Meaningful Healthcare Security: Does "Meaningful-Use" Attestation Improve Information Security Performance?

Juhee Kwon
Department of Information Systems, College of Business, City University of Hong Kong,
juhee.kwon@cityu.edu.hk

M. Eric Johnson
Owen Graduate School of Management, Vanderbilt University,
m.eric.johnson@owen.vanderbilt.edu

Abstract

Voluntary mechanisms are often employed to signal performance of difficult-to-observe management practices. In the healthcare sector, financial incentives linked to "meaningful-use" attestation have been a key policy initiative of the Obama administration to accelerate electronic health record (EHR) system adoption while also focusing providers on protecting sensitive healthcare data. As one of the core requirements, meaningful-use attestation requires healthcare providers to attest to having implemented security mechanisms for assessing the potential risks and vulnerabilities to their data. In this paper, we examine whether meaningful-use attestation is achieving its security objective. Using a propensity score matching technique, we analyze a matched sample of 925 U.S. hospitals. We find that external breaches motivate hospitals to pursue meaningful use and that achieving meaningful use does indeed reduce such breaches. We also find that hospitals that achieve meaningful use observe short-term increases in accidental breaches, but see longer-term reductions. These results have implications for managers and policy makers as well as researches interested in organizational theory and quality management.

Keywords: Meaningful-use attestation, Electronic healthcare records, Information security, Healthcare breaches

Introduction

Electronic health record (EHR) systems promise improved patient care and reduced cost (Blumenthal & Tavenner, 2010; Buntin, Burke, Hoaglin, & Blumenthal, 2011). With billions of dollars in incentives provided by the U.S. HITECH Act of 2009, EHR adoption in the U.S. has dramatically increased. However, despite rising EHR adoption, physician experience and other available evidence suggest that the promise is largely unfulfilled (Yasnoff, Sweeney, & Shortliffe, 2013). Many EHR systems are often ill-designed and poorly integrated into clinical workflow (Jha, 2010). Furthermore, digitizing healthcare data creates a much larger pool of potential data to steal. Sadly, information security mechanisms often do not reflect the pace with which healthcare data is being converted into an electronic format. Consequently, privacy advocates have argued that the move toward electronic health records could lead to a rising number of patients impacted by healthcare information breaches.

Under HITECH, the Centers for Medicare & Medicaid Services (CMS) provides incentive payments to hospitals and professionals who demonstrate "meaningful use" of certified EHRs technology. Beyond adopting and implementing EHRs, hospitals must "attest" that they have met certain measures or requirements regarding the EHR use for patient care as well as privacy and security provisions. The formal attestation of meaningful use requires healthcare providers to identify and implement administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic health information based on HIPAA Security Rule provisions (45 C.F.R. §§ 164.308)[1]. In other words, the attestation is effectively a confirmation or certification on the part of the eligible healthcare providers that they have met the requirements.

[1] US Department of Health & Human Services Health Information Privacy. Security Rule Guidance Material. See http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html.

In healthcare information security, meaningful-use standards only provide a baseline floor. There has been an active debate regarding the relationship between information security performance and security regulations. Drawing on the value of carrot (incentives) versus stick (penalties) policies, researchers have argued that some level of such mechanisms effectively induce healthcare providers to make appropriate security investments. Since non-certification (or non-compliance) can hurt a provider's public reputation, fears of these negative outcomes can motivate healthcare providers to take action to properly analyze their security risks and protect their data (Bulgurcu, Cavusoglu, & Benbasat, 2010; von Solms, 2005). Further, financial incentives for certification (or compliance) are a catalyst for pursuing meaningful use, which likely leads to improved security.

Some researchers argue that formal certification motivated by incentives induces organizations to simply meet the requirements for certification (Puhakainen & Siponen, 2010; S. Smith, Winchester, Bunker, & Jamieson, 2010). Such a "check box" approach of meeting the minimum standards may be helpful for those with poor security, but it rarely provides the kind of protection required to prevent a serious breach. Thus, although organizations often apply significant efforts to achieve certification, these requirements may not directly lead to significant security enhancement or to achieving other financial and clinical goals.

The rapid push for hospitals to achieve EHR meaningful-use standards motivated us to quantify the impact of such certification on the likelihood of subsequent healthcare information breaches. A stream of literature has examined the relationship between EHR adoption and healthcare information security. The outcomes of such research have important managerial implications on how hospitals develop security strategies and make investments in security.

However, no previous study has addressed the impact of meaningful-use attestation on data protection.

This study seeks to answer the following questions: Does a hospital's breach experience affect its pursuit meaningful-use attestation? How does the achievement of meaningful-use standards influence subsequent healthcare breaches across different breach types (i.e., accidental disclosure, malicious insiders, and external breaches)? Our findings provide theoretical and practical implications by identifying the interdependence between meaningful use of EHRs and healthcare information breaches. This study provides policy insights on effective security programs and the effect of meaningful use on security in complex healthcare environments.

