Review of National and State-Level Data Relating to Cyber Incidents and Cybersecurity at Healthcare Organizations

July 2024

By Ben Yelin, Program Director for Public Policy & External Affairs for the Center for Health and Homeland Security

Table of Contents

I. Summary of Recent High-Profile Cyber Incidents Across the Country

According to the Department of Health and Human Services Office of Civil Rights (OCR), which tracks health-related privacy breaches, the past five years have seen a 256% increase in large breaches of healthcare related organizations that involved hacking. Perhaps more concerning, the OCR reports that there has also been a 264% increase in the use of ransomware against healthcare related targets. A report by the FBI's Internet Crime Complaint Center found that in 2023 "Healthcare and Public Health" was the most affected critical infrastructure sector from ransomware attacks. The rise of ransomware is particularly alarming because, as evidenced in the ongoing UnitedHealth Group and Ascension cyber incidents, ransomware has the ability to paralyze an organization's operations.

As recently as 2015, most privacy breaches in the healthcare industry were due to data being lost or stolen (see Figure 1, based on OCR Reporting Data, below). More recently, privacy breaches have utilized various forms of hacking into IT networks, sometimes employing malware. These hackers would copy or remove PHI and extort the organization to avoid the public release of the information. However, until the more recent emergence of ransomware, these cyber incidents did not involve the widespread inability to access an organization's IT systems. Thus, the primary harms from this earlier generation of cyber-incident included:

1. The risk posed to customers of future identity theft
2. The reputational risk to the organization from failing to safekeep information, including risk of customer loss
3. Fines for the organization's risk management failures which enabled the PHI violations
4. Class-action lawsuits brought by patients whose data had been exposed by privacy breaches
5. The costs associated with notifications, paying for identity monitoring for impacted customers, and other specialized services required to manage the fallout and recovery from the privacy breach
6. Any ransom payments, if made

These are certainly significant costs, and they are sometimes enough by themselves to drive a company into bankruptcy following such a cyber-incident. For example, New York based American Medical Collection Agency entered bankruptcy due to the "costs of notification and remediation," along with the loss of several important customers after a 2019 cyber-incident exposed the data of 21 million people.

As bad as these harms are, however, this earlier generation of cyber-intrusion rarely had any discernible impact on customer services. There were costs incurred by the organization, to be sure, but nothing actually stopped working. A customer might (repeatedly) find out that their social security number was on the dark web, but their doctor was still able to access their electronic health record, ensure the correct medication was administered, and receive prompt payment for medical services provided. The patients were not in any immediate physical risk because of these non-ransomware cyber incidents.

The UnitedHealth Group and Ascension cyber-incidents were detected in February and May of 2024, respectively. These incidents mark a frightening departure from the dominant pattern of earlier cyber-attacks, which stole data but generally did not disable organizational functions. In both of these attacks, the cyber intruders used ransomware to encrypt critical systems, effectively preventing the organizations from performing many of their core tasks. While as many as one-third of Americans may have had their PHI compromised in the UnitedHealth Group breach, a much more immediate harm materialized in the form of many healthcare providers, pharmacies, and insurers across the country being unable to process claims or share other related information. Despite paying a $22 million ransom in bitcoin to the hackers, it took over a month for the company to restore basic functionality of its critical systems, though efforts are ongoing to restore access for all customers. A March survey performed by the American Hospital Association indicated that 74% of hospitals experienced direct impacts to patient care and 94% of hospitals experienced a negative financial impact from the loss of UnitedHealth's critical services. An April survey performed by the American Medical Association revealed that 90% of medical provider respondents reported that they continued to lose revenue from unpaid claims, and 62% were using personal funds to cover their medical practice's operating expenses.

The more recent Ascension cyber-incident had an even more pronounced impact on patient care. Ascension operates 142 hospitals, 40 senior living facilities, and more than 2,600 care sites across the country. At many of these locations, the ransomware eliminated the ability of medical providers to access Electronic Health Records, use phone systems, order tests, order procedures, order medications, and connect to external vendors and partners, among other services that were degraded. While the hospital system shifted to "downtime procedures" to deal with the lack of these systems, public reporting suggests that the downtime procedures were inadequate to deal with the breadth of systems affected or duration of the outage. These news reports carry multiple eye-witness reports of medication dosing errors and at least one patient fatality from delays in obtaining critical test results. Conditions were so bad at Ascension hospitals that one Michigan Ascension ER nurse told NPR that "[i]f I started having crushing chest pain in the middle of work and thought I was having a big one, I would grab someone to drive me down the street to another hospital." These examples show that today's threat actors, armed with ransomware, pose a threat that extends well beyond the more traditional privacy related risks of their predecessors. They now pose a direct and immediate threat to the lives of patients.

4

Where does that leave us? Healthcare-related privacy breaches today expose private health information for more people than in the past, are much more likely to be caused by cyber incidents (as opposed to theft or other methods of unauthorized disclosure), and those cyber incidents are more likely to use ransomware. As the Ascension attack painfully illustrates, cyber incidents at healthcare organizations are no longer just a privacy concern. Patients are being harmed, sometimes fatally, in real-time as these attacks unfold. Even where obvious patient harm does not materialize, such as in the UnitedHealth breach, patients still experience a substantial negative impact from delays, confusion over billing and insurance approvals, and restricted access to pharmacy services. Zooming out a bit further, patients are also certain to be harmed by the increased healthcare costs associated with healthcare providers needing to invest more in cybersecurity, pay more for liability insurance, or even choosing to pursue work outside of direct patient care in an effort to avoid the risks associated with being either the target or collateral damage from one of these attacks.

Figures 1-3 below are taken from The HIPPA Journal reporting and show nationwide trends compiled from OCR breach and HIPAA penalty data.

