DATA BREACH INFORMATION, HOSPITAL FINANCING, AND PATIENT OUTCOMES*

Banks Osborne

* Banks Osborne (bosbor14@vols.utk.edu) is a PhD student in Finance at the Haslam College of Business at the University of Tennessee, Knoxville, TN, 37996. I am grateful for the incredibly helpful guidance from Xuelin Li, Matthew Serfling, Zihan Ye, and seminar participants at the University of Tennessee.

DATA BREACH INFORMATION, HOSPITAL FINANCING, AND PATIENT OUTCOMES

May 6, 2024

ABSTRACT

I examine the costs and real effects of medical data breaches using a stacked difference-in-differences research design. I find that data breaches increase the cost of healthcare financing and examine three mechanisms that link data breaches to increased costs. Data breaches increase issuer credit risk, and hacks, specifically, decrease hospital revenues because patients substitute breached hospital services for the services of non-breached hospitals nearby. This substitution does not hurt the patients of breached hospitals but leads to worse outcomes for patients of nearby hospitals. Interestingly, although only hacks have an impact on hospital revenues, investors do not require an incremental premium for investing in bonds of hacked issuers. Lastly, I find evidence that the pricing of breached bonds is influenced by investor attention towards breaches. Altogether, my results suggest that investors are potentially uninformed regarding the nuances of different types of breaches and how the market responds to breaches may not necessarily reflect how the events actually affect breached entities.

Keywords: Municipal Bonds, Healthcare Finance, Cyber Risk, Data Breach, Data Security

JEL Classifications: G12, G31, H74, H75, I11, I14, L31

"The most significant and consequential cyberattack in American history began Feb. 21 against UnitedHealth Group's Change Healthcare, crippling financial operations for hospitals, insurers, pharmacies, and medical groups nationwide."

- Jakob Emerson and Rylee Wilson, *Becker's Health IT*, 2024

1. Introduction

Hospitals are crucial organizations in modern life. From aiding in 99% of births to caring for over 35% of deaths in the United States, the institutions offer a wide array of preventative and emergency care services to patients in all stages of life (MacDorman and Declercq, 2019; CDC, 2020). Furthermore, hospitals are major sources of revenue and employment in the local economy by doubling local business revenue and helping generate two outside jobs for every hospital position (AHA, 2022). Given the sensitive nature of the data that hospitals hold and the reach of hospitals' role in society, it is no surprise that they are targets of an ever-growing number of cyberattacks that threaten the economic and nonpecuniary benefits that hospitals offer society. For example, the 2021 ransomware attack on the non-profit Scripps Health system in San Diego reduced patient access to medical care during the breach and lost the hospital system over $100 million, primarily through litigation and lost revenue (Burky, 2023). Despite the potential for the events to adversely affect wider society, little is known about how the average breach actually affects hospitals or their stakeholders. In this paper, I examine how data breaches affect the healthcare market by identifying how they influence both hospital financing and patient outcomes.

Hospital data breaches serve as a unique setting to study how much data breaches cost in both financial and societal terms. First, healthcare data breaches are subject to federal Health Insurance Portability and Protection (HIPAA) reporting requirements and, consequently, are much less likely to suffer from sample selection bias than breaches of publicly traded firms. As such, a study of hospital breaches is not constrained to just hacks or events that happen after a state passes its own data breach notification laws (e.g., Huang and Wang, 2021; Jamilov et al., 2021; Kamiya et al., 2021). Relatedly, information about breached entities is cleanly identified and is simple to match to external databases because the processes following health-related data breaches are federally regulated. Lastly, the information environment surrounding health-related breaches uniquely contrasts that of corporate breaches. Whereas information about health breaches is released quickly, hospital performance and patient outcome data is sometimes released with significant delay, potentially taking one to two years for investors to gain access to the

information. These unique characteristics allow me to include every type of internal and external health-related data breach, cleanly match them to issuer- and hospital-level data, and test the role of information asymmetry in the pricing of data breaches (Amir et al., 2018). If breaches lead to adverse financial or patient outcomes, then investors should price any associated risks into the cost of hospital financing and breached entities should have worse prospects than non-breached ones. However, any pricing effects may be delayed if relevant information takes time for investors to process or if investors do not understand the information.

My primary identification strategy exploits the staggered timing of 82 data breaches on U.S. hospitals and compares breached hospitals to non-breached hospitals within the same state and year. Because recent research suggests that staggered difference-in-differences specifications may suffer from biases arising from heterogeneous treatment effects over time, I employ a stacked difference-in-differences specification to overcome possible heterogeneity in my estimation of the average treatment effect on the treated over time (Baker et al., 2022). In contrast to studies of corporate data breaches, my sample of events includes the near universe of breaches of hospitals that either issue bonds or report their performance to the Centers for Medicare and Medicaid Services (CMS) (Kamiya et al. 2021). Furthermore, I find that the propensity for a hospital to be breached is not strongly correlated with observable characteristics that may influence the likelihood of a breach. Consequently, my identification strategy allows me to identify the impact of data breaches on hospital outcomes using over 80 quasi-natural experiments.

I begin my primary analysis by examining the relationship between data breaches and hospital financing costs and find that breached hospitals suffer higher costs on new issues. Specifically, breached hospitals face offer yields (spreads over maturity-matched after-tax Treasury rates) that are 39.1 (65.0) basis points (bps) higher after a breach. This represents a 12.0% (21.1%) increase in financing costs, over $2 million annually, after a data breach. The cyber risk premium is 50% greater than the effect of Medicaid expansion on rural hospital yields and twice as large as the effect of opioid abuse on general obligation bond yields (Corgnaggia et al., 2021; Gao et al., 2022). Timing tests further indicate that the bond costs of breached and non-breached issuers exhibit parallel trends before a breach, and the increase in financing costs is delayed until investors can determine the financial repercussions of a breach for the issuer. These results are robust to the inclusion of county-level control variables; alternative econometric and sample construction specifications, such as using the staggered difference-in-differences estimator proposed by Borusyak et al. (2023); coarsened exact matching on bond characteristics; and constructing the control

group with only non-breached hospitals in the same county as the breached hospital. My results suggest that the market prices cyber risk and the premium is economically significant.

Credit rating agencies appear to have the same reservations towards breached issuers as investors do. Credit rating agencies reduce the ratings of new offers by breached issues by about 2.5 notches post-breach. Given that the average bond rating in my sample is BBB on an S&P scale, a data breach would downgrade the average breached hospital's bond to BB+, from investment grade to non-investment grade, holding all else equal. Furthermore, the downgrades appear to be concentrated in the year of a breach announcement and the years after hospital performance data is released. This result is consistent with real-world rating downgrades post-breach and the practical emphasis that agencies place on the potential governance and cash flow implications of breaches (Mitchell, 2021; Muolo, 2022). As such, credit ratings appear to be one channel through which data breaches influence issuer financing costs.

The term structure of the hospital bond market reveals how investors think cyber risk may threaten hospital performance, but it is unclear if investors view cyber risk as more of a short-term or long-term risk. Whereas anecdotal and research evidence show the effects of breaches are concentrated in the near term, cybersecurity experts expect breaches to worsen over time and have lingering consequences for breached entities (Cavusoglu et al., 2004; Huang and Wang, 2021; Kamiya et al., 2021; Brooks, 2022; Crosignani et al., 2023; Osborne, 2023). Defining short-term bonds as those with maturities less than 3 years, long-term bonds as maturities greater than 10 years, and mid-term bonds with maturities between the other two, I find that investors require a premium for investing in breached bonds of all maturities relative to non-breached bonds, and the increase in the yield and spread curves for breached bonds is statistically flat across maturities. This pattern contrasts risks that exist in only one subset of bonds (i.e., climate risk) and suggests that investors are uncertain regarding the future economic prospects of breached hospitals and that any immediate effects of breaches may be as bad as the long-term consequences (Grigoris, 2020; Painter, 2022).

I next address the role of information asymmetry in the pricing of data breaches by considering the incremental effect of hacks on breached hospitals' financing costs. Although previous empirical findings show that the market should require the greatest premium for investing in hacked entities, some evidence suggests that the market does not respond any differently to hacks than it would other manifestations of cyber risk, especially if investors are not fully informed regarding cyber risk (e.g., Campbell et al., 2003; Hovav and D'Arcy, 2003; Cavusoglu et al., 2004; Kannan et al., 2007; Kvochko and Pant, 2015; Ablan et

al., 2016; Huang and Wang, 2021; Kamiya et al., 2021; Mayer et al., 2021; Florakis et al., 2023). My identification strategy and sample of data breaches provides the opportunity to uniquely contribute to this debate with a stacked triple-differences test and a sample of all types of data breaches that does not suffer from sample selection bias. Interestingly, I find that the market does not require an incremental premium for investing in hacked hospitals. Instead, the new models imply that breached issuers suffer new offer yields (tax-adjusted spreads) that are 66.9 bps (109.1 bps) higher after a breach. This updated estimate reflects a 20.0% (35.4%) increase in new offer yields (tax-adjusted spreads), relative to the mean, post-breach. I proceed to examine whether this unexpected result is potentially influenced by investor information regarding the relative importance of hacks and stakeholder attention to breaches.

To do so, I first consider breaches' effect on hospital health as an additional channel through which they influence yields. If data breaches are costly events for hospitals, then they should be adversely associated with cash flow generating activity and balance sheet performance. Furthermore, hacked hospitals should have the worst outcomes if hacks are truly the worst events (Campbell et al., 2003; Kamiya et al., 2021). Using a triple-differences empirical design, I find that hacks are, indeed, the worst type of breach for a hospital. Hacked hospitals suffer a 6% loss in total patient revenue after a data breach, driven by a 10% (5%) decrease in inpatient (outpatient) revenue. Interestingly, data breaches are not associated with any adverse changes in breached hospital balance sheet accounts, but hospitals increase their amount of fixed equipment by 14% following breaches, consistent with prior evidence that breached hospitals increase their information technology (IT) spending in the period afterwards (Choi et al., 2020). However, I do not find that breaches are associated with any average decrease in cash flow. These findings contrast my market-based results that show investors care only about the occurrence of any breach but not incrementally about hacks. One possible reason investors may not require any incremental premium for hacks is because municipal bond investors, primarily retail investors, are limited in their information towards the nuances of cyber risk and apply equal weights to all events reported under HIPAA (Ablan et al., 2016; Mayer et al., 2021; MSRB, 2022). Alternatively, investors may be responding to changes in patient outcomes, which could ultimately manifest in worse hospital outcomes if providers prolong periods of lesser care.

Following Jencks et al. (2009) and Aghamolla et al. (2023), I use hospital-level data on 30-day patient readmission rates and patient surveys regarding their perception of care to examine if investors require higher yields due to worsened patient outcomes. Conditional on admission to a breached hospital,

patients receive the same quality of care they would expect to receive at a non-breached hospital, and patient care improves at breached hospitals. I theorize that the improvement in treated hospital care comes at the cost of neighboring hospitals' ability to care of patients who substitute away from breached hospital services. To test this theory, I use a control group that is comprised of only hospitals in the same county as the breached hospital and find that breached hospitals have lower readmission rates across every category than their counterfactuals, except after hacks. As further evidence, I show that non-breached (breached) *admission* rates for the conditions increase (decrease) post-breach. Patients choose to substitute breached medical services for those at non-breached hospitals, which hurts neighboring hospitals' quality of care. These results are consistent with a case study of the 2021 Scripps Health ransomware breach that shows patients substituted breached emergency medical services with those of non-breached hospitals in the surrounding area (Dameff et al., 2023). As such, investors' bond market response to breaches is unlikely a response to changes in care and more likely driven by the final factor I consider.

Lastly, I identify the role that investor and patient attention to news plays in mitigating information asymmetry surrounding hospital data breaches. Motivated by Da et al. (2011), I use Google Trends search volume index (SVI) of news articles that include the phrase "data breach" to proxy for attention around hospital data breaches. I collect SVI on news articles to better account for both the release of information related to cyber risk and potential stakeholder attention to data breaches. I repeat both my main financing test and the test of hospital cash flow generating activity and find that hospital financing costs increase, and hospital revenues decrease, as attention to breaches increases. In other words, when stakeholder attention to data breaches increases, the market's cyber risk premium begins to better reflect how patients and hospital revenues respond to data breaches. Although investors are likely ignorant to the differences in types of breaches, investor inattention also seems to play a major role in the mispricing of hacks.

My paper makes several contributions to the literature. First, it adds to a recent literature on hospital financing costs and, to the best of my knowledge, is the first to discuss the financial and real implications of cyber risk for hospitals (e.g., Cornaggia et al., 2021; Cornaggia et al., 2022; Gao et al., 2022; Aghamolla et al., 2023). I show that data breaches are associated with increased financing costs, large losses in hospital revenue, credit downgrades, and worsened patient outcomes for nearby hospitals. As such, my results have managerial and policy implications for municipalities. Hospitals would likely benefit from incorporating

stronger data protection policies, such as keeping an offline backup of their systems, improving employee data practices, or retaining executives and directors with cyber risk experience.

Relatedly, my paper also contributes to a recent literature on the repercussions of cyber risk for the stakeholders of targets (e.g., Ashraf, 2022; Crosigniani, 2023; Osborne, 2023). Although I do not show that breaches have an impact on the patients of breached hospitals, I provide evidence that patients substitute the services of breached hospitals for those of non-breached hospitals, ultimately harming the substituted hospitals. Similar to the effect observed in Dameoff et al.'s (2023) case study, hospital breaches seem to have a net negative effect on society by harming other hospitals' abilities to provide appropriate care.