Data

Data Sample

We use several data sources in this study. First, hospital data were collected from the Healthcare Information and Management Systems Society (HIMSS) Analytics™ Database. The database provides information about meaningful-use attestation, attestation date, and the adoption of health information technologies—EHRs and security software—in healthcare organizations. It also includes various descriptive variables, which we used as control variables such as the bed size of each healthcare organization, operating expense, net income, and so on. The HIMSS Analytics™ database has been widely used in previous studies to examine the impact of healthcare information systems (Angst & Agarwal, 2009; Hillestad et al., 2005; Miller & Tucker, 2009). Our data is limited to Medicare eligible hospitals and Medicare & Medicaid eligible hospitals that provided information on meaningful-use attestation. Our final sample includes 4,962 hospitals from January, 2008 to December, 2013.

Next, we used two data sources to obtain information on breaches: U.S. Health & Human Services (HHS)[2] and Privacy Clearinghouse[3]. During the study period (January 2008 to December 2013), 521 breaches occurred at hospitals that had reported their meaningful-use status in the HIMSS Analytics™ Database. Matching the HIMSS Analytics™ Database with the 521 reported breaches, we found that 380 unique hospitals experienced the 521 breaches, with 83 hospitals experiencing more than one breach. Table 1 shows descriptive statistics.

Variable Definitions

Meaningful Use of EHRs: Meaningful use in this study captures a hospital's formal attestation of stage 1 meaningful use (stage 1 is defined by HHS as the first stage of three stages. Stage 1 was put in place in 2011 with stage 2 and 3 requirements slated for later years). We coded the meaningful-use variable as one if a hospital achieved meaningful-use status and zero otherwise. Although the meaningful-use initiative was triggered by the HITECH Act in 2009, the official attestation period started in 2011 when hospitals began filing for incentive payments. Among our sample of 4,962 hospitals, 285 hospitals attested meaningful use in 2011, 837 hospitals in 2012, and 350 hospitals in 2013.

Breach types (Accidental, Malicious Insider, and External): Healthcare breaches stem from both internal failures (e.g., accidental disclosure or malicious insiders) and external threats (e.g., external hacker attacks) (see Figure 1). This study considers these three different types of breaches: accidental disclosure, malicious insiders, and external breaches.

"Accidental" breaches occur without an intent to access patient information. These breaches typically result from lost or misplaced devices including computers, laptops, and portable data

[2] Breaches Affecting 500 or More Individuals, see http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
[3] Chronology of Data Breaches Security Breaches 2005 – Present. see http://www.privacyrights.org/data-breach

storage. Nevertheless, such accidental disclosures may allow criminals to access and exploit patient data. Accidental breaches are mainly attributed to poor data handling policies and employees' carelessness. "Malicious" breaches are caused by insiders (i.e., employees or contractors), who gain unauthorized access to or use patient information for identity theft or other illegitimate purposes. Lastly, beaches by hacking into the network or devices stolen by an outside party are categorized as "External". Organizations often focus on preventing external threats rather than internal accidents, even though internal threats are not less harmful (Liu, Wang, & Camp, 2009; McFadzean, Ezingeard, & Birchall, 2007). This categorization allows us to examine how meaningful use impacts specific types of healthcare breaches.

EHR adoption level: In the healthcare sector, organizations often share patient information as patients move between local clinics, small hospitals, tertiary care centers, and long-term rehabilitation centers. Thus, significant value can be achieved through effective and secure communication of healthcare information from one healthcare provider to another. Indeed, that is an explicit expectation in the Stage 1 definition of "meaningful use" of EHRs. In this study, we classified hospitals' EHR capability into 1 of 7 levels[4] based on the applications deployed. Note the capability alone does not indicate meaningful use. A hospital must be effecting using the system capability to achieve meaningful use. Level 1 represents the simplest possible system while level 7 is the most advanced. Hospitals typically require a capability of level 3 or 4 to reach stage 1 meaningful uses. This allowed us to examine whether the hospital's capability level as well as meaningful-use attestation impacts breach occurrence. An overview of the levels can be found in Appendix B.

[4] HIMSS Analytics™ defined the 7 levels of the EHRs/EMRs. see http://www.himssanalytics.org/docs/emram.pdf

Control Variables: Control variables include *operating expense, net income, the number of fulltime employees, the number of beds, the number of security software applications,* and *year dummies. Operating expense* represents hospital spending on operations such as staffing, property expenses, etc. for the most recent fiscal year. *Net income* (revenues in excess of expenses) is the income that a system generated from patient care, investments and other sources for the most recent fiscal year. *The number of beds* was measured by the number of licensed beds in a healthcare facility. *Security software* includes applications such as anti-virus, encryption, firewall, intrusion detection, spam filter, and user authentication.

Empirical Analysis and Results

We aim to identify changes in breach performance consequent to meaningful-use attestation. Meaningful use could be correlated with, but not effect, healthcare breaches. If this form of self-selection bias is important, we anticipate that hospitals achieving meaningful-use status would perform better on breaches both prior to meaningful-use attestation as well as afterward.

T-tests within the total sample (see Table 2) revealed that bed sizes and breaches differed between hospitals with meaningful use and non-meaningful use during our study period. Thus, the healthcare breaches of these two groups are likely to differ in other ways as well. For instance, larger hospitals may have more resources to devote to both achieving meaningful use and other security strategies that impact breach performance. To eliminate these potential sources of bias, we performed a process of matching the treatment and control hospitals using an estimated propensity score based on the predicted probability of meaningful-use attestation.