Figure 1

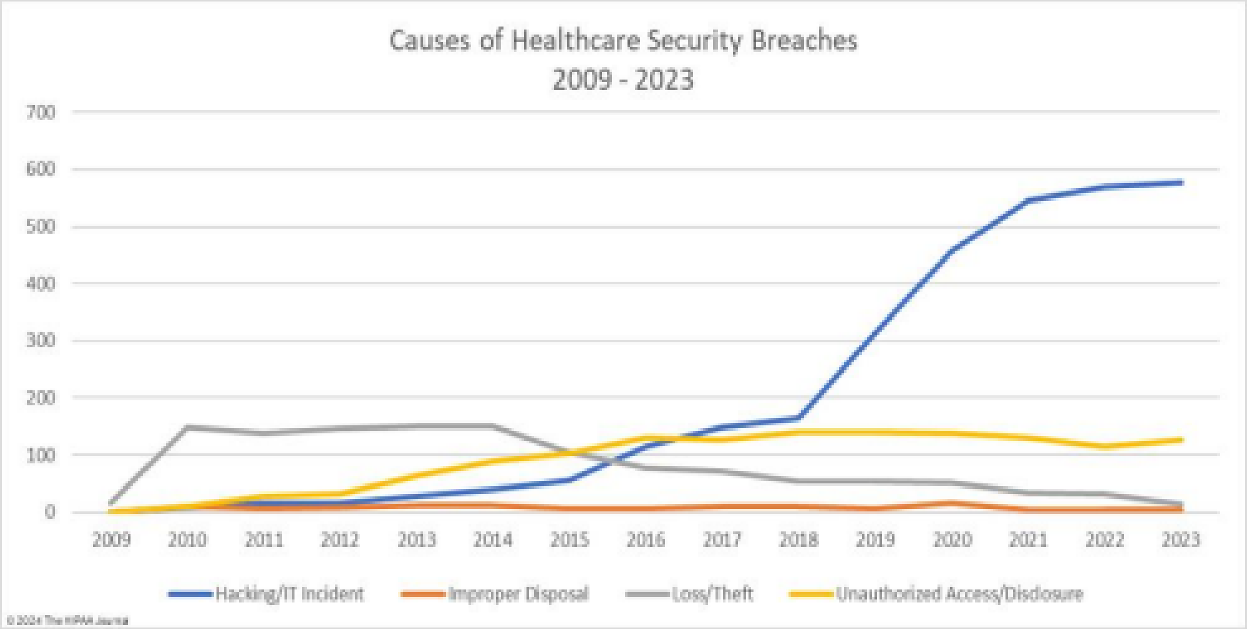


Figure 2

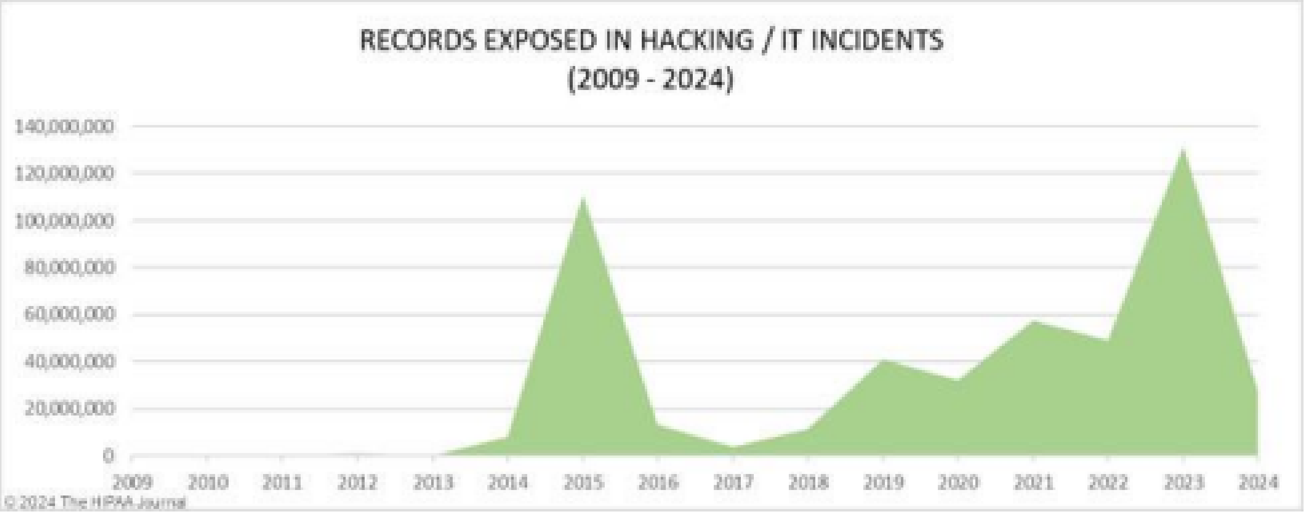
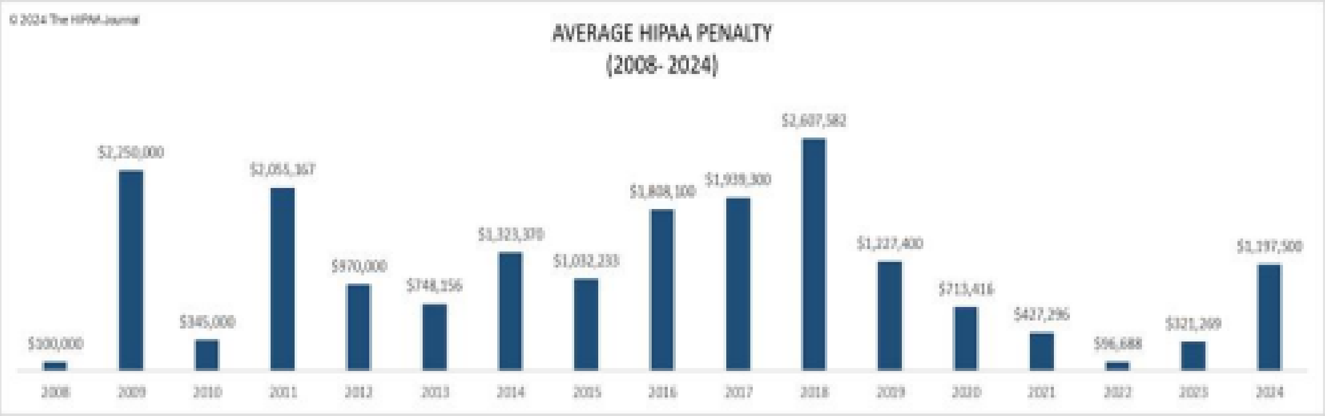