Lastly, my study adds to the broad literature on the relevance of mandatory disclosures (e.g., Griffin, 2003; Lerman and Livnat, 2010; Christensen et al., 2017; Noh et al., 2019; Cabezon, 2023). Because of my paper's unique setting, I am able to test how markets incrementally respond to hacks over other types of breaches when clear, federally regulated information about the events is produced quickly by targets who cannot indefinitely delay their reports (Campbell et al., 2003; Amir et al., 2018; Kamiya et al., 2021). My study produces two novel findings. First, hacks, on average, are not incrementally priced in the municipal bond market. Second, this mispricing is likely due to a combination of investor information regarding the relative importance of hacks and investor inattention.

The rest of my paper proceeds as follows. Section 2 describes HIPAA's notification laws and my data, and Section 3 outlines my identification strategy and results. Section 4 provides robustness tests. Section 5 concludes and highlights policy recommendations for government data security.

2. Data and Summary Statistics

2.1. HIPAA Notification Requirements

Passed in 1996, HIPAA is a broad-reaching federal regulation that was designed to modernize how the healthcare industry approaches medical information in a modern age. Although the act addresses a plethora of closely related subjects, such as health insurance and medical savings accounts, HIPAA is now largely synonymous with a patient's right to privacy regarding his or her medical history. Many organizations and providers, from individual doctors to insurance companies, in the healthcare industry are covered by HIPAA and must stringently protect patients' protected health information (PHI). Specifically, PHI is anything in a patient's medical record that (1) was recorded during the provision of a medical service

or created during the course of medical research and (2) an external party can use to identify a patient. Regarding the latter, the act explicitly defines 18 categories of identifiers that must be present with health-related information in order for any information to be protected under HIPAA.[1] The U.S. Department of Health and Human Services (HHS) enforces HIPAA and can assign both criminal and civil penalties to those who violate a patient's rights. Penalties for violating HIPAA vary with both the intent behind a breach and the severity of a breach, potentially resulting in up to 10 years in prison, a $1.5 million dollar fine, or a provider's exclusion from participating in Medicare.[2]

HIPAA introduced guidance regarding data breach notifications in April 2009, codified its data breach notification rule (45 CFR §§ 164.400-414) in August 2009, and began to enforce the rule in September 2009. Under the notification rule, a covered entity is to assume that the use or disclosure of PHI is a breach if the security or privacy of the information is compromised unless the entity is able to demonstrate that there is a low probability the PHI was actually compromised. Covered entities may use at least four factors to determine if a breach compromised the integrity of PHI, including: the extent of PHI involved, the identity of the unauthorized person who accessed PHI, whether the unauthorized person actually acquired or viewed PHI, and the extent to which the covered entity has mitigated the risk of a breach of PHI.[3] If a covered entity finds that a data breach of PHI has occurred, then the entity must notify several parties of the breach in a timely manner. The breached entity is required to notify the affected individuals via written notice sent by physical mail or email (if the victims have previously agreed to receive electronic communications) no later than 60 days following the entity's discovery of the breach. HIPAA requires the notifications to include details describing the breach, the types of information revealed in the

[1] These 18 identifiers include names, addresses, ages and dates, phone numbers, fax numbers, email addresses, Social Security Numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate numbers, vehicle identification numbers and license plate numbers, device identifiers and serial numbers, website URLs, IP addresses, biometric identifiers, full-face photos, and any other unique identifier or code that can identify the person to whom a medical record refers. De-identified medical data, by definition, is not considered PHI.

[2] There are numerous resources that describe HIPAA, PHI, and the penalties associated with violations in deeper detail. However, for a brief primer on the regulation, see the CDC's "Health Insurance Portability and Accountability Act of 1996 (HIPAA)", U.C. Berkeley's "HIPAA PHI: Definition of PHI and List of 18 Identifiers", and the AMA's "HIPAA Violations & Enforcement" online articles. Note that the 2009 data breach notification law is different from the 2003 Security Rule, which established standards to protect electronic PHI. See "The Security Rule", U.S. Department of Health and Human Services, and the Code of Federal Regulations 45, Parts 160 and 164.

[3] There are three exceptions to what HIPAA considers a breach. First, there is no breach if a member acting under the authority of a covered entity unintentionally acquires, accesses, or uses PHI in good faith or within the scope of authority. Second, there is no breach if a member of a covered entity inadvertently discloses PHI to another member of the same covered entity (or associated entity) who is also authorized to access PHI. Lastly, there is no breach if a covered entity has a good faith belief that an unauthorized individual who accessed PHI is unable to retain the PHI.

breach, the steps affected individuals should take to protect themselves from harm, what the covered entity is doing to investigate the breach and mitigate the potential harm arising from the event, what the covered entity is doing to prevent further breaches, and contact information for the covered entity. If the covered entity does not have sufficient or up-to-date information for at least 10 individuals, the entity must post an equivalent notice on its website's homepage for 90 days or in print at a newspaper or over broadcast media where the individuals are likely to reside. Covered entities must also notify the Secretary of HHS through a standardized online form (OMB 0945-0001), which will then post information about the breach on HHS's website.[4] If a breach involves the loss of 500 or more individuals' records, covered entities must additionally notify "prominent" media outlets via press releases or other means of mass communication, and HHS will conduct further investigation into the breach.[5]

HIPAA's PHI breach notification law is, arguably, the most stringent data breach notification law in the United States because of its strict notification requirements. Although the majority of states passed their own data breach notification laws by 2009, states may differ in both what they consider a breach and how they require breached entities to respond. As such, many corporations have significant leeway in choosing what and when to disclose about their data breaches under state regulations. Furthermore, the U.S. Securities and Exchange Commission, despite issuing guidance regarding the disclosure of cybersecurity risk in 2011, did not officially adopt any requirements for publicly traded companies to disclose events until 2023. The ambiguity surrounding data breach notification laws for non-PHI has allowed firms to either avoid notifying stakeholders of breaches, time their notifications in such a way as to minimize the disruption caused by the breaches, or even trade on inside information regarding breaches while the firm waits to disclose information (Amir et al., 2018; Lin et al., 2020; Kamiya et al., 2021). However, breaches of PHI are not afforded such opportunities because of HIPAA's notification requirements. Any covered entity located anywhere in the United States who experiences a breach of PHI must follow HIPAA's notification requirements or be severely punished by HHS.

As is standard in the cyber risk literature, I use the Privacy Rights Clearinghouse (PRC) dataset to collect my sample of breaches (Huang and Wang, 2021; Kamiya et al., 2021; Florakis et al., 2023). As

[4] Covered entities may report breaches to the Secretary of HHS involving less than 500 patients' records on an annual basis but are still required to notify the individuals within 60 days of discovery. Breaches involving 500 or more records must be reported to the Secretary within 60 days of discovery.

[5] See "Breach Notification Rule", U.S. Department of Health and Human Services, and the Code of Federal Regulations 74 FR 42767.

described in prior literature, PRC collects information on data breaches that are publicly disclosed through government agencies, including HHS. I begin by identifying breached medical providers.[6] However, I do not subset my events to include just entities that were hacked or events that involved malicious external actors, as Kamiya et al (2021) propose, because of HIPAA's 2009 data breach notification requirements. Restricting my sample to include medical events in and after 2009 ensures that my sample does not suffer from selection bias because I employ the near universe of mandatorily reported medical breaches.

2.2. Bonds and Hospitals

I use data from additional sources throughout my analysis. First, I collect municipal healthcare bonds from Mergent for the period 2006 to 2022.[7] In addition to bond *Yield*, I additionally proxy for the risk premiums investors demand for investing in municipal bonds with after-tax spreads over Treasuries (Cornaggia et al., 2022). I first compute a bond's spread as the difference between municipal bond yields and maturity-matched Treasury bond yields, using linear interpolation of Treasury yields when an exact match is unavailable. Then, I compute *Adjusted Spread* as the after-tax spread over Treasuries by using the highest marginal tax rates for a given year.[8] Following Aghamolla et al. (2023), I further collect hospital performance data from various CMS programs. Additionally, I obtain patients' 30-day readmission rates from the Health Care Reporting Information Systems (HCRIS) and patient satisfaction surveys come from the Hospital Consumer Assessment of Healthcare Providers and Systems (HCAHPS) over 2015 to 2022. Hospital financial and balance sheet data come from Care Compare over the period 2011 to 2019. Note that Care Compare is updated with a significant delay, sometimes taking up to two years to reflect a hospital's financials.[9] I discuss this unique attribute of Care Compare's data and exploit it in my analysis later.

I further restrict my sample of breaches to those that I can match to the issuers of municipal health-related bonds or hospital performance data. To identify "breached" bonds, I match the names of breached medical providers in the dataset to the names of every bond issuer in the same state and assign a variable *Breach* that equals one to each bond associated with a matched issuer.[10] Because medical data breaches are

[6] The PRC database identifies all breached healthcare entities with the *Type of Organization* flag "MED".
[7] I assume healthcare-related bonds are those with use of proceeds codes "OHCA", "HOEQ", "HOSP", and "NURS".
[8] State tax rates come from https://www.taxpolicycenter.org/statistics/historical-highest-marginal-income-tax-rates.
[9] See https://data.cms.gov/provider-data/topics/hospitals/measures-and-current-data-collection-periods.
[10] There is large variation in the names provided by Mergent. To standardize the list of potential names and aid in matching across datasets, I match each name Mergent provides to each other name associated with the same 5-digit

reported in a standardized manner, matching medical breaches to breached hospital outcomes is much simpler and cleaner than in studies of corporate data breaches. I identify exact matches between the hospitals in the PRC and CMS datasets and, similarly, assign a *Breach* value of 1 to all hospitals in which I can find a match. Control observations are all non-breached bonds and non-breached hospitals in the same state as a breached entity, and I assign all such observations a *Breach* value of 0. These restrictions provide a total of 82 unique breaches. Nineteen are matched to bond issuers, and 63 are matched to hospitals from CMS. For my analyses, I keep all rated bonds issued and all hospital observations within a seven-year window around a breach (i.e., three years before and three years after).

Lastly, I collect county-level data from two sources. First, I hand-collect each issuer's location through an iterative process because Mergent does not include the county location of issuers. I gather an issuer's county either from searching MSRB's Electronic Municipal Market Access (EMMA) system, scraping it directly from the name of the issuer, or searching for the name of the project through online search engines. If I cannot identify an issuer's county through any of the aforementioned steps, I assume that an issuer is located in the state capital and its county is the primary county in which the capital is located. Second, I collect county characteristics, *Population*, *Employment*, and *Per Capita Income*, from the Bureau of Economic Analysis. I match the economic data to bond issuers on county name, state name, and year but use lagged county characteristics in my analysis to avoid possibly endogenous controls.

2.3. Descriptive Statistics and Determinants of Breaches

Table 1 presents summary statistics for the main variables in this study. Panels A, B, C, and D present statistics related to my overall sample of bonds, hospital financials, patient 30-day readmission rates, and patient experience surveys, respectively. Table A1 in the appendix describes variable definitions.

CUSIP number. I use 5-digit CUSIP instead of 6-digit CUSIP to broaden my matches across issuers that are clearly related but received different CUSIP numbers in the application process. For example, the issuers "MONTGOMERY ALA MED CLINIC BRD 1976 EAST HEALTHCARE FAC REV" and "MONTGOMERY ALA MED CLINIC BRD HEALTH CARE FAC REV" have the 6-digit CUSIPS 61305R and 613058, respectively. Matching names based on the 6-digit CUSIP could cause me to assign treatment status to one set of bonds but not the other, although the issuers are clearly the same entity. However, matching on the 5-digit CUSIP 61305 avoids this mis-assignment problem. Furthermore, I assume that each alternative spelling of a name associated with the same 5- or 6-digit CUSIP belongs to the same underlying issuer. Additionally, Mergent sometimes lists cities and counties as the issuers of medical bonds instead of the name of the associated project. Consequently, using only names of breached medical providers would cause me to exclude valuable variation if one of these unnamed providers was breached. As such, I further include the sample of county and city events of Osborne (2023) to identify more issuers of breached medical bonds, but my main results are robust to their exclusion.

I winsorize all continuous variables at the 1st and 99th percentiles. My total sample includes 11,987 healthcare bonds, about 65k hospital-years of financial data, and about 10k hospital years of patient data. Breached hospitals issue about 7.8% of the healthcare bonds. The average bond in my sample has an initial offer yield of 3.3%, matures a little past 12 years after issuance, and provides a hospital $8.83 million in funding. The median total issue size is about $75.8 million. About 17% of bonds are funded via counties' general obligations, but the majority (83%) are funded via hospital revenues. The average bond is rated about BBB. Overall, my sample of hospital bonds largely reflects the samples of Corgnaggia et al. (2022) and Gao et al. (2022); and my sample of hospital and patient data is similar to Aghamolla et al. (2023).

I preface my primary analysis by examining the determinants of hospital data breaches in Table 2. I use a linear probability model to estimate the likelihood that a hospital is breached in any given year by conditioning on several factors. I include several lagged, logged independent variables to capture observable characteristics that may influence the propensity a hospital is breached. For example, the variables *Total Revenue*, *Total Assets*, *Total Liabilities*, and *Cash Holdings* all measure a hospital's size, potentially available (i.e., stealable) funds, or ability to pay hackers' ransoms. They also capture a hospital's potential defenses and data security practices under the assumption that larger hospitals with better cash flow could have more resources to devote to stronger data practices. The variable *Full-Time Employees* captures how a hospital's labor force may influence a data breach. Lastly, the variable *Beds* is the number of beds a hospital has and proxies for both the size of a hospital and its potential reputation. Model 1 includes hospital and year fixed effects to control for unobserved time series factors, such as the macroeconomic environment, and cross-sectional factors, such as a hospital's culture towards technological progress that may influence a hospital's propensity to be breached. Model 2 replaces the hospital and year fixed effects with county-year fixed effects to account for any role a hospital's local economic environment could have on data breaches or employees' data security practices.

