Cybersecurity Monitoring/Mapping of USA Healthcare (All Hospitals) - Magnified Vulnerability due to Shared IT Infrastructure, Market Concentration, & Geographical Distribution

William Yurcik[†]
Andreas Schick
U.S. Department of Health & Human Services (HHS)
<william.yurcik@cms.hhs.gov>

Stephen North
Infovisible
Oldwick, New Jersey USA

Michael T. Gastner
Singapore Institute of Technology

Fabio Roberto de Miranda; Rodolfo da Silva Avelino; Andre Filipe de Moraes Batista
Insper
São Paulo, Brazil

Gregory Pluta
Ian Brooks
University of Illinois at Urbana-Champaign USA

ABSTRACT

In October 2024, there are two defining characteristics of a healthcare provider: (1) geographic location and services available at their physical structure and (2) Internet connectivity and services available via their virtual presence. For previous centuries we focused on the first defining characteristic and now we need to shift to understand and address issues that may arise from the new second defining characteristic.

In this paper we address issues related to Internet connectivity and virtual presence of USA healthcare providers, especially hospitals, when ransomware cyberattacks resulting in service outages occur. We show the cybersecurity posture of a large critical national infrastructure (USA healthcare) can be measured, mapped, and quantitatively baselined. Empirical results reveal systemic issues in USA healthcare presenting "magnified vulnerabilities" in that a single exploit can have an outsized impact on an entire nationwide infrastructure. As the initial step toward addressing this issue, we document for the first time the magnified cybersecurity vulnerability of USA healthcare to shared IT infrastructure, market concentration, and the geographical distribution of hospitals.

CCS CONCEPTS

Security and Privacy;500, Human-Centered Computing--Visualization--Empirical Studies in Visualization;300.

KEYWORDS

cybersecurity ratings, hospital cybersecurity, ransomware

ACM Reference format:

William Yurcik, Andreas Schick, Stephen North, Michael T. Gastner, Fabio Roberto de Miranda; Rodolfo da Silva Avelino, Andre Filipe de Moraes Batista, Gregory Pluta, Ian Brooks. 2024. Cybersecurity Monitoring/Mapping of USA Healthcare (All Hospitals) – Magnified Vulnerability due to Shared IT Infrastructure, Market Concentration, & Geographical Distribution. *Proceedings of the 2024 ACM CCS Workshop on Cybersecurity in Healthcare (HealthSec'24).* October 14, 2024, Salt Lake City UT, USA, 8 pages. https://doi.org/10.1145/3689942.3694754

1 Motivation

USA Healthcare circa 2024 is a complex sociotechnical environment of systems, processes, and humans. There are system issues in industry structure, organizational structure, funding, and investment. There are process issues in clinical protocols, organizational procedures, regulatory compliance, and insurance authorizations. Lastly, and most problematic, there are fallible humans manifested by sick and/or injured patients with dynamic needs, medical staff with dynamic needs, and organizational culture developed over decades. While USA healthcare is known worldwide to leverage its complexity for effectiveness in patient care, complexity is also a potential danger in treating patients.

In 1991 the Harvard Medical Practice Study (HMPS) brought public awareness to patient safety in hospitals for the first time and as a result changes were implemented to improve patient safety [2]. However, a recent study of hospital patient safety events 27 years later reports that the harm rates are actually higher in 2018 than in the original 1991 HMPS study [1]. Another study in same year (2018) by the HHS Office of Inspector General reported that 25% of hospitalized Medicare patients experienced a harm event, with 43% of these harm events being preventable [19]. Of course, hospitals have dramatically evolved from 1991 to 2018, with integrated IT infrastructures, electronic health records, networked digital medical devices, and new virtual services. While these technological innovations are force multipliers to enable medical staff to handle more patients and make healthcare more effective for individual patient care, the evidence shows technology has not made healthcare safer, and in many instances these innovations

[†] Corresponding Author; Official Organizational Disclaimer: "The views presented herein do not represent the views of the Federal Government."

Proceedings of the 2024 ACM Workshop on Cybersecurity in Healthcare (HealthSec '24), October 14, 2024, Salt Lake City, UT, USA.

ISBN 979-8-4007-1238
https://doi.org/10.1145/3689942.3694754

have made healthcare more brittle, less resilient to preventable harm events. Our motivation is a specific type of attack event - ransomware cybersecurity incidents that cause a healthcare provider system outage and a significant patient care harm impact.

2 Background

The Cybersecurity & Infrastructure Security Agency (CISA) has identified sixteen U.S. critical national infrastructure sectors [9]. One of these critical national infrastructures is explicitly identified as the “Healthcare and Public Health Sector”. In 2019 CISA went deeper to identify fifty-five National Critical Functions (NCFs) [10].[1] Four of these fifty-five NCFs are the primary responsibility of the “Healthcare and Public Health Sector” as shown in Figure 1. These four Healthcare-NCFs need to be balanced since they may conflict in different situations.

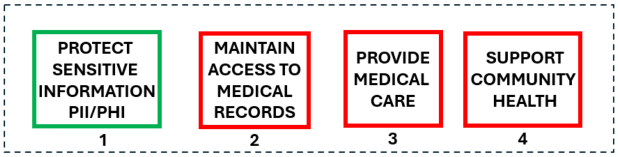

PROTECT SENSITIVE INFORMATION PII/PHI
1
MAINTAIN ACCESS TO MEDICAL RECORDS
2
PROVIDE MEDICAL CARE
3
SUPPORT COMMUNITY HEALTH
4

Figure 1. Healthcare National Critical Functions

While there are four Healthcare-NCFs, the majority of our laws, best practices, and processes are focused on only the first NCF (protecting PII/PHI Healthcare-NCF-1), not on the three NCFs addressing healthcare resilience (Healthcare-NCF-2/3/4).

