Hacked to Pieces?
The Effects of Ransomware Attacks on Hospitals and Patients

Claire C. McGlave, MPH
Hannah T. Neprash, PhD
Sayeh S. Nikpay, PhD*

ABSTRACT

As cybercriminals increasingly target healthcare, hospitals face the growing threat of ransomware attacks. Ransomware is a type of malicious software that prevents users from accessing electronic systems and demands a ransom to restore access. In this paper, we create and link a database of hospital ransomware attacks to Medicare administrative claims data. We quantify the effects of ransomware attacks on hospital operations and patient outcomes. Ransomware attacks decrease hospital volume by 17-25% during the initial attack week, reducing revenue even further. We find that ransomware attacks increase in-hospital mortality for patients who are already admitted at the time of attack.

KEYWORDS: Hospitals, Cybersecurity, Health Care

JEL CLASSIFICATION: H51, I10, I11, I18, L86

*McGlave: University of Minnesota (email: mcgl0066@umn.edu); Neprash: University of Minnesota (email: hneprash@umn.edu); Nikpay: University of Minnesota (email: snikpay@umn.edu). We thank Eric Barette, Mike Chernew, Betsy Cliff, Dori Cross, David Cutler, Ezra Golberstein, Katherine Hicks-Courant, Peter Huckfeldt, Jared Huling, Rob Huckman, Karen Joynt Maddox, Amol Navathe, Michael Puskarich, Alan Rozenshtein, Aaron Schwartz, Nicholas Tilipman, Beth Virnig, and seminar participants at ASHEcon and the Midwest Health Economics Conference at DePaul University for useful feedback. Research reported in this publication was supported by the NIHCM Foundation.

I. Introduction

Spending on hospital care represents nearly 7% of GDP in the United States (CDC 2023, CMS.gov 2023). Hospitals increasingly rely on interconnected electronic systems to deliver care (Adler-Milstein, DesRoches et al. 2015). These include everything from electronic health records to remote patient monitoring technology, sophisticated imaging equipment, and telemedicine platforms. As this technological sophistication and interconnectedness has increased, so has vulnerability to cyberattacks, which rose dramatically during the COVID-19 pandemic (CISA 2020). Ransomware attacks are the most common form of cyberattack, wherein cybercriminals install malicious software that prevents users from accessing their electronic systems and demand a ransom to restore access (Federal Bureau of Investigation 2021). During a ransomware attack, cybercriminals motivate payment of the ransom by threatening to release stolen data, severely disrupting business operations, or both. These strategies have found fertile ground in hospital settings, where data include patient financial and medical information, and operational disruptions threaten the ability to provide safe and timely care (Decker, Wood et al. 2023).

In this paper, we examine the effects of hospital ransomware attacks on patient care and health outcomes. Since news coverage of these attacks frequently documents operational disruptions such as electronic health record downtime, canceled or delayed care, and ambulance diversion, one might presume that ransomware attacks on hospitals would be harmful to the health of patients. However, a large literature in health economics documents overtreatment – particularly in hospitals and ERs – without evidence of improvements in patient health (Fisher, Wennberg et al. 2003, Fisher, Wennberg et al. 2003, Baicker and Chandra 2004, Danagoulian, Grossman et al. 2020). This literature suggests that a decrease in treatment intensity due to a ransomware attack may not necessarily harm patients. Taken together, these bodies of literature suggest that the expected impact of hospital ransomware attacks on patients' health outcomes is ambiguous.

To address this question, we create a novel dataset of ransomware attacks on healthcare providers and link it to fee-for-service Medicare administrative claims data (Neprash, McGlave et al. 2022). We exploit the staggered and plausibly exogenous timing of hospital ransomware attacks to identify their causal effect on hospital operations and patient outcomes. We compare outcomes before and during ransomware attacks in the attacked versus control hospitals.

Our results are striking: during the initial week of a ransomware attack, hospital volume falls by 17-25 percent in the ER, inpatient, and outpatient settings. Medicare revenue declines 19-41 percent at ransomware-attacked hospitals. We find limited evidence that case mix changes at ransomware-attacked hospitals, though we do observe a decrease in the share of patients admitted for acute cardiovascular events. Ransomware attacks increase the in-hospital mortality rate for patients already admitted to ransomware-attacked hospitals on the date of attack discovery. Mortality effects are most pronounced for patients at hospitals experiencing particularly severe ransomware attacks and for Black patients.

We find that ransomware attacks imposed considerable externalities on non-attacked neighboring hospitals. When we compare market-level event study results to hospital-level results, we find minimal evidence of a decrease in market-level hospital volume. This implies that nearby non-attacked hospitals absorb most of the displaced patient volume from the attacked hospital during a ransomware attack. However, we document no evidence of an increase in mortality for patients admitted to non-attacked neighboring hospitals. While only a small share (i.e., roughly four percent) of U.S. hospitals experienced a ransomware attack between 2016 and 2021, our findings suggest that 1 in 4 hospital markets experienced spillover effects from a ransomware attack during our study period.

To our knowledge, this is the first paper to study the effects of ransomware attacks on any industry, including health care. This paper contributes to the literature studying the causal effects of capacity strain (of which ransomware attack is just one example) in health care. The capacity literature is modest due to the challenge of obtaining causal estimates, given the endogeneity between capacity and utilization of healthcare services. Existing papers largely exploit variation in supply that is unrelated to patient demand, or vice versa, finding mixed results for patient health outcomes. One recent analysis exploits plausibly exogenous variation in emergency admissions to document an increase in the likelihood of unplanned hospital readmission as an effect of hospital crowding (Hoe 2022). Studying primary care provision in Senegal, researchers find no evidence of lower care quality during times of exogenously high workload (Kovacs and Lagarde 2022). In contrast, an older analysis of nursing strikes at hospitals documents a large increase in mortality and hospital readmissions – a pattern attributed by the authors to lower quality of patient care during a time of capacity strain (Gruber and Kleiner 2012). A subset of this literature has focused more specifically on disparities in health outcomes, finding evidence that Black patients' health suffers more than white patients' health during times of capacity strain (Gourevitch, Plough et al. 2019, Singh and Venkataramani 2022). Some studies within this literature have used granular electronic health record data to show that these disparities are likely driven by additional biases in clinician decision-making, hospital processes, and/or allocation of health care resources that emerge or worsen as capacity strain increases (Singh and Venkataramani 2022).

This paper also joins a mixed literature on the marginal value of medical care. Using a regression discontinuity design, a canonical analysis finds large returns (i.e., mortality reductions) to medical spending in the neonatal intensive care units (Almond, Doyle et al. 2010), while a more recent paper on marginally diagnosed patients with diabetes find no sustained improvements due to higher spending in clinical measures of health (Alalouf, Miller et al. 2023). Other studies have relied on natural experiments to identify the causal effect of more or less intensive medical treatment. Comparing mortality among patients admitted to the hospital for acute cardiovascular care during national cardiology meetings (i.e., when less senior physicians were working) compared to non-meeting dates, researchers found that patients were less likely to receive intensive treatment without any effect on mortality (Jena, Prasad et al. 2015). Exploiting the exogenous timing of unannounced hospital accreditation visits, researchers found lower mortality rates for patients hospitalized during weeks when hospitals experienced safety inspections and presumably increased their intensity of care, compared to non-inspection weeks (Barnett, Olenski et al. 2017).