Propensity score matching is widely used to select treatment and control groups who resemble each other in all relevant characteristics before an event (in our case, meaningful-use attestation) to create a statistical equivalence between the two groups (Rishika, Kumar,

Janakiraman, & Bezawada, 2013; Rosenbaum & Rubin, 1983). Matching on a propensity score allows us to identify a control group of non-meaningful-use hospitals with similar meaningful-use determinants (e.g., size, EHR adoption, etc.) and pre-period healthcare breaches to those who achieved meaningful use. In order for the propensity score matching approach to be possible, data should be available for both the treatment and control groups. Following an approach outlined in earlier studies (Heckman, Ichimura, & Todd, 1997; Levine & Toffel, 2010; J. A. Smith & Todd, 2005), we utilize a panel data of hospital-level characteristics for both groups prior to meaningful-use attestation.

Selection Analysis

Our selection analysis first seeks to discern whether the two groups (those who achieve meaningful use and those who don't) are similar in size, EHR adoption, and healthcare breaches prior to meaningful-use attestation. We begin by assessing whether prior breaches affect a hospital's propensity of achieving meaningful use by controlling for bed sizes and the levels of EHR adoption. We estimate a probit model where the dependent variable is a dummy, coded one at year *t*, if a hospital attested to meaningful use in that year:

$$MU_{it} = F(Accidental_{it-1\&-3}, External_{it-1\&-3}, Malicious_{it-1\&-3}, BreachedRecords_{it-1\&-3}, EHR\ Stage_{1-7,it}, Security_{it}, OpCost_{it}, Bedsize_{it}, YearDummies) + \varepsilon_{it} \quad (1)$$

where F(·) is the probit function; The subscript, $t_{-1\&-3}$ is the annual average number of breaches that occurred in the last 36 months: the annual average number of accidental, malicious insider, and external breaches at year *t*. The model also includes the annual average number of the total records affected by the breaches. The EHR level, number of security applications, total operating expense, and bed size are included as control variables for each year *t*.

Using the above propensity score matching approach, our model could still suffer from unobservable factors that influence both meaningful use and breaches in the last 36 months before meaningful-use attestation at year *t*, leading to a biased result. In order to address this concern, we employed use a two-step procedure proposed by Heckman (1979). First, we used a probit model to estimate the probability that a hospital experiences a breach as a function of organizational resources such as size, expense, security resources, and the level of EHR adoption.

$$Breach^{*}_{t-1\&-3} = F(\, w_{it} \mid EHR\ Stage_{1-7,it-1\&-3}, Security_{it-1\&-3}, \\ OpCost_{it}, FTE_{it-1\&-3}, YearDummies) \; + u_{it} \tag{2}$$

$Breach^{*}_{t-1\&-3}$ is a binary variable that indicates whether a hospital experienced a breach in the last 36 months before year *t*. The model (2) predicts the probability of breach occurrence (see Appendix C). The error term, u_{it} is attributable to unobservable characteristics that affect breach occurrence. u_{it} captures effects that would be included in the explanatory variables, but cannot be measured. In the Model (1), if unobservable effects captured in $\varepsilon_i$are the same as in u_i from (2), then $\varepsilon_{it}$and u_{it} will be correlated. For example, regardless of whether meaningful use is achieved or not, a hospital with better human resources or security policies would outperform hospitals lacking them. Therefore, ε_i and u_i will be correlated (ρ) unless these factors can be measured and included in X_{it}. Thus, our selection analysis model controls for potential bias and non-zero ρ (λ_{it}). The final model can be specified as:

$$MU_{it} = F(\, X_{it}, |Accidental_{\,it-1\&-3}, External_{\,it-1\&-3}, Malicious_{\,it-1\&-3}, \\ BreachedRecords_{\,it-1\&-3}, EHR\ Stage_{1-7,it}, Security_{it}, OpCost_{it}, \\ Bedsize_{it}, YearDummies, \lambda_{it}) \; + \varepsilon_{it} \tag{3}$$

Results from the Selection Analysis

Financial incentives are the primarily motivation for hospitals to attest to meaningful use and most hospitals are expected to eventually reach meaningful-use standards. Security management is just one requirement among 13 required items for meaningful-use attestation. However, breach incidents can impact a hospital's plan to attest. Breaches could negatively or positively affect a hospital's plan (or roadmap) to pursue meaningful (either postpone or expedite).

Table 3 presents the results from the selection analysis. Our results suggest that hospitals that suffer breaches arising from malicious insiders are less likely to achieve meaningful use (-0.633, $p< 0.01$). Since malicious insiders are often an organizational and human resource issue, this result is not so surprising. On the other hand, those that experienced attacks from outside intruders were more likely to later attest meaningful use of EHRs (1.595, $p < 0.0001$). Managers in many industries are motivated by external attacks. That motivation leads hospitals to focus more effort on improving security procedure to prevent external attacks for reaching meaningful use standards. Breaches resulting from accidental disclosure do not seem to have any significant effect on meaningful use (0.091, $p = 0.423$). We also found that the size of breach impacted the likelihood of meaningful-use attestation with those experiencing larger breaches being less likely to achieve meaningful use (0.569, $p < 0.01$). Large breaches likely require significant management effort (e.g., to manage breach disclosure), thus distracting efforts away from achieving meaningful use.