No one factor is a consistently strong predictor of hospital data breaches. In fact, the only variable with any association with data breaches is *Cash Holdings*, which positively predicts the events only in the model that controls for local economic conditions. According to Model 2, a 1% increase in a hospital's stored cash increases the likelihood of a data breach by 0.05%. No other factor, including hospital revenues or the number of employees, appears to be relevant for the likelihood that a hospital reports a breach to HIPAA. Overall, hospital data breaches appear to be randomly assigned, so I assume that data breaches are

exogenous shocks to hospitals for the purposes of my following analyses (e.g., Amir et al., 2018; Kamiya et al., 2021; Ashraf, 2022; Crosignani et al, 2023). Nonetheless, I choose to follow the municipal bond literature and control for a county's lagged population, per capita income, and employment in my bond analyses to account for how these characteristics may affect investors' responses to a breach (Cornaggia et al., 2018; Gustafson et al., 2023). Similarly, I follow Aghamolla et al. (2023) and control for a hospital's lagged total income, bed days, cash holdings, liabilities, and total patient revenue in my hospital analyses.

3. Empirical Strategy and Results

In this section, I examine how data breaches affect hospital financing costs and identify the channels through which the events influence investors. I also document the real effects of breaches.

3.1. Identification Strategy

My primary model is the following stacked difference-in-differences regression specification with three years of pre-breach and three years of post-breach data (i.e., a seven-year window):

$$y_{i,t} = \beta_1 Breach_i \times Post_t + \beta_2 Breach_i + \beta_3 Post_t + \gamma' Controls_{i,t} + \omega_{s,e} + \varphi_{t,e} + \varepsilon_{i,t}. \quad (1)$$

My primary dependent variables include *Yield* and *Adjusted Spread* for the municipal financing models. The coefficient β_1 estimates the impact of data breaches on hospital outcomes and is my coefficient of interest. *Breach* is an indicator that equals one if a bond is issued by a breached entity and zero otherwise. *Post* is an indicator that equals one if a bond is issued after a data breach. Following the municipal bond literature, I include several bond and county characteristics as controls. The continuous bond characteristics I include are a bond's coupon rate, maturity, inverse maturity, and corresponding maturity-matched Treasury yield (which is excluded from the *Adjusted Spread* model). I also control for whether an observation is a callable, negotiated, or general obligation bond with respective indicator variables. I also include the prior year's population, per capita income, and employment of the issuer's county to account for any potential differences between breach and non-breach counties and to control for factors that may affect an issuer's ability to repay its debts (Cornaggia et al., 2021; Cornaggia et al., 2022). I do not include a bond's rating in my primary analysis because it would be an endogenous control variable, as I hypothesize that credit risk is one of the channels through which data breaches influence the cost of capital.

I use a stacked difference-in-differences specification because standard staggered difference-in-differences models may be subject to biases arising from heterogenous treatment effects over time. In fact, estimates of the average treatment effect on the treated (ATT) produced via staggered difference-in-differences estimators may even have the opposite sign of the true treatment effect. I overcome this challenge by implementing the stacked difference-in-differences estimator (Cengiz et al., 2019). Following Baker et al. (2022), I structure my data in such a way to create an event-specific dataset for each treatment group and its clean control group to represent a singular "experiment" for each breach. Treated hospitals are those that experience a data breach, and treated bonds are any bonds issued by a breached hospital. Control hospitals are those that are never breached but are in the same state as the breached ones. Next, I "stack" all the breach-specific datasets together. Even though each event happens at a different time, the stacked dataset aligns all the breach-specific datasets together in event-time because I take a sample of bonds within a seven-year window of each event. As such, I essentially have 82 quasi-natural experiments from which to estimate the impact of data breaches on several hospital outcomes.[11]

Alongside the stacked difference-in-differences design, I include issuer-event ($\omega_{s,e}$) and year-event ($\varphi_{t,e}$) fixed effects in my primary model to further ensure my comparisons of treatment and control outcomes are within the same issuer-experiment and year-experiment. I choose to cluster standard errors at the issuer-level to account for residuals being correlated within a hospital over time.

My identification strategy exploits variation from multiple sources. First, it relies upon a clean shock to treatment group outcomes. With the inclusion of year fixed effects, my model differences out any unobserved cross-sectional factors that might affect both treatment and control groups simultaneously (Cornaggia et al., 2022). This first difference helps ensure that my estimate of the average treatment effect on the treated, β_1, is not biased by any omitted variables – such as a general macroeconomic conditions or annual trends in cyberattacks – that might be relevant to either group's outcomes post-breach. Furthermore, with the inclusion of issuer fixed effects, my model differences out any unobserved time-invariant hospital-specific factors, such as a hospital's governance structure or workplace culture towards data security, that may endogenously affect a hospital's financing. Used together, the fixed effects reveal how the cost of financing changes for breached entities after a data breach.

[11] Specifically, I have 19 events that I match to issuers in Mergent and 63 that I match to hospitals in CMS's databases. Although the number of data breach events is seemingly small, the numbers parallel studies that use changes in state-level laws that affect a large number of corporations in a limited number of states (Serfling, 2016).

Second, my identification strategy exploits the staggered nature of data breaches. Breaches affect hospitals between 2005 and 2016, allowing me to capture all relevant events over the sample period and mitigate concerns that a singular contemporaneous trend might confound the treatment assignment. Treatment hospitals enter my sample three years before they suffer a data breach and exit three years afterwards, so I observe both their pre- and post-breach financing costs. I assign the breach date of the treated hospital to all non-treated hospitals in the same state because control hospitals do not experience their own data breaches. This allows me to observe all pre- and post-breach outcomes for treated and control hospitals over the same seven-year window centered on the treated hospital's breach. Given that I choose plausible counterfactuals for treated hospitals and control for characteristics that are related to the issuers' ability to repay their debts, this difference-in-differences research design forms a quasi-natural experiment that allows me to uniquely identify the effect data breaches have on hospitals' cost of capital.

3.2. Impact of Breaches on Hospital Financing

I begin by quantifying how data breaches impact hospital financing costs using the dependent variables *Yield* and *Adjusted Spread* in Table 3. I find that financing costs increase for hospitals after a data breach. Model 1 shows that treated issuers' initial offer yields are 47.8 bps higher after a breach. With the inclusion of bond- and county-level controls in Model 2, I find that issuer yields increase 44.3 bps after a breach. Economically, this translates to a 14.2% increase in annual borrowing costs – about $2.75 million for the median issuer.[12] This result holds when using *Adjusted Spread* as the dependent variable as well. Model 4 shows that tax-adjusted spreads for medical bond issuers increase 74.9 bps (25.1%, relative to the mean value) after a breach. The cyber risk premium is 50% greater than the effect of Medicaid expansion on rural hospital yields and twice as large as the effect of opioid abuse on general obligation bond yields (Corgnaggia et al., 2021; Gao et al., 2022).

My identification strategy and interpretation of the stacked difference-in-differences estimator relies on the parallel trends and exogeneity assumptions of any standard difference-in-differences test. I first test the parallel trends assumption for each of my dependent variables with a dynamic analysis in Figure 1. Specifically, I replace *Post* in Eqn. (1) with six indicator variables to capture the subperiods surrounding the year of a breach and, following econometric tradition, use the year immediately before the

[12] I utilize the modified duration approach to calculate the increase in borrowing costs for breached issuers. $2.75 M = $75.8 M (median annual issuance) × 8.367 (median duration) × (0.0044/(1 + 0.0327/2)).

event as the reference period. Given that all of the coefficients for the pre-periods are statistically indifferent from zero, I find no evidence that treatment and control bonds follow different trends before a hospital is breached. The relationship between data breaches and financing costs exists solely after a breach. However, the post-event timing is especially interesting because it contrasts the more immediate timing of when cyberattacks impact corporate outcomes (e.g., Akey et al., 2021; Huang and Wang, 2021; Kamiya et al., 2021; Crosignani et al., 2023). Despite HIPAA requiring hospitals to report breaches within 60 days, the market takes about two years to positively adjust its risk premium for breached hospitals. Intriguingly, the market's delay roughly corresponds to how long hospitals may take to fully report their financial and operational data to CMS (i.e., one-and-a-half to two years). Such a delay implies that there is significant information asymmetry between issuers and investors in the period immediately after a breach, and investors seem to not respond to the average breach until after they can gauge its financial implications.[13] I explore the potential roles of information asymmetry surrounding hospital outcomes in later tests.

Additionally, endogeneity is unlikely to be a major concern for my use of the stacked difference-in-differences estimator. First, breaches are always unexpected shocks and, many times, undefendable events for even the largest, best-equipped corporations (Kamiya et al., 2021; Crosignani et al., 2023). It is unreasonable to assume that hospitals, who are less prepared for data breaches with their security resources, or their investors, would be in a better position to respond to breaches before an announcement than corporations. Second, there is no reason for the municipal bond market to price a treated hospital's bonds as if a breach already occurred before the issuer notifies the public of the breach, especially because breached entities have incentive to conceal details until they are legally obligated to report them (Amir et al., 2018). Lastly, although I cannot deny that some events are potentially nonrandom, I previously show in Table 2 that there is no consistently strong predictor of hospital data breaches, including cash-flow-related

[13] One could argue that the market's delayed response is rather the result of delayed data breach notifications by CMS. Theoretically, investors may not receive information about a breach less than a year after the event if (1) the breach affects less than 500 individuals, (2) they themselves are not affected by the breach, and (3) neither the breached party nor the affected individuals notify the broader public or a news source. If all three of the conditions are met, then investors could have no information about potential data breaches until one year has past (i.e., the maximum time a breached hospital has to report an event). Combined with delayed reporting of financial data, investors would still have no picture of how a breach influenced hospital health until one to two years after a breach. However, this scenario does not explain the pattern exhibited in Figure 1. In untabulated tests, I examine whether breaches that affect more than 500 records exhibit the same timing as breaches that affect less than 500 records because markets should respond more quickly to information about the former group, given HIPAA's reporting requirements. I find that investors quickly respond to breaches that affect less than 500 records, suggesting that they do not have to wait long to incorporate new information about the breaches or for CMS to disseminate information about the breach.

variables and hospital size. It is likely safe to assume that hospital data breaches are the random result of either hackers succeeding in breaching a target's defenses or employees failing to practice proper data protection protocols. Nonetheless, my models control for a handful of characteristics that may be theoretically associated with the propensity an event may occur, thereby reducing the influence of any potentially observable or unobservable confounding factors. As such, β_1 is the difference-in-differences estimator and may be interpreted as the average treatment effect on the treated.

3.2. Connection between Breaches and Increased Costs

Both cybersecurity experts and the finance literature suggest that data breaches can affect victims by increasing their exposure to certain types of risk, and this subsection aims to identify the channels that link data breaches to increased bond premiums (e.g., Campbell et al., 2003; Tanimura and Wehrly, 2015; Amir et al., 2018; Akey et al., 2021; Huang and Wang, 2021; Kamiya et al., 2021; Ashraf, 2022). In doing so, I present evidence that investors are not fully informed in their pricing decisions.

3.2.1. Credit Risk and the Term Structure of Cyber Risk

The connection between issuer credit risk and data breaches is straightforward theoretically. Data breaches could increase issuers' credit risk if the events hinder hospitals from promptly repaying their debts. If there is an association between data breaches and credit risk, then breached issuers should have lower credit ratings on new bond issues after their first data breach, relative to non-breached issuers (Kamiya et al., 2021). To test this hypothesis, I conduct a timing test of bond ratings (*Max Rating*) in the same stacked difference-in-differences framework and present the results of my rating timing analysis in Figure 2.

Data breaches are associated with significant bond ratings cuts. Although treated hospitals have higher ratings than control hospitals before a breach, I find that credit rating agencies reduce the ratings of new issues by breached issuers by about 2.5 notches post-breach. Furthermore, the rating reduction is constant for the duration of the post-period. Given that the average bond rating in my sample is BBB on an S&P scale, a data breach would downgrade the average hospital's bond to BB+, holding all else equal. In other words, the average hospital with investment-grade bonds should expect to see its bonds drop to non-investment grade after a data breach. Interestingly, the statistical significance of the post-period downgrade appears to be concentrated in the year of a breach announcement and the years after hospital performance data is released (i.e., years 2+). This result is consistent with the magnitude of real-world rating downgrades

post-breach and anecdotal evidence that rating agencies emphasize the potential governance and cash flow implications of hospital data breaches (Mitchell, 2021; Muolo, 2022). As such, credit ratings appear to be one channel through which data breaches influence issuer financing costs.