Finally, this paper joins a modest, predominantly clinical, literature studying data breaches in health care. These papers have relied largely on public data on data breaches affecting health care providers and other entities covered by the Health Insurance Portability and Accountability Act (HIPAA). As such, it includes a very wide range of data breaches (e.g., misplaced laptops, inappropriate record access, cyberattack). Using this public data source, researchers document an increase in data breaches over the past decade (Bai, Jiang et al. 2017, McCoy and Perlis 2018), with one quasi-experimental paper finding that hospital quality deteriorates following a breach (Choi, Johnson et al. 2019). We add to this literature by using a novel data source limited exclusively to ransomware attacks (i.e., a form of cyberattack designed specifically to maximally disrupt business operations), rather than the universe of data breaches. In summary, this analysis advances the existing literature by using a novel dataset to pursue the first quasi-experimental analysis of ransomware attacks in any industry. It combines multiple datasets to examine the impact of attacks on hospitals and their patients.

II. Background

Ransomware Activity in the Health Care Sector

The Federal Bureau of Investigation defines ransomware as “a type of malicious software, or malware, that prevents you from accessing your computer files, systems or networks and demands you pay a ransom for their return” (Federal Bureau of Investigation 2021). Ransomware attacks have been a cybersecurity threat across a variety of sectors for years, however their increasing prevalence in the healthcare sector coincided largely with the COVID-19 pandemic (CISA 2020). From 2016 to 2021, ransomware attacks on healthcare providers more than doubled (Neprash, McGlave et al. 2022) and current law enforcement estimates suggest a continuation of that trend.

The US healthcare sector is especially vulnerable to ransomware attacks. Clinicians rely on many electronic systems, including electronic health records (EHRs), imaging technology, medication dispensing systems, patient monitoring technology, telehealth platforms, and other tools essential to patient care. While disruptions to these systems likely affect care delivery in every clinical setting, we focus on hospitals in this paper – as this is likely where ransomware attack-induced disruptions have the most potential for harm, due to the severity of conditions treated in hospitals settings.

News coverage of prominent ransomware attacks on US hospitals documents chaotic disruptions to healthcare delivery. Describing an attack on Universal Health Services (UHS) in 2020, a clinical staff member working at the time said, “We are using paper for everything. All computers are completely shut down” (Newman 2020). Another employee at a UHS hospital said, “As of right now, we have no access to any patient files, history, nothing…doctors aren’t able to access any type of X-rays, CT scans” (Bajak and Alonso-Zaldivar 2020). Reflecting on a ransomware attack that disabled chemotherapy infusion technology, a nurse at the University of Vermont Medical Center said she could compare the past few weeks to only one experience – working in a burn unit following the Boston Marathon bombing (Barry and Perlroth 2020). During a 2022 ransomware attack on CommonSpirit Health (the second-largest hospital chain in the US), ER nurses at St. Michael Medical Center in Silverdale, Washington reportedly called 911 to request assistance, saying that they were “drowning” in patients without the capacity to care for them (Pilling 2022). While these examples are striking, it is important to note tremendous variation in the severity of ransomware attacks on hospitals – with many attacks reportedly causing much more limited or no organizational disruptions whatsoever (Neprash, McGlave et al. 2022).

Despite this paper’s focus on hospital victims within the United States, cybercrime is a global industry. A common business model for ransomware perpetrators is ransomware-as-a-service (RaaS), wherein ransomware operators write malicious software and affiliates pay to launch ransomware attacks. While the RaaS business model doesn’t fully homogenize all ransomware attacks, it does create many similarities between - and repeat uses of – malicious ransomware code. Methods for infiltrating a target organization’s electronic infrastructure are constantly evolving, but typically rely on phishing email campaigns (i.e., emails appearing to come from trusted sources, but actually infecting a user’s computer with malware if they click on a link) or intentional exploitation of known security vulnerabilities in widely used software (Decker, Wood et al. 2023). Both strategies have worked effectively on hospital targets, where a large number of employees frequently exchange email and other electronic communication without a focus on identifying phishing attempts – and legacy software applications may not be updated or patched with appropriate frequency (Gordon, Wright et al. 2019). Additionally, the strain on hospitals resulting from the novel COVID-19 pandemic appears to have expanded opportunities for cyberattack due to the stress placed on health care providers and the rapid adoption of less-than-secure telehealth platforms. Documents obtained by journalists and law enforcement show an intentional strategy on the part of large ransomware actors (e.g., Trickbot) to target the health care sector during COVID-19 (Burgess 2022).

III. Data and Empirical Approach

Data

We rely primarily on data from two sources: a 100% sample of Medicare administrative claims data for fee-for-service enrollees and the Tracking Healthcare Ransomware Events and Traits (THREAT) database. While Medicare claims are used extensively in the health economics literature, the latter is a novel resource built by this study team. Together, these data sources enable us to identify ransomware-attacked hospitals (as well as non-attacked hospitals located nearby) and track outcomes of interest before and after attacks.

THREAT Database

The THREAT database is a comprehensive list of ransomware attacks on healthcare providers, occurring between January 1, 2016 and December 31, 2021 (Neprash, McGlave et al. 2022). This dataset combines proprietary information from HackNotice (a cybersecurity threat intelligence monitoring company that helps businesses identify and respond to attacks) with data from the US Department of Health and Human Services Office of Civil Rights (HHS OCR) Data Breach Portal. The latter contains publicly available information that is collected when HIPAA-covered entities report breaches of protected health information, as mandated by the Health Information Technology for Economic and Clinical Health Act of 2009. Finally, we catalog news coverage and public disclosures of operational disruptions occurring during each ransomware attack. Common disruptions include ambulance diversion (i.e., a protocol by which ERs instruct ambulances to deliver patients to other facilities), canceled appointments or surgeries, and electronic system downtime (i.e., typically electronic health records, but sometimes also imaging technology). Additional details on protocols for creation and validation of the THREAT database have been published elsewhere (Neprash, McGlave et al. 2022).

The THREAT database identifies 374 distinct ransomware attacks on health care providers occurring from 2016 to 2021. Of these, 74 attacks affected a total of 163 U.S. hospitals. Appendix figure A.1 plots the distribution of attacked hospitals over time. Aligning with past descriptive work and warnings from the federal government, ransomware attacks on hospitals are increasing in frequency during the study period (CISA 2020, Cybersecurity & Infrastructure Security Agency 2021, Neprash, McGlave et al. 2022).

Fee-for-Service Medicare Claims Data

This study uses research-identifiable files containing 2016-2021 claims data for Medicare fee-for-service enrollees (ResDAC 2023). Various measures rely on claims in the Inpatient, Outpatient, and Carrier Files (i.e., physician services), in addition to the Medicare Beneficiary Summary Files. We link the THREAT database to Medicare claims using the Medicare CMS Certification Number, which uniquely identifies hospitals.

Data on Hospital Characteristics

To quantify hospital characteristics, we rely on data from the American Hospital Association (AHA) Annual Survey. Hospital characteristics of interest from the AHA survey include system membership, presence of an ER and/or obstetric unit, and designation as a Critical Access Hospital, Sole Community Hospital, or Rural Referral Center. Additionally, the AHA survey provides hospital address information, from which we are able to identify its tertiary market (defined as a Hospital Referral Region) and state.

