DOI: 10.1111/1475-6773.13203

RESEARCH ARTICLE

HSR Health Services Research

Data breach remediation efforts and their implications for hospital quality

Sung J. Choi PhD[1] | M. Eric Johnson PhD[2] | Christoph U. Lehmann MD[3]

[1]Department of Health Management and Informatics, University of Central Florida, Orlando, Florida

[2]Owen Graduate School of Management, Vanderbilt University, Nashville, Tennessee

[3]Department of Biomedical Informatics, Vanderbilt University, Nashville, Tennessee

Correspondence
Sung J. Choi, PhD, Department of Health Management and Informatics, University of Central Florida, 528 West Livingston St Room 402D, Orlando, FL
Email: sung.choi@ucf.edu

Funding information
National Science Foundation, Grant/Award Number: CNS-1329686

Abstract

Objective: To estimate the relationship between breach remediation efforts and hospital care quality.

Data Sources: Department of Health and Human Services' (HHS) public database on hospital data breaches and Medicare Compare's public data on hospital quality measures for 2012-2016.

Materials and Methods: Data breach data were merged with the Medicare Compare data for years 2012-2016, yielding a panel of 3025 hospitals with 14 297 unique hospital-year observations.

Study Design: The relationship between breach remediation and hospital quality was estimated using a difference-in-differences regression. Hospital quality was measured by 30-day acute myocardial infarction mortality rate and time from door to electrocardiogram.

Principal Findings: Hospital time-to-electrocardiogram increased as much as 2.7 minutes and 30-day acute myocardial infarction mortality increased as much as 0.36 percentage points during the 3-year window following a breach.

Conclusion: Breach remediation efforts were associated with deterioration in timeliness of care and patient outcomes. Thus, breached hospitals and HHS oversight should carefully evaluate remedial security initiatives to achieve better data security without negatively affecting patient outcomes.

KEYWORDS
data breach, privacy, quality of care, security

1 | BACKGROUND

Reports of the latest data breaches are highlighted regularly in news headlines.[1] As part of the Health Information Technology for Economic and Clinical Health (HITECH) Act, health care providers, health plans, and other entities covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) are required to notify affected individuals, the U.S. Department of Health and Human Services (HHS), and the media following a significant breach of protected health information.[2] Such reported breaches are investigated by the Office for Civil Rights (OCR), which enforces privacy and security rules and (with HHS) oversees corrective action.

The events following a breach are summarized in Figure 1A. Breaches are typically discovered some time after their occurrence. Discovery may be nearly immediate, while some breaches may take days or weeks to discover. Breaches affecting more than 500 individuals must be disclosed to the OCR within 60 days of discovery. Investigations of such reported breaches may take several months to a year. After the investigation is settled, the affected entity is monitored by HHS, typically for 3 years, during which time the breached entity proposes corrective actions. HHS approved corrective actions

are implemented by the affected entity,[3,4] which may include penalties, new information technology systems, staff training, and revision of policies and procedures.[3,5]

Corrective actions are intended to remedy the deficiencies in privacy and security of protected health information. However, enhanced security measures may introduce usability—which we define as the ease of use—problems. New security procedures typically alter how clinicians access and use clinical information in health information systems and may disrupt the provision of care as providers require additional time to learn and use the new or modified systems.[6-11]

1.1 | Conceptual model

Breach remediation refers to the corrective actions and changes introduced by the breached hospital, both voluntarily and mandated by HHS. Figure 1B shows a conceptual model that hypothesizes the relationship between breach remediation and hospital quality. Remediation activity may introduce changes that delay, complicate, or disrupt HIT and patient care processes.[12-15] Furthermore, changes in HIT systems are associated with learning, training, and support costs that may raise usability challenges and unexpected errors.[16] Remediation efforts to repair the damage from a data breach and improve security incur financial costs.[17,18] Our analysis focuses on the relationship between breach remediation and hospital quality (Figure 1B). Hospital quality measures for acute conditions and timeliness may be negatively affected by these remedial changes because of delays and disruptions in care. This relationship is potentially confounded by unobserved hospital characteristics. Our regression model estimated the relationship between breach remediation and hospital quality, adjusting for potential confounders. Specific remedial changes implemented at breached hospitals were not directly observed. Rather, we estimated breach remediation using dummy variables, which identify when breached hospitals implement remedial changes. After breach discovery, it may take 2-4 years for the hospital to implement remedial actions. Therefore, changes in hospital quality due to remediation may be observed long after the time of breach.

In the conceptual model, hospital quality does not directly affect security efforts such as breach remediation. We are not aware of formal regulations or cases where enforcement agencies intervened to remediate hospitals HIT because they have poor care quality, even though poorly implemented electronics health records (EHR) have been associated with safety concerns.[19]

Hospital characteristics may be associated with breaches and remediation effort along with hospital quality. Previous studies suggested that larger teaching hospitals were associated with breaches.[20,21] Large hospitals store more patient data, making them more attractive targets for external attackers. Large hospitals have more clinicians and staff, who access patient data, creating more internal vulnerabilities that can expose patient data. Teaching hospitals have more frequent clinician turnovers from residency and fellowship programs therefore may have greater vulnerabilities in training employees effectively, managing data access credentials, and implementing security procedures. Hospital financial performance may be associated with the financial burden of remediation costs and hospital quality. These challenges to estimating the direct effect of breach remediation on hospital quality are addressed in the empirical model.

Hospital data breaches provide a unique opportunity to study how solutions and fixes to information security problems are related to patient outcomes. Subsequent to a breach, organizations must take action to mitigate the failure and improve security. Such actions can be diverse, from adopting new policies and procedures to installing new security technologies. Taking advantage of financial incentives provided by HITECH, many hospitals made investments in more secure HIT, replacing or enhancing their EHRs. New systems often support advanced security features such as stronger authentication procedures and time-outs for inactivity. Following a breach, data handling and access privilege policies typically change.