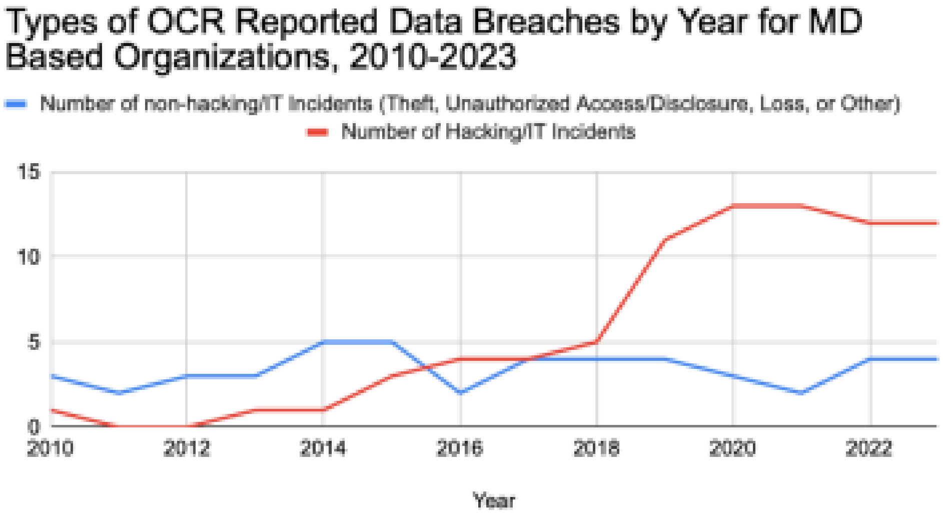
Figure 3



II. Maryland-specific analysis

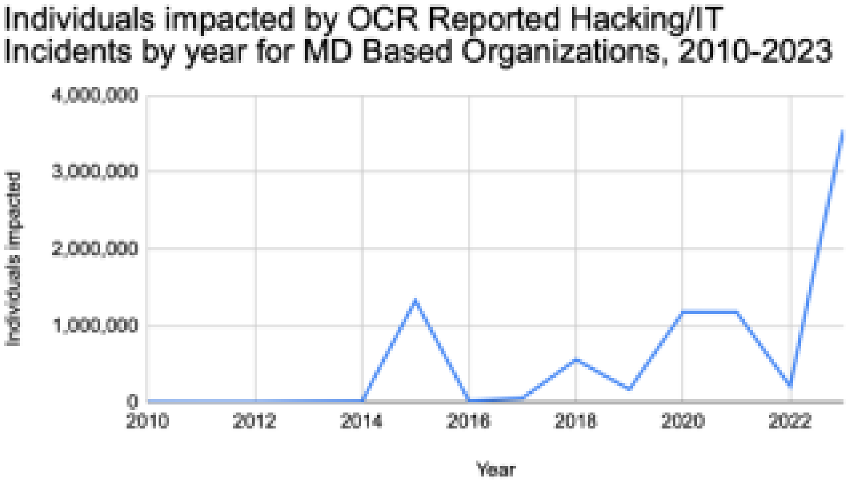
Healthcare-related organizations operating in Maryland have experienced similar patterns of hacking/IT incidents as those observed nationally. Specifically, according to the information publicly reported by the Department of Health and Human Services Office of Civil Rights (OCR) regarding data breaches impacting 500 or more individuals, since 2010 Maryland based organizations have suffered 84 breaches categorized as "hacking/IT incidents" Of these breaches, 55 were of healthcare providers, 18 were of business associates, and 11 were of health plans. As the below graph indicates (Figure 4), the rate of these hacking/IT incidents has picked up considerably in recent years, with hacking/IT incidents exceeding data breaches caused by other forms of data compromise every year since 2018, and the gap appears to be widening.

Figure 4



Additionally, the number of individuals impacted in these breaches is rising rapidly. Hacking/IT incidents are responsible for 89% of the total number of individuals impacted by the reported Maryland data breaches, despite only constituting 64% of reported breaches since 2010. From the first reported breach related to a hacking/IT incident in 2010 to the end of 2013, less than 10,000 individuals were impacted (7,400 total, with zero reported in 2011 and 2012). In 2014, more people were impacted than in the prior four years combined (10,766), and this trend has continued to accelerate since that time. In 2023, over 3.5 million individuals were impacted by hacking/IT incidents. The graph below (Figure 5) illustrates this rapid growth. Note that due to the wide range in reported values, the numbers prior to 2014 and for 2016 look like zero on this scale, but there were over 40,000 people affected across those years. Similarly, though 2022 looks like a very low number, it is actually 209,213–nearly 20 times higher than the 2014 value.

Figure 5



Of the health-care related organizations represented in this database of Maryland-based incidents, 65% of the hacking/IT incidents occurred at healthcare providers (55 out of 84 incidents), while 21% were from business associates (18 out of 84 incidents) and 13% were health plans (11 out of 84 incidents). It should be noted that all of these numbers represent an undercount of the scale of the problem, because OCR is only required to publicly report those incidents involving data breaches for 500 or more individuals.

Another helpful reference for understanding how Maryland compares to other similar states is a report compiled by the Maryland Healthcare Commission in 2021. It also relies on the OCR data, and it zooms in on the years 2018-2020. In addition to breaking down the type of breach by the type of covered entity, this study also analyzed MD as a part of a cohort of 7 other states which had similar per-capita hospital inpatient rates over the studied period. Thus, the report allows for a comparison of MD breach data to each of the other 7 states in the cohort, as well as to national averages. One of the observations that can be drawn out of the report is that, at least for the years 2018-2020, MD had the highest number of breaches per-capita of the cohort states, and also had more records compromised per-capita than the average state in the cohort, as shown in the below table (Figure 6) taken from page 6 of the report:

Figure 6

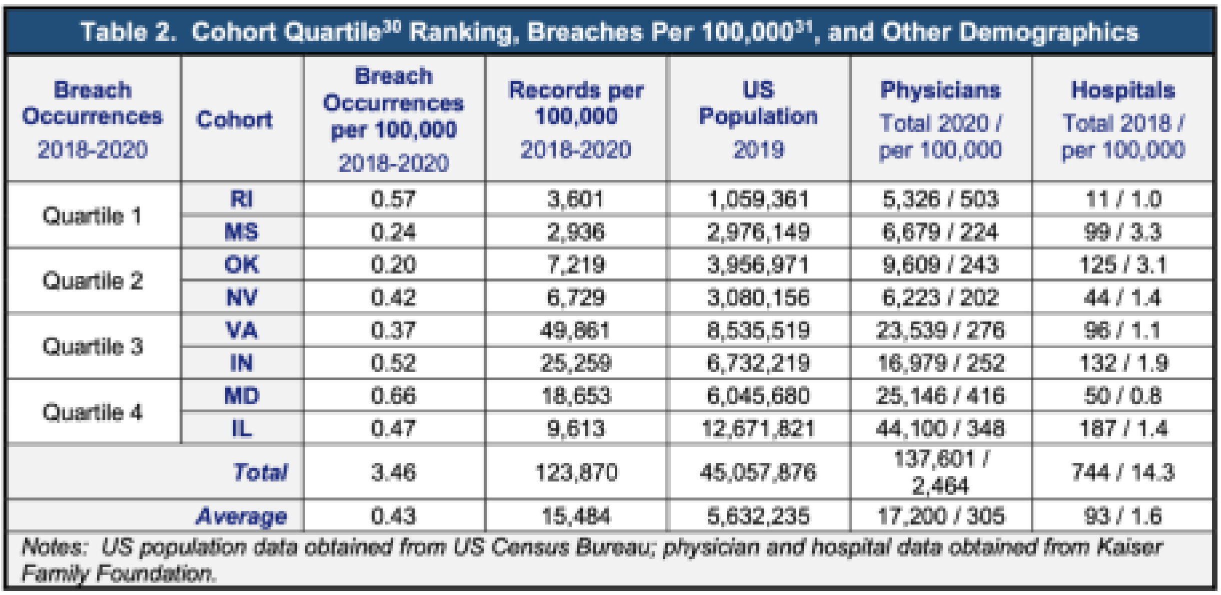


Table 2. Cohort Quartile[30] Ranking, Breaches Per 100,000[31], and Other Demographics