The focus of cybersecurity protection specific to healthcare began with the 1996 Federal law - Health Insurance Portability and Accountability Act (HIPAA) [21] - which requires the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. HIPAA created initial emphasis on healthcare privacy compliance over maintaining healthcare operations resilience. Due to this initial emphasis, current laws protect data more than patient care.[2]

While harmful, healthcare privacy breach incidents which compromise patient data do not directly and/or immediately jeopardize human life. Privacy breach incidents can be compensated with monetary damages and plaintiffs are often made whole albeit after much effort and time delay. The overemphasis on breach incidents resulting from Healthcare NCF-1 and HIPAA is manifested in recent cybersecurity events which have caused hospital administrators that detect or suspect IT compromise to decide to immediately shut down all IT operations (satisfying Healthcare NCF-1). However, this shutdown decision also simultaneously interrupts all hospital operations (not satisfying Healthcare NCFs-2/3/4) which has a direct immediate harm impact on patient care, sometimes for large vulnerable patient populations as we will see later in this paper.

To illustrate the impact of shutting down a hospital’s IT system on patient care, an incomplete list includes the termination of: (1) all diagnostic medical treatment dependent on medical records and laboratory test results; (2) surgery dependent on automated equipment; (3) use of all automated medical devices including life support; (4) all pharmacy orders; (5) technology-based safety-checks, (6) insurance pre-authorization determining healthcare decisions; (7) admissions and scheduling, including emergency ambulance diversions to other hospitals; and (8) patient transfer to other hospitals since cybersecurity events typically require weeks to recover. Each of these eight impacts leads to degraded essential clinical functions and adverse patient outcomes such as morbidity/mortality events.[3] For a more in-depth discussion of the ransomware outage impacts on hospital clinical functions see [33].

Cybersecurity protection against ransomware outages is patient care! The remainder of this paper describes proactive cybersecurity engagement management designed to minimize, and eventually eliminate preventable cybersecurity ransomware outage events, and in so doing protect and improve patient care.

3 Cybersecurity Ratings

One of the most frustrating and ultimately dangerous things about cybersecurity is that you can *almost* measure it.[4] There are many component parts that can and/or should be measured and considered as of an overall cybersecurity posture. Composing an overall security posture from component parts is elusive, currently an unsolved problem, and may never be completely solved in a rigorous, complete framework [22].

Nonetheless, there remains a vital organization and engineering need to accurately assess overall security posture beyond subjective qualitative opinion. The work we present here quantitatively assesses overall cybersecurity posture while acknowledging it is an approximation. Insisting on a perfect formal solution that may never be found should not prevent implementation of a workable approximation, especially when a vital need exists.

NIST defines a security metric as a useful measurement that can be used to support human decision-making toward improving cybersecurity performance [30]. Despite this simple definition, a consensus/best-practice set of security metrics to monitor cybersecurity does not exist, rather security metrics are determined by the unique characteristics of enterprise environments and selected by cybersecurity analysts in positions of responsibility.

Cybersecurity ratings based on security metrics are a numerical data reduction technique for combining security metrics, analogous to a credit score encompassing overall credit risk by a creditor, and similar to how the value of a stock/bond encompasses financial reports and market conditions [6].

BitSight invented the cybersecurity ratings industry by creating an algorithm based on security metrics to produce quantitative security scores (ranging 200-900) for systems and organizations

[1] National Critical Functions are defined by CISA as “the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.”

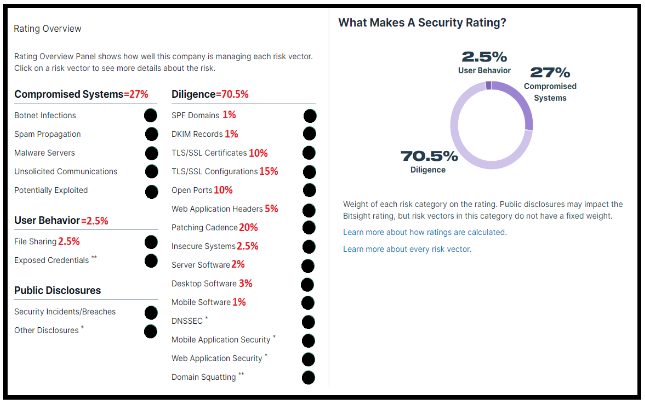
[2] Josh Corman, former chief strategist for the CISA Covid task force, put it bluntly: “We have more regulatory incentive to have a corpse with their privacy intact than to keep patients alive.” [34]

[3] A lawsuit filed by plaintiff Teiranni Kidd against Springhill Memorial Hospital in 2019 alleges that Kidd's daughter, Nicko Silar, suffered birth complications and subsequently died due to a cybersecurity ransomware attack in which hospital clinicians did not have timely access to the baby's fetal monitoring results, which showed that the child was in distress during Kidd's labor [24].

[4] This observation is a paraphrase of what Matt Blaze insightfully expressed about cryptography, a data protection technique within cybersecurity [5].

[4]. BitSight is unique in that it incorporates large-scale analysis based on Internet traffic gathered outside of an organization's security perimeter (not egress/ingress traffic) in addition to low frequency network and port scans of an enterprise attack surface.[5]

Figure 2 shows the security metrics and corresponding weights used by BitSight to calculate their cybersecurity ratings. BitSight groups these security metrics (aka risk vectors) into four categories: (1) Diligence, (2) Compromised Systems, (3) User Behavior, and (4) Public Disclosures. The largest weight is the Diligence risk vector (70.5%) which measures 11 different metrics for best practice implementation. The 4 additional metrics listed under Diligence are currently in beta and do not affect ratings. The next largest weight is the Compromised Systems risk vector (27%) which measures 5 different metrics for evidence of preventing (or lacking to prevent) malicious or unwanted software. The smallest weight is the User Behavior (2.5%) risk vector which measures 3 different activity metrics (open ports, password re-use, and file sharing traffic). Unlike the other three risk vectors, absence of a public disclosure in public reports does not positively boost ratings while the report of a breach will have a negative ratings impact.



Rating Overview

Rating Overview Panel shows how well this company is managing each risk vector. Click on a risk vector to see more details about the risk.