In terms of the organizational perspective, Table 2 shows that meaningful use is more likely to be acquired by larger hospitals. As expected, EHR capability is associated with attestation of meaningful use. Note that attestation generally requires level 3 or above capability. The average

bed size of hospitals with meaningful use is 221, compared with 150 for hospitals with without meaningful use. The probit model estimated a *bed size* coefficient of 1.109 ($p < 0.001$).

Developing Matched Groups

We constructed the matched groups in three steps. We first generated propensity scores by estimating the probit model (1) for meaningful use, and then we conducted single nearest neighbor matching. Specifically, we matched each hospital with meaningful use at year *t* to a hospital with non-meaningful use having the most similar propensity score for that year. We made best matches first and next-best matches within 0.001, the maximum difference allowance, until no further matches could be made. Of the 1,191 meaningful-use hospitals for which we estimated propensity scores, we successfully matched 925 hospitals with meaningful use to 925 control hospitals.

Lastly, we conducted *t*-tests to examine whether the groups differed or not. Table 4 provides summary statistics. The results revealed that the groups differed on only 2 of the 16 metrics (i.e., EHRs level 3 and 7) at the 5% level and 2 others (i.e., EHRs level 5 and 6) at the 10 % level. We ran our evaluation model on these matched groups (See Table 4).

Treatment Analysis

Finally, with the matched-pair sample, we assessed whether hospitals without meaningful use and with meaningful use experienced similar data breach occurrences after meaningful-use attestation. In the treatment model, we divided outcomes (healthcare breaches) into two periods. The first period considers the difference in data breach occurrences compared to 12 months before and after meaningful use as a dependent variable. The next period considers the difference between the first and the second 12 months after meaningful use. This categorization allows us to examine increasing or decreasing rates over time post meaningful use. We estimated the

following model for each outcome (ΔB_{it}): $\Delta B_{tot,it}$, $\Delta B_{acc,it}$, $\Delta B_{mal,it}$, and $\Delta B_{ex,it}$ at hospital i in year t.

$$\Delta B_{it} = \beta_{0i} + \beta_1 MU_{it} + \beta_2 OpCost_{it} + \beta_3 NetIncome_{it} + \beta_4 Bedsize_{it} \quad (4)$$
$$+ \beta_5 Security_{it} + \beta_{6-12} EHR\ Stage_{1-7,it} + \gamma_k YearDummies + \delta\lambda_{it} + \epsilon_{it}$$

Only the hospitals with meaningful use in each pair of the matched sample have a positive value for dichotomous variable (MU_{it}), which is coded 1 after meaningful-use attestation, and 0 otherwise. Our primary interest is the coefficient, β_1, which represents the estimated effect of meaningful use. We also included a set of control variables: operating expenses, net income, bed size, security software, the numbers of EHRs applications and year dummies (see Table 5 and 6).

Results from the Treatment Analysis

The First-year Effects: The result of the evaluation model (4) for the first-period outcomes are presented in Table 5. Surprisingly, the numbers of total breaches and accidental breaches increases in the first year after achieving meaningful use (0.197 and 0.200 at $p < 0.01$, respectively). Accidental breach occurrences were been found to be about 20% higher in hospitals with meaningful use than non-meaningful use. However, meaningful-use hospitals had less external breach occurrences in the first year (-0.008 at $p < 0.1$).

Recall that the selection model indicated that those who experienced external breaches were more likely to later achieve meaningful, while prior accidental breaches did not have any effect and malicious insiders' breaches reduced the likelihood of achieving meaningful use. Combined with the results from the selection model, those from the treatment model suggest that when a hospital experiences an attack or intrusion from outsiders, the hospital is more likely to subsequently attest meaningful use. Indeed, those hospitals reduce external breaches in year 1

post meaningful use. On the other hand, accidental breaches increased in that period. This is not surprising as improving security and meeting meaningful-use standards makes it more likely the hospitals would discover and report accidental breaches.

The Second-year Effects: The results for breaches in year 2 post attestation are presented in Table 6. Interestingly, in the second year, we found that effects of meaningful use on total and accidental breaches are the opposite to those of meaningful use in the first year. The coefficients of total and accidental breaches are -0.190 and -0.183 at $p < 0.01$, respectively. Hospitals with meaningful use have less accidental breach occurrences in year 2 by about 20%. This indicates that while achieving meaningful use may lead to the discovery of more accidental disclosures in year 1, it significantly decreases accidental breaches over time. Given that one of meaningful-use purposes is to implement a security risk management process, the systematic and standardized approach of meaningful use improves security processes as well as tracking accidental disclosures often caused by a lack of data handling standards. Our results suggest that tracking ability also leads to actual data protection over time, because a hospital learns its vulnerable points via tracking ability. Moreover, meeting meaningful-use standards could help a hospital to effectively integrate EHR systems into its workflow, thus reducing the need to move data into unsecure formats like spreadsheets and also allowing better tracking of lost devices and accidental disclosure.

Meaningful use does not have any significant effect on external breaches in the second year (over year 1), whereas it significantly decreases external breaches in the first year. Preventing external threats is challenging, because external threats are ever-changing and difficult to predict. Although meaningful use requires a hospital to conduct a security risk analysis and to implement security updates as necessary, it would be outdated within a short time. This implies that

meaningful-use attestation may be more effective in reducing accidental breaches, which can be improved by elevating internal security risk analysis and processes, rather than on external breaches, which are caused by unexpected threats.