Breach Occurrences 2018-2020	Cohort	Breach Occurrences per 100,000 2018-2020	Records per 100,000 2018-2020	US Population 2019	Physicians Total 2020 / per 100,000	Hospitals Total 2018 / per 100,000
Quartile 1	RI	0.57	3,601	1,059,361	5,326 / 503	11 / 1.0
	MS	0.24	2,936	2,976,149	6,679 / 224	99 / 3.3
Quartile 2	OK	0.20	7,219	3,956,971	9,609 / 243	125 / 3.1
	NV	0.42	6,729	3,080,156	6,223 / 202	44 / 1.4
Quartile 3	VA	0.37	49,861	8,535,519	23,539 / 276	96 / 1.1
	IN	0.52	25,259	6,732,219	16,979 / 252	132 / 1.9
Quartile 4	MD	0.66	18,653	6,045,680	25,146 / 416	50 / 0.8
	IL	0.47	9,613	12,671,821	44,100 / 348	187 / 1.4
	Total	3.46	123,870	45,057,876	137,601 / 2,464	744 / 14.3
	Average	0.43	15,484	5,632,235	17,200 / 305	93 / 1.6

Notes: US population data obtained from US Census Bureau; physician and hospital data obtained from Kaiser Family Foundation.

III. Sampling of regulations and legislation being pursued in other states

A review of regulatory and legislative action being pursued in other States to address healthcare-related cybersecurity issues was conducted for this report. Due to the widely varying approaches that states take to document the relevant information, there are likely some pending regulations or laws that are not captured in this review, but the examples below nonetheless highlight the wide array of different approaches being pursued at the state-level to bolster healthcare cybersecurity.

Oklahoma and New York are both taking an approach that seeks to get hospitals to develop robust cybersecurity programs. However, they are taking different angles on the problem. New York is creating a regulation that requires substantial and fairly specific actions by hospitals to create a cybersecurity program. The associated regulatory impact statement acknowledges that this will likely cost millions of dollars for many of the hospitals governed by the regulation. Oklahoma, on the other hand, passed a law in 2023 attempting to incentivize (vice requiring) hospitals to develop robust cybersecurity programs by creating a new affirmative defense to negligence lawsuits stemming from cybersecurity breaches. To be able to qualify to use the affirmative defense to such lawsuits, the hospitals have to have a cybersecurity program that meets certain requirements spelled out in the legislation.

New Jersey is perhaps the next most active state on this front, with three bills pending in the current legislative session. One of those bills effectively combines the other two by creating a new requirement for businesses in healthcare, finance, and essential infrastructure to report cybersecurity incidents to the state and prepare a detailed cybersecurity plan. Unlike the New York regulation, the proposed New Jersey bill would require organizations to use the most up-to date cybersecurity frameworks issued by several specific organizations, listed as: (1) the Framework for Improving Critical Infrastructure Cybersecurity developed by the National Institute of Standards and Technology; (2) the Center for Internet Security Critical Security Controls; or (3) the International Organization for Standardization and International Electromechanical Commission 2700 series of standards for an information security management system.

There have been a few states that have proposed some form of ban on hospitals or other entities paying ransom for cyber-incidents, but no examples could be located of such a bill becoming law. For example, there was one bill proposed during New York's 2021-2022 legislative session, which would have imposed a $10,000 civil fine for any hospital. It appears to have died in committee.

There are other approaches being pursued that are more removed from the healthcare industry, but that nonetheless would impact it in some way. Alaska, for example, makes a cyber security vulnerability assessment available to organizations in critical infrastructure sectors. In California, regulators are in the early stages of making a rule to require all businesses (above a certain size) to undergo periodic cybersecurity audits. There was also a Texas law enacted in 2023 that requires all businesses to report data breaches to the State in 30 days (shortening the prior 60 day window).

Many States have implemented some form of legislation providing for enhanced privacy protections for consumers. Though not directly targeted at the healthcare industry, these bills tend to raise the costs of data breaches and create new requirements that in theory could lead to hospitals investing more in their cybersecurity efforts. This is an indirect effect of such legislation, so laws that fell into this category were not included in this review. However, a very useful tracker of such state-level data privacy laws already in effect and currently under consideration, including comparisons of the types of provisions in each, is maintained by the International Association of Privacy Professionals and is a good starting point for someone seeking to get a high-level view of the status of these privacy-related statutes.

This review found that most states have not yet made a significant move towards addressing the cybersecurity risk in the healthcare sector. To the extent states are moving towards taking action on this front, it appears to be primarily focused on requiring or incentivizing hospitals to have cybersecurity plans. New York's regulation is the most detailed attempt identified in this review to address the threat healthcare-related cyber-incidents entail. New Jersey appears to be following the lead of New York and seems to be on track to pass legislation requiring a cybersecurity plan and imposing reporting requirements by the end of the current legislative session. Oklahoma is also encouraging the development of cybersecurity plans by hospitals, via the carrot of creating a liability shield for those that comply with some baseline cybersecurity requirements. Periodic efforts by multiple states to make paying ransoms illegal have not been successful.

IV. Current cybersecurity posture of the healthcare industry

A number of recent wide-ranging surveys have been conducted of healthcare organizations which capture the current cybersecurity posture of the industry. These surveys are reviewed below. They demonstrate both the current rate of adoption of various cybersecurity frameworks, the incidence rate of different types of cybersecurity threats, and trends in cybersecurity spending.