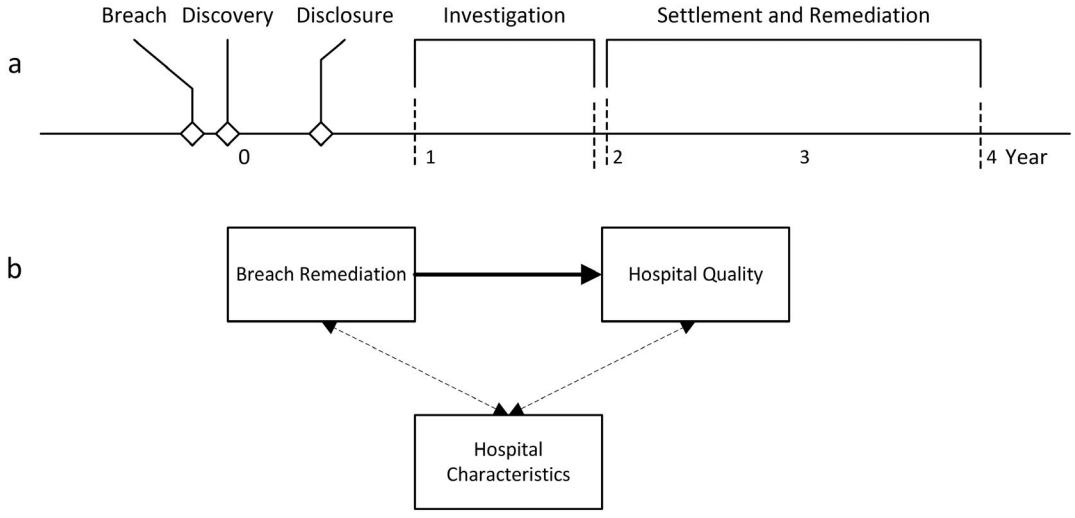

FIGURE 1 Timeline (A) and Conceptual Model (B)

Health systems are encouraged to implement auditing systems that can capture digital forensic evidence.[22] Management best practice includes planning, training, incentives, and penalties to prevent breaches.[23] Security best practice includes locking up physical devices, data encryption, and stronger passwords.[24] Single sign-on authentication may be used to improve password management.[25] These interventions require hospital staff to acclimate to new systems, learn new procedures, and adjust to new, and sometimes more cumbersome and time-consuming ways, of obtaining and manipulating patient data. Unsurprisingly, there is little literature documenting the specific experiences of a breached health system. Data breach and remediation are traumatic and embarrassing to an organization, and the incident is often reported in the media. Hospitals may be reluctant to draw further attention by publishing the details in a case study or a peer-reviewed journal article. A brief informal survey of chief medical informatics officers showed that publishing on breach remediation would be considered negatively by their institutions and was perceived as counterproductive as the new measures should not be advertised.

The aim of this paper was to estimate the long-term relationship between breach remediation and care quality. Using a difference-in-differences approach, we analyze a panel of nonfederal acute-care inpatient hospitals from 2012 to 2016 to evaluate patient outcomes and timeliness of care in the years sequent to a breach.

2 | METHODS

2.1 | Data

Health and Human Services maintains a public database of breaches reported from October 2009 to the present affecting 500 or more individuals.[1] Our analysis included breaches reported to the HHS and the Privacy Rights Clearinghouse (PRC) database between January 1, 2012, and December 31, 2016. The PRC aggregates reported breaches from public sources including the media, blogs, and government.[26]

The Centers for Medicare and Medicaid Services (CMS) provides public use data on Medicare-certified hospitals. Healthcare Cost Report Information System (HCRIS) provides data on hospital characteristics and financial variables.[27] Medicare Hospital Compare provides data on hospital quality measures.[28] Data on hospital breaches from HHS and PRC databases were merged with HCRIS and Hospital Compare data for the years 2012-2016.

As a proxy for care quality, we focused on the time from "door to electrocardiogram" (ECG) and the "30-day mortality rate for acute myocardial infarction" (AMI). For patients with symptoms suggestive of ST-segment elevation myocardial infarction (STEMI), guidelines recommend ECG acquisition and interpretation within 10 minutes of arrival in emergency department[29] as delays in the diagnosis and treatment on the order of minutes are associated with increased mortality and worse cardiac functional outcomes.[30] The 30-day mortality rate (Percent) was obtained from Hospital Compare.[31] The rate is calculated using data collected over past 36 months—the denominator includes Medicare beneficiaries aged 65 or older—and the measure is adjusted for patient characteristics to permit comparisons between hospitals. We also employed the time from door to ECG in Hospital Compare,[28] which is the median number of minutes for patients with symptoms suggestive of ST-segment elevation myocardial infarction from arrival at the hospital to receiving an ECG. Time to ECG is calculated using data collected over past 12 months, and the denominator includes adults aged 18 or older admitted to an emergency department with appropriate symptoms.

The 36-month collection period improves the estimation of comparable mortality rates for hospitals that admit a small number of patients by increasing the number of observed cases and mortalities. It also improves the precision of the risk adjustment method. The long collection period allows more hospitals to be included in the analysis; however, it produces a smoothing effect. For our analysis, the smoothing effective is not a problem because we focused on long-term associations with remediation efforts rather than the immediate changes associated with a breach.