Measures of Hospital Operations

To test for changes in hospital operations during ransomware attacks, we calculate Medicare volume (inpatient, outpatient, and ER) and Medicare revenue at the hospital-week (and market-week) level. Since Medicare sets prices administratively, any difference between revenue and volume reflects differences in the intensity of treatment provided and the case mix of admitted patients.

Additional measures of hospital operations include the count of ER visits arriving via ambulance - as indicated by an ambulance claim on the same day (Barosso 2015, ResDAC 2017), the share of ER evaluation and management visits billed at the highest possible intensity levels (i.e., levels 4 or 5), the count of elective versus non-elective admissions (Gluckman, Spinelli et al. 2020, Ly, Blegen et al. 2023), the average length of inpatient stay (i.e., the number of days elapsed from inpatient admission to discharge) for discharges to home, the count of clinicians providing services, and the count of outpatient visits by service type. We use the Berenson-Eggers Type of Service taxonomy to classify visits based on whether they included eight types of health care services: anesthesia, durable medical equipment, evaluation and management, imaging, procedures, treatments, tests, and other (Templeman, Field et al. 2021).

Measures of Case Mix

To test for changes in the types of patients treated during ransomware attacks, we calculate four weekly measures in both the ER and inpatient settings: the average age of patient treated, the average number of chronic conditions recorded (in the previous calendar year) for patients treated, and the share of patients treated who were dually eligible for Medicare and Medicaid. In both settings, we additionally calculate the share of patients treated for acute cardiovascular emergencies (i.e., heart attack, stroke, and sepsis), using diagnosis codes recorded on ER and inpatient claims. For inpatient admissions, we also calculate the average Diagnosis Related Group (DRG) weight across all inpatient admissions initiated during a given week. Since the DRGs coding scheme increases with severity of illness and complexity of patient care, an increase in this measure suggests an increase in the burden of illness among patients admitted to any given hospital.

Measures of Patient Outcomes

Using Medicare data, we quantify two widely-used health outcomes: mortality and hospital readmission. We identify in-hospital mortality via the discharge status listed on each inpatient admission and ER claim – and mortality within 30 days of inpatient discharge based on whether each inpatient admission had a death date listed for that patient (in the Medicare Beneficiary Summary File) within 30 days of inpatient discharge. Patients are considered to be readmitted if they have any inpatient hospital admission claims (at any hospital) within 30 days of their live inpatient discharge.

Empirical Approach

Hospital- and Market-Level Analysis

Our research design exploits the staggered and plausibly random timing of ransomware attacks to identify the effect on hospital operations and patient outcomes. There are two factors that could predict ransomware attacks: characteristics of the specific hospitals that are attacked, and relative timing of those attacks. We test whether ransomware attacks appeare to be random by predicting attacks based on hospital characteristics. We find that ransomware-attacked hospitals are higher volume, more likely to operate an obstetric unit, and less likely to be rurally located than hospitals that did not experience ransomware attacks from 2016 to 2021 (Appendix Table A.1). However, no observable hospital characteristics consistently predict the *timing* of ransomware attacks, conditional on experiencing an attack. We test this assumption by comparing time-variant hospital characteristics across weeks leading up to a ransomware attacks. We show that inpatient visit volume, revenue, and mortality rates do not differ in the weeks preceding a ransomware attack (Appendix Table A.2).

For each of the 74 ransomware attacks involving hospitals, we define attacked hospital(s) as treated. Attacks frequently involve more than one hospital. Control hospitals are other short-term acute care hospitals providing general medical and surgical services in the same state as the attacked hospital(s), but not the same Hospital Referral Region (HRR). By carving out attacked hospitals' nearest neighbors (i.e., those in the same HRR), we avoid including hospitals subject to spillover effects during a ransomware attack – such as an inflow of ER patients when a ransomware-attacked hospital engages ambulance diversion protocol. While such spillovers are of interest themselves, including them would likely be a violation of the stable unit treatment value assumption. Additionally, restricting the control group to hospitals in the same state ensures that treated and control hospitals are exposed to the same state-level policy licensure restrictions that may affect the types of care provided at each hospital.

As an alternative specification, we again define treated hospitals as those experiencing the current ransomware attack. Control hospitals are those that experience an attack more than five weeks in the future. This specification directly leverages the random timing of attacks and is similar to other recent stacked event study designs (Deshpande and Li 2019). However, it is less ideal for our setting, given the concentration of ransomware attacks in the later years (i.e., 2020 and 2021) of our study period (Figure A.1).

For the set of treated and control hospitals in every attack, we calculate event weeks relative to the date of ransomware attack discovery (i.e., this is typically the date that data are encrypted and/or systems are disabled and the hospital receives a ransom demand). We include data from the five weeks and after the date of attack discovery. Having constructed a separate version of this claims dataset for each of our 74 ransomware attacks, we append all datasets together - yielding 1,468 hospital-week observations for treated hospitals and 75,747 hospital-week observations for control hospitals. To implement our stacked event study design, we estimate the following equation:

(1) $Y_{hat} = \propto_h + \gamma_t + I_{at}^{\tau} + \sum_{\tau=-5}^{4} \delta_\tau (Attacked_h \times I_{at}^{\tau}) + \epsilon_{hat}$

where Y_{hat} is an outcome for hospital *h* involved in ransomware attack *a* in week t. $\propto_h$ are hospital fixed effects, which control for time-invariant differences between attacked and non-attacked hospitals. γ_t are calendar-week-by-year fixed effects to control for seasonality and time trends in outcome variables (especially important since the study period includes the COVID-19 pandemic – a time of tremendous fluctuations in hospital volume and operations).

The I_{at}^{τ} are indicators equal to 1 if quarter t is τ weeks after (or before, if negative) the week of the ransomware attack discovery date and 0 otherwise. The variable $Attacked_h$ equals 1 if the hospital experienced a ransomware attack and 0 otherwise. As such, $\tau = 0$ represents the first week following the discovery of the ransomware attack and $\tau = -1$ describes the week prior to the ransomware attack. We weight observations by each hospital's count of Medicare admissions during the year preceding the attack. The coefficients of interest are δ_τ, which quantify the difference between treated and control hospitals in the outcome Y_{hat}, τ quarters after the ransomware attack. The figures presented in the results section plot the δ_τ estimates in event time. We cluster standard errors at the attack level (i.e., 74 clusters), as that is the level of variation in our data.

In addition to the hospital-level analysis, we also conduct a stacked event study at the market (i.e., HRR) level. The former identifies the effect of ransomware attacks on the attacked facilities themselves, while the latter accounts for any spillover effects on non-attacked hospitals in the same market. Treated markets are defined as any HRR containing a ransomware-attacked hospital, while control markets are defined as other HRRs in the same state as an attacked hospital, but not directly containing an attacked hospital. Market-level analyses use an estimating equation similar to equation 1, but indexed at the market, rather than hospital level:

$$(2)\ Y_{mat} = \propto_m + \gamma_t + I_{at}^{\tau} + \sum_{\tau=-5}^{4} \delta_\tau (Attacked_m \times I_{at}^{\tau}) + \epsilon_{mat}$$

where Y_{mat} is an outcome for market *m* involved in ransomware attack *a* in week t. $\propto_m$ are market fixed effects and γ_t are calendar-week-by-year fixed effects. The coefficients of interest were again δ_τ – quantifying the difference between treated and control hospital markets in the outcome Y_{mat}, τ quarters after the ransomware attack.