Compromised Systems=27%

Botnet Infections ●
Spam Propagation ●
Malware Servers ●
Unsolicited Communications ●
Potentially Exploited ●

User Behavior=2.5%

File Sharing 2.5% ●
Exposed Credentials ** ●

Public Disclosures

Security Incidents/Breaches ●
Other Disclosures * ●

Diligence=70.5%

SPF Domains 1% ●
DKIM Records 1% ●
TLS/SSL Certificates 10% ●
TLS/SSL Configurations 15% ●
Open Ports 10% ●
Web Application Headers 5% ●
Patching Cadence 20% ●
Insecure Systems 2.5% ●
Server Software 2% ●
Desktop Software 3% ●
Mobile Software 1% ●
DNSSEC * ●
Mobile Application Security * ●
Web Application Security * ●
Domain Squatting ** ●

What Makes A Security Rating?

Weight of each risk category on the rating. Public disclosures may impact the Bitsight rating, but risk vectors in this category do not have a fixed weight.

Learn more about how ratings are calculated.

Learn more about every risk vector.

Figure 2. What Makes a BitSight Security Rating? (2023 rating algorithm graphic used with permission from BitSight)

For transparency BitSight publishes and revises its ratings algorithm annually (security metrics and corresponding weights) given user input, changes in the Internet threat environment, and security metric improvements. This follows well-established standards by ratings organizations in other industries.[6]

4 Baselining Cybersecurity of USA Healthcare

Given the cybersecurity ratings capability provided with BitSight collaboration, we seek to use this new capability to characterize the cybersecurity posture of USA healthcare. The problem we face in this next step is that USA healthcare is both huge and heterogeneous.

Healthcare includes all organizations, people, and actions whose primary intent is to promote, restore, and/or maintain health. This includes medical providers (doctors/dentists/mental-health-professionals), out-patient urgent care, community clinics, nursing homes, specialized medical equipment providers and manufacturers, health insurers, the pharmaceutical industry, blood banks, and many different types of hospitals. USA healthcare covers a current population of 333M people, with private group insurance plans covering about 66% of the population, Medicaid covering 89M, Medicare covering 64.5M, the Affordable Care Act covering 21M, and 26M people with no health insurance.[7] In 2022, USA healthcare expenditure accounted for $4.5 trillion which is 17.3% of the U.S. GDP.[8]

Figure 3 breaks down USA healthcare into different sectors and shows security ratings for a sampling of organizations within each sector. Given the different sectors within USA healthcare, we considered analysis options and decided upon hospitals as the best sector to study first in more depth since it is a central convergence point. Hospitals touch every part of the industry including patient healthcare management, most providers have hospital privileges, and hospitals are typically the parent organization of subsidiary activity such as ancillary out-patient services/facilities.

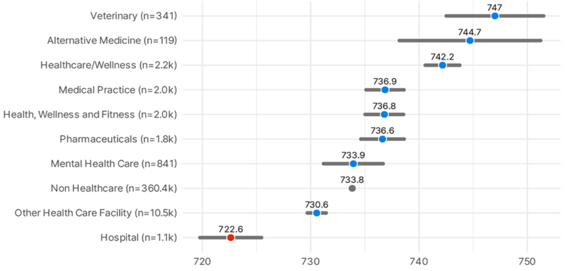


Figure 3. Cybersecurity Rating Statistics for Different USA Healthcare Sectors [credit to Ben Edwards/BitSight - used with permission]

Figure 4 shows scatter plots of the security ratings for 70% of USA hospitals – each dot represents a hospital system consisting of multiple hospitals. The vertical axis is cybersecurity rating value, the horizontal axis is the logarithm (base e) of the number of in-patient beds. These hospital cybersecurity ratings are updated nightly, and analysts use this information to identify cybersecurity events before they are publicly reported. The ultimate use of this visualized information is for prevention, using a prioritization strategy to identify and remediate hospital cybersecurity vulnerabilities before they can be exploited and/or notifying a hospital before it is otherwise aware.

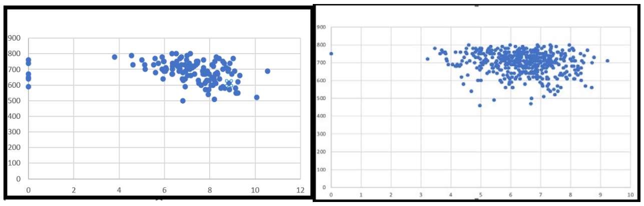


Figure 4. Distribution of Cybersecurity Ratings for (a) Hospitals in USA Interstate Systems [126 systems, 2,612 hospitals] and (b) Hospitals in USA Intrastate Systems [523 systems, 2,571 hospitals]

[5] BitSight uses a variety of tools and techniques to gather data from billions of online events and stored data points, including: crawlers, sinkholes, P2P network monitoring, honeypots, BitTorrent monitoring, spam traps, darknet traffic monitoring, network/port scanning, and open source reports.

[6] securities, credit, and insurance ratings organizations

[7] As of May 2022 exactly 64,553,288 people were enrolled in Medicare and exactly 88,978,791 people were enrolled in Medicaid and Children's Health Insurance Program (CHIP). About 12M individuals are dually eligible for both Medicare and Medicaid, so are counted in the enrollment figures for both programs. In January 2024 the Affordable Care Act's Health Insurance Marketplace reached 21M for the 2024 plan year. In September 2023, the U.S. Census reported that for 2022 the number of uninsured U.S. citizens reached a record low of 26M or 7.9%. Note due to significant overlaps in coverage these numbers do not add to the current USA population for the year of study [5].

[8] In 2022, National Healthcare Expenditure (NHE) grew 4.1% to $4.5 trillion, or $13,493 per person, and accounted for 17.3% of Gross Domestic Product in 2022 [5].

Just as different healthcare sectors show different cybersecurity rating characteristics, different hospital systems show different cybersecurity ratings characteristics as shown in Table 1. Note that the IHS and VHA hospital systems have distinctly non-overlapping mean confidence intervals from the other two systems shown. These differences in cybersecurity rating characteristics are being studied and hypothesized to be related to management structure.