The 30-day mortality rate is a widely adopted quality measure and permits national comparison of hospitals.[32-34] AMI is an acute event, in which a hospitalized patient's outcome depends on the quality of emergency department, cardiac catheterization laboratory, and inpatient care.[35] Also, acute medical events like AMI are less prone to selection bias due to patient's hospital choice, because treatment typically occurs at the nearest hospital, which reduces the possibility of patients avoiding a hospital with known poor quality or known data breaches, making AMI a good focus for the DID analysis.

Our hypothesis was that remediation efforts to enhance security would likely increase the time to access the EHR, order, review, and execute the ECG and thus result in an increase in time to treatment. By focusing on a condition that requires timely treatment (in minutes) and has both a readily available process measure (time to ECG) as well as a patient outcome measure (mortality), we anticipated to see an impact of breach mediation efforts. Treatments for other conditions for which measures exist, like pneumonia or heart failure, are less sensitive to diagnostic and therapeutic delays or disruptions and thus we would not expect to see a significant impact.

The raw data panel consisted of 5248 hospitals with repeated measurements over time yielding 33 175 observations uniquely identified at a hospital-year. Data were restricted to nonfederal acute-care inpatient hospitals. Hospitals in the U.S. territories and Maryland (which has a prospective payment system waiver) were excluded. To maintain consistency in the financial data, the data were restricted to hospitals that filed HCRIS within 360 and 370 reporting days. When a hospital submitted multiple reports in a given year, the most recent report was used. These restrictions yielded 3353 acute-care hospitals with 15 948 observations. Finally, observations with missing values in the dependent or independent variables were removed from analysis. Of 4197 observations were missing the 30-day AMI mortality rate, accounting for most of the missing values. The final study panel consisted of 3025 hospitals with 14 297 hospital-year observations.

2.2 | Generalized difference-in-differences model

Breaches arise from many different sources. Demand for health data on the black market makes hospitals a lucrative target for external attackers.[36,37] Internal vulnerabilities in hospital information systems may be exploited by external attackers or by insiders, who may inappropriately disclose data. But regardless of the source, the resulting discovery and remediation of a breach can be viewed as a random shock to a hospital's care delivery system. While agents affiliated with a hospital may benefit from intentionally leaking information (eg, hospital staff selling patient data to a third party for personal gains), agents (and the hospital itself) face criminal indictment, fines, and business losses from intentional or negligent breaches,[38] which disincentivize intentional breaches. Thus, a hospital data breach can be framed as a natural experiment to estimate the relationship between breach remediation and patient outcomes. Past research focused the short-term (days to months) impact of breaches. In this study, we examine the associations with longer-term remedial changes (years) as hospitals work to improve security.

The association between breaches and hospital outcomes was estimated using a generalized difference-in-differences (DID) framework with multiple pre- and postperiods.[39] Data breaches represent random shocks reported in a specific year, though susceptible to measurement error from the actual year of breach. Panel data provide pre- and postbreach measures of quality. The DID strategy controls for time trends in outcomes among the breached hospitals, assuming that the breached hospitals would have followed the same trend if they had not been breached, to isolate the change in outcomes associated with the breach.

The dependent variables were 30-day mortality rate for acute myocardial infarction (AMI) and time from door to electrocardiogram (ECG). The independent variables of interest were the relative-time-to-breach dummies that were set to 1 when the hospital was in the breached group, and the year of the observation was n years relative to the hospitals' specific time of breach. The relative time (n) was set to 0 on the year of the breach, we observed 4 years before and after the breach. One year before breach was set as the omitted category. The coefficients on the relative-time-to-breach dummies estimated the change in quality associated with breach remediation.

The DID model controlled for the hospital-specific fixed effects and year fixed effects. An organization's safety culture captures the knowledge, beliefs, and attitudes regarding safety in the organization.[40] Safety and security are rooted in cultures that emphasize the importance of well-designed processes and heightened awareness of goals. We suggest that patient safety and data security cultures are closely related. The overall hospital safety climate, influenced by organizational policy regarding safety, has been associated with readmissions for AMI and heart failure.[35,41] Hospital fixed effects are conceptually equivalent to assigning a dummy variable to each hospital, which effectively controls for unobserved confounders such as hospital-specific characteristics, like safety culture, that are constant in the short run.

The DID model included covariates for time-varying hospital characteristics that may be correlated with both breach remediation and hospital quality as described in the conceptual model. Covariates included operating revenue, number of beds, length of stay, bed occupancy rate, *meaningful use* status (meaningful user of certified electronic health records as defined in HITECH), patient

TABLE 1 Summary of breaches by year and type of breach

Type of Breach	2012	2013	2014	2015	2016	All
Hacking/IT Incident	7	4	11	9	13	44
Improper Disposal	2	2	1	1	0	6
Loss	18	22	11	6	3	60
Multibreach	2	2	2	0	0	6
Other	5	3	5	0	0	13
Theft	16	12	19	15	4	66
Unauthorized Access/Disclosure	13	29	23	29	18	112
All	64	74	75	60	38	311

Type of breach	Individuals affected
Hacking/IT Incident	11 101 099
Improper Disposal	23 970
Loss	825 439
Multibreach	47 790
Other	367 372
Theft	365 874
Unauthorized Access/Disclosure	1 295 153
All	14 026 697

Note: From the total of 311 breaches, six did not report the number of individuals affected.

satisfaction, and patient safety indicators. The DID model was estimated using a fixed-effects regression. Our analysis was performed using Stata version 14 and R version 3.2.[42,43] Standard errors are heteroskedasticity robust and allow for within hospital correlation.

3 | RESULTS

3.1 | Descriptive statistics

Table 1 shows the summary of hospital data breaches affecting 311 hospital-years. The three most common breach types were unauthorized access (112), loss (60), and theft (66). A subset of breaches affecting 305 hospital-years reported the number of individual records breached. While prone to error and underreporting, this measure is a proxy for the severity of a breach. Affected individual records totaled approximately 14 million. From 2012 to 2016, a small group of breaches (43) affected the majority (11 million) of individuals.