Lastly, we find no effect of meaningful use on breaches arising from malicious insiders. These breaches are more likely related to human resource management rather than security risk analysis.

Conclusions

We examined whether meaningful-use attestation of EHRs affects the likelihood of subsequent healthcare breaches. We compared the effects of meaningful use on three different types of healthcare breaches (i.e., accidental, external, and malicious insider) in the first year and second year after attestation.

We found that hospitals are more likely to achieve meaningful use following an external breach than they are after accidental and external breaches. Moreover, achieving meaningful use effectively reduces external breaches in year 1. However, those that achieve meaningful use do not see any further reductions in year 2. On the other hand, achieving meaningful use makes hospitals more likely to find accidental breaches in the year after. In the longer term, those that achieve meaningful use experience fewer accidental breaches (the trends of breach occurrences are described in Figure 1). This result suggests that while external breaches may motivate hospitals to pursue meaningful use or help them reach the required standards, achieving meaningful use enables them to over the time reduce accidental breaches as well as quickly reduce external breaches. Further progress on preventing external breaches may require ongoing effort beyond achieving stage 1 meaningful use.

Acknowledgement

This research was partially supported by the National Science Foundation, Grant Award Number CNS-1329686.

References

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

Blumenthal, D., & Tavenner, M. (2010). The "Meaningful Use" Regulation for Electronic Health Records. *New England Journal of Medicine, 363*(6), 501-504. doi: 10.1056/NEJMp1006114

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance:: An Empirical Study of Rationali-BASED BELIEFS AND INFORMATION SECURITY AWARENESS. *MIS Quarterly, 34*(3), 523-548.

Buntin, M. B., Burke, M. F., Hoaglin, M. C., & Blumenthal, D. (2011). The Benefits Of Health Information Technology: A Review Of The Recent Literature Shows Predominantly Positive Results. *Health Affairs, 30*(3), 464-471. doi: 10.1377/hlthaff.2011.0178

Heckman, J. J., Ichimura, H., & Todd, P. E. (1997). Matching as an econometric evaluation estimator: Evidence from evaluating a job training programme. *Review of Economic Studies, 64*(4), 605-654. doi: 10.2307/2971733

Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville, R., & Taylor, R. (2005). Can electronic medical record systems transform health care? Potential health benefits, savings, and costs. *Health Affairs, 24*(5), 1103-1117. doi: 10.1377/hlthaff.24.5.1103

Jha, A. K. (2010). Meaningful Use of Electronic Health Records The Road Ahead. *Jama-Journal of the American Medical Association, 304*(15), 1709-1710.

Levine, D. I., & Toffel, M. W. (2010). Quality Management and Job Quality: How the ISO 9001 Standard for Quality Management Systems Affects Employees and Employers. *Management Science, 56*(6), 978-996. doi: 10.1287/mnsc.1100.1159

Liu, D. B., Wang, X. F., & Camp, L. J. (2009). Mitigating Inadvertent Insider Threats with Incentives. In R. Dingledine & P. Golle (Eds.), *Financial Cryptography and Data Security* (Vol. 5628, pp. 1-16).

McFadzean, E., Ezingeard, J. N., & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review, 31*, 622-660. doi: 10.1108/14684520710832333

Miller, A. R., & Tucker, C. (2009). Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records. *Management Science, 55*(7), 1077-1093. doi: 10.1287/mnsc.1090.1014

Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly, 34*(4), 757-778.

Rishika, R., Kumar, A., Janakiraman, R., & Bezawada, R. (2013). The Effect of Customers' Social Media Participation on Customer Visit Frequency and Profitability: An Empirical Investigation. *Information Systems Research, 24*(1), 108-127. doi: 10.1287/isre.1120.0460

Rosenbaum, P. R., & Rubin, D. B. (1983). THE CENTRAL ROLE OF THE PROPENSITY SCORE IN OBSERVATIONAL STUDIES FOR CAUSAL EFFECTS. *Biometrika, 70*(1), 41-55. doi: 10.1093/biomet/70.1.41

Smith, J. A., & Todd, P. E. (2005). Does matching overcome LaLonde's critique of nonexperimental estimators? *Journal of Econometrics, 125*(1-2), 305-353. doi: 10.1016/j.jeconom.2004.04.011

Smith, S., Winchester, D., Bunker, D., & Jamieson, R. (2010). Circuits of Power: A Study of Mandated Compliance to An Information Systems Security De Jure Standard in A Government Organization. *Mis Quarterly, 34*(3), 463-486.

von Solms, S. H. (2005). Information Security Governance - Compliance management vs operational management. *Computers & Security, 24*(6), 443-447. doi: 10.1016/j.cose.2005.07.003

Yasnoff, W. A., Sweeney, L., & Shortliffe, E. H. (2013). Putting Health IT on the Path to Success. *Jama-Journal of the American Medical Association, 309*(10), 989-990.