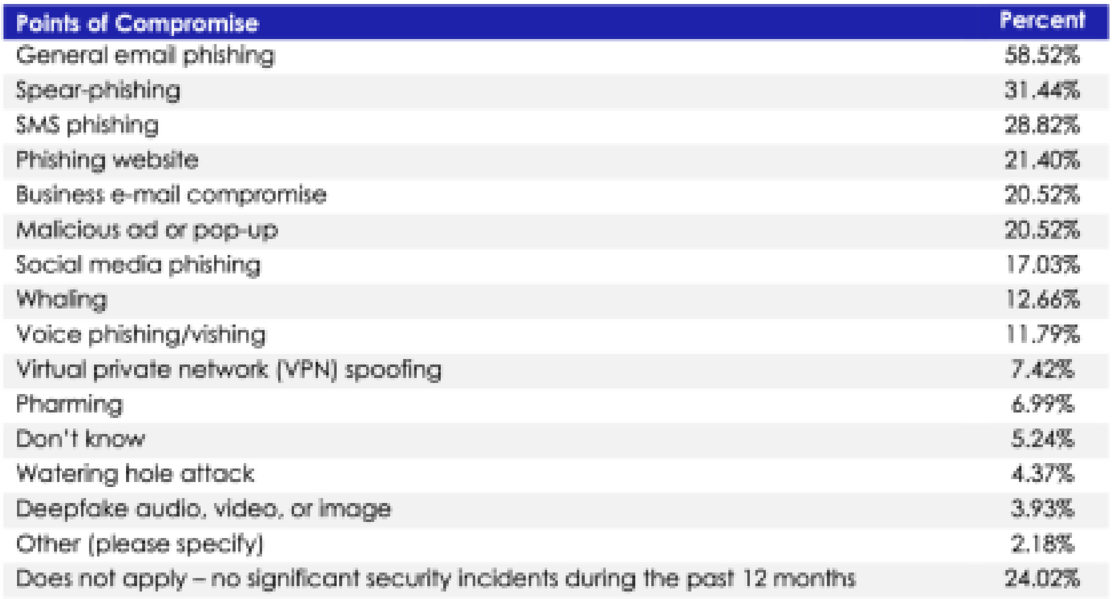
2023 Healthcare Information and Management Systems Society (HIMSS) Healthcare Cybersecurity Survey, available at https://www.himss.org/sites/hde/files/media/file/2024/03/01/2023-himss-cybersecurity-surveyx.pdf

- Reviews a broad range of information from healthcare cybersecurity professionals regarding budgets, workforce challenges, perceptions of the threat environment, AI adoption, oversight, and areas for future focus. Key highlights are below:
    - Recruiting cybersecurity professionals is a significant challenge due to both lack of qualified workers and inadequate budgets for hiring (page 5)
    - Retaining cybersecurity professionals is also challenging for reasons including lack of professional growth opportunities and inadequate compensation (page 6)
    - Inadequate investment (at the organizational level) in cybersecurity is hampering cybersecurity efforts (page 6)
    - Cybersecurity spending was reported to be on the rise, with most organizations (55.31%) reporting increased spending in 2023 versus 2022.
    - Traditionally, healthcare organizations tended to spend 6% or less of the IT budget on cybersecurity, but that is trending up, and in 2023 the average cybersecurity expenditure out of the IT budget was 7% or higher (pages 7-8). The below graphic (Figure 7) is from page 8 of the survey report showing the reported expenditures from 2023 data:

Figure 7: Percent of Organization's IT Budget Spent on Cybersecurity

- The majority of respondents (54.59%) reported that their organization experienced a significant security incident in the past 12 months (page 9)
- General email phishing was cited as the most frequent initial source of compromise in significant security incidents, as shown below (Figure 8, taken from page 11 of the survey report) along with other initial points of compromise:

Figure 8: 2023 Security Incidents: Initial Points of Compromise



Points of Compromise	Percent
General email phishing	58.52%
Spear-phishing	31.44%
SMS phishing	28.82%
Phishing website	21.40%
Business e-mail compromise	20.52%
Malicious ad or pop-up	20.52%
Social media phishing	17.03%
Whaling	12.66%
Voice phishing/vishing	11.79%
Virtual private network (VPN) spoofing	7.42%
Pharming	6.99%
Don't know	5.24%
Watering hole attack	4.37%
Deepfake audio, video, or image	3.93%
Other (please specify)	2.18%
Does not apply – no significant security incidents during the past 12 months	24.02%

Healthcare Cybersecurity Benchmarking Study 2024, available at [https://h-isac.org/partnered report-healthcare-cybersecurity-benchmarking-study-2024/](https://h-isac.org/partnered-report-healthcare-cybersecurity-benchmarking-study-2024/)

- Out of 58 healthcare industry respondents, (54 payer or provider organizations and 4 healthcare vendors), 57% used the NIST Cybersecurity Framework (see below for more details on this framework) as their primary cybersecurity framework, while another 14% used it but not as the primary cybersecurity framework. 29% used the Healthcare Industry Cybersecurity Practices (HICP). The study found that "high NIST CSF and HICP coverage is a strong indication of cybersecurity preparedness" (page 2).
- This survey also breaks down the types of functions healthcare organizations have focused on protecting, and those functions which are more neglected, observing in part that "[a]verage coverage across the five NIST CSF functions shows that organizations are generally more reactive than proactive in their approach to cybersecurity, with the Identify function having the lowest coverage and the Respond function having the highest. This year's HICP coverage is also similar to last year's, confirming that most organizations have Email Protection Systems in place but have a long way to go with Medical Device Security and Data Protection and Loss Prevention." (page 3 is the source of Figures 9 and 10 below)

Figure 9

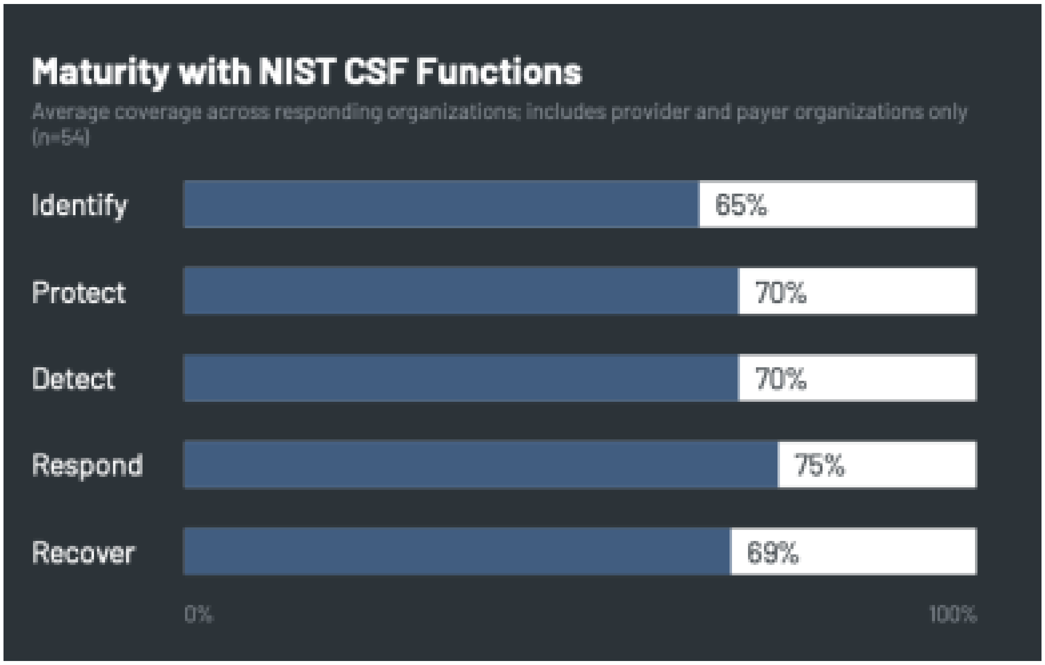
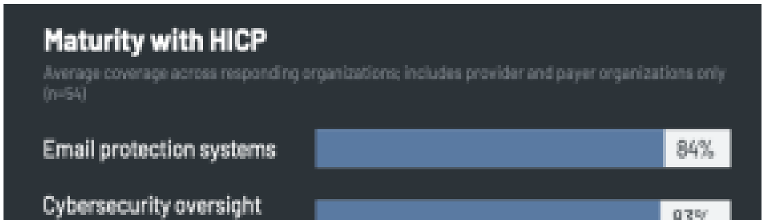