Furthermore, the term structure of the hospital bond market reveals whether investors view cyber risk as more of a short-term or a long-term risk for hospital performance. If investors believe that hospitals will suffer more in the short-term but eventually recover, then they should require greater premiums for short-term bonds than they do bonds of longer maturities. The same is true for their reservations of long-term risk, as well. However, empirical research and anecdotal evidence are unclear regarding the nature of cyber risk. On one hand, there is evidence that most Internet users are not prepared for an immediate breach and the effects are concentrated in the near term (Cavusoglu et al., 2004; Kamiya et al., 2021). On the other hand, cybersecurity experts expect data breaches to worsen over time, and some research shows that breaches have lingering consequences for victims (Huang and Wang, 2021; Brooks, 2022; Crosignani et al., 2023; Osborne, 2023). The hospital bond market provides a unique setting to contribute to this debate by providing an opportunity to evaluate how significant information asymmetry of underlying issuer health affects investor expectations of cyber risk over different time horizons.

Defining short-term bonds as those with maturities less than 3 years, long-term bonds as maturities greater than 10 years (*Long-Term*), and mid-term bonds with maturities between the other two (*Mid-Term*), I employ another stacked triple difference-in-differences style test to evaluate the term structure of treated hospital bonds. I separately interact two additional indicators for mid-term and long-term bonds with *Breach×Post*. The first additional triple interaction is *Breach×Post×Mid-Term*, and the second is *Breach×Post×Long-Term*. Because I include the term *Breach×Post*, each of the respective pairings associated with all the interaction terms, and the level effects, I can interpret the coefficients associated with both of the triple interactions as the additional premium required for investing in bonds of the associated maturity bin over short-term bonds. I present the term structure estimation in Table 4 for my main two dependent variables of interest using the same control variables from prior models.

Investors require a premium for bonds of all maturities, as indicated by the coefficients on *Breach×Post* in Models 1 and 2 (0.414 bps and 0.703 bps, respectively). However, neither coefficient associated with the triple interaction terms is statistically significant, implying that investors do not differentiate between short-, mid-, or long-term bonds.

To validate this finding, I plot the term structure of treated hospital bonds in Figure 3. To do so, I subset the data on all bonds issued after a breach occurs, interact the variable *Breach* with a set of yearly timing variables that indicate when a bond matures, and include the same controls as before. The breached hospitals' yield and tax-adjusted spread curves show that the premiums for breached bonds are significantly different than the premiums of non-breached bonds across most maturities, but both curves appear relatively flat across maturities. Sixteen (out of 19) of the coefficients for *Yield* indicate a premium between 0.25 and 0.50 bps over control bonds with a similar maturity, and the same pattern exists for the *Adjusted Spread* curve. Investors do not seem to be concerned about how cyber risk will influence issuers within a certain horizon, contrasting risks that exist in only one subset of bonds, such as climate risk (Painter, 2022).

The interpretation underlying these results is intuitive. This pattern suggests that investors are uncertain regarding the future economic prospects of breached hospitals and that the immediate aftermath of a breach may be as bad as its long-term consequences (Grigoris, 2020). Stated differently, investors weigh the immediate repercussions of a breach with as much importance as they do the longer-term effects of the breach, but there is too much uncertainty to know when the effects will culminate. The results also imply that investors do not believe hospital cyber defense will ever completely mitigate cyber risk, a thought consistent with those of cybersecurity professionals.[14]

It is easy to reconcile such a response of uncertainty. First, history shows that victims of data breaches take time to respond to the events. Whereas some companies emerge seemingly unscathed immediately after a breach, others take years.[15] Because there is so much uncertainty regarding how and when the consequences will manifest, investors discount all such probable outcomes into the bonds of all maturities. Secondly, investors may not be not fully informed about hospital data breaches and simply treat all breaches the same (i.e., information asymmetry exists). In this scenario, investors will still purchase the treated hospital bonds at a discount because they recognize that a potential threat to cash flows has occurred, but they will not discriminate based on the details of a breach (Ablan et al., 2016; Mayer et al., 2021).

[14] See "Three Reasons Why the Cybersecurity Industry May Never Catch up to Cybercrime," *Forbes*, August 31, 2017.

[15] For example, Target took almost five years to pay the final financial loss from litigation related to its 2013 data breach. See "Target to Pay $18.5 Million to 47 States in Security Breach Settlement", *New York Times*, May 23, 2017.

3.2.2. Hacks and the Role of Information Asymmetry

I begin to address the role of information asymmetry in the pricing of data breaches by considering the incremental effect of hacks on breached hospitals' financing costs. Ex ante, it is unclear theoretically whether the hospital bond market should require a larger premium for hacked issuers. On one hand, there are numerous empirical findings that suggest hacks are the worst type of realized cyber risk because they are associated with greater financial losses than other realizations of cyber risk and are, arguably, more likely to be covered in the news because of the reputational damage they cause (e.g., Campbell et al., 2003; Hovav and D'Arcy, 2003; Cavusoglu et al., 2004; Huang and Wang, 2021; Kamiya et al., 2021; Florakis et al., 2023). If investors incorporate all relevant information about breaches into financing costs, then they should require an additional premium for investing in the bonds of hacked issuers.[16] As alluded to before, though, some evidence suggests that the market may not respond differently to hacks than it would other breaches. If investors do not have cyber risk expertise, understand that different types of breaches have varying levels of repercussions, or just not pay attention to news, then they may not respond incrementally to hacks (e.g., Kannan et al., 2007; Kvochko and Pant, 2015; Ablan et al., 2016; Mayer et al., 2021).

My identification strategy and sample of data breaches provides the opportunity to uniquely contribute to this debate with a stacked triple-differences test and a sample of all types of data breaches that does not suffer from sample selection bias. The stacked triple-differences test builds upon Eqn. (1) by interacting an additional variable *Hack*, an indicator that equals one for events that are reported as hacks by external parties and zero otherwise, and the existing interaction terms. I include each of the level terms and their interaction pairs to interpret the coefficient on the triple interaction as the difference-in-difference-in-differences estimator and present the results of the stacked triple-differences test in Table 4.

Contrary to expectations, the coefficient on the triple-differences estimator is not statistically significant in any model, implying that investors do not require incrementally larger premiums after hacks. Instead, the coefficient on *Breach*×*Post* increases in economic magnitude and statistical significance across each model. Models 2 and 4 now imply that hospitals' initial offer yields (tax-adjusted spreads) increase 66.9 (109.1) bps after a breach. Relative to the mean values, the updated estimates reflect a 20.0% (35.4%) increase in yields (tax-adjusted spreads) post-breach. Yet, the insignificant triple-differences coefficient

[16] It is important to note that breached medical providers detail whether they are hacked by an external party in their required reports.

may indicate an appropriate response from investors if information indicates that hospital fundamentals are not affected after a hack. I explore two reasons, information about hospital health and investor attention, behind the insignificant relation between financing costs and hacks in later tests.

3.2.3. Hospital Health: Cash Flow Risk

Next, I examine the connection between data breaches and hospital health. The first aspect of hospital health I consider is hospital cash flows. If data breaches are costly events for hospitals, then they should be associated with losses in revenue, increases in liabilities, or selloffs of assets; and the worst outcomes should be reserved for hacked hospitals (Campbell et al., 2003; Kamiya et al., 2021).

I utilize a stacked triple-differences methodology where my triple interaction is between the independent variables *Breach*, *Post*, and *Hack* to test the relation between hospital cash flows and data breaches. Because this is a hospital-level test, my dependent variables of interest are now (total) *Patient Revenue*, *Outpatient Revenue*, *Inpatient Revenue*, and *Bed Utilization*; and each dependent variable is transformed by the natural logarithm of one plus the underlying data. I follow Aghamolla et al. (2023) and include the lagged hospital-level variables *log Hospital Income*, *log Bed Days*, *Cash Holdings*, *log Liabilities*, and *Total Patient Revenue* as controls. These control variables should mitigate the effect that characteristics like hospital size, access to funding, or cash levels might have on the *Breach* treatment effect. Furthermore, I include data breaches only between the years of 2015 and 2017, due to data constraints from CMS, to ensure that I have a full three years of pre- and post-breach outcomes and hospital-event and year-event fixed effects to parallel my bond-level tests (Baker et al., 2023). I present the results of my first test of hospital health post-breach in Panel A of Table 6.

Hacks are, indeed, the worst type of breach for a hospital to experience. Hacked hospitals suffer a 6% loss in total patient revenue after a data breach, and this effect is primarily driven by a 10% (5%) decrease in inpatient (outpatient) revenue. Additionally, hacked hospitals see a 2.3% decrease in their bed utilization rates post-breach, implying these hospitals generate less revenue on inpatient services and use fewer beds post-breach. Interestingly, I do not find that non-hack data breaches are associated with any average decrease in cash flow. These findings are directly opposite those of the bond-level tests that show investors care about the presence of any type of data breach but do not incrementally price the presence of a hack. There is a connection between data breaches and hospital cash flow risk, but the effect exists only in the subset of treated hospitals for which the market does not require incremental premiums. If bond prices

reflect the discounted future cash flows of affected hospitals, it would seem that what investors think will happen does not fully reflect what actually does.

Why might investors not require an incremental premium for investing in bonds issued by a hacked hospital when only hacks threaten hospital cash flows? Investors may be limited in their information regarding the differences between hacks and non-hacks. Municipal bond investors, primarily retail investors, are likely uninformed regarding the nuances of cyber risk and apply equal weight to any cyber event reported under HIPAA (Ablan et al., 2016; Mayer et al., 2021; MSRB, 2022). Alternatively, investors may be responding to changes in patient outcomes, which could adversely affect future hospital cash flows if providers prolong periods of lesser care. The evidence thus far points more towards the former explanation, but I rule out the alternative in later tests that examine patient outcomes.

3.2.4. Hospital Health: Fundamental Risk

The second aspect of hospital health that I consider is the balance sheet (i.e., fundamental risk). If breaches increase fundamental risk, then treated hospitals should present with symptoms of corporate failure after a breach. Following Aghamolla et al. (2023), my dependent variables that measure hospital health are (total) *Assets*, *Liabilities*, *Cash*, and *Fixed Equipment*. Each dependent variable is scaled by the hospital's lagged *Total Revenue* and transformed by the natural logarithm of one plus the underlying data. I employ another stacked triple-differences methodology and present the results in Panel B of Table 6.

As with the cash flow-related tests, non-hacks are not associated with any adverse average changes in hospital balance sheets. Hacks are associated with decreases in hospital assets, but the relationship is statistically insignificant. Instead, hospitals increase their fixed equipment by 14% after any type of breach. This increase is consistent with prior evidence that breached hospitals increase their IT spending after a data breach to improve security (Choi et al., 2020). Although there is evidence that hacks negatively impact hospital cash flows, data breaches, on average, do not appear to harm hospital balance sheets.

3.3. Data Breaches and Patient Outcomes

I next examine whether investors require premiums for breached hospital bonds because of how data breaches affect patient care. Hypothetically, if data breaches adversely impact patient care, then patients should provide negative reports about their care and have worse outcomes than the patients of non-breached providers. The worst outcomes should be reserved for hospitals that are hacked. To test these

hypotheses, I utilize a similar triple-differences framework with the same hospital-level controls as before. I include hospital-event and year-event fixed effects to parallel my bond-level tests (Baker et al., 2023). However, I must further restrict my sample of data breaches to include only those between the years of 2017 and 2018, due to data constraints from CMS's patient survey data, to ensure that I have a balanced panel of pre- and post-breach outcomes.

Like Aghamolla et al. (2023), I measure the patient care experience by first using patient survey data with seven proxies. The seven dependent variables I use are *Recommend "Yes"*, *Room Always Clean*, *Doc Comm Always Clear*, *Nurse Comm Always Clear*, *Recovery Info Always Clear*, *Room Always Quiet*, and *Rate "9-10"*. The variables are the percentage of patients who positively affirm their hospital's level of care in each of the respective categories. I present the results of my analysis of survey results in Table 7. I find that there is no association between data breaches and how patients rate their hospital care experience. Patients of treated hospitals report no differences in their quality of care across any dimension post-breach than patients of the same hospital before a breach.

However, patient survey data can be skewed by a plethora of unmeasurable factors. To mediate this concern and address whether patient care changes post-breach, I employ additional data from CMS that measures 30-day readmission rates for four of the most frequent ailments of emergency department patients. The diagnoses include pneumonia (*PN*), heart failure (*HF*), heart attack (acute myocardial infarction, *AMI*), and chronic obstructive pulmonary disease (*COPD*). If hospitals' level of care suffers because of breaches, then their readmission rates should increase, indicating that care providers were unable to properly treat the underlying ailment during a patient's first visit (Jencks et al., 2009). Following Aghamolla et al. (2023), I examine both the level and log-transformed hospital readmission rates in Table 8.

Panel A of Table 8 presents results based on my main sample specification with the control hospitals being all non-breached hospitals in the same state as a breached entity. I find exactly the opposite effect of what would be expected if data breaches adversely affect patient care. In fact, treated hospitals' readmission rates for heart failure and COPD patients decrease by 11.6% and 15.9%, respectively, after a breach. Under the traditional interpretation of these results, it would seem that data breaches actually improve patient care; but that initially seems implausible given that I previously find patients of treated hospitals report no statistically meaningful change in care post-breach. However, the quality of breached hospitals' services

could improve relative to those of non-breached hospitals if future patients choose to substitute away from the services of the breached providers, thereby increasing the provider-to-patient ratio.

I formally test my substitution hypothesis in Panel B of Table 8 where I restrict the control hospitals to include only non-breached hospitals in the same county as a breached hospital. Anecdotes suggest that readmission rates for competing hospitals should increase when a sudden substitution of healthcare services occurs (Burky, 2023). As such, the negative effect on treated hospitals' readmission rates should be even greater when treated hospitals are compared to their close competitors. I find that the 30-day readmission rates for pneumonia, heart attacks, and COPD decrease on average 14.4%, 30.2, and 29.2% after a data breach, respectively. Additionally, hacked hospitals experience economically meaningful increases in their readmissions for each condition when compared to the outcomes of non-breached hospitals within the same county, implying that hacks lead to subpar qualities of care.