Table 1. Descriptive Statistics

Variable	Mean	Std Dev	Min	Max
Operating Expense	0.148	0.255	0.001	9.503
Net Income	0.006	0.110	-8.515	1.548
N of Beds	0.168	0.188	0.002	1.868
N of FTE	1.470	59.403	0.011	6354
Level1 EHR	3.478	0.961	0	10
Level 2 EHR	0.902	0.306	0	2
Level 3 EHR	3.734	1.543	0	9
Level 4 EHR	1.412	0.639	0	3
Level 5 EHR	1.096	1.015	0	6
Level 6 EHR	0.432	0.498	0	2
Level 7 EHR	2.438	1.706	0	13
Total Breaches#	0.054	0.289	0	5
Accidental #	0.036	0.219	0	4
External	0.006	0.094	0	3
Malicious #	0.018	0.156	0	3
Breached records#	0.939	27.288	0	1700
Meaningful Use	0.258	0.437	0	1
The numbers of hospitals				
2011 Meaningful Use	285			
2012 Meaningful Use	837			
2013 Meaningful Use	350			

Note. The number of hospitals is 5,007, and the total observations are12,013 from 2008 to 2013.

Table 2. T-tests in the **total sample**

	No Meaningful Use	Meaningful Use	t-value	Pr > |t|
Control Variables				
Operating Expense	0.1311	0.1972	-12.24	<.0001
Bed size	0.1499	0.2206	-18.27	<.0001
Security SW	7.5944	9.8131	-19.82	<.0001
EHR Level 1	3.3776	3.7687	-20.00	<.0001
EHR Level 2	0.8779	0.9714	-14.80	<.0001
EHR Level 3	3.4675	4.5006	-33.57	<.0001
EHR Level 4	1.3004	1.7332	-33.98	<.0001
EHR Level 5	0.9701	1.4596	-23.65	<.0001
EHR Level 6	0.37	0.6114	-23.77	<.0001
EHR Level 7	2.2438	2.9963	-21.55	<.0001
The difference of Breach occurrence				
Total Breaches	0.0467	0.074	-4.53	<.0001
Accidental	0.0312	0.0494	-4.00	<.0001
Malicious	0.0155	0.0245	-2.79	0.0053
External	0.00336	0.0129	-4.89	<.0001
Affected Records	0.7455	1.4978	-1.32	0.1863

Note. *Hospitals with meaningful use: 1,472 and hospitals without meaningful use: 3,535. The total observations are 3.092 and 8,917, respectively.*

Table 3. Predicting the certified Meaningful Use of EHRs

	The Certified Meaningful Use (0 or 1)		
	Estimate	**StdErr**	**P value**
Intercept	-7.595	0.580	<.0001
Operating Expense	-0.265	0.218	0.224
N of Beds	1.109	0.244	<.0001
Security SW	0.019	0.006	0.002
EHR Level 1	0.172	0.042	<.0001
EHR Level 2	-0.552	0.156	0.000
EHR Level 3	0.317	0.027	<.0001
EHR Level 4	1.155	0.064	<.0001
EHR Level 5	0.258	0.033	<.0001
EHR Level 6	0.050	0.061	0.417
EHR Level 7	0.069	0.020	0.001
$Accidental_{-1\&-3}$	0.091	0.114	0.423
$External_{-1\&-3}$	1.595	0.373	<.0001
$Malicious_{-1\&-3}$	-0.633	0.226	0.005
$BreachedRecords_{-1\&-3}$	-0.007	0.004	0.077
The prob of a $breach_{-1\&-3}$ (λ)	0.569	0.162	0.001
Year dummy			
Likelihood Ratio	1769.01		<.0001
Score	1503.53		<.0001
Wald	1230.27		<.0001
R-Square	0.189		
Adjusted R-Square	0.271		

Note. Variables subscripted "-1" is one lag, and "-1&-3" are averages of one, two and three year

Table 4. T-tests in the matched-pair sample

	No Meaningful Use	Meaningful Use	t-value	Pr > |t|
Control Variables				
Operating Expense	0.194	0.203	-0.710	0.478
Net income	0.009	0.011	-0.680	0.499
Bed size	0.215	0.221	-0.590	0.552
Security SW	9.234	9.431	-0.850	0.397
EHR Level 1	3.671	3.653	0.500	0.618
EHR Level 2	0.973	0.976	-0.400	0.691
EHR Level 3	4.460	4.562	-1.960	0.050
EHR Level 4	1.749	1.767	-0.820	0.411
EHR Level 5	1.393	1.521	-2.760	0.006
EHR Level 6	0.576	0.640	-2.810	0.005
EHR Level 7	2.921	3.091	-2.190	0.029
The Number of Breach occurrence $_{t\text{-}1\&\text{-}3}$				
Total Breaches	0.060	0.071	-0.86	0.392
Accidental	0.046	0.053	-0.63	0.526
Malicious	0.014	0.018	-0.71	0.480
External	0.002	0.005	-1.25	0.213
Affected Records	0.333	0.465	-0.75	0.455

Note. *one to one matching: each group has 925 hospitals.*

Table 5. The Impact of the Meaningful Use on the increase of breaches in the first year