Figure 10



American Medical Association Informal Provider Survey Results Regarding the Change Healthcare cyberattack impact, accessible at https://www.ama-assn.org/system/files/change healthcare-survey-results.pdf

- A useful reference for demonstrating the degree of vulnerability of providers to a cyberattack on a critical business partner. It does not include details on what cybersecurity measures providers are taking, but for this particular attack (the UnitedHealth Group/Change Healthcare cyberattack) the problem was not the healthcare providers' cybersecurity posture. Rather, healthcare providers who suffered no breach of their own were nonetheless severely harmed by a breach at a critical partner. This serves as a reminder that it is not enough to require healthcare providers to have robust cybersecurity, because they can still be crippled by the loss of key services provided by third-party vendors that are targeted by cyberattacks.

NIST Cybersecurity Framework (CSF), available at https://www.nist.gov/cyberframework

- This is one of the cybersecurity frameworks cited as being widely employed in the above referenced *Healthcare Cybersecurity Benchmarking Study 2024*. This is also one of the three frameworks expressly mentioned in the proposed New Jersey legislation discussed in the legislation section of this report.

Healthcare Industry Cybersecurity Practices (HICP), available at https://405d.hhs.gov/cornerstone/hicp#best-practices

- This is a second cybersecurity framework cited by the *Healthcare Cybersecurity Benchmarking Study 2024* as being widely employed in the healthcare industry. The HICP consists of 10 healthcare-specific cybersecurity practices that are based on the main healthcare industry cybersecurity threats.

V. Information on costs of cyber incidents

In a 2023 study, IBM Security found that the average cost of a data breach in the healthcare industry was 10.93 million (see Figure 11 below, taken from page 13 of the IBM study). The study also found that the average cost for a data breach for a healthcare organization went up 53.3% from 2020-2023 (page 13). In a 2019 study, the Health Sector Cybersecurity Coordination Center of the Department of Health and Human Services reviewed the costs of healthcare sector data breaches, finding that the average cost to an organization per stolen healthcare record in 2018 was as high as $408 (page 4).

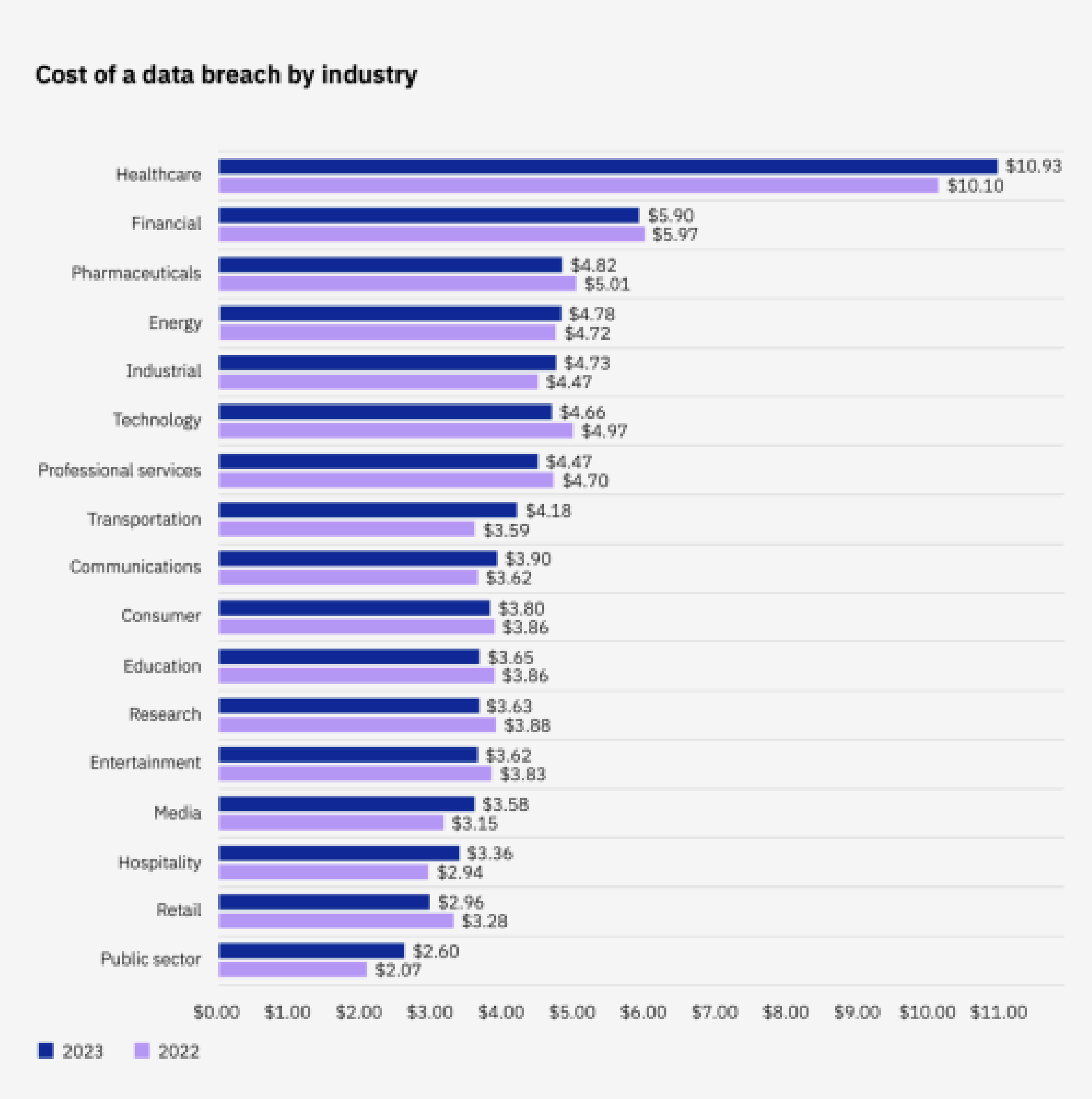
Specific information on the actual costs of business disruptions caused by cybersecurity incidents varies widely with the type of attack and is often not reported publicly. However, some insight into the magnitude of costs from business disruptions in the ransomware era can be gained by referencing the most recent earnings report from UnitedHealth Group, which provided estimated costs from the most recent cyber attack discussed in the first section of this report. UnitedHealth Group reported $279 million in business disruption costs from this attack, plus $593 million in direct response costs (page 5 of the enclosure to the earnings report, titled “Earnings by Business-Supplemental Financial Information”). These costs did not include fines and litigation costs that will undoubtedly substantially raise the final cost of this cyber attack. While most medical organizations are far smaller than UnitedHealth Group, and thus might expect far lower costs, it is worth noting that business disruption costs accounted for nearly ⅓ of total costs reported thus far. It is unclear if this is a ratio of business disruption costs-to-total costs of a cyber-attack that can be expected in future attacks, but it suggests that healthcare companies facing ransomware attacks can expect substantial costs due to business disruption.