Admission-Level Analysis

For measures of health outcomes (i.e., mortality and hospital readmission) – which remain at the admission-level because they cannot be neatly aggregated to the hospital-week level – we estimate the following difference-in-differences equation:

$$(3)\quad Y_{ihat} = \propto_h + \gamma_t + AlreadyAdmittedAtAttackStart_{ihat} + Attacked_{ha} + AlreadyAdmittedAtAttackStart_{ihat} \times Attacked_{ha} + X_{ihat} + \epsilon_{ihat}$$

Y_{ihat} is a binary outcome (e.g., 30-day mortality) for admission *i* at hospital *h* involved in ransomware attack *a* at time *t.* $\propto_h$ are hospital fixed effects. γ_t are day-of-the-week, calendar month, and year fixed effects. The first difference is captured by $AlreadyAdmittedAtAttackStart_{ihat}$, which equals 1 if the admission had already started (and not yet concluded) on the date of ransomware attack discovery and 0 if the admission concluded prior to the attack. This variable is populated based on attack date for every admission at the attacked hospital and hospitals within the same state. We note that we expect patients admitted at the start of each ransomware attack to be sicker than patients admitted in the five weeks prior to the attack. This is due to the sample construction requirement that the former group be admitted prior to the attack and discharged on or after the date of attack discovery, while the latter group is required to have been admitted prior to the attack and discharged prior to the attack. However, the main effect in the difference-in-differences estimating equation will absorb this difference in patient severity.

The second difference is captured by $Attacked_{ha}$, which equals one if the admission occurred at the hospitals that experience ransomware attack *a*, and 0 if the admission occurred at non-attacked hospitals in the same state. In an alternative specification, we use admissions at hospitals experiencing attacks five or more weeks in the future as controls for currently attacked admissions. In both cases, we note that $Attacked_{ha}$ is not collinear with hospital fixed-effects because the same hospital can appear as a non-attacked (i.e., control) and attacked (i.e., treated) hospital in the data at different times.

The coefficient on the interaction term $AlreadyAdmittedAtAttackStart_{ihat} \times Attacked_{ha}$ represents the differential health effect of already being admitted at the time of attack to a ransomware-attacked hospital. X_{ihat} is a vector of admission-level characteristics, including patient age, patient sex, patient race, whether the patient is dually eligible for Medicaid and Medicare, chronic condition count in the year prior to admission, whether the admission involves treatment in the intensive care unit, whether the admission is elective, whether the admission involves a primary diagnosis of acute cardiovascular event including heart attack, sepsis, or stroke (since these are common diagnoses that require timely treatment), and DRG weight (i.e., a standardized measure of treatment intensity and resource use).

As in the event study analysis, we include only admissions starting five or fewer weeks prior to the attack and we exclude admissions at non-attacked hospitals in the same hospital referral region (again to avoid spillover effects). We cluster standard errors at the ransomware attack level. A causal interpretation of the interaction term in this difference-in-differences model relies on the belief that hospitals cannot anticipate the timing of a ransomware attack and adjust their patient population in advance (see Appendix Table A.2 for evidence supporting this assumption).

As an alternative control group, we compare admissions at ransomware-attacked hospitals to contemporaneous admissions at hospitals experiencing ransomware attacks in the future. We also test for a differential mortality effect among admissions starting during the initial week of a ransomware attack, at attacked versus non-attacked hospitals. This estimating equation is identical to Equation 3 except that we substitute $AdmittedDuringInitialAttackWeek_{ihat}$ (equal to 1 if the admission started during the first seven days after attack discovery date) for $AlreadyAdmittedAtAttackStart_{ihat}$. We omit admissions where patients are still hospitalized at the start of the attack, yielding a comparison group of admissions that conclude prior to each ransomware attack. Despite controlling for observable patient- and admission-level characteristics, a causal interpretation of the interaction term in this modified specification of Equation 3 is more difficult, since hospitals likely adjust their patient mix during a ransomware attack in ways that are correlated with health outcomes.

IV. Results

Effect of Ransomware Attacks on Attacked Hospitals

We first analyze the effect of experiencing a ransomware attack on hospital operations. Figure 1 shows an immediate decline in ER, inpatient, and outpatient hospital volume during the initial week of a ransomware attack. Depending on the setting, the initial volume reduction ranges from 16.7% to 25.4%. However, volume in all hospital settings recovers to pre-attack levels within two to three weeks. Reductions in volume correspond to reductions in Medicare revenue, ranging from 19.2% to 40.6%, across hospital settings. Figure A.2 repeats Figure 1 using the alternative control group of hospitals experiencing future ransomware attacks – finding very similar volume and revenue reduction patterns.

Table A.3 presents estimates for additional, more granular, measures of hospital operations, which delivers a detailed understanding of the overall effects on volume and revenue. Decomposing inpatient admission volume into elective and non-elective admissions reveals that the overall decrease in admissions volume is driven solely by a decrease in non-elective admissions (Table A.3). Decomposing the outpatient revenue impact by type of service reveals the largest decrease in revenue from imaging service, which declines an average of 44.1% in the initial ransomware attack week (Table A.3). Additional reductions appear in the number of ER visits arriving via ambulance and ER visit intensity. During a ransomware attack, hospitals treat 26.2% fewer patients arriving at the ER via ambulance – which is consistent with frequent decisions to divert ambulances during this event. Other measures of hospital operations such as clinical staffing levels do not change differentially during an attack at attacked versus control hospitals.

Given the dramatic decrease in hospital volume during the initial weeks of a ransomware attack, we next investigate whether the types of patients treated (i.e., patient case mix) changed (Table 1). In the ER setting, we find little evidence of a case mix change during ransomware attacks. Measures of inpatient case mix also show few changes during a ransomware attack. However, the share of patients hospitalized for acute cardiovascular events decreases by 1.71 percentage points (an 11.6% decrease relative to baseline) during the initial attack week.

Effect of Ransomware Attacks on Attacked Markets

The effect of ransomware attacks may extend beyond attacked hospitals - potentially affecting the entire hospital market, if nearby hospitals absorb displaced patient demand. In this section, we present stacked event study results at the HRR-week level. Any difference between hospital-level and market-level results indicates spillover effects of the ransomware attack on non-attacked hospitals nearby.

Market-level results regarding patient volume and Medicare revenue reveal considerable spillover effects for non-attacked hospitals in the same HRR as an attacked hospital. Figure 2 shows that market-level ER visit volume and revenue remains unchanged during the first five weeks of a ransomware attack. Comparing that estimate with the sizeable reduction in ER volume observed at attacked hospitals, we conclude that nearby hospitals absorb nearly all displaced ER volume during a ransomware attack. Nearby non-attacked hospitals also absorb displaced inpatient volume, though market-level inpatient revenue still falls by 4.4% (significant at $P<0.1$) during the initial attack week. We find little evidence to suggest that ER or inpatient hospital admission case mix changes at the market level, during a ransomware attack (Table A.4).