	Total Breaches	*Accidental Breaches*	*External Breaches*	*Malicious Breaches*
	$\Delta B_{tot,i(12m)}$	$\Delta B_{acc,i(12m)}$	$\Delta B_{mal,i(12m)}$	$\Delta B_{ex,i(12m)}$
Intercept	-0.176 (0.208)	-0.192 (0.203)	0.001 (0.019)	0.016 (0.035)
Meaningful Use	0.197*** (0.044)	0.2*** (0.043)	-0.008* (0.004)	0.006 (0.007)
Operating Expense	0.052 (0.132)	0.197 (0.129)	-0.089*** (0.012)	-0.055** (0.022)
Net Income	1.32* (0.724)	0.633 (0.707)	0.058 (0.067)	0.629*** (0.122)
NofBeds	-0.043 (0.175)	-0.146 (0.17)	0.09*** (0.016)	0.014 (0.029)
Security SW	-0.003 (0.005)	-0.003 (0.004)	0.000 (0.000)	0.000 (0.001)
EHR Level 1	-0.011 (0.032)	-0.009 (0.031)	-0.002 (0.003)	-0.001 (0.005)
EHR Level 2	-0.071 (0.158)	-0.079 (0.154)	-0.002 (0.015)	0.01 (0.027)
EHR Level 3	0.012 (0.023)	0.013 (0.022)	0.000 (0.002)	0.000 (0.004)
EHR Level 4	0.056 (0.055)	0.068 (0.054)	0.000 (0.005)	-0.011 (0.009)
EHR Level 5	0.097*** (0.024)	0.09*** (0.023)	0.002 (0.002)	0.006 (0.004)
EHR Level 6	0.029 (0.046)	0.034 (0.045)	0.001 (0.004)	-0.006 (0.008)
EHR Level 7	-0.009 (0.015)	-0.01 (0.015)	0.001 (0.001)	0.000 (0.003)
Year Dummies				
Observations	1,850	1,850	1,850	1,850
R square	0.0521	0.0554	0.052	0.0285
F value	4.55***	4.86***	4.54***	2.43

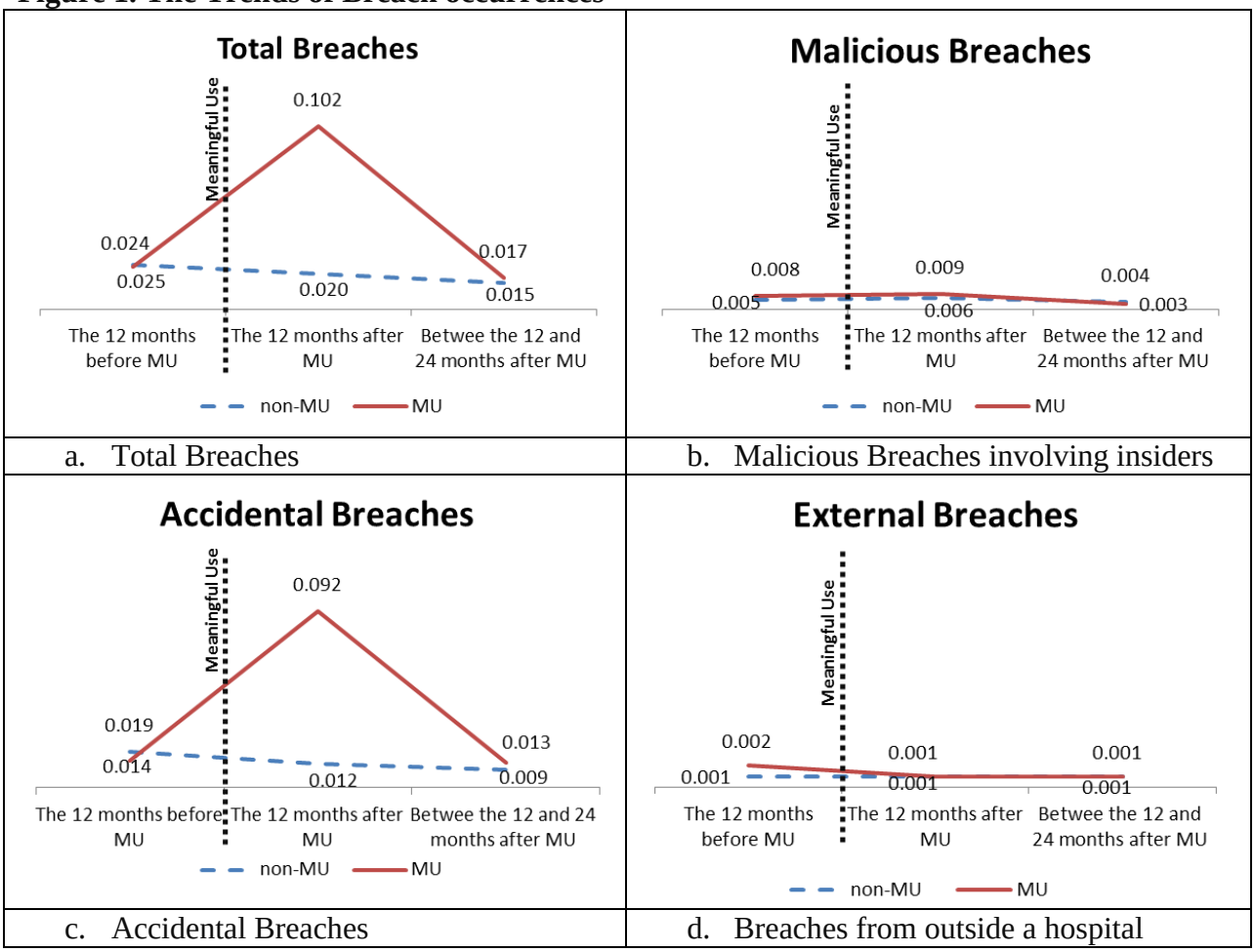
Note. *Standard errors are in parentheses. P-values are represented by * Significant at p <0.1, ** Significant at p<0.05, *** Significant at <0.01.*