Characteristics of the hospital-year observations by breach status are summarized in Table 2. As expected, the timing of breaches varied across the sample years. Given the cumulative effect among the breached hospitals, most of the prebreach hospital-year observations came from years 2012-2014 while most postbreach observations came from years 2014-2016. Because of variability in breach event timing, it was impossible to assign the never-breached hospitals into a pre- or postevent category based on time. Therefore, the never-breached hospital-year observations were pooled into a single control group (Table 2).

The percentage of not-for-profit hospitals was similar between the control group and the breached group. However, the breached group had a higher proportion of public hospitals, while the control group had a higher proportion of for-profit hospitals. Hospitals in the breached group were more likely to be major teaching hospitals. Patient satisfaction measures were similar between the control group and the breached group, and satisfaction within the breached group did not vary between the pre- and postbreach group.

The overall trends for 30-day AMI mortality and time from door to ECG from 2012 to 2016 for all hospitals show improvement in 30-day mortality rate and time to ECG (Appendix S1: Figure S1a,b). The trends in 30-day AMI mortality rate were stratified to never-breached hospitals and hospitals that were breached in 2015 (Appendix S1: Figure S2a). The two groups had parallel trends from 2012 to 2014, but then the breached hospitals crossed the parallel trend in 2016 with a more positive slope relative to the never-breached hospitals resulting in higher mean mortality rates than the never-breached hospitals. However, the point estimate was not statistically significant. The trends in time to ECG were also stratified between the two groups (Appendix S1: Figure S2b). The two groups showed parallel trends from 2013 to 2015, with point estimates that were not significantly different. However, in 2016 the breached hospitals had significantly longer time to ECG (11 minutes) than the never-breached hospitals (8 minutes).

The control group and the prebreach group had similar distributions for the 30-day AMI mortality rate. The mean 30-day AMI mortality rate for the prebreach group was 14.98 percent; for the control group, it was 14.74 percent (not statistically different). Mean time to ECG was longer for the prebreach group than the control group (9.4 minutes vs 8.6 minutes), but again not statistically significant. The mean number of beds for the prebreach group was nearly two times larger than the control group (410 vs 220). Among the breached group, the number of beds was higher in the postbreach group.

3.2 | DID estimates

Difference-in-differences estimates for 30-day AMI mortality rate are summarized in Figure 2 (regression coefficients shown in Appendix S1: Table S1). The y-intercept is the expected 30-day AMI mortality rate at 1 year before the breach. It represents the baseline 30-day AMI mortality if a breach had not occurred, and for ease of interpretation, we centered it at zero instead of the grand mean. The plotted points are the expected 30-day AMI mortality rate at the relative breach time, adjusting for the baseline rate, yearly time trends, time-invariant hospital effects, and time-varying hospital characteristics. At 1, 2, 3 years after the breach, the 30-day AMI mortality rate point estimates were significantly higher than the baseline. Model estimates indicate that a data breach was associated with a 0.23 percentage point increase in the 30-day AMI mortality rate 1 year after the breach, 0.36 percentage point increase 2 years after the breach, and 0.35 percentage point increase 3 years after the breach (Appendix S1: Table S1). The 30-day AMI mortality rate of breached hospitals did not differ significantly from the never-breached hospitals in the prebreach periods.

Difference-in-differences estimates for time from door to ECG are summarized in Figure 3 (regression coefficients shown in Appendix S1: Table S2). The y-intercept is the expected time to ECG at 1 year before the breach reflecting the baseline time to ECG if a breach had not occurred. At 0, 1, 3, 4 years after the breach, the time to ECG point estimates is significantly longer than the baseline. The time to ECG of breached hospitals did not differ significantly from the never-breached hospitals in the prebreach periods. We found that a data breach was associated with a 1.4-minute increase in time to ECG 1 year after the breach. The elevated time to ECG persisted with a 2.7-minute and a 2-minute increase in time to ECG at 3 and 4 years after the breach, respectively.

4 | DISCUSSION

Hospital data breaches were associated with higher 30-day AMI mortality rates in the years following the breach. Over the past few years, overall improvements in AMI treatment have resulted in the 30-day AMI mortality rate decreasing about 0.4 percentage points annually from 2012 to 2014 (Appendix S1: Figure S1). A 0.23-0.36 percentage point increase in 30-day AMI mortality rate after a breach effectively erases a year's worth of improvement in the mortality rate. The national estimate for the number of hospital

TABLE 2 Mean and (SD) shown for continuous variables. Count and (percent) shown for categorical variables

	Never-breached	Prebreach	Postbreach
N	12985	426	886
AMI mortality rate	14.74 (1.47)	14.98 (1.69)	14.38 (1.54)
Time to ECG (min)	8.55 (14.67)	9.42 (6.97)	8.99 (5.53)
Operating revenue ($M)	213.89 (263.26)	485.58 (512.55)	611.97 (653.91)
Net operating revenue ($M)	2.16 (73.49)	−23.67 (160.25)	−21.56 (236.52)
Operating margin	−0.03 (0.50)	−0.07 (0.39)	−0.05 (0.33)
Number of beds	219.59 (239.66)	410.23 (343.83)	496.12 (1280.36)
LOS	4.33 (4.66)	4.61 (0.88)	4.84 (0.94)
Occupancy rate	0.52 (0.51)	0.63 (0.16)	0.65 (0.17)
Meaningful user: yes	9294 (71.6)	270 (63.4)	636 (71.8)
Ownership			
Nonprofit	7976 (61.4)	300 (70.4)	595 (67.2)
Profit	3123 (24.1)	26 (6.1)	105 (11.9)
Public	1886 (14.5)	100 (23.5)	186 (21.0)
Teaching status			
Major teaching	1004 (7.7)	132 (31.0)	301 (34.0)
Minor teaching	3067 (23.6)	120 (28.2)	250 (28.2)
Nonteaching	8914 (68.6)	174 (40.8)	335 (37.8)
Rural: yes	3840 (29.6)	69 (16.2)	112 (12.6)
Year			
2012	2659 (20.5)	198 (46.5)	64 (7.2)
2013	2616 (20.1)	131 (30.8)	133 (15.0)
2014	2591 (20.0)	72 (16.9)	189 (21.3)
2015	2558 (19.7)	25 (5.9)	236 (26.6)
2016	2561 (19.7)	0 (0.0)	264 (29.8)