Effect of Ransomware Attacks on Patient Health Outcomes

Panel A of Table 2 presents the results of Equation 3, comparing health outcomes for patients hospitalized at the time of attack (rather than discharged in the five weeks prior), at attacked and non-attacked hospitals. We find a marginally statistically significant (P=0.07) differential increase in in-hospital mortality of 0.77 percentage points for patients of ransomware-attacked hospitals who are hospitalized at the time of the attack. Compared to the in-hospital mortality rate of patients discharged in the five weeks prior to attack, this represents a 20.7% relative increase in in-hospital mortality. We find no similar increase for 30-day mortality, nor for 30-day readmissions.

Repeating the analysis using contemporaneous admissions at subsequently-attacked hospitals as a control group, we find similar, though slightly larger, results (Panel B of Table 2). In-hospital mortality for patients already admitted to treated hospitals at the start of the attack increases differentially by 1.2 percentage points relative to patients already admitted at control hospitals (a 36.0% relative increase). We find no similar increase for 30-day mortality, nor for 30-day readmissions. Repeating the analyses with both control groups, but omitting the two largest attacks (i.e., one attack affecting 11 hospitals and another affecting 22 hospitals) yields very similar results (Table A.5) – ruling out the possibility that a single large attack drives our findings.

Focusing specifically on the most severe ransomware attacks (i.e., the 31 attacks where news coverage documented ambulance diversion and/or delays for scheduled care), we find larger in-hospital mortality effects (Table 3). In-hospital mortality for patients already hospitalized at a ransomware-attacked hospital increases between 1.28 and 1.87 percentage points (depending on the control group used) – representing a 35.9-55.3% relative increase when compared to the pre-attack mean.

We also find a disproportionate in-hospital mortality effect for already-admitted Black patients (Table A.6). In-hospital mortality for patients already hospitalized at a ransomware-attacked hospital increases by 2.20 and 2.27 percentage points (a relative increase of 61.8-73.0%). We find no similar increase in 30-day mortality or 30-day readmissions.

Table A.7 presents the result of a modified Equation 3, comparing health outcomes for patients admitted during the first week of ransomware attack (rather than discharged in the five weeks prior), at attacked and non-attacked hospitals. We find an in-hospital mortality differential increase of 0.43-0.54 percentage points for patients of ransomware-attacked hospitals who are admitted during the initial attack week (a 12.6-14.5% relative increase). We find no similar increase for 30-day mortality, nor for 30-day readmissions.

Finally, we repeat our analyses for neighboring hospitals (i.e., any non-attacked hospital in the same HRR) that did not themselves experience an attack. The previous section's comparison of hospital-level and market-level event study findings suggests that these hospitals absorb much of the displaced hospital volume during ransomware attacks. However, we find no evidence of increased mortality or readmission rates for patients already admitted to neighboring non-attacked hospitals at the time of attack nor patients admitted during the first week (Table A.8).

V. Discussion

In this paper, we provide the first empirical evidence on the effect of ransomware attacks on hospital operations and health outcomes. We find that ransomware attacks immediately affect hospital operations - causing large reductions in ER, inpatient, and outpatient hospital volume and even larger reductions in Medicare revenue for care provided. The latter finding likely reflects diminished capacity to provide certain types of care for patients who are treated during ransomware attacks, due to outages in the electronic systems required to render certain services (i.e., imaging services, drug infusions). To contextualize these estimates, we note that they are more than half the volume reduction experienced by the average U.S. hospital during the initial month of the COVID-19 pandemic (Heist, Schwartz et al. 2021). While large, these effects are temporary, with a return to pre-attack levels occurring within a few weeks of the ransomware attack. A back-of-the-envelope calculation using these estimates suggests that the average hospital loses ½ to 1% of their annual operating revenue during a ransomware attack.[1] Assuming no change to hospital cost structures in the year of the attack – a conservative assumption, given our inability to include additional post-attack expenditures related to investigation and/or legal fees – this has serious implications for hospital profit margins, most of which are in the low single digits.

In addition to drastically reducing hospital volume and revenue, ransomware attacks increase the likelihood of in-hospital mortality for patients already admitted on the date of attack discovery. The magnitude of this mortality effect was large, but comparable to effects observed in other examples of capacity strain, such as nursing strikes (Gruber and Kleiner 2012). Mortality effects are most pronounced for patients at hospitals experiencing the most severe ransomware attacks and for patients of color. The latter finding is consistent with an emerging literature showing that underserved patient populations

[1] The average U.S. short-term acute care hospital providing general medical and surgical services (according to the AHA survey) reported annual net operating revenue of $228 million in 2019. This implies weekly net operating revenue of $4.4 million. Using hospital-reported service-specific breakdowns of overall charges, we estimate that inpatient care accounts for 57% ($2.5m) of net operating revenue for the average hospital, while outpatient accounts for 31% ($1.4m), ED accounts for 3% ($145k), and other services (i.e., post-acute care) account for the remaining 9% ($382k). We then applied the event study coefficient estimates for the initial weeks of a ransomware attack to these numbers, resulting in an estimate of $1.5m lost revenue due to ransomware attack. This represents 0.66% of annual net operating revenue for the average hospital.

bear the brunt of the negative consequences when health care providers experience capacity strain (Singh and Venkataramani 2022).

The mortality consequences of ransomware attacks will not surprise some in the cybersecurity and law enforcement communities, where ransomware attacks are viewed as “threat to life” crimes. However, quantifying the harm to hospitals and patients from ransomware attacks underscores the importance of policy action to reduce the incidence of ransomware attacks in health care. This should be a combination of policies designed to reduce the likelihood of any successful ransomware attacks (e.g., minimum cybersecurity standards for hospitals) and policies designed to reduce the severity of ransomware attacks when they do happen (e.g., incident planning requirements).

REFERENCES

Adler-Milstein, J., C. M. DesRoches, P. Kralovec, G. Foster, C. Worzala, D. Charles, T. Searcy and A. K. Jha (2015). "Electronic Health Record Adoption In US Hospitals: Progress Continues, But Challenges Persist." Health Affairs **34**(12): 2174-2180.

Alalouf, M., S. Miller and L. R. Wherry (2023). "What Difference Does a Diagnosis Make? Evidence from Marginal Patients." American Journal of Health Economics.

Almond, D., J. J. J. Doyle, A. E. Kowalski and H. Williams (2010). "Estimating Marginal Returns to Medical Care: Evidence from At-Risk Newborns." Quarterly Journal of Economics **125**(2): 591-634.

Bai, G., J. X. Jiang and R. Flasher (2017). "Hospital Risk of Data Breaches." JAMA internal medicine **177**(6): 878-880.

Baicker, K. and A. Chandra (2004). "Medicare spending, the physician workforce, and beneficiaries' quality of care." Health Aff (Millwood) **Suppl Web Exclusives**: W4-184-197.

Bajak, F. and R. Alonso-Zaldivar. (2020, September 29, 2020). "Suspected ransomware attack hobbles major hospital chain's U.S. facilities." PBS News Hour, from https://www.pbs.org/newshour/nation/suspected-ransomware-attack-hobbles-major-hospital-chains-u-s-facilities.