To further validate the substitution hypothesis, I compare the total number of patients *admitted* by treated and neighboring control hospitals for each condition in the years around a breach in Figure 4. Leading up to the data breach, treated hospitals serve a larger number of patients for each condition, on average, than control hospitals. However, there is a large drop in the number of patients that treated hospitals admit in the period after a breach that roughly corresponds with the increase in the number of patients that control hospitals admit in the same period. The substitution effect leads control hospitals to eventually serve a greater number of patients, on average, than the breached hospitals. These results are consistent with the 2021 Scripps Health ransomware breach that shows patients substituted breached emergency medical services with those of non-breached hospitals in the surrounding area (Dameff et al., 2023).

Altogether, patient care at treated hospitals does not seem to directly suffer post-breach, except after a hack. Conditional on admittance to a hospital, patients report the same average level of care before and after an event. However, new patients appear to substitute breached medical services for those at non-breached hospitals, likely thinking that their care would be lesser at a breached hospital. This substitution appears to adversely affect nearby hospitals' level of care and own readmission rates.[17] Investors may require greater premiums for breached hospital bonds out of concern that breaches will lead to lesser care,

[17] Burky (2023) states that the Scripps ransomware hack necessitated a crisis-level response from non-breached emergency departments in the surrounding area to keep up with substituted patient demand.

but their reservations are seemingly misplaced. Changes in patient care do not fully explain investors' response to data breaches, especially since they do not respond to the worst types of events.

3.4. The Role of Attention

Lastly, I identify the role of investor and patient attention to news in mitigating information asymmetry surrounding hospital data breaches. If attention mitigates information asymmetry around breaches, my previous results should be weaker when attention on data breaches is greater. Alternatively, attention could accentuate misinformation and information asymmetry. Motivated by Da et al. (2011), I use Google Trends SVI of news articles that include the phrase "data breach" to proxy for attention around hospital data breaches. I base my collection of SVI on news articles to better account for both the release of information related to cyber risk and potential stakeholder attention to data breaches, but my results are qualitatively similar if base SVI on standard search queries. I collect SVI at the state-level for each issuer and hospital for a seven-year window surrounding their breaches, average the SVI to the yearly-level for each state-event, and identify whether an observation is associated with a high (low) SVI. I assume that SVI is high (low) if it is greater (lower) than the median SVI for the overall sample.

I repeat both the financing and hospital cash flow tests of Tables 4 and 6 in Panels A and B of Table 9, respectively. I find that the effects of data breaches are much greater when there is more attention on data breaches. For example, the effect of hacks on total patient revenue in high-SVI periods is over twice as large as the effect in low-SVI periods. Furthermore, hospital financing costs increase almost exclusively in high-SVI periods, implying there is a dimension of investor attention on breaches at play. As stakeholder attention to data breaches increases, both investors and patients penalize breached hospitals more.

Building on the evidence presented earlier in my paper and by Ablan et al. (2016) and Mayer et al. (2021), it is likely safe to assume that municipal bond market investors do not fully understand the differences between hacks and non-hacks. However, attention certainly plays a strong role in how stakeholders respond to the events. Intriguingly, though, stakeholder attention does not seem to align what investors believe will happen to breached issuers with what actually happens to them post-breach. If anything, attention simply accentuates investor misunderstanding surrounding data breaches.

4. Robustness Tests

In this section, I briefly address three potential concerns with my methodology. The first concern centers on the robustness of the stacked difference-in-differences methodology. The second and third concerns pertain to my construction of counterfactual observations. I address each criticism by reproducing the main results from Table 3 using alternative econometric or sample specifications.

4.1. Alternative Approach to Dealing with Heterogeneous Treatment Effects

The first criticism I address focuses on limitations potentially imposed by the stacked difference-in-differences estimator. Although the model is designed to be robust to heterogenous treatment effects over a sample period, the stacked difference-in-differences estimator may be considered less flexible than other alternatives to the staggered difference-in-differences estimator (Baker et al., 2022). As such, I ensure robustness to the methodology proposed by Borusyak et al. (2023) and use a similar set of control variables to my main specification and control bonds from never treated issuers over the entire sample period.

I present the results in Panel A of Table 10 and find that my main results hold. Models 1-4 all produce coefficients of the ATT that are both statistically significant and similar in magnitude to those produced by the stacked difference-in-differences estimator. According to the imputation estimator proposed by Borusyak et al. (2023), data breaches increase the new offer yields of breached hospitals by almost 42 bps and tax-adjusted spreads by about 82 bps, or 12.8% and 26.6% relative to the mean of each variable, respectively. My main result is robust to alternative econometric methodologies.

4.2. Sample Construction and Alternative Counterfactuals

It could be that my results are driven by my sample construction choices (i.e., using all non-treated issuers in the same state as a breached issuer could be too broad of a control group). As such, I employ two alternative approaches to constructing my controls.

First, I identify control observations by matching treated bonds to control observations on bond characteristics using coarsened exact matching. This approach may help difference out the effect that any observable bond characteristic may have on the outcome and may control for any systemic differences between treated and non-treated issuers. I match each treated bond to a control bond issued within the same year and that has the same categorical characteristics (i.e., callable, negotiated, etc.). I split the continuous bond-level control variables from Table 3, county population, and county employment into four bins and further match the treated observations to the control observations within the same bin. I repeat my main

analysis using the coarsened exact matched sample in Panel B of Table 10. Although the matched sample produces estimates of the ATT that are larger than the baseline coefficients in Table 3 without control variables, the coefficients are similar in magnitude when the models are estimated with control variables.

Second, instead of using all non-breached issuers within a state as controls, I use only non-breached neighboring issuers within the same county. This difference in the construction of the control group may better account for the influence of any unobserved factors, such as geography or demographic differences that may be associated with a population's response to a breach, on the cost of hospital financing. If breaches truly affect hospital financing and societal outcomes, then the effect should exist when contrasting breached issuers with their geographical neighbors. I present the results of my second alternative approach to constructing the counterfactuals in Panel C of Table 10. The sample size decreases to a total of 2.8k bonds, but the main results still hold. The estimated coefficients are larger than those presented in Table 3 but are more comparable to those presented in Table 5. Furthermore, the results are largely in line with both those presented in Table 3 and the other robustness tests. My methodology is robust to alternative sample specifications.

5. Conclusion

Although cyberattacks and data breaches are known to be costly events for victims, little is known about how the events affect stakeholders of breached entities. Likewise, most of the extant empirical research assumes that market participants know both the extent and nature of data breaches when examining how they affect real and financial outcomes. Because of the strict medical data breach reporting requirements but delayed reporting of hospital finances, the hospital bond market provides a unique opportunity to identify how data breaches affect non-breached stakeholders and how information asymmetry about data breaches influences the stakeholder response.

Using the universe of medical data breaches, this paper is the first to examine how data breaches affect hospital financing and patient outcomes. I find that breaches increase the cost of hospital bonds and are associated with increases in a hospital's credit and cash flow risk. Although breaches do not adversely affect patient outcomes of breached hospitals, patients still substitute their demand of breached hospital services for the services of non-breached hospitals, degrading the quality of services and patient care that those competing hospitals provide. I further find that hacks are the most adverse type of breach for hospitals, but investors do not incrementally respond to hacks relative to other types of breaches. Investors seem

uninformed regarding the nuances of different types of breaches, and attention on data breaches accentuates or eliminates their response to the events. Whereas investors hardly require any premium for investing in breached hospital bonds when a breach occurs in a period of lesser attention, both patients and investors heavily penalize breached hospitals when breaches occur in periods of greater attention.

My study has important implications for researchers, policymakers, and patients. First, my bond-level results imply that investors may not fully grasp the importance or relevance of different types of data breaches and how the events affect underlying cash flows. This lack of understanding leads some hospitals to pay more for their debt than they likely should. Second, my hospital-level results imply that data breaches have adverse consequences for local non-breached hospitals. Although breaches do not affect the outcomes of breached hospitals, patients appear to move to competing hospitals, a response which could easily lead to crisis-level scenarios where healthcare providers are unable to properly serve a larger influx of patients. To alleviate these concerns, policymakers could require stronger IT standards for hospitals to minimize the number of hacks from occurring. Additionally, policymakers could implement regulations and programs that aid hospitals' post-hack recovery, increase investor awareness of cyber risk, or implement programs to quickly restore public trust in breached hospitals.

References

Ablan, L., P. Heaton, D. Lavery, and S. Romanosky, 2016, Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information, *RAND Corporation*, Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf.

Aghamolla, C., P. Karaca-Mandic, X. Li, and R. Thakor, 2023, Merchants of Death: The Effect of Credit Supply Shocks on Hospital Outcomes, *NBER Working Paper28709.*

Akey, P., S. Lewellen, I. Liskovich, and C. Schiller, 2021, Hacking Corporate Reputations, *Working Paper*.

American Hospital Association (AHA), 2022, Fact Sheet: Economic Contribution of Hospitals, Available at: https://www.aha.org/fact-sheets/2022-02-25-fact-sheet-economic-contribution-hospitals#:~:text=When%20you%20add%20in%20these,U.S.%20(see%20Figure%202).

Amir, E., S. Levi, and T. Livne, 2018, Do Firms Underreport Information on Cyber-attacks? Evidence from Capital Markets, *Review of Accounting Studies* 23, 1177-1206.

Ashraf, M., 2022, The Role of Peer Events in Corporate Governance: Evidence from Data Breaches, *The Accounting Review* 97, 1-24

Borusyak, K., X. Jaravel, and J. Spiess, 2023, Revisiting Event Study Design: Robust and Efficient Estimation, *Review of Economic Statistics* Forthcoming.

Brooks, C., 2022, Alarming Cyber Statistics for Mid-Year 2022 that You Need to Know, *Forbes*, July 3, 2022.

Burky, A., 2023, Scripps Ransomware Post-Mortem Reveals Significant Ripple Effects for Nearby Hospitals, FierceHealthCare.com, Available at: https://www.fiercehealthcare.com/health-tech/scripps-ransomware-post-mortem-shows-cybersecurity-regional-problem.

Cabezon, F., 20203, The Effect of Mandatory Information Disclosure on Financial Constraints, *SSRN Working Paper* 3725099.

Campbell, K., L. Gordon, M. Loeb, and L. Zhou, 2003, The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market, *Journal of Computer Security* 11, 431-448.

Cavusoglu, H., B. Mishra, and S. Raghunathan, 2004, 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, 69-104.

Cengiz, D., A. Dube, A. Lindner, and B. Zipperer, 2019, The Effect of Minimum Wages on Low-Wage Jobs, *Quarterly Journal of Economics* 134, 1405-1454.

Centers for Disease Control and Prevention (CDC), 2020, QuickStats: Percentage of Deaths, by Place of Death – National Vital Statistics System, United States, 2000-2018, *Morbidity and Mortality Weekly Report* 69, 611.

Cheng, X. and S. Walton, 2019, Do Nonprofessional Investors Care about How Data Breaches are Disclosed, *Journal of Information Systems* 33, 163-182.

Choi, S., M. E. Johnson, and J. Lee, 2020, An Event Study of Data Breaches and Hospital IT Spending, *Health Policy and Technology* 9, 372-378.

Christensen, H., E. Floyd, L Liu, and M. Maffett, 2017, The Real Effects of Mandated Information on Social Responsibility in Financial Reports: Evidence from Mine-Safety Records, *Journal of Accounting and Economics* 64, 284-304.

Cornaggia, J., K. Cornaggia, and R. Israelsen, 2018, Credit Ratings and the Cost of Municipal Financing, *Review of Financial Studies* 31, 2038–2079.

Cornaggia, K., J. Hund, G. Nguyen, and Z. Ye, 2021, Opioid Crisis Effects on Municipal Finance, *Review of Financial Studies* 35, 2019-2066.

Cornaggia, K., X. Li, and Z. Ye, 2022, Virtual Competition and the Cost of Capital: Evidence from Telehealth, *Working Paper*.

Crosignani, M., M. Macchiavelli, and A. Silva, 2023, Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains, *Journal of Financial Economics* 147, 432-448.

Da, Z., J. Engelberg, and P. Gao, 2011, In Search of Attention, *Journal of Finance* 66, 1461-1499.

Dameff, C., J. Tully, T. Chan, E. Castillo, S. Savage, T. Hemmen, B. Clay, and C. Longhurst, 2023; Ransomware Attack Associated with Disruptions at Adjacent Emergency Departments in the US, *JAMA Network Open* 6, e2312270.

Florakis, C., C. Louca, R. Michaely, and M. Weber, 2023, Cybersecurity Risk, *Review of Financial Studies* 36, 351-407.

Gao, P., C. Lee, and D. Murphy, 2022, Good for Your Fiscal Health? The Effect of the Affordable Care Act on Healthcare Borrowing Costs?, *Journal of Financial Economics* 145, 464-488.

Griffin, P., 2003, Got Information? Investor Response to Form 10-K and Form 10-Q EDGAR Filings, *Review of Accounting Studies* 8, 433-460.

Grigoris, F., 2020, The Term Structure of Municipal Bond Yields, Local Economic Conditions, and Local Stock Returns, PhD Thesis, The University of North Carolina at Chapel Hill.

Gustafson, M., P. Haslag, D. Weagley, and Z. Ye, 2023, A Flash in the Pan(demic)? Migration Risks and Municipal Bonds, *Available at SSRN 4029984*.