RATING STATS	IHS	VHA	INTERSTATE SYSTEMS	INTRA-STATE SYSTEMS
MEAN	719.78	753.78	682.72	699.34
95% CI	+/- 7.25	+/- 2.96	+/- 12.00	+/- 5.62
MEDIAN	730	760	690	710
RANGE	650-760 (110)	690-780 (90)	500-800 (300)	460-800 (340)

Table 1. Cybersecurity Ratings for USA Hospital Systems

This empirical data shows that USA healthcare can be baselined for cybersecurity starting with hospitals and moving to other healthcare sectors. Security ratings provide quantitative baseline statistics as points-of-reference against which cybersecurity posture can be analyzed and compared. Security rating baselines have also provided other important insights such as magnified cybersecurity vulnerabilities present within the U.S, hospital sector which we discuss in more detail in Section 6.

5 A Deeper Dive into USA Hospitals

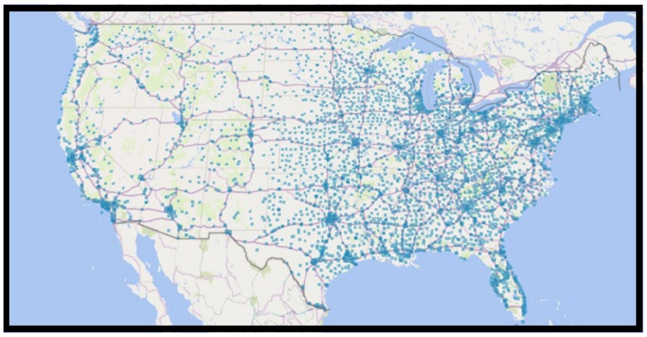


Figure 5. USA Hospitals Mapped to Geographical Coordinates
(hospitals in Alaska & Hawaii are not included in this display)

Before embarking on USA hospital security ratings monitoring and analysis we performed an inventory of the assets to be protected. Figure 5 shows all USA hospitals mapped to their geographical coordinates in the continental USA. We used multiple sources to assemble a database of 7,490 USA hospitals hosted at the University of Illinois.

According to the American Hospital Association, a hospital is state-licensed institution whose function is to provide diagnostic and therapeutic patient services for medical conditions, with organized physician staff and registered nursing.[9] The functional hospitals we track include general hospitals, Short-Term Acute Care Hospitals (STACH), Long-Term Acute Care Hospitals (LTACH), Inpatient Rehabilitation Facilities (IRF), Skilled Nursing Facilities (SNF), short stay hospitals, behavioral hospitals, psychiatric care hospitals, children's hospitals, women's hospitals, teaching hospitals, and specialty care hospitals (cancer care, eye surgery, etc). Legally-defined categories of hospitals include Acute Care/Critical Access Hospitals (CAH, fewer than 25 in-patient beds and greater than 35 miles from the next nearest hospital) and Safety-Net Hospitals (designated by the proportion of charity care provided).

For cybersecurity analysis, USA hospitals can be separated into two classes – (1) hospitals managed within an organizational system and (2) independent hospitals unaffiliated with an organizational system. We identified five special cases of USA hospital systems for analysis as: (1) Indian Health Service (IHS) Hospitals, (2) Veterans Health Administration (VHA) Hospitals, (3) Defense Health Agency (DHA) Hospitals, (4) Interstate Hospital Systems, and (5) Intrastate Hospital Systems. These five hospital systems include 70% of all the hospitals in the USA, with the remaining hospitals being independent unaffiliated hospitals.

For discussion purposes of this paper, we provide a brief background about each of these five special cases of USA hospital systems. The Indian Health Service (IHS) is the primary healthcare provider for federally recognized American Indian tribes and Alaskan natives consisting of approximately 2.6 million people belonging to 574 tribes in 37 states. The U.S. Veterans Health Administration (VHA) is the largest healthcare system in the world providing healthcare for about 9M non-active/discharged veterans of the U.S. military. The U.S. Defense Health Agency (DHA) is operated by the U.S. Department of Defense as the healthcare provider for 9.4M active-duty members of the U.S. military with hospitals and clinics worldwide.

U.S. hospitals are increasingly combining into systems of multiple hospitals – combining for reasons beyond the scope of this paper. We subdivided these hospitals systems into two categories for analysis: (1) Interstate Hospitals Systems containing hospitals in multiple states and (2) Intrastate Hospital Systems containing hospitals all within one state. This separation based on state boundaries is meaningful since hospital administration is generally governed by state regulations/certifications/laws.

6 Magnified Cybersecurity Vulnerabilities

In proactively monitoring and mapping all USA hospitals we have identified three magnified cybersecurity vulnerabilities. We refer to these three vulnerabilities as magnified since a single cybersecurity event can have an outsized impact on the entire USA healthcare infrastructure.

6.1 Shared IT Infrastructure in Hospital Systems

Shared IT infrastructure is the first magnified cybersecurity vulnerability we identified. This magnified vulnerability has been manifested in ransomware outages in large interstate hospital

[9] <aha.org>

systems which have occurred within the last year: {in chronological order}[10]

- ***Prospect Medical Holdings*** *(August 2023);* simultaneous ransomware outage at 17 in-patient hospitals spread across 4 states [CA(7), CT(3), PA(5), RI(2)] with 3,600 beds & 166 associated out-patient clinics.

- ***Ardent Health Services*** *(November 2023);* simultaneous ransomware outage at 30 in-patient hospitals spread across 4 states [NJ(2), NM(8), OK(12), TX(8)] with 4,300 beds and 200 associated out-patient clinics and 1,300 aligned provides including partially-owned hospitals in 3 states [ID(1), KS(1), NJ(2)]

- ***Ascension Health*** *(May 2024);* simultaneous ransomware outage at 127 in-patient hospitals spread across 12 states [AL(5), FL(10), IL(16), IN(24), KS(7), MD(1), MI(16), NY(1), OK(6), TN(11), TX(14), WI(16)] with 21,000 beds - one of the largest hospital systems in the U.S.

Note the chronological trend toward larger hospital system ransomware outages, the increasing number of affected entities ranging from the number to in-patient hospitals and associated beds, to the number of associated out-patient clinics (which is typically an order of magnitude larger than the number of hospitals in the system). Not included is the number of medical providers and the number of patients associated with these hospital systems which are conservatively estimated to be on the order hundreds of thousands to millions.