Other costs that can be expected for affected organizations include regulatory fines (see figure 3 above), ransom payments, and class action lawsuits. One study by law firm BakerHostetler, which has tracked and reported data from data breach incidents for nearly a decade, reported that the “[a]verage ransom paid (for all industries) increased 15% in 2022 to $600,688. The health care industry saw the largest increase in average ransom paid ($1,562,141, up 78% from 2021).” This indicates that healthcare organizations are paying significant ransoms when targeted and that those ransoms are well above the average for other industries. The $22 million ransom paid by UnitedHealth Group in response to its recent cyber incident is consistent with this trend.

Class action lawsuits are also on the rise, with a 2023 Bloomberg Law study finding a noticeable acceleration in the filing of class action lawsuits related to healthcare data breaches (see Figure 12 below, taken from the study). While the costs associated with class action lawsuits vary widely based on the facts of the case, one ongoing Maryland case gives a rough sense of the magnitude of costs that Maryland-based firms might expect. In a recent ruling in *Brent v. Advanced Medical Management*, a U.S. District Court in Maryland rejected a proposed settlement valued at $3,000,000 for a data breach class action lawsuit stemming from a breach that affected over 300,000 individuals. Thus, it is reasonable to anticipate class action lawsuit costs to a compromised organization of several million dollars for a medium to large-sized breach.

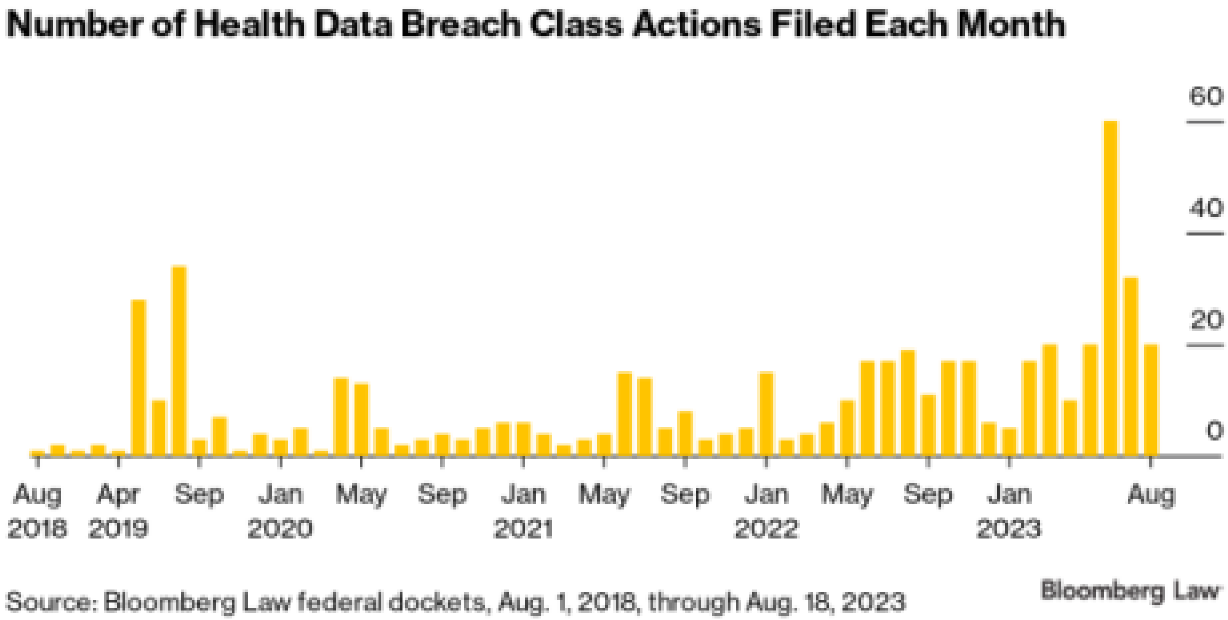
Taken together, the data indicates that healthcare organizations face rapidly increasing costs from cyber incidents that are becoming increasingly damaging and affecting increasingly larger groups of people. There is no indication that these trends will slow in the near future.

Figure 11 Cost of a data breach by industry (in millions of US Dollars)



Cost of a data breach by industry

Figure 12



Number of Health Data Breach Class Actions Filed Each Month

Source: Bloomberg Law federal dockets, Aug. 1, 2018, through Aug. 18, 2023

Bloomberg Law

Works Cited

All works cited below are in the order they appear in the report. Links to each are also included in the body of the report when these works are referenced.

“Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information,” U.S. Department of Health and Human Services Office for Civil Rights, accessible at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf, last visited 19 July 2024.

“HHS Office for Civil Rights Issues Letter and Opens Investigation of Change Healthcare Cyberattack,” U.S. Department of Health and Human Services Press Office (March 13, 2024), accessible at https://www.hhs.gov/about/news/2024/03/13/hhs-office-civil-rights-issues-letter opens-investigation-change-healthcare-cyberattack.html, last visited 19 July 2024.

“Internet Crime Report 2023,” FBI Internet Crime Complaint Center, accessible at https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf last visited 19 July 2024.

Steve Alder, “Healthcare Data Breach Statistics,” The HIPAA Journal (18 July 2024), accessible at https://www.hipaajournal.com/healthcare-data-breach-statistics/, last visited 19 July 2024.