discharges for AMI fluctuated around 556 000 discharges annually between 2005 and 2014.[44] On average, a data breach at a nonfederal acute-care inpatient hospital was associated with an additional 23-36 deaths per 10 000 AMI discharges per year.

Time from door to ECG significantly increased after a breach and the elevated time to ECG persisted at 4 years after the breach. Security typically adds inconvenience by design—making it more inconvenient for the adversary. For example, stricter authentication methods, such as passwords with two-factor authentication, are additional steps that slow down workflow in exchange for added security. Lost passwords and account lockouts are nuisances that may disrupt workflow. The persistence in the longer time to ECG suggests a permanent increase in time requirement due to stronger security measures.

Timely evaluation and treatment of ST-segment elevation myocardial infarction (STEMI) have been associated with better patient outcomes.[29,45-48] The American Heart Association/American College of Cardiology (AHA/ACC) guideline recommends a time to ECG of < 10 minutes for STEMI patients, because exceeding this threshold results in worse outcomes.[49] The prolonged time to ECG after the breach is a potential mediator for the increased AMI mortality rate after the breach.

Remediation efforts after a data breach vary depending on the type of breach and perceived weaknesses to a repeat attack. However, common approaches include additional verification layers during sign-on, shortened inactivity periods to automatic sign-out, and additional acknowledgment steps that delay the access to patient data and may lead to inefficiencies or delays in care. Especially in the case of a patient with chest pain arriving in the emergency department, any delay in registering the patient and accessing the patient's record will lead to delay in ordering and executing the ECG. With every minute delay affecting mortality, delays in access to the electronic health record may prove detrimental. Han et al[14] described the impact that a new electronic record had on mortality of children. The inability to preregister patients transported into the pediatric intensive care unit resulted in delayed ordering of medications and increased mortality. Security solutions designed to reduce the likelihood of breaches may need “break the glass” functionalities to reduce the likelihood of delayed or compromised care.

Changes in HIT and patient care processes in response to a data breach introduce usability challenges and unintended side effects that frustrate clinicians and disrupt patient care.[12] Frustrated clinicians bypassing new systems and processes with ad hoc workarounds avoid system safeguards and create new opportunities

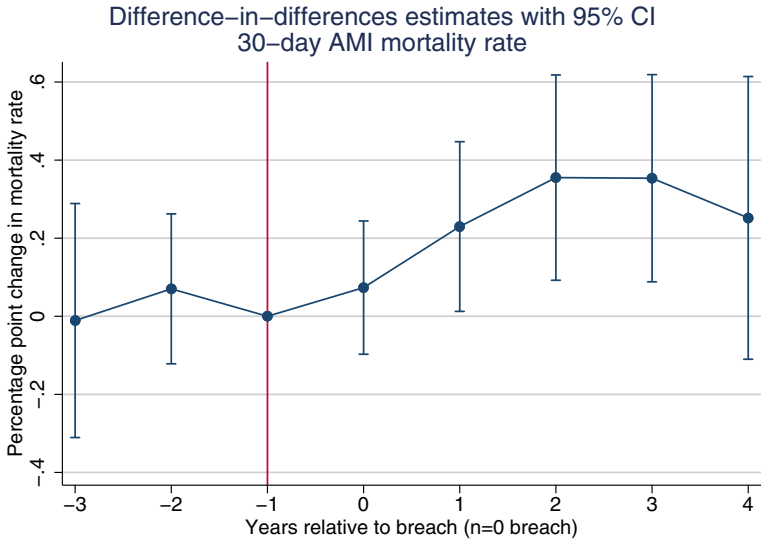

FIGURE 2 Plot of the difference-in-difference model for AMI mortality rate [Color figure can be viewed at wileyonlinelibrary.com]

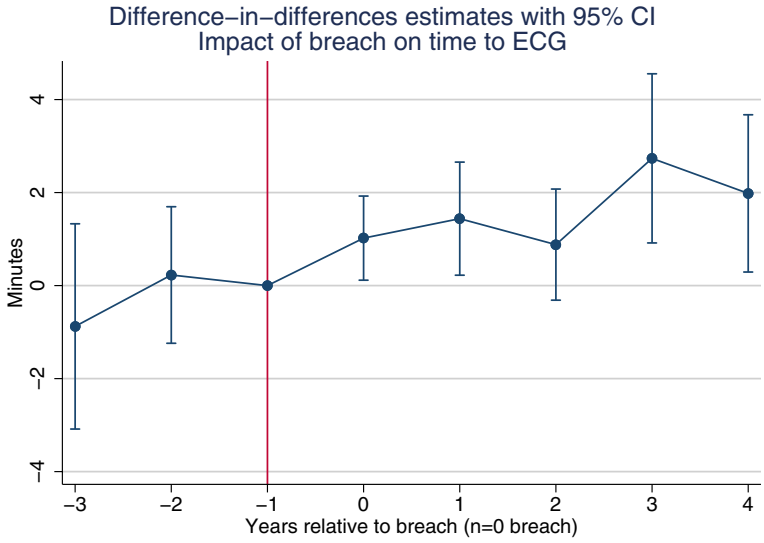

FIGURE 3 Plot of the difference-in-difference model for time to ECG [Color figure can be viewed at wileyonlinelibrary.com]