The common characteristic behind these simultaneous hospital outages is a shared IT infrastructure between all the hospitals in the system. It makes business sense to share one common IT infrastructure for a specific organizational function across an entire enterprise instead of supporting multiple isolated systems performing the same function. **However shared IT infrastructure creates a magnified vulnerability when one shared hospital IT system goes down, all the hospitals in the entire hospital system suffer the same common IT outage simultaneously**. These shared hospital IT systems include, but are not limited to these typical/general IT systems:

- external public-facing communication system
- internal staff communication system
- EMS telemetry communication systems
- electronic health record system
- patient registration system
- patient scheduling system
- patient billing system
- patient pre-authorization insurance system
- medical device network
- pharmacy system
- laboratory test system

For a more in-depth discussion of the impact of a ransomware outage on hospital IT systems see [33].

A fundamental issue that needs to be studied is hospital IT system resilience. If one shared hospital IT system is compromised, other shared hospital IT systems should still be able to independently operate, especially if systems are isolated through network segmentation. It is unclear the extent of ransomware-incurred hospital IT outages versus hospital self-inflicted shutdowns of shared IT systems when a compromise is suspected and/or detected by hospital system IT staff.

Since there are currently no hospital reporting requirements for hospital IT outages that do not involve PII/PHI breaches,[11] there has been much hearsay, guessing, and informed conjecture but no evidence-based detailed technical information shared about hospital ransomware outages other than sanitized information-poor mass media, social media, and hospital public relations/corporate governance reports. As a direct result there have been no hospital ransomware lessons learned and, as to be expected, there are now repeated ransomware attacks on the same target. McLaren Health Care (13 hospital system) has been the victim of two similar ransomware attacks in less than a year (August 2023/August 2024).

6.2 Economic Market Concentration

Economic market concentration within the U.S. healthcare industry is the second magnified cybersecurity vulnerability we identified. USA healthcare is unique as the only developed country in the world without a universal/national healthcare system. USA healthcare is a mixed economic system combining individual out-of-pocket payments, private health insurance (primarily linked with employment), and publicly-funded government health insurance (Medicaid and Medicare)[12] where healthcare assets are both private and publicly-owned and prices are set by both supply-and-demand and regulatory fiat. For example, U.S. hospitals have been historically established by charitable organizations resulting in the current mix of non-profit hospitals (based on regional/community needs), for-profit hospitals, and government hospitals.

U.S. healthcare sectors currently exist with monopoly/oligopoly market concentration -- this is where economic analysis is linked with cybersecurity. Economic market concentration affects cybersecurity risk in three dimensions: [17, 18]

(1) **Threat** - Market concentration affects cybersecurity threat targeting, dominant firms are more attractive targets for potential ransomware payment.

(2) **Vulnerability** – Market concentration affects cybersecurity vulnerability assessment; adversaries focus on dominant entity attack surface vulnerabilities.

(3) **Impact** - Market concentration affects cybersecurity event impact, exploitation of systemic single-points-of-failure entities can impact an entire healthcare sector at a national scale, the entire USA healthcare industry, or even the national U.S. economy.

That market concentration is linked with cybersecurity system risk is not theoretical conjecture for USA healthcare. In 2023 the

[10] All the cybersecurity ransomware attacks on hospital systems mentioned in this section have been widely reported in the open source mass media (details easily found via google) as well independently verified by the authors.

[11] A ransomware attack requires file access in order to encrypt a file so if PII/PHI is present in any of the ransomware encrypted files then, by definition, a PII/PHI breach has occurred.

[12] With some variation by state.

UnitedHealth Group had $325bn in revenue and $25bn in pre-tax profit, ranking it the 5th largest corporation in the U.S. behind only Walmart, Amazon, Apple, and ExxonMobil [13]. Through UnitedHealth Group's multiple business lines, its 100M+ customers touch about one-third of the entire U.S. population [35]. On February 27th 2024, the U.S. Department of Justice sued UnitedHealth Group under antitrust law [25].[13] Just days before this antitrust action a UnitedHealth subsidiary, Change Healthcare, had reported an evolving cybersecurity event to the U.S. Securities and Exchange Commission. This evolving cybersecurity event would eventually result in UnitedHealth CEO Andrew Witty testifying for hours before the U.S. Congress where he described, in excruciating detail, the cybersecurity posture of UnitedHealth.

Change Healthcare is one of three Pharmacy Benefit Managers (PBMs) which combine to control over 80% of the U.S. market [12].[14] PBMs are key pharmaceutical industry intermediaries between drug manufacturers, health insurers, drug wholesalers, and retail pharmacies which emerged in the 1950s in response to demand for specialized management of prescription drug benefits. Over time vertical integration has occurred such that PBMs now control the pharmaceutical supply chain including formularies, mail orders, pharmacy networks between manufacturers/ wholesalers, and retail claims processing [26, 31, 32].

The PBM Change Healthcare cybersecurity ransomware outage event first detected on February 22nd 2024 evolved to disrupt a critical mass of drug prior authorization claims processing capability large enough to create a cascading impact on the entire U.S. drug industry. **This outsized impact of this single ransomware cybersecurity event on the entire U.S. drug industry had a root cause with the market concentration of national pharmacy claims clearinghouse processing within one entity -- PBM Change Healthcare.**

BitSight cybersecurity rating information on Change Healthcare prior to this event reveals multiple exploitable cybersecurity vulnerabilities. While a PBM cybersecurity failure disrupting the nationwide U.S. drug industry could have been theoretically predicted, it was not until this event occurred that the outsized impact of economic market concentration on healthcare cybersecurity has now become a realized strategic concern for U.S. healthcare national critical infrastructure.