Table 6. The Impact of the Meaningful Use on the increase of breaches in the second year

	Total Breaches	*Accidental Breaches*	*External Breaches*	*Malicious Breaches*
	$\Delta B_{tot,i(24m)}$	$\Delta B_{acc,i(24m)}$	$\Delta B_{mal,i(24m)}$	$\Delta B_{ex,i24m)}$
Intercept	0.201 (0.206)	0.227 (0.2)	-0.001 (0.013)	-0.009 (0.031)
Meaningful Use	-0.19*** (0.043)	-0.183*** (0.042)	0.001 (0.003)	-0.003 (0.007)
Operating Expense	-0.225* (0.131)	-0.242* (0.127)	0.001 (0.008)	-0.039** (0.02)
Net Income	-0.562 (0.718)	-0.715 (0.698)	0.001 (0.044)	0.781*** (0.108)
NofBeds	0.088 (0.173)	0.156 (0.168)	-0.005 (0.011)	-0.05* (0.026)
Security SW	0.002 (0.004)	0.003 (0.004)	0.000 (0.000)	-0.001 (0.001)
EHR Level 1	0.019 (0.031)	0.006 (0.031)	0.002 (0.002)	0.01** (0.005)
EHR Level 2	0.092 (0.156)	0.099 (0.152)	0.001 (0.009)	0.002 (0.024)
EHR Level 3	-0.029 (0.022)	-0.023 (0.022)	0.000 (0.001)	-0.006* (0.003)
EHR Level 4	-0.06 (0.054)	-0.057 (0.053)	-0.005* (0.003)	-0.009 (0.008)
EHR Level 5	-0.096*** (0.024)	-0.096*** (0.023)	0.001 (0.001)	0.004 (0.004)
EHR Level 6	-0.031 (0.045)	-0.047 (0.044)	0.002 (0.003)	0.009 (0.007)
EHR Level 7	0.017 (0.015)	0.014 (0.014)	0.000 (0.001)	0.003 (0.002)
Year Dummies				
Observations	1,850	1,850	1,850	1,850
R square	0.0580	0.614	0.0058	0.0588
F value	5.10***	5.42***	0.48	5.18***

Note. *Standard errors are in parentheses. P-values are represented by * Significant at p <0.1, ** Significant at p<0.05, *** Significant at <0.01.*

Figure 1. The Trends of Breach occurrences



a. Total Breaches

b. Malicious Breaches involving insiders

c. Accidental Breaches

d. Breaches from outside a hospital

Appendix A. Privacy and security requirements for Stage 1 of Meaningful Use[5]

Measure 12: Provide patients with an electronic copy of their health information, upon request. More than 50 percent of all patients who request an electronic copy of their health information are provided it within three business days.

Measure 15: Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities. Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.

[5] http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/Hospital_Attestation_Worksheet.pdf

Appendix B. EHRs (or EMRs) Applications

EHR adoption Level	EHR Applications
Level 1	Laboratory/ Radiology Information System Pharmacy Management System
Level 2	Clinical Data Repository Clinical Data Support System(CDSS) inference engine including Medical Terminology/Controlled Medical Vocabulary
Level 3	Clinical Decision Support System (flow sheets) Electronic Medication Administration Record (EMAR) EHR/Enterprise HER, Nursing Documentation
Level 4	Clinical Decision Support (Clinical Protocol) Computerized Practitioner Order Entry (CPOE) Order Entry (Includes Order Communications)
Level 5	Patient Portal, Physician Portal RFID - Patient Tracking, Telemedicine
Level 6	Physician Documentation (structured templates) Full CDSS(variance & compliance)
Level 7	Medical record fully electronic Data warehousing in use
Security	Anti-virus, Encryption, Firewall, Intrusion detection, Spam filter, User Authentication

Appendix C. Predicting the probability of breach occurrence

	Breach Occurrence$_{-1\&-3}$ (0 or 1)			
	Estimate	**StdErr**	**t value**	**P value**
Intercept	-3.071	0.174	-17.700	<.0001
Operating Expense $_{t-1\&-3}$	0.874	0.163	5.350	<.0001
N of FTE $_{t-1\&-3}$	0.102	0.029	3.530	0.0004
Security SW $_{t-1\&-3}$	-0.007	0.006	-1.100	0.2702
EHR Level 1 $_{t-1\&-3}$	0.123	0.043	2.890	0.0038
EHR Level 2 $_{t-1\&-3}$	0.312	0.150	2.080	0.0378
EHR Level 3 $_{t-1\&-3}$	0.026	0.024	1.110	0.2677
EHR Level 4 $_{t-1\&-3}$	0.275	0.065	4.210	<.0001
EHR Level 5 $_{t-1\&-3}$	0.072	0.044	1.640	0.101
EHR Level 6 $_{t-1\&-3}$	-0.157	0.068	-2.300	0.0214
EHR Level 7 $_{t-1\&-3}$	-0.061	0.031	-2.000	0.0458
Likelihood Ratio	644.57			