for errors.[13,14] Enhanced security measures in response to a data breach are likely to worsen the usability of the HIT system, which not only diminishes the effectiveness of its intended function but also spawns new errors that worsen the quality of care provided to patients. Installation of new health IT requires clinicians and staff to learn new processes, procedures, and ways to coordinate their workflow.[15] Clinicians adjusting to new processes and systems do so in the presence of patients, which detracts from time spent communicating with the patient and diminishes the patient experience and satisfaction.[50]

While short-term disruptions are not addressed in this paper, the recent emergence of hospital ransomware attacks has created short-term disruptions to hospital services and there are growing fears of attacks on the care delivery system itself.[51] Ransomware attacks involve an attacker holding data hostage in exchange for payment. Ransomware attacks are considered more disruptive to hospital operations than the breaches considered in this study. In extreme cases, hospital data breaches can also negatively affect the accuracy and timeliness of patient information available to providers. A hacking incident may temporarily disrupt hospital's servers, making patient data unavailable to providers while the servers are being patched or repaired. Severe hacking attacks may force hospitals to revert to paper charts.[52,53] Instances of unauthorized access suggest that existing systems may have weaknesses verifying provider or patient identity, which may increase the risk of a provider inadvertently accessing or editing information on the wrong patient.[54] Inaccuracies or delays in patient information resulting from changes or enhancements in security are likely to disrupt the care process and adversely affect patient outcomes. Downtimes in electronic health records because of maintenance or malfunction has been associated with disruptions in laboratory and medication orders as a result of patient identification and communication problems.[55] The data breaches studied in our analysis came from 2012 to 2016 and ransomware or infrastructure attacks were rare before 2016. Our findings suggest that ransomware attacks might have an even stronger short-term

negative relationship with patient outcomes than the long-term remediation efforts studied here.

Future work on hospital data security needs to address the implications of ransomware attacks for patient outcomes. Ransomware attacks that affect hospitals and entire health systems are executed in a matter of days.[51] The shock of ransomware attacks on hospitals and patients can be framed as a natural experiment. Ransomware attacks are likely to be initiated by opportunistic external adversaries motivated by financial reward; therefore, the model for ransomware attacks has a smaller threat of confounding variables related to patient outcomes. Using inpatient discharge data, rather than hospital level aggregate data used in this study, will reveal implications for patients. Studying ransomware attacks will also provide insights into long-run changes on hospitals associated with remediation activities, which may persist years after the attack.

4.1 | Limitations

Our analysis cannot rule out the possibility of unobserved environmental events correlated with both breach remediation and hospital quality. Also, we do not directly observe remediation activities implemented by hospitals. By parsimony, we associate the deterioration in quality after a breach to remediation rather than environmental events.

An unobserved time-varying variable related to both breach remediation and quality is a potential confounder. The breach impact estimates were similar between the models with and without the patient safety indicators. The findings suggest that patient safety indicators were not confounding factors, but raise new concerns whether these indicators were effective controls for care quality problems.

A key assumption in our DID model is that hospitals' safety culture and management style are fixed in the short run. We did not observe data on hospital mergers and acquisition, changes in system affiliation, or changes in ownership during the study period. Such organizational changes may be correlated with the probability of breach, implementation of breach remediation, and hospital quality.

We did not observe time-variant characteristics of the hospitals' health IT system. Meaningful user status was used as a proxy for the maturity of the health IT system. But the health IT vendor and product may be correlated with breach remediation and quality. The DID model assumed that health IT characteristics were fixed in the short run, which may be reasonable given that health IT systems are large capital expenditures. However, changes in hospitals' health IT during the study period may confound the model estimates.

The never-breached hospital-year observations were pooled into a single control group limiting the comparability of the time-varying characteristics between the never-breached group and the pre-breach group.

5 | CONCLUSION

The health services literature has shown mixed findings on the effect of health IT adoption on hospital quality. Health IT promises quality improvements and cost savings but its benefits are elusive because of learning, implementation, and usability issues that hinder clinicians. Hospitals adopting health IT anticipate learning costs and prepare clinicians with training and support months in advance of implementation. Despite the preparations, significant usability challenges and unexpected errors are inevitable.[16] Analogous to adoption of health IT, the remediation activities to improve security in health IT systems following a breach introduce new changes into complex work environments, which may disrupt care processes and explain our findings of reduced quality.[56-58]

Health data breaches have significant consequences for patients, providers, and payers and contribute to quality of care problems. Protecting health information is an important responsibility of all parties in the health care industry. Our results indicate that breaches and the subsequent HHS-mandated corrective actions and hospital remediation may have adverse implications for quality of care. Breached hospitals should carefully consider remedial security initiatives to limit inadvertent delays and disruptions associated with new processes, procedures, and technologies.

ACKNOWLEDGMENTS

Joint Acknowledgment/Disclosure Statement: This work was partially supported by a collaborative award from National Science Foundation award CNS-1329686. Dr. Christoph U. Lehmann works for the American Academy of Pediatrics as the Director of the Child Health Informatics Center. He receives royalties for the book "Pediatric Informatics". He serves as the president of the International Medical Informatics Association. He is past chair of the Clinical Informatics subboard at the American Board of Preventive Medicine. He is the editor in chief of Applied Clinical Informatics.