Barnett, M. L., A. R. Olenski and A. B. Jena (2017). "Patient Mortality During Unannounced Accreditation Surveys at US Hospitals." JAMA Internal Medicine **177**(5): 693-700.

Barosso, G. (2015). How to Identify Hospital Claims for Emergency Room Visits in the Medicare Claims Data, ResDAC.

Barry, E. and N. Perlroth (2020). Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack. New York Times.

Burgess, M. (2022). Inside Trickbot, Russia's Notorious Ransomware Gang. Wired.

CDC. (2023). "Health Expenditures." from https://www.cdc.gov/nchs/fastats/health-expenditures.htm.

Choi, S. J., M. E. Johnson and C. U. Lehmann (2019). "Data breach remediation efforts and their implications for hospital quality." Health Services Research **54**(5): 971-980.

CISA, F., HHS, (2020). "Joint Cybersecurity Advisory: Ransomware Activity Targeting the Healthcare and Public Health Sector."

CMS.gov. (2023). "NHE Fact Sheet." from https://www.cms.gov/research-statistics-data-and-systems/statistics-trends-and-reports/nationalhealthexpenddata/nhe-fact-sheet.

Cybersecurity & Infrastructure Security Agency (2021). Provide Medical Care Is In Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm.

Danagoulian, S., D. S. Grossman and D. Slusky (2020). "Office Visits Preventing Emergency Room Visits: Evidence From the Flint Water Switch." NBER Working Paper 27098.

Decker, E., R. Wood, S. Mohiuddin, D. Nock and A. Venugopalan (2023). Hospital Cyber Resiliency Initiative Landscape Analysis. HHS 405(d), Department of Health and Human Services.

Deshpande, M. and Y. Li (2019). "Who Is Screened Out? Application Costs and the Targeting of Disability Programs." American Economic Journal: Economic Policy **11**(4): 213-248.

Federal Bureau of Investigation. (2021). "Ransomware." Retrieved October 9, 2021, 2021, from https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware.

Fisher, E. S., D. E. Wennberg, T. A. Stukel, D. J. Gottlieb, F. L. Lucas and E. L. Pinder (2003). "The implications of regional variations in Medicare spending. Part 1: the content, quality, and accessibility of care." Ann Intern Med **138**(4): 273-287.

Fisher, E. S., D. E. Wennberg, T. A. Stukel, D. J. Gottlieb, F. L. Lucas and E. L. Pinder (2003). "The implications of regional variations in Medicare spending. Part 2: health outcomes and satisfaction with care." Ann Intern Med **138**(4): 288-298.

Gluckman, T. J., K. J. Spinelli, M. Wang, A. Yazdani, G. Grunkemeier, S. M. Bradley, J. H. Wasfy, A. Goyal, A. Oseran and K. E. Joynt Maddox (2020). "Trends in Diagnosis Related Groups for Inpatient Admissions and Associated Changes in Payment From 2012 to 2016." JAMA Network Open **3**(12): e2028470-e2028470.

Gordon, W. J., A. Wright, R. Aiyagari, L. Corbo, R. J. Glynn, J. Kadakia, J. Kufahl, C. Mazzone, J. Noga, M. Parkulo, B. Sanford, P. Scheib and A. B. Landman (2019). "Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions." JAMA Network Open **2**(3): e190393-e190393.

Gourevitch, R. A., A. Plough, K. Donato and N. Shah (2019). "Who Is Harmed When Labor Floors Are Busy? A Racial Disparities Analysis." Obstetrics & Gynecology **133**.

Gruber, J. and S. A. Kleiner (2012). "Do Strikes Kill? Evidence from New York State." American Economic Journal: Economic Policy **4**(1): 127-157.

Heist, T., K. Schwartz and S. Butler (2021). Trends in Overall and Non-COVID-19 Hospital Admissions. Kaiser Family Foundation.

Hoe, T. P. (2022). "Does Hospital Crowding Matter? Evidence from Trauma and Orthopedics in England." American Economic Journal: Economic Policy **14**(2): 231-262.

Jena, A. B., V. Prasad, D. P. Goldman and J. Romley (2015). "Mortality and treatment patterns among patients hospitalized with acute cardiovascular conditions during dates of national cardiology meetings." JAMA Intern Med **175**(2): 237-244.

Kovacs, R. and M. Lagarde (2022). "Does high workload reduce the quality of healthcare? Evidence from rural Senegal." Journal of Health Economics **82**: 102600.

Ly, D. P., M. B. Blegen, M. M. Gibbons, K. C. Norris and Y. Tsugawa (2023). "Inequities in surgical outcomes by race and sex in the United States: retrospective cohort study." BMJ **380**: e073290.

McCoy, T. H., Jr and R. H. Perlis (2018). "Temporal Trends and Characteristics of Reportable Health Data Breaches, 2010-2017." JAMA **320**(12): 1282-1284.

Neprash, H. T., C. C. McGlave, D. A. Cross, B. A. Virnig, M. A. Puskarich, J. D. Huling, A. Z. Rozenshtein and S. S. Nikpay (2022). "Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021." JAMA Health Forum **3**(12): e224873-e224873.

Newman, L. (2020). A Ransomware Attack Has Struck a Major US Hospital Chain. Wired Magazine.

Pilling, N. (2022). Faced with an overwhelmed ER, a St. Michael Medical Center nurse called 911 for help. Kitsap Sun.