Hovav, A., and J. D'Arcy, 2003, The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms, *Risk Management and Insurance Review* 6, 97-121.

Huang, H., and C. Wang, 2021, Do Banks Price Firms' Data Breaches?, *The Accounting Review* 96, 261-286.

Jamilov, R., H. Rey, and A. Tahoun, 2021, The Anatomy of Cyber Risk, *NBER Working Paper 28906*.

Jencks, S. F., M. V. Williams, and E. A. Coleman, 2009, Rehospitalizations among Patients in the Medicare Fee-for-Service Program, *New England Journal of Medicine* 360, 1418-1428.

Lerman, A. and J. Livnat, 2009, The New Form 8-K Disclosures, *Review of Accounting Studies* 15, 752-778.

Lin, Z., T. Sapp, J. Ulmer, and R. Parsa, 2020, Insider Trading Ahead of Cyber Breach Announcements, *Journal of Financial Markets* 50, 100527.

Kamiya, S., J. Kang, J. Kim, A. Milidonis, and R. Stulz, 2021, Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms, *Journal of Financial Economics* 139, 719-749.

Kannan, K., J. Rees, and S. Sridhar, 2007, Market Reactions to Information Security Breach Announcements: An Empirical Analysis, *International Journal of Electronic Commerce* 12, 69-91.

Kvochko, E., and R. Pant, 2015, Why Data Breaches Don't Hurt Stock Prices, *Harvard Business Review*.

MacDorman, M. and E. Declercq, 2019, Trends and State Variations in Out-of-Hospital Births in the United States, 2004-2017, *Birth* 46:279-288.

Mayer, P., Y. Zou, F. Schaub, and A. Aviv, 2021, "Now I'm a Bit Angry:" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them, *30th USENIX Security Symposium*.

Municipal Rulemaking Securities Board (MSRB), 2022, Trends in Municipal Securities Ownership.

Muolo, D., 2022, Cybersecurity Investments Could Go by the Wayside at Cash-Strapped Hospitals, Fitch Warns, FierceHealthcare.com, Available at: https://www.fiercehealthcare.com/providers/cybersecurity-preparations-could-go-wayside-cash-strapped-hospitals-fitch-warns.

Noh, S. E. So, and J. Weber, 2019, Voluntary and Mandatory Disclosures: Do Managers View Them as Substitutes?, *Journal of Accounting and Economics* 68, 101243.

Osborne, B., 2023, When Government Catches the (Cyber) Bug: The Costs and Real Effects of Municipal Cyberattacks, *Working Paper*.

Painter, M., 2020, An Inconvenient Cost: The Effects of Climate Change on Municipal Bonds, *Journal of Financial Economics* 135, 468-482.

Serfling, M., 2016, Firing Costs and Capital Structure Decisions, *Journal of Finance* 71, 2239-2285.

Table A1
Variable Definitions

This table provides the definitions for the main variables used in this study. Variables used as controls are indicated by a checkmark in the second column. All continuous variables are winsorized in the analysis, and variables denominated in dollars are inflation-adjusted to 2009 dollars.

Variable	Definition
Adjusted Spread	*Yield* divided by 1 minus the highest state-level marginal tax rate for each year in my sample, less the corresponding *Treasury Yield*
Always Clean	The proportion of patients who report that their room was always clean
Amount	The bond issue amount
Assets	A hospital's total reported assets
Bed Days	A hospital's number of beds multiplied by the number of days in a year
Bed Utilization	A hospital's total number of discharges divided by *Bed Days*
Breach	An indicator that equals 1 if an observation is from a breached entity, 0 otherwise
Callable	An indicator that equals 1 if a bond is callable, 0 otherwise
Cash	A hospital's total cash in hand or in banks
Coupon	A bond's coupon amount from SDC
Doctor Always Clear	The proportion of patients who report their doctors always communicated clearly
Employment	The county employment level from the BEA's CAIN30 dataset
Fixed Equipment	A hospital's reported value of fixed assets
GO Bond	An indicator that equals 1 if a bond is a general obligation bond
Hospital Income	A hospital's total income
Liabilities	A hospital's total current and long-term liabilities
Inpatient Revenue	A hospital's revenue from inpatient services
Inverse Maturity	One divided by *Maturity*
Maturity	The difference between a bond's maturity and settlement dates
Max Rating	A factor variable defined from 1 to 21 for the highest credit rating assigned to a bond; lower numbers are higher rated bonds
Negotiated	An indicator that equals 1 if a bond is negotiated, 0 otherwise
Nurse Always Clear	The proportion of patients who report their nurses always communicated clearly
Outpatient Revenue	A hospital's revenue from outpatient services
Per Capita Income	County-level per capita income from the BEA's CAIN30 dataset
Population	The county population level from the BEA's CAIN30 dataset
Post	An indicator that equals 1 if an observation is in a year after an attack, 0 otherwise
Rate "9-10"	The proportion of patients who report they would rate a hospital a "9" or "10"
Recommend "Yes"	The proportion of patients who report they would recommend a hospital
Recov Info Always Clear	The proportion of patients who report their recovery information was always clear
Room Always Quiet	The proportion of patients who report their room was always queit
SVI	The log of the yearly mean of the Google Trends score for the phrase "data breach" within a hospital's state
Tax Exempt	An indicator that equals 1 if a bond is tax exempt, 0 otherwise
Treasury Yield	The maturity-matched yield on Treasury bonds, linearly interpolated for missing maturities
Yield	A bond's initial offer yield from SDC

Figure 1
Analysis of Parallel Trends

This figure presents stacked difference-in-difference coefficient estimates of my two main dependent variables on a set of timing variables interacted with *Breach*. The timing indicators are defined relative to the year of breach, where *Breach* is year *t*. Following econometric tradition, I exclude the period *t-1* in my estimation. I use the variables *Coupon*, *Maturity*, *Inverse Maturity*, *Logged Issue Size*, *Callable*, *Negotiated*, *GO Bond*, *Tax Exempt*, *lag Population*, *lag Per Capita Income*, and *lag Employment* as control variables. The model with *Yield* as a dependent variable includes the corresponding *Treasury Yield* as a control. The coefficients for the controls and level effects are omitted for brevity. I include issuer-event and year-event fixed effects in each model (Baker et al., 2022). Standard errors are clustered by issuer in all models, and the bars represent the 95% confidence interval. All variables are defined in the appendix.

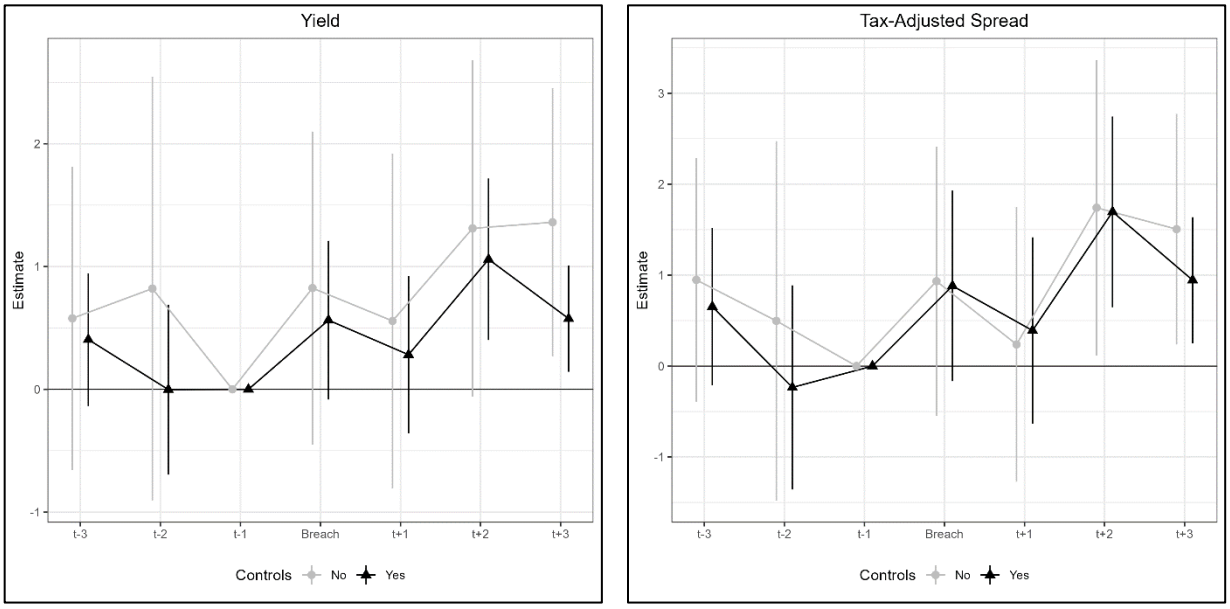

Figure 2
The Timing of Bond Downgrades

This figure presents stacked difference-in-difference coefficient estimates of my max rating variables on a set of timing variables interacted with *Breach*. The timing indicators are defined relative to the year of breach, where *Breach* is year *t*. Following econometric tradition, I exclude the period *t-1* in my estimation. I estimate one model without controls and one model with controls. I use the corresponding *Treasury Yield* and the variables *Coupon*, *Maturity*, *Inverse Maturity*, *Logged Issue Size*, *Callable*, *Negotiated*, *GO Bond*, *Tax Exempt*, *lag Population*, *lag Per Capita Income*, and *lag Employment* as control variables. The coefficients for the controls and level effects are omitted for brevity. I compute the post-breach effect on bond ratings by averaging the four post-breach timing coefficients and testing its statistical significance using a Wald chi-squared test. I include issuer-event and year-event fixed effects in each model (Baker et al., 2022). Standard errors are clustered by issuer in all models, and the bars represent the 95% confidence interval. All variables are defined in the appendix.

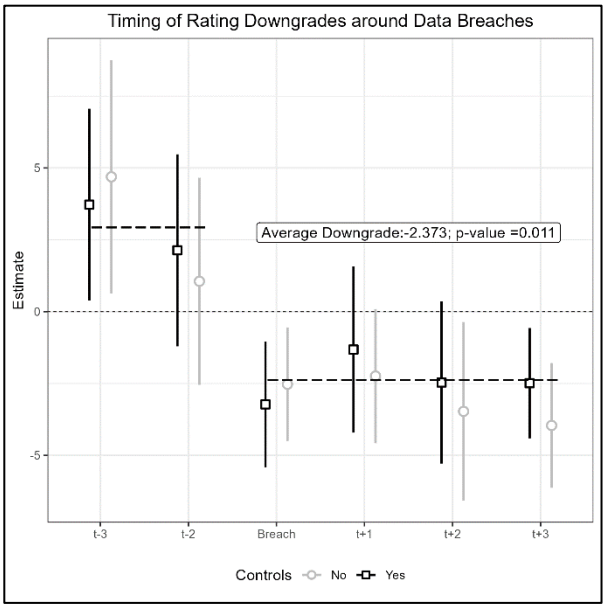

Figure 3
Yield and Spread Curves of Treated Bonds

This figure presents the yield and spread curves of breached hospital bonds after a data breach for bonds that mature 2 to 25 years in the future. The point estimate for each maturity is based on a stacked difference-in-difference coefficient estimate of my two main dependent variables on a set of maturity timing variables interacted with *Breach*. I use the variables *Coupon*, *Maturity*, *Inverse Maturity*, *Logged Issue Size*, *Callable*, *Negotiated*, *GO Bond*, *Tax Exempt*, *lag Population*, *lag Per Capita Income*, and *lag Employment* as control variables. The model estimating the yield curve includes the corresponding *Treasury Yield* as a control. The coefficients for the controls and level effects are omitted for brevity. I include issuer-event and year-event fixed effects in each model (Baker et al., 2022). Standard errors are clustered by issuer in all models, and the bars represent the 95% confidence interval. I do not present the estimates for bonds with maturities longer than 25 years because there are few observations with maturities longer than 25 years. All variables are defined in the appendix.

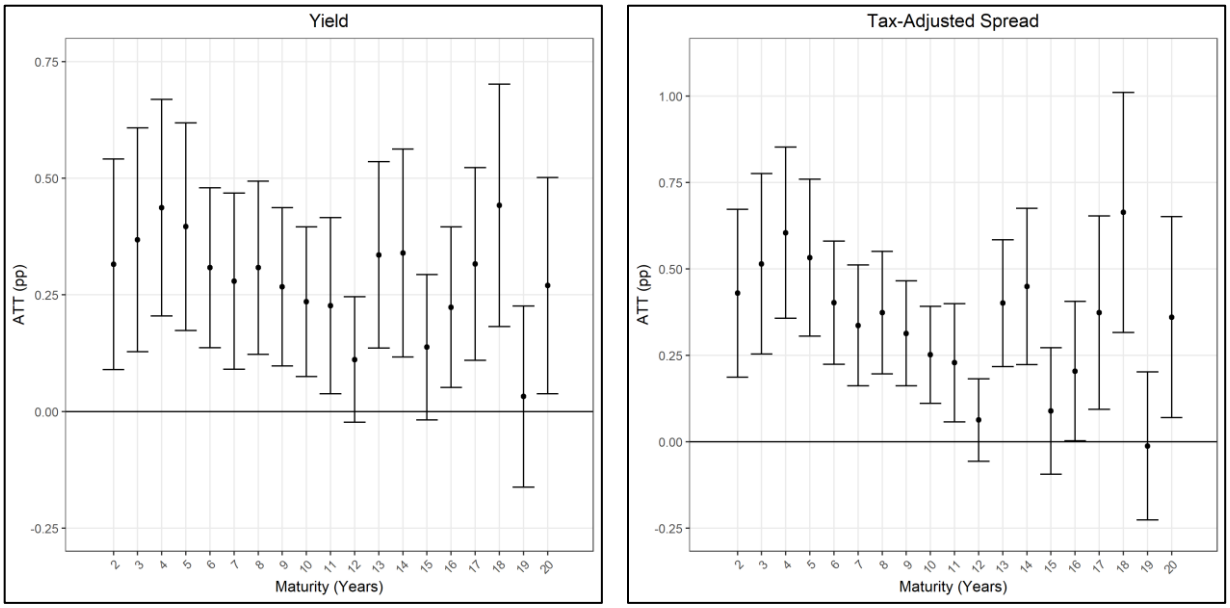

Figure 4
Treated and Control Hospital Admissions for Health Conditions around Data Breaches

This figure compares the average number of patients that treated and control hospitals serve in the years around a breach for my four main patient health outcomes (i.e., admissions for *AMI*, *COPD*, *HF*, and *PN*). Control hospitals are non-breached hospitals in the same county as a breached hospital. All variables are defined in the appendix.