ORCID

Sung J. Choi https://orcid.org/0000-0003-0299-5382

Christoph U. Lehmann https://orcid.org/0000-0001-9559-4646

REFERENCES

1. U.S. Department of Health & Human Services. Breach report. Published 2016. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. Accessed September 22, 2016.
2. U.S. Department of Health & Human Services. Breach notification rule. Published 2016. http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html. Accessed September 22, 2016.
3. Department of Health and Human Services. University of California settles HIPAA Privacy and Security case involving UCLA Health System facilities. Published 2011. http://wayback.archive-it.org/3926/20140108162127/http://www.hhs.gov/news/press/2011pres/07/20110707a.html. Accessed September 11, 2017.
4. Department of Health and Human Services. Advocate Health Care Settles Potential HIPAA Penalties for $5.55|HHS.gov. Published 2016. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ahcn/index.html. Accessed September 11, 2017.

5. Department of Health and Human Services. Enforcement Process|HHS.gov. Published 2017. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html. Accessed September 11, 2017.
6. Freudenheim M. Many hospitals resist computerized patient care—the New York Times. *The New York Times*. April 6, 2004.
7. Bhattacherjee A, Hikmet N. Physicians' resistance toward healthcare information technology: a theoretical model and empirical test. *Eur J Inf Syst*. 2007;16(6):725-737.
8. Boyer E. Understanding usability-related information security failures in a healthcare context. *NSUWorks Grad Sch Comput Inf Sci*. September 2014.
9. Schultz EE, Proctor RW, Lien M-C, Salvendy G. Usability and security an appraisal of usability issues in information security methods. *Comput Secur*. 2001;20(7):620-634.
10. Al-Gahtani SS, King M. Attitudes, satisfaction and usage: factors contributing to each in the acceptance of information technology. *Behav Inf Technol*. 1999;18(4):277-297.
11. Markus ML, Lynne M. Power, politics, and MIS implementation. *Commun ACM*. 1983;26(6):430-444.
12. Koppel R. Great Promises of Healthcare Information Technology Deliver Less. In: Weaver CA, Ball MJ, Kim GR, Kiel JM, eds. *Healthcare Information Management Systems*. Cham: Springer International Publishing; 2016:101–125. https://doi.org/10.1007/978-3-319-20765-0_6
13. Campbell EM, Sittig DF, Ash JS, Guappone KP, Dykstra RH. Types of unintended consequences related to computerized provider order entry. *J Am Med Inform Assoc*. 2006;13(5):547-556.
14. Han YY, Carcillo JA, Venkataraman ST, et al. Unexpected increased mortality after implementation of a commercially sold computerized physician order entry system. *Pediatrics*. 2005;116(6):1506-1512.
15. Meyerhoefer CD, Deily ME, Sherer SA, et al. The consequences of electronic health record adoption for physician productivity and birth outcomes. *ILR Rev*. 2016;69(4):860-889.
16. Schwartzberg D, Ivanovic S, Patel S, Burjonrappa SC. We thought we would be perfect: medication errors before and after the initiation of Computerized Physician Order Entry. *J Surg Res*. 2015;198(1):108-114.
17. Romanosky S. Examining the costs and causes of cyber incidents. *J Cybersecurity*. 2016;2(2):121-135. https://doi.org/10.1093/cybsec/tyw001
18. Ponemon Institute. 2016 cost of data breach study: United States; 2016.
19. Bresnick J. Patient safety errors are common with electronic health record use. Health IT analytics. Published 2017. https://healthitanalytics.com/news/patient-safety-errors-are-common-with-electronic-health-record-use. Accessed December 2, 2018.
20. Bai G, Jiang J, Flasher R. Hospital risk of data breaches. *JAMA Intern Med*. 2017;313(14):1424.
21. Gabriel MH, Noblin A, Rutherford A, Walden A, Cortelyou-Ward K. Data breach locations, types, and associated characteristics among US hospitals. *Am J Manag Care*. 2018;24(2):78-84.
22. Chernyshev M, Zeadally S, Baig Z. Healthcare data breaches: implications for digital forensic readiness. *J Med Syst*. 2019;43(1):7.
23. Fernández-Alemán JL, Sánchez-Henarejos A, Toval A, Sánchez-García AB, Hernández-Hernández I, Fernandez-Luque L. Analysis of health professional security behaviors in a real clinical setting: an empirical study. *Int J Med Inform*. 2015;84(6):454-467.
24. UC Santa Cruz. Security breach examples and practices to avoid them. Published 2015. https://its.ucsc.edu/security/breaches.html. Accessed April 8, 2019.
25. Heckle RR, Lutters WG. Tensions of network security and collaborative work practice: understanding a single sign-on deployment in a regional hospital. *Int J Med Inform*. 2011;80(8):e49-e61.
26. Privacy Rights Clearinghouse. Privacy rights clearinghouse chronology of data breaches. Published 2017. https://www.privacyrights.org/data-breach. Accessed September 1, 2017.
27. Centers for Medicare & Medicaid Services. Hospital Cost Report Information System; 2016.
28. Centers for Medicare & Medicaid Services. Medicare Hospital Compare. Published 2016. https://www.medicare.gov/hospitalcompare/about/what-is-HOS.html. Accessed September 22, 2016.
29. Yiadom MYAB, Mumma BE, Baugh CW, et al. Measuring outcome differences associated with STEMI screening and diagnostic performance: a multicentred retrospective cohort study protocol. *BMJ Open*. 2018;8(5):e022453.
30. Shiomi H, Nakagawa Y, Morimoto T, et al. Association of onset to balloon and door to balloon time with long term clinical outcome in patients with ST elevation acute myocardial infarction having primary percutaneous coronary intervention: observational study. *BMJ*. 2012;344:e3257.
31. Centers for Medicare & Medicaid Services. Acute myocardial infarction (AMI): hospital 30-day, all-cause, risk-standardized mortality rate (RSMR) following AMI hospitalization. National Quality Measures Clearinghouse. Published 2016. https://www.qualitymeasures.ahrq.gov/summaries/summary/49187. Accessed September 22, 2016.
32. Krumholz HM, Lin Z, Keenan PS, et al. Relationship between hospital readmission and mortality rates for patients hospitalized with acute myocardial infarction, heart failure, or pneumonia. *JAMA*. 2013;309(6):587.
33. Centers for Medicare & Medicaid Services. Medicare program; hospital inpatient prospective payment systems for acute care hospitals and the long-term care hospital prospective payment system and FY 2012 rates; hospitals' FTE resident caps for graduate medical education payment. Final rules. *Fed Regist*. 2011;76(160):51476-51846.
34. Centers for Medicare & Medicaid Services. Medicare program; hospital inpatient value-based purchasing program. Final rule. *Fed Regist*. 2011;76(88):26490-26547.
35. Hansen LO, Williams MV, Singer SJ. Perceptions of hospital safety climate and incidence of readmission. *Health Serv Res*. 2011;46(2):596-616.
36. Humer C, Finkle J. Your medical record is worth more to hackers than your credit card. *Reuters*. September 24, 2014.
37. Beek C, McFarland C, Samani R. Health warning: cyberattacks are targeting the health care industry; 2016.
38. U.S. Department of Health & Human Services. HIPAA compliance and enforcement. Published 2016. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html. Accessed January 2, 2017.
39. Jacobson LS, Lalonde RJ, Sullivan DG. American Economic Association earnings losses of displaced workers earnings losses of displaced workers. *Am Econ Rev*. 1993;83(4):685-709.
40. Zohar D. Safety climate in industrial organizations: theoretical and applied implications. *J Appl Psychol*. 1980;65(1):96-102.
41. Singer SJ, Falwell A, Gaba DM, et al. Identifying organizational cultures that promote patient safety. *Health Care Manage Rev*. 2009;34(4):300-311.
42. StataCorp. Stata Statistical Software: Release 14; 2015.
43. R Core Team. R: A language and environment for statistical computing; 2018.
44. Agency for Healthcare Research and Quality. HCUP projections acute myocardial infarction and acute stroke 2005 to 2016; 2016.
45. Gibson CM, Pride YB, Frederick PD, et al. Trends in reperfusion strategies, door-to-needle and door-to-balloon times, and in-hospital mortality among patients with ST-segment elevation myocardial infarction enrolled in the National Registry of Myocardial Infarction from 1990 to 2006. *Am Heart J*. 2008;156(6):1035-1044.