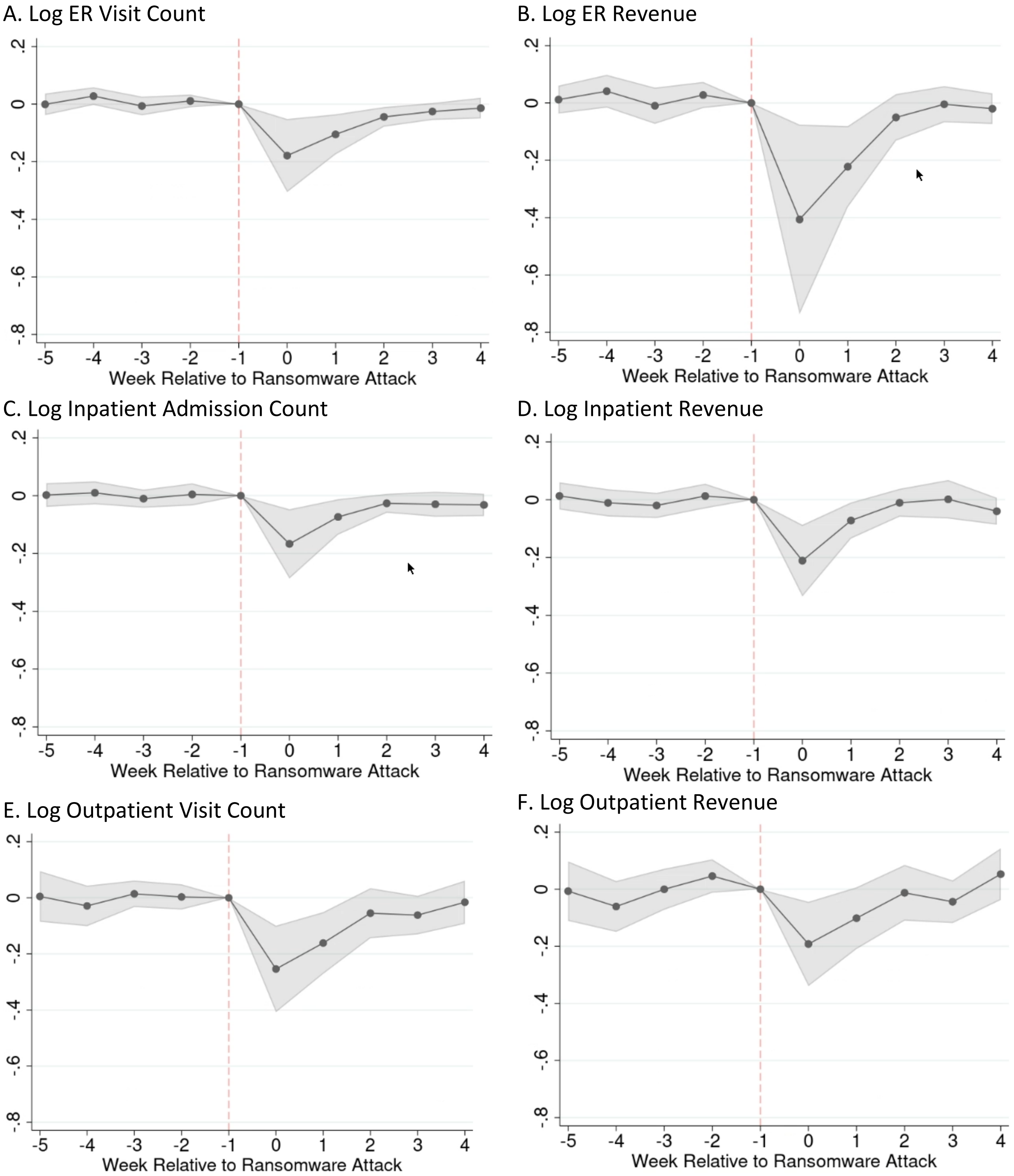
ResDAC (2017). Medicare Carrier and Outpatient Files: Identifying Ambulance Services.

ResDAC. (2023). "Find, Request, and Use CMS Data." from https://resdac.org/.

Singh, M. and A. S. Venkataramani (2022). "Capacity Strain and Racial Disparities in Hospital Mortality." Working Paper.

Templeman, M. L., L. Field and S. Ode (2021). Restructured BETOS Classification System (RBCS) 2021 Annual Update.

Figure 1. Effect of Ransomware Attacks on Volume and Revenue at Ransomware-Attacked Hospitals


A. Log ER Visit Count

B. Log ER Revenue

C. Log Inpatient Admission Count

D. Log Inpatient Revenue

E. Log Outpatient Visit Count

F. Log Outpatient Revenue

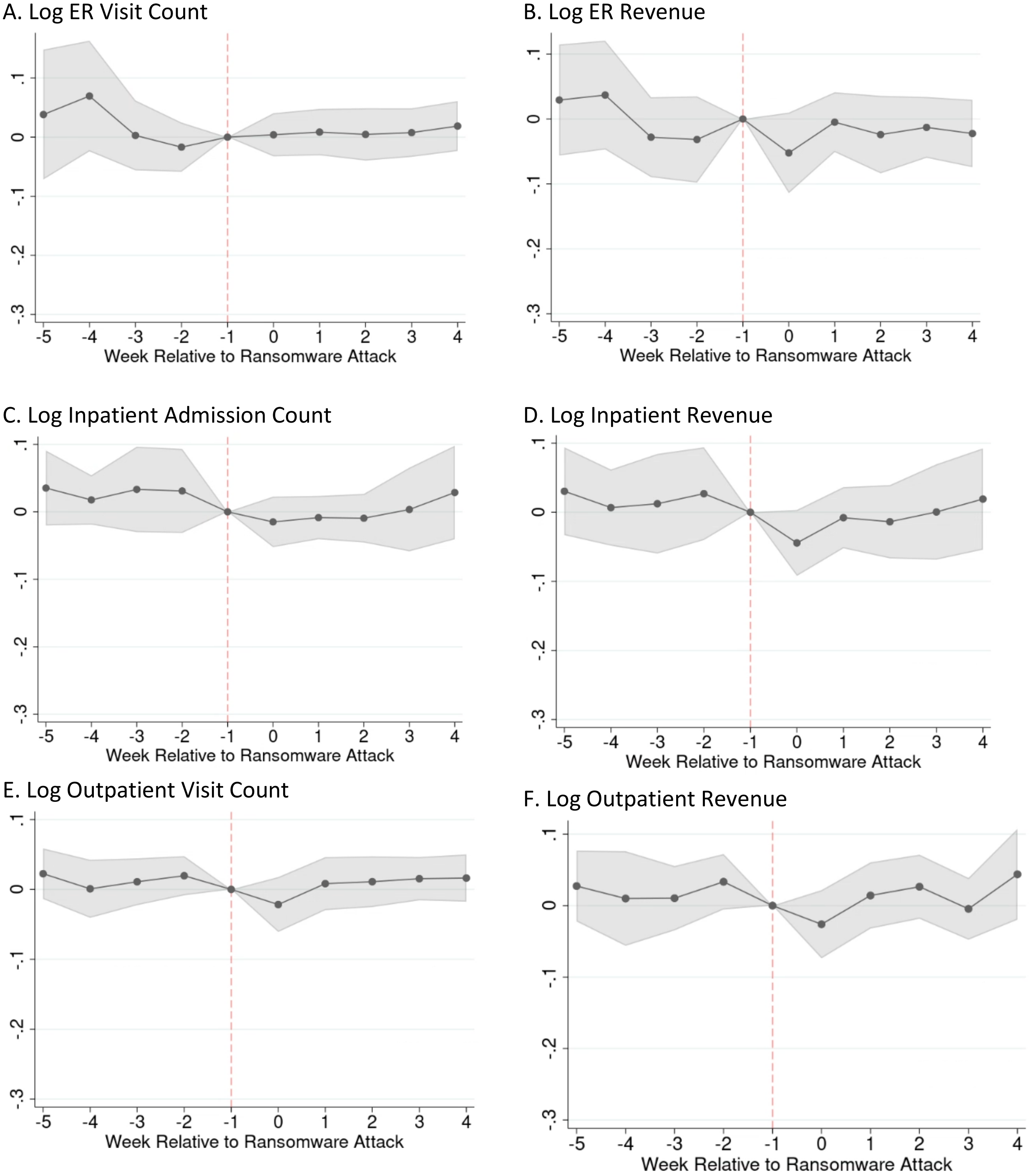
Note: This figure plots estimates of the effect of ransomware attacks on emergency room (ER), inpatient, and outpatient hospital volume and Medicare revenue. Specifically, the figure plots estimates of δ_τ coefficients from Equation 1. Shaded regions show 95 percent confidence intervals. The week prior to the attack is the reference period. Regressions are weighted by Medicare volume in the relevant setting (i.e., inpatient admissions, ER visits, outpatient visits) in the year prior to ransomware attack.