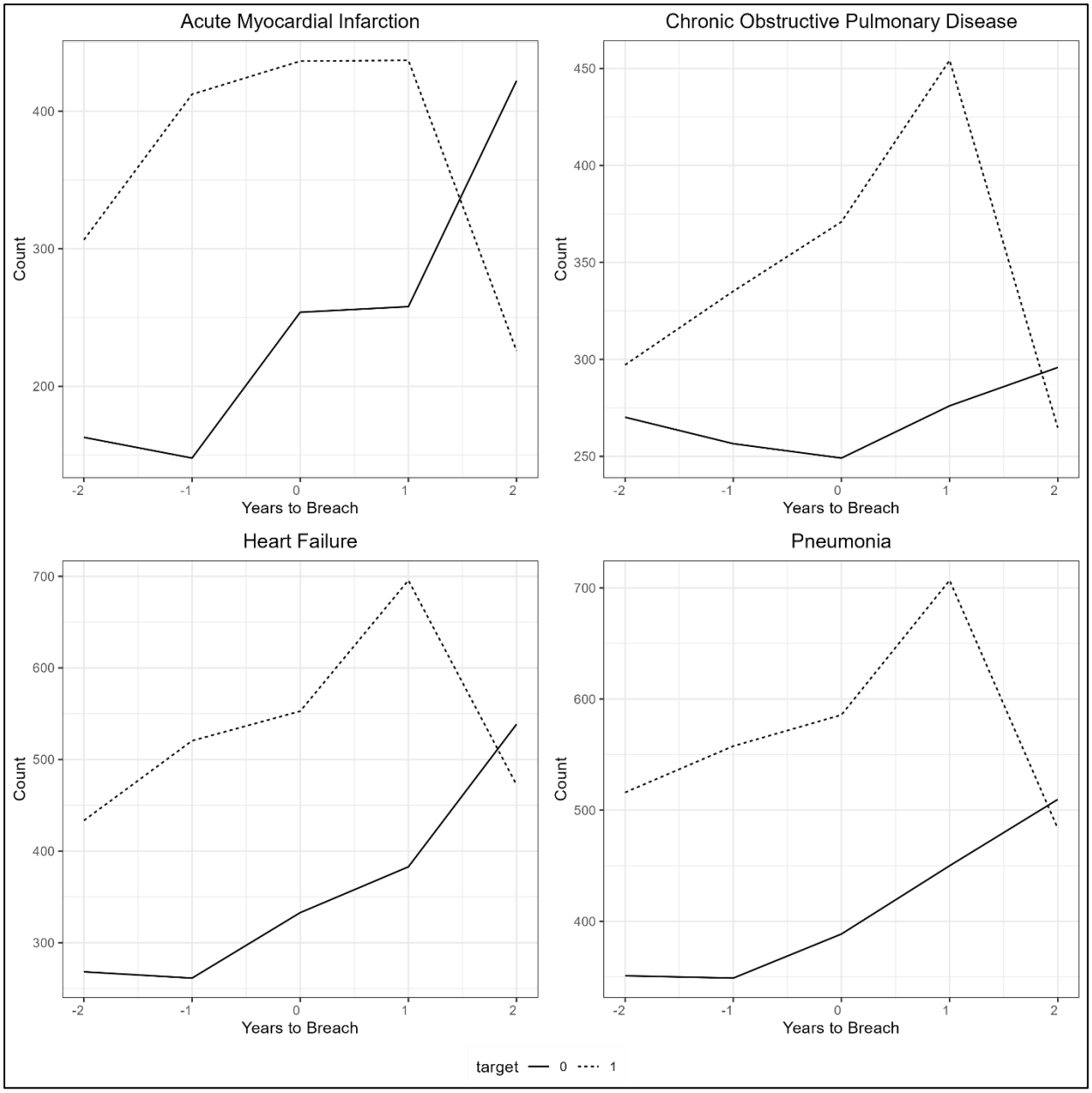

Table 1
Descriptive Statistics for Municipal Bonds and Hospitals

This table presents summary statistics for my main sample of breached entities and their counterfactuals. Panel A presents statistics for my overall sample of bonds, and Panel B presents statistics related to hospital financial and balance sheet outcomes. Panel C describes 30-day patient readmission rates for my main patient outcomes, and Panel D overviews patients' self-reported care measures. Panel C presents statistics for my main sample of stacked county data. Each panel also names the source of the data. All continuous data are winsorized at the one percent levels.

Panel A: Overall Sample of Bonds (Mergent)						
	N	Mean	SD	Pctl(25)	Median	Pctl(75)
Yield (%)	11,987	3.11	1.28	2.19	3.09	3.93
Adj Spread (%)	11,987	2.98	1.45	1.92	2.92	3.84
Issue Size (1,000s)	11,987	141,029.30	157,009.10	27,595.00	84,745.00	200,000.00
Bond Size (1,000s)	11,971	8,644.62	16,956.25	915	2,720.00	7,775.00
Coupon (%)	11,987	4.35	1	4	5	5
Maturity (Years)	11,987	11.91	7.36	6.34	10.42	15.78
Max Rating	11,987	9.1	4.58	5	8	14
GO	11,987	0.14	0.35	0	0	0
Callable	11,987	0.53	0.5	0	1	1
Negotiated	11,987	0.87	0.34	1	1	1
Tax Exempt	11,987	0.97	0.18	1	1	1
Population$_{t-1}$ (1,000s)	11,987	1,008.22	819.03	435.49	799.68	1,485.22
Per Capita Income$_{t-1}$ (1,000s)	11,987	44	9.61	37.94	41.89	48.87
Employment$_{t-1}$ (1,000s)	11,987	647.42	511.82	252.14	752.77	841.53
Panel B: Hospital Financials (CMS Care Compare)						
log Total Revenue (TR)	65,240	19.38	1.62	18.1	19.49	20.69
log Outpatient Revenue	65,280	18.33	2.15	17.23	18.82	19.85
log Inpatient Revenue	70,223	18.49	1.89	17.21	18.62	20.01
log Hospital Income	49,216	15.59	1.74	14.49	15.67	16.84
log Assets/TR$_{t-1}$	64,793	0.38	0.36	0.16	0.28	0.46
log Liabilities/TR$_{t-1}$	64,434	0.21	0.29	0.07	0.15	0.27
log Cash/TR$_{t-1}$	63,772	0.04	0.09	0.0001	0.01	0.05
log Fixed Equipment/TR$_{t-1}$	38,878	0.06	0.11	0.01	0.02	0.06
log Bed Days	74,181	10.54	1.1	9.69	10.64	11.39
Bed Utilization (%)	74,044	0.44	0.23	0.27	0.44	0.6
Panel C: Patient 30-Day Readmission Rates (CMS HCRIS)						
Pneumonia	10,535	0.12	0.13	0.03	0.07	0.16
Heart Failure	9,572	0.2	0.2	0.05	0.11	0.28
Heart Attacks	5,670	0.16	0.15	0.05	0.1	0.21
COPD	9,670	0.19	0.18	0.06	0.11	0.26

Table 1
(Continued)

Panel D: Patient Satisfaction of Care (CMS HCAHPS)						
Recommend "Yes" (%)	8,173	70.08	10.1	64	70	77
Always Clean (%)	8,173	17.89	4.42	15	18	21
Doctor Always Clear (%)	8,173	80.06	6.02	76	80	84
Nurse Always Clear (%)	8,173	78.6	5.86	75	79	82
Recov Info Always Clear (%)	8,173	86.07	4.08	84	87	89
Room Always Quiet (%)	8,173	59.2	11.22	51	58	67
Rate "9-10" (%)	8,173	70.66	9.08	65	71	77

Table 2
The Determinants of Hospital Data Breaches

This table analyzes which characteristics are associated with hospital data breaches using a linear probability model. The dependent variable is a binary indicator that equals one if a hospitals' data are breached in a given year and zero otherwise, and all independent variables are both lagged and logged. Model 1 uses hospital and year fixed effects, and Model 2 replaces the fixed effects with county-year fixed effects to capture any effect the hospital's local economic environment has on its propensity to be breached. Standard errors are clustered by hospital in both models , and *t*-statistics are presented in parentheses. All variables are defined in the appendix. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	Dependent Variable: 1(Breach)	
	(1)	(2)
Total Revenue	0.001	-0.001
	(0.563)	(-0.573)
Total Assets	0.001	0.001
	(0.738)	(0.648)
Total Liabilities	0.0001	0.0003
	(0.388)	(0.697)
Cash Holdings	0.0001	0.001**
	(0.653)	(2.536)
Full-Time Employees	-0.001	0.002
	(-1.024)	(1.485)
Beds	-0.0004	-0.0004
	(-0.445)	(-0.462)
Hospital FEs	Yes	No
Year FEs	Yes	No
County-Year FEs	No	Yes
Observations	26,670	26,670
Adj R^2	-0.007	-0.064

Table 3
Impact of Data Breaches on Cost of Hospital Financing

This table presents stacked triple difference-in-difference coefficient estimates of my two main dependent variables on *Breach*, *Post*, *Hack*, interactions between each pair of the variable, and an interaction between *Breach, Post*, and *Hack*. Each model includes *Coupon*, *Maturity*, *Inverse Maturity*, *Logged Issue Size*, *Callable*, *Negotiated*, *GO Bond*, *Tax Exempt*, *lag Population*, *lag Per Capita Income*, and *lag Employment* as control variables. Model 2 also includes the corresponding *Treasury Yield* as a control. The coefficients for the controls are omitted for brevity. I include issuer-event and year-event fixed effects in the models (Baker et al., 2022). Standard errors are clustered by issuer in all models , and *t*-statistics are presented in parentheses. All variables are defined in the appendix. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	Dependent Variable			
	Yield		Adjusted Spread	
	(1)	(2)	(3)	(4)
Breach×Post	0.478**	0.443**	0.480	0.749***
	(1.98)	(2.48)	(1.38)	(2.65)
Controls	No	Yes	No	Yes
Issuer×Event FEs	Yes	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes	Yes
Observations	11,987	11,987	11,987	11,987
Adj R^2	0.472	0.893	0.476	0.789

Table 4
Term Structure of Breached Hospital Bonds

This table presents stacked difference-in-difference coefficient estimates of my two main dependent variables on *Breach*, *Post*, *Mid-Term*, *Long-Term*, and interactions between each of the terms. Each model includes *Coupon*, *Maturity*, *Inverse Maturity*, *Logged Issue Size*, *Max Rating*, *Callable*, *Negotiated*, *GO Bond*, *Tax Exempt*, *lag Population*, *lag Per Capita Income*, and *lag Employment* as control variables. Model 1 also includes the corresponding *Treasury Yield* as a control. The coefficients for the controls are omitted for brevity. I include issuer-event and year-event fixed effects in the models (Baker et al., 2022). Standard errors are clustered by issuer in all models, and *t*-statistics are presented in parentheses. All variables are defined in the appendix. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	Dependent Variable	
	Yield	Adjusted Spread
	(1)	(2)
Breach×Post	0.443*	0.735**
	(1.94)	(2.20)
Breach×Post×Mid-Term	0.100	0.204
	(0.455)	(0.712)
Breach×Post×Long-Term	-0.039	-0.061
	(-0.308)	(-0.394)
Controls	Yes	Yes
Issuer×Event FEs	Yes	Yes
Year×Event FEs	Yes	Yes
Observations	11,987	11,987
Adj R^2	0.893	0.792

Table 5
The Incremental Effect of External Hacks on Hospital Financing

This table presents stacked triple difference-in-difference coefficient estimates of my two main dependent variables on *Breach*, *Post*, and an interaction between *Breach* and *Post*. Each model includes *Coupon*, *Maturity*, *Inverse Maturity*, *Logged Issue Size*, *Callable*, *Negotiated*, *GO Bond*, *Tax Exempt*, *lag Population*, *lag Per Capita Income*, and *lag Employment* as control variables. Model 2 also includes the corresponding *Treasury Yield* as a control. The coefficients for the controls are omitted for brevity. I include issuer-event and year-event fixed effects in the models (Baker et al., 2022). Standard errors are clustered by issuer in all models, and *t*-statistics are presented in parentheses. All variables are defined in the appendix. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	Dependent Variable			
	Yield		Adjusted Spread	
	(1)	(2)	(3)	(4)
Breach×Post×Hack	-0.297	-0.261	-0.835	-0.449
	(-0.663)	(-0.702)	(-1.27)	(-0.746)
Breach×Post	0.655**	0.584*	0.978*	0.992**
	(2.29)	(1.87)	(1.89)	(1.99)
Controls	No	Yes	No	Yes
Issuer×Event FEs	Yes	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes	Yes
Observations	11,987	11,987	11,987	11,987
Adj R^2	0.472	0.893	0.476	0.789

