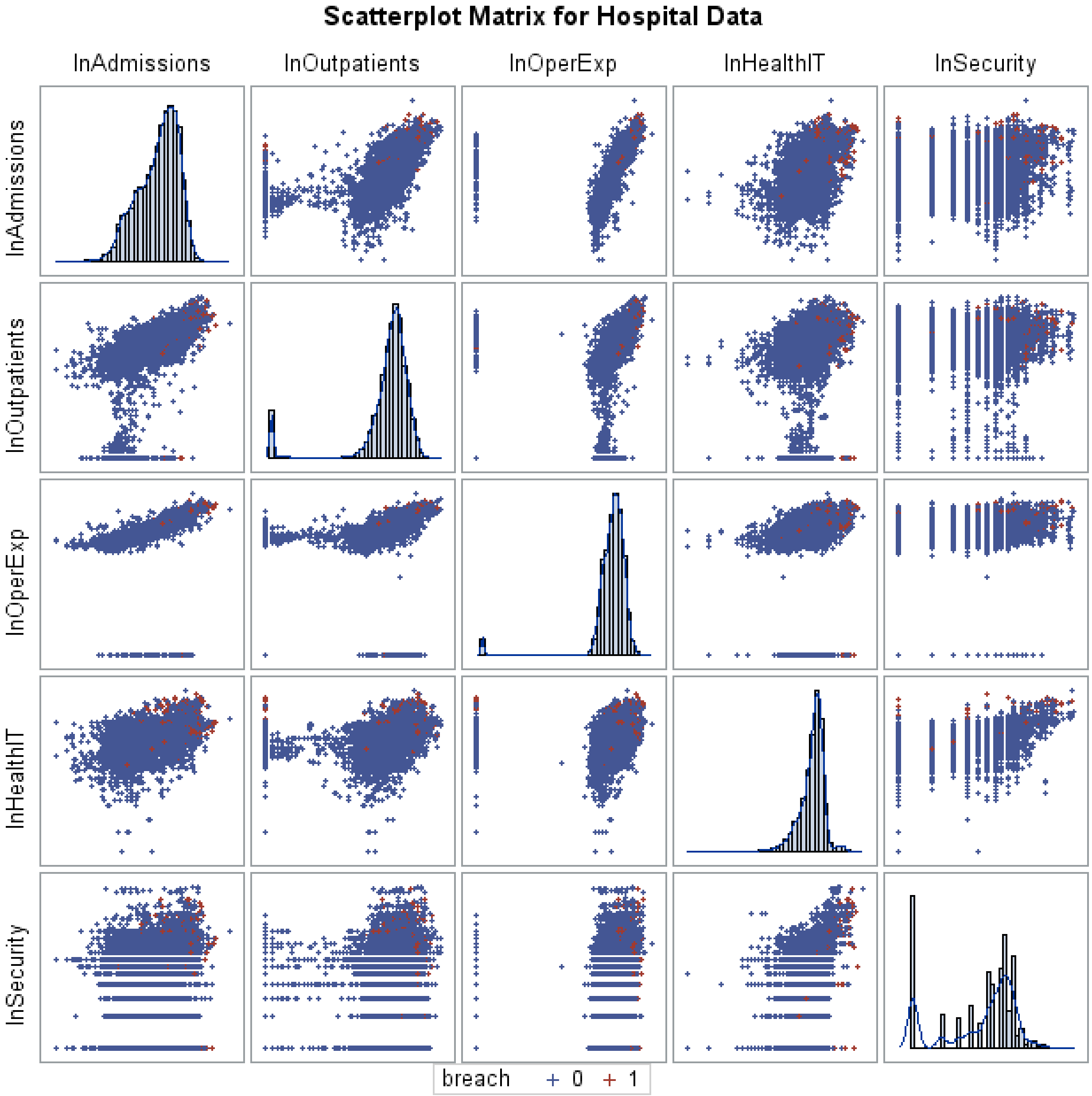
Market Share	Competitive market			Noncompetitive market		
	Model(2)	Model(3)	Model(4)	Model(2)	Model(3)	Model(4)
Variables	**Breach**	**Breach# (3years)**	**Breach Size (3years)**	**Breach**	**Breach# (3years)**	**Breach Size (3years)**
Intercept	3.386 (2.659)	3.66 (2.562)	3.191 (2.611)	-1.177 (0.894)	-1.145 (0.889)	-1.189 (0.902)
Breach	-0.02 (0.176)			0.04 (0.089)		
PreBreach		**-0.987** *** **(0.185)**			-0.045 (0.092)	
lnAffectedRecords			**-0.124** *** **(0.023)**			-0.01 (0.013)
lnAdmissions	-0.341 * (0.194)	-0.223 (0.188)	-0.151 (0.194)	-0.025 (0.061)	-0.028 (0.061)	-0.026 (0.062)
lnOpExp	-0.25 * (0.139)	-0.137 (0.135)	-0.093 (0.139)	0.001 (0.021)	0.001 (0.021)	0.001 (0.021)
lnEHRs	0.117 *** (0.043)	0.098 ** (0.041)	0.101 ** (0.042)	-0.03 (0.02)	-0.03 (0.02)	-0.035 * (0.021)
lnHealthIT	-0.655 (0.505)	-1.01 ** (0.491)	-1.038 ** (0.498)	0.186 (0.215)	0.178 (0.215)	0.195 (0.218)
lnSecurity	0.022 (0.026)	0.041 * (0.025)	0.04 (0.025)	-0.019 (0.013)	-0.018 (0.013)	-0.017 (0.014)
Affiliation	-0.004 (0.003)	-0.004 (0.003)	-0.004 (0.003)	0.002 (0.002)	0.002 (0.002)	0.002 (0.002)
Academic	-1.108 *** (0.233)	-0.889 *** (0.228)	-0.933 *** (0.231)	-0.037 (0.133)	-0.039 (0.133)	-0.052 (0.136)
MUyears	0.064 (0.221)	0.147 (0.212)	0.109 (0.214)	0.122 (0.152)	0.119 (0.151)	0.108 (0.158)
MarketShare	0.449 ** (0.21)	0.327 (0.203)	0.348 * (0.206)	0.19 *** (0.068)	0.193 *** (0.067)	0.183 *** (0.069)
lnFTE	0.817 ** (0.356)	0.542 (0.346)	0.412 (0.357)	0.002 (0.056)	0.005 (0.056)	0.006 (0.057)
lnNofHospitals	0.044 (0.123)	0.137 (0.12)	0.134 (0.122)	0.168 *** (0.063)	0.173 *** (0.063)	0.168 *** (0.064)
R-Square	0.134 ***	0.197 ***	0.201 ***	0.047	0.047	0.048
Adj R-Sq	0.106	0.170	0.174	0.015	0.016	0.016
Obs	380	380	372	381	381	373

Notes. Standard errors are in parentheses. P-values: * Significant at p <0.1, ** Significant at p<0.05, *** Significant at <0.01

Appendix B1. The study period


The period to collect *prebreaches*
The period for the observations
2007
2008
2009
2010
2011
2012
2013
The period for prebreaches
2010
The period for prebreaches
2011
The period for prebreaches
2012
The period for prebreaches
2013

Appendix B2. The scatter plot matrix for hospital hata


Scatterplot Matrix for Hospital Data
lnAdmissions
lnOutpatients
lnOperExp
lnHealthIT
lnSecurity
lnAdmissions
lnOutpatients
lnOperExp
lnHealthIT
lnSecurity
breach + 0 + 1