6.3 Geographic Distribution

Geographic distribution of physical healthcare facilities is the third magnified cybersecurity vulnerability we identified, specifically we will again focus on the USA hospital sector. **Despite the advent of significant virtual healthcare services available via the Internet, healthcare services availability at physical geographic locations *close-in-time* to patients is still critically important, and in cases of emergency healthcare often a matter of life and death.**

For emergency medicine the term *"golden hour"* refers to the hour immediately after a medical event (heart attack, stroke, trauma event, etc.) when rapid intervention makes the most difference between life and death.[15] In practice, the time duration depends on the exact nature of the medical event. Figure 6 provides critical timeframes for four different medical events [33]. For emergency medicine having healthcare services within these timeframes is critical for the public health of a regional community.

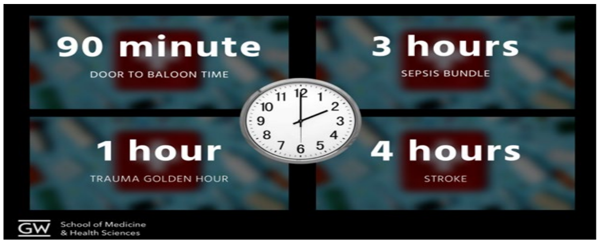


Figure 6. Critical Timeframes for Emergency Patient Care [Figure used with permission from Natalie Sullivan & Kristin Raphel of George Washington University Hospital]

Beyond emergency medicine, patient travel distance to the nearest hospital (PTD) and patient travel time to the nearest hospital (PTT) metrics have been widely studied. Using PTD as a surrogate for PTT, the median U.S. straight-line PTD was 6.6 miles with 75% of the distances less than 15 miles and 90% of the distances less than 30 miles [38]. The shortest distances were in the northeast and metropolitan areas across the U.S. and the longest distances were in the South-East, South-Central and rural areas dispersed across the U.S. [38]. Differences in PTD have been shown to directly reflect access to care, healthcare decision-making, healthcare costs, inequities in healthcare, and patient outcomes [27, 38].

Previously we defined one criteria of a Critical Access Hospital (CAH) as being greater than 35 miles from the next nearest hospital. The intent of the CAH designation is to improve access to healthcare by keeping hospitals with essential services within rural communities for close-in-time access.[16] **However, *if a CAH closes or is unavailable due to a cybersecurity ransomware outage,* the next closest hospital for emergency services and/or other health services will likely put patient care in jeopardy for an entire region.**

CAH closures occur due to a complex range of factors (including cybersecurity breaches and outages) and this is having a measured effect on PTT with its subsequent impact on patient care. From 2005 to 2015, the USA population who lives longer than 60 minutes from a hospital has increased 80% [29]. Of the services previously offered by a closed CAH, the average increase in distance to obtain those same services post-CAH-closure was approximately 20 miles [37]. A 2017 study reports that 10% of the U.S. rural population (4M people) do not have an acute care hospital within their entire county [7]! An unexpected emergent finding is increasing urban

[13] This was just one of multiple recent antitrust actions filed against UnitedHealth; in July 2024 UnitedHealth abandoned acquisition of Stewardship Health following DOJ opposition [36]; in 2023 nonprofit hospitals and doctors in California sued over market power abuse in the physician market [11], and ironically the DOJ unsuccessfully sued in 2022 to block its acquisition of Change Healthcare arguing prophetically that this would provide monopolistic control of claims processing tools [23].

[14] additionally six PBMs make up 94% of the U.S. market. [12]

[15] The term "golden hour" is attributed to R. Adams Cowley who served many years as Head of University of Maryland Shock Trauma Center (STC) in Baltimore City MD USA. Dr. Cowley transformed PTD/PTT metrics with the use of helicopters for rapid medical evacuation of civilians thus establishing the first statewide EMS system. STC was the nation's first, and remains the only, integrated trauma hospital reporting an annual flow of 8K patients with an astounding 97% survival rate. <umms.org>

[16] Congress created the Critical Access Hospital (CAH) designation through the Balanced Budget Act of 1997 (Public Law 105-33)

hospital mortality outcomes, spillover effects related to increased travel times to an urban hospital for rural population time-sensitive emergency cases [20].

Available space for patient care is the second dimension of the CAH closure problem, not only does a hospital have to be close-in-time but it needs to have staffed and supplied in-patient bed space available.[17] Recall another defining criteria of a CAH is having fewer than 25 beds so ideal CAH capacity is not large to begin with. For an extreme recent example of space challenges for patient care, the healthcare system stress caused by the lack of available staffed and supplied bed space within hospitals during the Covid19 pandemic resulted in 12 states adopting Crisis Standards of Care (CSC), the most extreme operating condition for a hospital [8].[18]

Thus, the challenge is to identify and cyberprotect specific CAHs which are potential ransomware outage cascading single-points-of-failure in two dimensions - (1) close-in-time and (2) in-patient bed capacity. To identify the candidate CAHs for special cybersecurity protection demands detailed analysis by county across each state. For scale consideration, the U.S. has 3,143 counties, or county equivalents. Toward addressing this challenge we decided to employ high-level visualization techniques to focus our efforts.

A choropleth map uses color shades over geographical areas in direct relation to a defined data variable as a visual technique to intuitively communicate an underlying data distribution [28]. Figure 7a shows the distribution of in-patient beds per 1K state population using the 2020 USA census. As shown in the color legend, the number of in-patient beds per 1K state residents varies from VT (2.0) to SD (5.98). One counter-intuitive result shows states with poor healthcare metrics report relatively higher in-patient bed density (e, g, KY, LA, MS, WV).

Cartogram mapping is the ideal mechanism to illustrate distortions in USA hospital coverage. A cartogram substitutes a mapping variable for space/geometry of a reference map [16]. The substitute variable used in Figure 7b is the 2020 USA census population in each state. Thus, this cartogram generated using a flow-based method [15] represents each state with an area proportional to its population. Grid cells are overlaid the scale of the quantities represented [14]. In Figure 7(b), each grid cell corresponds to a population of 10 million. Using the same color scale as in Figure 7(a), this cartogram reveals that some states with small populations have high bed-to-population ratios, such as the District of Columbia (DC) and North and South Dakota (ND and SD), with 5.77 and 5.04 beds per thousand residents, respectively. California (CA), the most populous state, ranks sixth lowest in bed-to-population ratio (2.61).