Table 6
Cash Flow and Fundamental Risk: Data Breaches and Hospital Health

This table presents stacked triple difference-in-difference coefficient estimates of several variables that measure hospital fundamental outcomes on *Breach*, *Post*, *Hack*, and interactions between each of the terms. I include events between the years of 2015 and 2017 to ensure I have three years of pre- and post-breach outcomes. Each outcome is transformed by one plus the natural logarithm of the underlying variable. Panel A presents the effect of data breaches on hospital cash flow generating activity, and Panel B presents the effect of breaches on the hospital balance sheet. Each outcome variable in Panel B is further scaled by the lagged total hospital revenue. Following Aghamolla et al. (2023), I include the lagged variables *log Hospital Income*, *log Bed Days*, *Cash Holdings*, *log Liabilities*, and *Total Patient Revenue* as controls. I compute the total effect of interaction terms and test for the sum's significance using a Wald chi-squared test. The coefficients for the controls are omitted for brevity. I include hospital-event and year-event fixed effects in the models (Baker et al., 2022). Standard errors are clustered by issuer in all models, and *t*-statistics are presented in parentheses. All variables are defined in the appendix. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	logarithm of 1 + *Dependent Variable*			
Panel A: Hospital Cash Flow Generating Activity				
	Patient Revenue	Outpatient Revenue	Inpatient Revenue	Bed Utilization
	(1)	(2)	(3)	(4)
Breach×Post×Hack	-0.060*	-0.015	-0.101**	-0.023*
	(-1.684)	(-0.294)	(-2.342)	(-1.683)
Breach×Post	-0.009	-0.017	0.019	0.022*
	(-0.300)	(-0.409)	(0.614)	(1.962)
Total Effect	-0.068	-0.032	-0.082	0.002
P-Value	<0.001	0.152	0.001	0.842
Controls	Yes	Yes	Yes	Yes
Hospital×Event FEs	Yes	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes	Yes
Observations	44,665	44,663	44,665	44,645
Adj R^2	0.990	0.982	0.990	0.935
Panel B: Hospital Balance Sheet				
	Assets/TR	Liabilities/TR	Cash/TR	Fixed Equipment/TR
	(1)	(2)	(3)	(4)
Breach×Post×Hack	-0.014	-0.007	0.0003	-0.058
	(-0.593)	(-0.859)	(0.234)	(-1.492)
Breach×Post	0.005	0.009	0.001	0.008*
	(0.378)	(1.226)	(0.535)	(1.710)
Total Effect	-0.009	0.001	0.001	-0.049
P-Value	0.476	0.681	0.251	0.122
Controls	Yes	Yes	Yes	Yes
Hospital×Event FEs	Yes	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes	Yes
Observations	44,661	44,442	44,650	27,273
Adj R^2	0.956	0.973	0.997	0.907

Table 7
Data Breaches and Patient Care Experience

This table presents stacked triple difference-in-difference coefficient estimates of several variables that measure how patients rate their experience while admitted to a hospital on *Breach*, *Post*, *Hack*, and interactions between each of the terms. I include events between the years of 2017 and 2018 to ensure I have at least two years of pre- and post-breach outcomes. Each outcome measures how patients perceive their experience at a hospital. Following Aghamolla et al. (2022), I include the lagged variables *log Hospital Income*, *log Bed Days*, *Cash Holdings*, *log Liabilities*, and *Total Patient Revenue* as controls. I compute the total effect of interaction terms and test for the sum's significance using a Wald chi-squared test. The coefficients for the controls are omitted for brevity. I include hospital-event and year-event fixed effects in the models (Baker et al., 2022). Standard errors are clustered by hospital in all models, and *t*-statistics are presented in parentheses. All variables are defined in the appendix. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	Dependent Variable						
	Recommend "Yes"	Room Always Clean	Doc Comm Always Clear	Nurse Comm Always Clear	Recovery Info Always Clear	Room Always Quiet	Rate "9-10"
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Breach×Post×Hack	-1.369	-1.015	-1.065	-0.124	0.467	-1.650	-1.972
	(-0.546)	(-0.866)	(-0.699)	(-0.074)	(0.351)	(-0.846)	(-1.287)
Breach×Post	0.612	0.979	0.746	-0.348	0.761	0.844	0.602
	(0.716)	(1.120)	(1.398)	(-0.750)	(0.889)	(0.924)	(0.839)
Total Effect	-0.757	-0.036	-0.319	-0.472	1.228	-0.806	-1.369
P-Value	0.694	0.970	0.798	0.695	0.117	0.573	0.367
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hospital×Event FEs	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	5,861	5,861	5,861	5,861	5,861	5,861	5,861
Adj R^2	0.876	0.643	0.819	0.821	0.698	0.881	0.848

Table 8
Data Breaches and Patient Readmission Rates

This table presents stacked triple difference-in-difference coefficient estimates of several variables that measure patient readmission rates for various diagnoses on *Breach*, *Post*, *Hack*, and interactions between each of the terms. I include events between the years of 2017 and 2018 to ensure I have two years of pre- and post-breach outcomes. Each outcome measures common measures of patient care quality, namely, the 30-day readmission rates for pneumonia (PN), heart failure (HF), heart attacks (AMI), and chronic obstructive pulmonary disease (COPD). The outcomes in Models 1-4 are transformed by the natural logarithm, and the outcomes in Models 5-8 are in percentage points. Following Aghamolla et al. (2023), I include the lagged variables *log Hospital Income*, *log Bed Days*, *Cash Holdings*, *log Liabilities*, and *Total Patient Revenue* as controls. I compute the total effect of interaction terms and test for the sum's significance using a Wald chi-squared test. Panel A (B) presents results based on a control group that is comprised of all non-breached hospitals in the same state (county) as the breached hospital. The coefficients for the controls are omitted for brevity. I include hospital-event and year-event fixed effects in the models (Baker et al., 2022). Standard errors are clustered by hospital in all models, and *t*-statistics are presented in parentheses. All variables are defined in the appendix. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	Dependent Variable							
Panel A: Control Group of All Non-Breached Hospitals in Same State								
	log(PN)	log(HF)	log(AMI)	log(COPD)	PN	HF	AMI	COPD
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Breach×Post×Hack	-0.056	0.143	-0.067	0.116	-0.003	0.055***	-0.011	0.021
	(-0.835)	(1.62)	(-0.583)	(1.43)	(-0.413)	(2.81)	(-0.601)	(1.16)
Breach×Post	-0.017	-0.116**	-0.094	-0.159**	-0.002	-0.031***	-0.003	-0.022
	(-0.337)	(-2.57)	(-1.18)	(-2.22)	(-0.430)	(-3.20)	(-0.176)	(-1.27)
Total Effect	-0.073	0.027	-0.161	-0.043	-0.005	0.025	-0.014	-0.001
P-Value	0.063	0.586	0.005	0.227	0.377	0.048	0.041	0.970
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hospital×Event FEs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	8,401	7,815	5,308	7,888	8,401	7,815	5,308	7,888
Adj R^2	0.983	0.985	0.975	0.978	0.943	0.954	0.931	0.943
Panel B: Control Group of Non-Breached Hospitals in Same County								
Breach×Post×Hack	0.148	-0.043	0.347***	0.216**	0.026*	0.060*	0.055***	0.050**
	(1.25)	(-0.444)	(3.50)	(2.27)	(1.77)	(1.75)	(4.23)	(2.03)
Breach×Post	-0.144*	-0.116	-0.302***	-0.292***	-0.009	-0.023	-0.040***	-0.038*
	(-1.83)	(-1.61)	(-3.37)	(-4.18)	(-0.983)	(-0.974)	(-3.55)	(-1.98)
Total Effect	0.003	-0.160	0.045	-0.076	0.018	0.036	0.015	0.012
P-Value	0.959	<0.001	0.002	0.156	0.057	0.089	<0.001	0.515
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hospital×Event FEs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	1,173	1,162	946	1,138	1,173	1,162	946	1,138
Adj R^2	0.995	0.995	0.996	0.993	0.968	0.966	0.989	0.972

Table 9
Yields and Hospital Financials around Periods of Interest in Data Breaches

This table presents stacked triple difference-in-difference coefficient estimates of several variables that measure the issuer cost of debt outcomes from Table 4 and hospital financial outcomes from Panel A of Table 7 on *Breach*, *Post*, and *Hack* and interactions between each of the terms. The *Low Attention* (left) half of the table is based on a sample split of observations with less than the median search volume index (SVI), and the *High Attention* (right) half of the table is the complement. The variable *SVI* is the average yearly Google Trends search volume index for the phrase "data breach" in the hospitals' respective states. I restrict base SVI on news articles to account for the spread of information regarding breaches and, therefore, the potential attention given to events. Following Aghamolla et al. (2023), I include the lagged variables *log Hospital Income*, *log Bed Days*, *Cash Holdings*, *log Liabilities*, and *Total Patient Revenue* as controls. The coefficients for the controls are omitted for brevity. I include hospital-event and year-event fixed effects in the models (Baker et al., 2022). Standard errors are clustered by issuer in all models, and *t*-statistics are presented in parentheses. All variables are defined in the appendix. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	Low Attention				*High Attention*			
Panel A: Hospital Financials								
	logarithm of 1 + *Dependent Variable*							
	Pat Rev	Outpat Rev	Inpat Rev	Bed Util	Pat Rev	Outpat Rev	Inpat Rev	Bed Util
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Breach×Post×Hack	-0.062**	-0.011	-0.095*	-0.018	-0.127**	-0.068	-0.135***	-0.003
	(-2.30)	(-0.310)	(-1.85)	(-1.21)	(-2.10)	(-0.593)	(-4.07)	(-0.137)
Breach×Post	-0.006	-0.011	0.018	0.016	-0.013	-0.046	0.022	0.015
	(-0.235)	(-0.387)	(0.430)	(1.51)	(-0.233)	(-0.459)	(0.800)	(0.878)
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hospital×Event FEs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	18,489	18,487	18,489	18,468	18,672	18,672	18,672	18,664
Adj R^2	0.992	0.986	0.990	0.951	0.990	0.983	0.991	0.938
Panel B: Issuer Cost of Debt								
	Yield		Adjusted Spread		Yield		Adjusted Spread	
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Breach×Post	0.448	0.403	0.366	0.713*	0.214	0.737***	0.474*	1.23***
	(0.669)	(1.56)	(0.477)	(1.77)	(1.47)	(3.28)	(1.98)	(3.34)
Controls	No	Yes	No	Yes	No	Yes	No	Yes
Hospital×Event FEs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	5,466	5,466	5,466	5,466	6,466	6,466	6,466	6,466
Adj R^2	0.534	0.933	0.597	0.853	0.355	0.847	0.316	0.727

Table 10
Robustness of Financing Tests

This table presents robustness tests for my main results in Table 3. I use a stacked difference-in-difference estimation in each model outside of those in Panel A, and the columns represent coefficient estimates of my three main dependent variables on *Breach*, *Post*, and an interaction between *Breach* and *Post*. Each model includes *Coupon*, *Maturity*, *Inverse Maturity*, *Logged Issue Size*, *Callable*, *Negotiated*, *GO Bond*, *Tax Exempt*, *lag Population*, *lag Per Capita Income*, and *lag Employment* as control variables. Models 1 and 2 also includes the corresponding *Treasury Yield* as a control. The coefficients for the controls are omitted for brevity. I include state-event and year-event fixed effects in the models (Baker et al., 2022). Panel A presents my main financing test models using an alternative methodology (Borusyak et al., 2021) over the same sample period as my primary sample. Panel B presents the main results based on a coarsened exact matched sample. I split the continuous bond characteristics, county population, and county employment into four bins and match breached bonds to control bonds to those that are issued within the same year and bin and that have the same binary characteristics. Panel C presents the main results when using only non-breached issuers in the same county as the breached hospital as the control group. Standard errors are clustered by issuer in all models and presented in parentheses. All variables are defined in the appendix. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	Dependent Variable			
	Yield		Adjusted Spread	
	(1)	(2)	(3)	(4)
Panel A: Alternative Estimator (Boruysyak et al., 2023)				
Breach×Post	0.364***	0.419***	0.821***	0.821***
	(5.02)	(4.60)	(6.93)	(6.64)
Controls	No	Yes	No	Yes
Issuer FEs	Yes	Yes	Yes	Yes
Year FEs	Yes	Yes	Yes	Yes
Observations	16,416	16,416	16,416	16,416
Panel B: Coarsened Exact Matched Sample				
Breach×Post	0.805**	0.536***	1.16**	0.966***
	(2.31)	(4.29)	(2.13)	(3.69)
Controls	No	Yes	No	Yes
Issuer×Event FEs	Yes	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes	Yes
Observations	970	970	970	970
Adj R^2	0.323	0.913	0.377	0.814
Panel C: Control Group of Non-Breached Issuers in Same County				
Breach×Post	0.641**	0.513*	0.988*	0.829**
	(2.32)	(1.90)	(1.82)	(2.08)
Controls	No	Yes	No	Yes
Issuer×Event FEs	Yes	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes	Yes
Observations	2,810	2,810	2,810	2,810
Adj R^2	0.424	0.843	0.360	0.723