46. McNamara RL, Wang Y, Herrin J, et al. Effect of door-to-balloon time on mortality in patients with ST-segment elevation myocardial infarction. *J Am Coll Cardiol*. 2006;47(11):2180-2186.
47. Terkelsen CJ, Sørensen JT, Maeng M, et al. System delay and mortality among patients with STEMI treated with primary percutaneous coronary intervention. *JAMA*. 2010;304(7):763.
48. Hudson MP, Armstrong PW, O'Neil WW, et al. Mortality implications of primary percutaneous coronary intervention treatment delays: insights from the assessment of pexelizumab in acute myocardial infarction trial. *Circ Cardiovasc Qual Outcomes*. 2011;4(2):183-192.
49. Antman EM, Anbe DT, Armstrong PW, et al. ACC/AHA guidelines for the management of patients with ST-elevation myocardial infarction. *J Am Coll Cardiol*. 2004;44(3):E1-E211.
50. Sharma L, Chandrasekaran A, Boyer KK, McDermott CM. The impact of health information technology bundles on hospital performance: an econometric study. *J Oper Manag*. 2016;41:25-41.
51. Green M. Hospitals are hit with 88 percent of all ransomware attacks. *Beckers Hosp Rev*. July 2016.
52. Wong J. Los Angeles hospital returns to faxes and paper charts after cyberattack. *The Guardian*. February 16, 2016.
53. Cox J, Turner K, Zapotosky M. Virus infects MedStar Health system's computers, forcing an online shutdown. *Wash Post*. March 2016.
54. Adelman JS, Kalkut GE, Schechter CB, et al. Understanding and preventing wrong-patient electronic orders: a randomized controlled trial. *J Am Med Inform Assoc*. 2013;20(2):305-310.
55. Larsen E, Fong A, Wernz C, Ratwani RM. Implications of electronic health record downtime: an analysis of patient safety event reports. *J Am Med Inform Assoc*. 2017;25:187-191.
56. Jones SS, Adams JL, Schneider EC, Ringel JS, McGlynn EA. Electronic health record adoption and quality improvement in US hospitals. *Am J Manag Care*. 2010;16(12 Suppl HIT):SP64-SP71.
57. Ash JS, Sittig DF, Dykstra R, Campbell E, Guappone K. The unintended consequences of computerized provider order entry: findings from a mixed methods exploration. *Int J Med Inform*. 2009;78:S69-S76.
58. Harrison MI, Koppel R, Bar-Lev S. Unintended consequences of information technologies in health care—an interactive sociotechnical analysis. *J Am Med Inform Assoc*. 2007;14(5):542-549.

SUPPORTING INFORMATION

Additional supporting information may be found online in the Supporting Information section at the end of the article.

How to cite this article: Choi SJ, Johnson ME, Lehmann CU. Data breach remediation efforts and their implications for hospital quality. *Health Serv Res*. 2019;54:971–980. https://doi.org/10.1111/1475-6773.13203