When the number of beds is normalized by the number of hospitals instead of population, a different picture emerges in Figures 7(c) and (d). In 7(d), each grid cell corresponds to 200 hospital beds. As indicated by the colors, many states with a high per-capita number of beds have few beds per hospital (e.g., ND, SD, and LA). Comparing the cartograms in 7(b) and 7(d) reveals that California has fewer hospitals (6.5% of all US hospitals) than its share of the US population (11.6%) would suggest. In contrast, Louisiana (LA) hosts 4.1% of the hospitals but only 1.4% of the population.

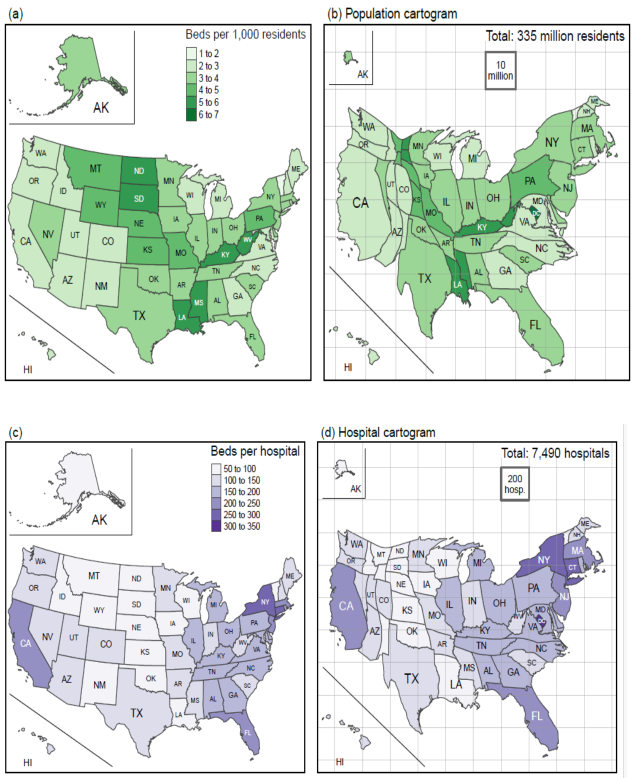


Figure 7. Maps showing the distribution of hospitals and hospital beds in the USA. (a) Choropleth map displaying hospital beds per 1,000 residents by state. (b) Cartogram where states are scaled according to population. (c) Choropleth map depicting the number of beds per hospital. (d) Cartogram where states are scaled according to the number of hospitals.

7 Summary

We first showed results showing that it is possible to quantitatively baseline the cybersecurity posture of a large critical national infrastructure – the U.S. hospital healthcare sector. We accomplish this with an implementation combining the use of data reducing cybersecurity ratings and data visualization techniques. To our knowledge this is the first Internet cybersecurity management findings for a large national infrastructure.

Second, we describe how monitoring and mapping the U.S. hospital healthcare sector resulted in identifying three systemic “magnified” cybersecurity vulnerabilities within U.S. healthcare. Magnified vulnerabilities in the sense that a single cybersecurity incident can have an outsized impact on an entire nationwide infrastructure.

The first magnified cybersecurity vulnerability we identified was shared IT infrastructure in hospital systems such that when one

[17] Often referred to as the three S’s – Space / Supplies / Staff.

[18] CSC preserves functioning during scarcity, curtailing services & adjusting patient care to available resources. < https://www.ncbi.nlm.nih.gov/books/NBK32748/ >

shared hospital IT system goes down due to a cybersecurity incident, all the hospitals in the entire hospital system suffer the same common IT outage simultaneously - as documented in three large hospital system outages we list.

The second magnified cybersecurity vulnerability we identified was economic market concentration within U.S. healthcare sectors such that a single cybersecurity outage disruption occurring within a single monopolist/oligopolist can have an outsized impact on an entire nationwide infrastructure - as documented in the recent PBM Change Healthcare event we describe.

The third magnified cybersecurity vulnerability we identified was a single cybersecurity event causing an outage at a rural hospital (and/or specifically a Critical Access Hospital) can jeopardize healthcare services for a large patient population in an entire region.

In conclusion, we recommend a proactive approach to cybersecurity management that considers complex healthcare systems composed of potentially many organizations connected by business relationships and interdependent computer networks. Our motivation is increased priority on assessment of patient impact in all its facets. Each of the magnified cybersecurity vulnerabilities we have identified within the U.S. healthcare system are critically important to address and will be the focus of our future research team efforts. Cybersecurity protection in the healthcare context is patient care!

ACKNOWLEDGMENTS

This research was enabled through a cooperative agreement between the University of Illinois at Urbana-Champaign and BitSight. BitSight provided no financial support to this research. Cybersecurity ratings for hospitals presented in this research were processed by BitSight engineers led by Rhonda O'Kane and supported by Tadd Hopkins, Tim Jackson, Tom Linehan, and Will Ricardi. Geocoding was provided by GeoCoder.ca who provided public service access to their geography mapping scripts. Geocode provided no financial support to this research. Coauthor MTG is supported by the Ministry of Education, Singapore, under its Academic Research Fund Tier 2 (EP2) programme (Award No. MOE-T2EP20221-0007).

REFERENCES

[1] David Bates et al. 2023. The Safety of Inpatient Health Care. *New England Journal of Medicine.* 388:2 142-153.

[2] T.A. Brennan, et. al. 1991. Incidence of Adverse Events and Negligence in Hospitalized Patients: Results of the Harvard Medical Practice Study I. *New England Journal of Medicine.* 324 370-376.

[3] Matt Blaze. "Afterword" within Bruce Schneier. 1996. *Applied Cryptography 2nd Edition*. 1996.

[4] Stephen Boyer, Nagarjuna Venna, and Megumi Ando (BitSight Technologies Inc. filed September 22, 2011), *Information Security Assessment System U.S. Patent 20160205126*, granted July 14, 2016.

[5] Centers for Medicare & Medicaid Services (CMS) *National Health Expenditures (NHE) 2024 Fact Sheet* <https://www.cms.gov/data-research/statistics-trends-and-reports/national-health-expenditure-data/nhe-fact-sheet>

[6] Sung J. Choi and M. Eric Johnson. 2021. The Relationship Between Cybersecurity Ratings and the Risk of Hospital Data Breaches. *Journal of the American Medical Informatics Association*, Vol 00(No 0), 1–8.