“Attorney General James Holds American Medical Collection Agency Responsible for 2019 Data Breach,” Office of the New York State Attorney General Press Release (11 March 2021), accessible at https://ag.ny.gov/press-release/2021/attorney-general-james-holds-american medical-collection-agency-responsible-2019, last visited19 July 2024.

“Frequently Asked Questions,” UnitedHealth Group, accessible at https://www.unitedhealthgroup.com/ns/changehealthcare/faq.html, last visited 19 July 2024.

“Cybersecurity Event Update,” Ascension, accessible at https://about.ascension.org/en/cybersecurity-event, last visited 19 July 2024.

“What We Learned: Change Healthcare Cyber Attack,” Energy & Commerce Chair Rodgers Blog (3 May 2024), accessible at https://energycommerce.house.gov/posts/what-we-learned change-healthcare-cyber-attack, last visited 19 July 2024.

“AHA Survey: Change Healthcare Cyberattack Significantly Disrupts Patient Care, Hospitals’ Finances,” American Hospital Association, accessible at https://www.aha.org/2024-03-15-aha survey-change-healthcare-cyberattack-significantly-disrupts-patient-care-hospitals-finances, last visited 19 July 2024.

"Change Healthcare cyberattack impact: Key takeaways from informal AMA follow-up survey," American Medical Association (29 April 2024), accessible at https://www.ama assn.org/system/files/change-healthcare-follow-up-survey-results.pdf, last visited 19 July 2024.

Rachana Pradhan & Kate Wells, "Cyberattack led to harrowing lapses at Ascension hospitals, clinicians say," National Public Radio (19 June 2024), accessible at https://www.npr.org/2024/06/19/nx-s1-5010219/ascension-hospital-ransomware-attack-care lapses, last visited 19 July 2024.

Andrew N. Pollak et al., "Health Care Data Breaches: Perspectives on Breach Trends in Maryland and Comparative States," Maryland Health Care Commission (September 2021), accessible at https://mhcc.maryland.gov/mhcc/pages/hit/hit_cybersecurity/documents/Health_Care_Data_Bre a ches_Rpt.pdf, last visited July 19, 2024.

"Hospital Cybersecurity Requirements," Proposed New York State Regulation 405.46 of Title 10 (Health) of the Official Compilation of Codes, Rules, and Regulations of the State of New York, accessible at https://regs.health.ny.gov/sites/default/files/proposed regulations/Hospital%20Cybersecurity%20Requirements.pdf, last visited 19 July 2024.

"Oklahoma Hospital Cybersecurity Protection Act of 2023," Oklahoma H.B. 2790, enacted 26 April 2023, accessible at http://webserver1.lsb.state.ok.us/cf_pdf/2023-24%20ENR/hB/HB2790%20ENR.PDF, last visited 19 July 2024.

"Senate Committee Substitute for Senate, Nos. 3100 and 3101," State of New Jersey 221st Legislature, adopted by Senate Committee 13 June 2024, accessible at https://www.njleg.state.nj.us/bill-search/2024/S3100, last visited 19 July 2024.

"Cybersecurity Framework," National Institute of Standards and Technology, accessible at https://www.nist.gov/cyberframework, last visited 19 July 2024.

"CIS Critical Security Controls," Center for Internet Security, accessible at https://www.cisecurity.org/controls, last visited 19 July 2024.

"ISO/IEC 2700 family Information Security Management," International Organization for Standardization, accessible at https://www.iso.org/standard/iso-iec-27000-family, last visited 19 July 2024.

"Senate Bill S6806A," The New York State Senate 2021-2022 Legislative Session, accessible at https://www.nysenate.gov/legislation/bills/2021/S6806#, last visited 19 July 2024.

"Cyber Security Vulnerability Assessment," Alaska Division of Homeland Security and Emergency Management Planning Section, accessible at https://ready.alaska.gov/Plans/CSVA, last visited 19 July 2024.

"Proposed Rulemaking Draft: Cybersecurity Audit Regulations," California Privacy Protection Agency (December 2023), accessible at https://cppa.ca.gov/meetings/materials/20231208_agenda_item2a_cybersecurity_audit_regulatio ns_clean.pdf, last visited 19 July 2024.

"Texas S.B. 768," Texas Legislative Session 88(R), Texas Legislature Online, accessible at https://capitol.texas.gov/BillLookup/History.aspx?LegSess=88R&Bill=SB768, last visited 19 July 2024.

"US State Privacy Legislation Tracker 2024," International Association of Privacy Professionals, accessible at https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf, last visited 19 July 2024.

"2023 HIMSS Cybersecurity Survey," Healthcare Information and Management Systems Society (HIMSS), accessible at https://www.himss.org/sites/hde/files/media/file/2024/03/01/2023-himss cybersecurity-survey-x.pdf, last visited 19 July 2024.

"Partnered Report: Healthcare Cybersecurity Benchmarking Study 2024: Improving Cybersecurity Preparedness through NIST CSF & HICP Best Practices," Health-ISAC, accessible at https://h-isac.org/partnered-report-healthcare-cybersecurity-benchmarking-study 2024/, last visited 19 July 2024.

"Health Industry Cybersecurity Practices," HHS 405(d), accessible at https://405d.hhs.gov/cornerstone/hicp#best-practices, last visited 19 July 2024.

"Cost of a Data Breach Report 2023," IBM Security, accessible at https://www.ibm.com/downloads/cas/E3G5JMBP, last visited 19 July 2024.

"A Cost Analysis of Healthcare Sector Data Breaches," Health Sector Cybersecurity Coordination Center (HC3) (12 April 2019), accessible at https://www.hhs.gov/sites/default/files/cost-analysis-of-healthcare-sector-data-breaches.pdf, last visited 19 July 2024.

"UnitedHealth Group Reports First Quarter 2024 Results," UnitedHealth Group (16 April 2024), accessible at https://www.unitedhealthgroup.com/content/dam/UHG/PDF/investors/2024/UNH Q1-2024-Release.pdf, last visited 19 July 2024.

"BakerHostetler Launches 2023 Data Security Incident Response Report," BakerHostetler LLP (27 April 2023), accessible at https://www.bakerlaw.com/insights/bakerhostetler-launches-2023-data-security-incident-response-report/, last visited 19 July 2024.

Skye Witley & Christopher Brown, "Health Data Breach Class Actions Surge as Cyberattacks Climb," Bloomberg Law (22 August 2023), accessible at https://news.bloomberglaw.com/privacy-and-data-security/health-data-breach-lawsuits-surge-as cyberattacks-keep-climbing, last visited 19 July 2024.

Brent v. Advanced Medical Management LLC, Civil No. JKP-23-3254 (D. Md., May 7, 2024), accessible at https://caselaw.findlaw.com/court/us-dis-crt-d-mar/116158943.html, last visited 19 July 2024.