Table 1. Effect of Ransomware Attacks on Hospital Case Mix at Ransomware-Attacked Hospitals

		Attack	Attack	Attack
	Baseline Mean	Week 1	Week 2	Week 3
	(Weeks -5 to -1)	(Relative to Week -1)		
Emergency Room Case Mix				
Average Age	70.79	-0.40 (0.28)	0.17 (0.19)	-0.05 (0.17)
Average Chronic Condition Count	4.27	-0.07 (0.06)	-0.04 (0.04)	-0.03 (0.04)
Dually eligible for Medicare and Medicaid, %	41.06	-0.95 (0.66)	-1.04 (0.51)	-0.10 (0.51)
Acute Cardiovascular Event Visits, %	5.96	-1.21 (0.76)	-0.43 (0.28)	0.23 (0.33)
Inpatient Case Mix				
Average Age	74.21	0.35 (0.21)	0.49 (0.21)	0.25 (0.18)
Average Chronic Condition Count	4.47	-0.06 (0.05)	-0.02 (0.05)	0.01 (0.04)
Dually eligible for Medicare and Medicaid, %	36.74	-0.62 (0.82)	-0.53 (0.71)	0.40 (0.80)
Acute Cardiovascular Event Admissions, %	14.80	-1.71 (0.64)	-0.01 (0.44)	0.10 (0.48)
Non-Elective Admissions, %	84.07	-5.06 (3.50)	-1.66 (1.21)	-0.41 (0.54)
Average Inpatient DRG Weight	1.33	-0.05 (0.03)	0.02 (0.03)	0.06 (0.02)

Note: This table presents estimates of the effect of ransomware attacks on measures of hospital case mix. Specifically, the table presents estimates of δ_τ coefficients (for tau = 0, 1, and 2) from Equation 1, which is a regression of the dependent variable on hospital fixed effects, week-by-year fixed effects, event week indicators, and event week indicators interacted with an indicator for treatment (i.e., ransomware attack). Regressions are weighted by Medicare volume in the relevant setting (i.e., inpatient admissions, ER visits, outpatient visits) in the year prior to ransomware attack.

Figure 2. Effect of Ransomware Attacks on Volume and Revenue in Ransomware-Attacked Markets


A. Log ER Visit Count

B. Log ER Revenue

C. Log Inpatient Admission Count

D. Log Inpatient Revenue

E. Log Outpatient Visit Count

F. Log Outpatient Revenue

Note: This figure plots estimates of the effect of ransomware attacks on emergency room (ER) and inpatient hospital volume and Medicare revenue. Specifically, the figure plots estimates of δ_τ coefficients from Equation 2. The shaded regions show 95 percent confidence intervals. The week prior to the ransomware attack is the reference period.

Table 2. Effect of Ransomware Attacks on Health Outcomes

	In-Hospital Mortality	30day Mortality	30day Readmissions
Panel A			
Already admitted when attack started	0.0016 (0.0013)	0.0291 (0.0011)	0.0310 (0.0015)
Attacked hospital	0.0005 (0.0016)	0.0002 (0.0018)	0.0048 (0.0025)
Already admitted when attack started * attacked hospital	0.0077 (0.0042)	0.0017 (0.0051)	-0.0053 (0.0044)
Admission-level covariates	✓	✓	✓
Day-of-the-week, month, and year fixed effects	✓	✓	✓
Hospital fixed effects	✓	✓	✓
Pre-attack mean	0.0372	0.0624	0.1653
N =	1,719,465	1,719,465	1,651,449
Panel B			
Already admitted when attack started	0.0002 (0.0019)	0.0280 (0.0013)	0.0322 (0.0011)
Attacked hospital	-0.0039 (0.0013)	-0.0019 (0.0016)	0.0031 (0.0022)
Already admitted when attack started * attacked hospital	0.0123 (0.0047)	0.0029 (0.0054)	-0.0068 (0.0043)
Admission-level covariates	✓	✓	✓
Day-of-the-week, month, and year fixed effects	✓	✓	✓
Hospital fixed effects	✓	✓	✓
Pre-attack mean	0.0338	0.0599	0.1684
N =	1,847,930	1,847,930	1,782,529

Note: This table shows estimates of the effect of ransomware attacks on health outcomes, including mortality (in-hospital and within 30-days of admission) and 30-day readmissions. Estimates come from the difference-in-differences specification in Equation 3. In Panel A, control admissions comprise those at hospitals in the same state, but not the same HRR as the attacked hospital. In Panel B, control admissions comprise those at hospitals that would subsequently experience ransomware attacks, at least five weeks in the future. Admission-level covariates include whether the admission was elective or non-elective, whether the admission involved care in the intensive care unit, whether the admission was for an acute cardiovascular emergency, the Medicare Severity Diagnostic Related Grouping weight, patient age, patient race, patient sex, patient chronic condition count (from the year prior to hospitalization), and whether the patient was dually eligible for Medicare and Medicaid.

Table 3. Effect of the Most Severe Ransomware Attacks on Health Outcomes

	In-Hospital Mortality	30day Mortality	30day Readmissions
Panel A			
Already admitted when attack started	0.0010 (0.0018)	0.0324 (0.0013)	0.0302 (0.0028)
Attacked hospital	0.0028 (0.0021)	0.0008 (0.0028)	0.0135 (0.0046)
Already admitted when attack started * attacked hospital	0.0128 (0.0053)	0.0026 (0.0069)	0.0009 (0.0053)
Admission-level covariates	✓	✓	✓
Day-of-the-week, month, and year fixed effects	✓	✓	✓
Hospital fixed effects	✓	✓	✓
Pre-attack mean	0.0357	0.0633	0.1668
N =	786,152	786,152	755,732
Panel B			
Already admitted when attack started	-0.0036 (0.0021)	0.0302 (0.0016)	0.0343 (0.0019)
Attacked hospital	-0.0027 (0.0013)	-0.0018 (0.0021)	0.0088 (0.0024)
Already admitted when attack started * attacked hospital	0.0187 (0.0061)	0.0052 (0.0069)	-0.0035 (0.0050)
Admission-level covariates	✓	✓	✓
Day-of-the-week, month, and year fixed effects	✓	✓	✓
Hospital fixed effects	✓	✓	✓
Pre-attack mean	0.0338	0.0594	0.1636
N =	786,152	786,152	606,588

Note: This table shows estimates of the effect of ransomware attacks on health outcomes, including mortality (in-hospital and within 30-days of admission) and 30-day readmissions. Estimates come from the difference-in-differences specification in Equation 3. In Panel A, control admissions comprise those at hospitals in the same state, but not the same HRR as the attacked hospital. In Panel B, control admissions comprise those at hospitals that would subsequently experience ransomware attacks, at least five weeks in the future. Admission-level covariates include whether the admission was elective or non-elective, whether the admission involved care in the intensive care unit, whether the admission was for an acute cardiovascular emergency, the Medicare Severity Diagnostic Related Grouping weight, patient age, patient race, patient sex, patient chronic condition count (from the year prior to hospitalization), and whether the patient was dually eligible for Medicare and Medicaid. The sample is limited to the most severe ransomware attacks (N=31), where news coverage indicated that the attacked hospital(s) was forced to divert ambulances and/or delay pre-scheduled care.