[7] M. Clawar et al. 2018. Access to Care: Populations in Counties With No FQHC, RHC, or Acute Care Hospital. *NC Rural Health Research Program.*

[8] Cybersecurity Infrastructure and Security Agency (CISA), 2021. Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm. *CISA INSIGHTS,* September 2021.

[9] Cybersecurity & Infrastructure Security Agency (CISA). *Critical Infrastructure Sectors.* <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>.

[10] Cybersecurity & Infrastructure Security Agency (CISA). *National Critical Functions.* <https://www.cisa.gov/topics/risk-management/national-critical-functions>.

[11] *Emanate Health v. Optum Health.* 2023. California Central District Court – No. 2:23-cv-09872.

[12] Adam J. Fein, 2023. The Top Pharmacy Benefit Managers of 2022: Market Share and Trends for the Biggest Companies. *Drug Channels Institute,* May 23, 2023.

[13] Fortune 500 – The Largest Companies in the U.S. by Revenue. *Fortune Magazine*. 2023. https://fortune.com/ranking/fortune500/2023/

[14] Kevin L.T. Fung, Simmon T, Perrault, and Michael T. Gastner, 2023. Effectiveness of Area-to-Value Legends and Grid Lines in Contiguous Area Cartograms. *IEEE Transactions on Visualization and Computer Graphics*. May 2023, 1-18.

[15] Michael T. Gastner, Vivien Seguy, and Pratyush More. 2018. Fast Flow-Based Algorithm for Creating Density-Equalizing Map Projection. *Proceedings of the National Academy of Sciences, 115(10).* https://www.pnas.org/doi/abs/10.1073/pnas.1712674115

[16] Michael T. Gastner and M.E.J Newman, 2006. Optimal Design of Spatial Distribution Networks. *Phys. Rev. E 74(1), American Physical Society.* https://link.aps.org/doi/10.1103/PhysRevE.74.016117

[17] Dan Geer et. al. 2003. CyberInsecurity: The Cost of Monopoly – How the Dominance of Microsoft's Products Poses a Risk to Security. *Computer & Communications Industry Association Report.*

[18] Dan Geer, Eric Jardine & Eireann Leverett. 2020. On Market Concentration and Cybersecurity Risk, *Journal of Cyber Policy*. DOI: 10.1080/23738871.2020.1728355

[19] C. A. Grimm. 2022. Adverse Events in Hospitals: A Quarter of Medicare Patients Experienced Harm in October 2018. *U.S. Department of Health and Human Services (HHS), Office of Inspector General (OIG),* OEI-06-18-00400.

[20] K. Gujral and A. Basu. 2019. Impact of Rural and Urban Hospital Closures on Inpatient Mortality. *National Bureau of Economic Research,* Wkg. Paper 26182.

[21] *Health Insurance Portability and Accountability Act of 1996.* Public Law 104–191, August 21, 1996.

[22] INFOSEC Research Council. 2005 Hard Problem List. November 2005.

[23] S. Liss. 2022. Judge Denies DOJ's Move to Block $13B UnitedHealth, Change Deal. *Healthcare Dive.* September 20, 2022.

[24] M. K. McGee. 2021. Lawsuit: Hospital's Ransomware Attack Led to Baby's Death. *HealthInfoSec,* October 21, 2021.

[25] A. W. Mathews and Dave Michaels. 2024. U.S. Opens UnitedHealth Antitrust Probe. *Wall Street Journal*, February 27, 2024.

[26] T. Joseph Matttingly II and David Hyman. 2023. Pharmacy Benefit Managers – History, Business Practices, Economics. And Policy. *JAMA Health Forum* 4(11).

[27] S. McCarthy et al. 2021. Impact of Rural Hospital Closures on Health-Care Access. *J Sur Res*. 2021:258: 170-178.

[28] M. Meyer, F. R. Broome, and R. H. Schweitzer Jr.. 1975. Color Statistical Mapping by the U.S. Bureau of the Census. *The American Cartographer,* Volume 2 Issue 2, 101-117.

[29] R.M. Mullner and D.G. Whiteis. 1988. Rural Community Hospital Closure and Health Policy. *Health Policy*, 10(2): 123-135.

[30] National Institute for Standards and Technology (NIST). 2024. *Measurement Guide for Information Security: Volume 1 – Identifying and Selecting Measures. NIST SP 800-55.*

[31] R. Robbins and R. Abelson. 2024. A Shadow Industry – How Pharmacy Benefit Managers Inflate the Cost of Prescription Drugs for Millions of People. *NY Times,* 60(194).

[32] J. Shepperd. 2020. Pharmacy Benefit Managers, Rebates, & Drug Prices: Conflicts of Interest in the Market for Prescription Drugs. *Yale Law & Policy Review*.

[33] Natalie Sullivan and Kristin Raphel. 2024. Clinical and Hospital System Emergency Management: Implications of Cyberthreats Beyond Privacy Concerns. *ACM CCS Workshop on Cybersecurity in Healthcare (HealthSec'24).*

[34] B. Trang. 2024. Why U.S. Health Care Cybersecurity Laws are Better at Protecting a Corpse's Privacy than Patients' Lives. *STAT+,* Aug. 13, 2024.

[35] UnitedHealthcare - Individuals Served by Segment 2023. *Statista*. https://www.statista.com/statistics/622420/individuals-served-by-unitedhealthcare-by-segment/

[36] U.S. Department of Justice. 2024. *UnitedHealth Group Abandons Two Acquisitions Following Antitrust Division Scrutiny,* July 24, 2024.

[37] U. S. Government Accountability Office. 2020. *Rural Hospital Closures-Affected Residents Had Reduced Access to Health Care Services.*

[38] A.J. Weiss et al. Methods for Calculating Patient Travel Distance to Hospital in HCUP Data. 2021. *U.S. Agency for Healthcare Research and Quality (AHRQ).*