

Yelin Testimony - SB691 2025.pdf

Uploaded by: Ben Yelin

Position: FAV



TESTIMONY IN SUPPORT OF SB691- CYBERSECURITY - HEALTHCARE ECOSYSTEM

EDUCATION, ENERGY AND THE ENVIRONMENT

FEBRUARY 27, 2025

Chair Feldman, Vice Chair Kagan, and members of the Committee - thank you for the opportunity to testify in support of SB691 – Cybersecurity – Healthcare Ecosystem.

My name is Ben Yelin, and I am the Program Director for Public Policy & External Affairs at the University of Maryland Center for Health and Homeland Security. During the interim, we worked with Senator Hester on a report detailing the frequency and impact of cyber-attacks on the entities making up the healthcare ecosystem: hospitals, insurance companies, community health centers and more. An analysis of this threat landscape was sobering. Healthcare is an attractive target for cyber criminals for several reasons. First, the system contains valuable data, including patient protected health information (PHI) and personal identifying information (PII). This valuable data can be sold on the dark web for amounts far exceeding, for example, stolen credit card information. Second, the disruption to health systems is devastating in its impact to communities. It can cause downstream effects that lead to bad patient outcomes. Cyber criminals are fully aware that the potential for this catastrophic disruption may be an incentive for these healthcare entities to pay significant ransoms.

The numbers back up the nature of this threat. Nationally, there has been a 254% increase in cyber attacks on health systems over the past five years.¹ In the last year for which data were available, 3.5 million Maryland residents were impacted by hacking/IT incidents in the health care sector. With the frequency of these attacks, we've seen both significant kinetic and financial impacts to not just the health systems themselves, but to our communities. According to one recent study², of the 68% of hospitals impacted by ransomware attacks, 28% reported an increase in the mortality rate, 59% reported delays in procedures and tests leading to poor outcomes, and 44% reported increases in complications during medical procedures. In terms of financial impacts, a 2024 study indicated that hospitals suffering a cyber incident lost an average of \$1.47 million in revenue.

What makes attacks in healthcare unique is that an attack on one part of the ecosystem has a cascading impact in the entire ecosystem. When Change Health Care, a subsidiary of UnitedHealth Group, suffered a cyber attack, the impacts were devastating, even though the attack had **no direct impact** on hospitals, providers or insurers. But because Change Health Care served as an intermediary to facilitate important functions like eligibility checks, insurance claims submissions and billing services for care centers and pharmacies, the entire ecosystem suffered. 74% of affected hospitals suffered impacts to patient care, while 94% reported a significant or substantial impact.

The breadth and depth of this problem highlights the need for a comprehensive, common-sense policy framework to protect the healthcare ecosystem in Maryland. SB691 represents such an approach.

¹ Data Breach Statistics, <https://www.hipaajournal.com/healthcare-data-breach-statistics/>

² 2024 Ponemon Healthcare Cybersecurity Report, [https://assets.turtl.co/customer-assets/tenant%3Dteam/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report-2024%20\(1\).pdf](https://assets.turtl.co/customer-assets/tenant%3Dteam/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report-2024%20(1).pdf)



Under this bill, healthcare entities must adopt cybersecurity standards that are equal to or exceed industry standards as outlined by the National Institute of Standard and Technology (NIST) framework. To ensure compliance with these standards, entities would be subject to third party audits to evaluate the entity's practices and resources. Upon completion of these audits, entities would submit a report to the Maryland Health Care Commission (MHCC), who would aggregate the data and draft a report outlining the system's current cybersecurity posture, to be submitted to the State Chief Information Security Officer. This critical information will ensure that the State can identify gaps and issue recommendations to improve cybersecurity for the entire ecosystem. The bill also includes other valuable provisions, including incident reporting requirements, and the creation of a stakeholder workgroup to resolve outstanding issues.

SB691 is not an entirely novel approach. In 2023, the General Assembly enacted SB800/HB969 which instituted similar obligations for another critical infrastructure sector: state utilities. That bill also included a requirement that entities adopt cybersecurity standards incorporating NIST standards and guidance, a provision requiring third party cybersecurity audits, and another mandating incident reporting. While obligations under this bill and SB800/HB969 may at times seem inconvenient for individual entities, the General Assembly has recognized that when it comes to critical infrastructure, a holistic regulatory framework that makes there are no vulnerability weak points can prevent the kinetic and financial impacts of a cyber incident.

For these reasons, I respectfully request a favorable report on SB691.

Clay House__SB 691__Favorable 20250227 2.pdf

Uploaded by: Clay House

Position: FAV

TESTIMONY PRESENTED TO THE
HEALTH AND GOVERNMENT OPERATIONS COMMITTEE

SB 691
CYBERSECURITY - HEALTHCARE ECOSYSTEM

MR. CLAY HOUSE
5221 BORDEAUX CV
ELLICOTT CITY, MD 21043
February 27, 2025

Madam Chair, Mister Vice Chair, and members of the committee, good afternoon and thank you for the opportunity to testify in favor of SB 691. I am Clay House, a 20-year Maryland resident who recently retired as Vice President/Chief Information Security Officer at CareFirst.

The financial and patient safety threats of cyberattacks against the healthcare ecosystem are clear. Financially, the healthcare industry experiences the highest average cost per breach at \$9.8M.¹ As bad as that is, now imagine being a patient, or a family member of a patient, needing care only to have it delayed because of a system outage somewhere in the healthcare ecosystem. These attacks do more than disrupt the business – they put lives at risk. They create barriers to care, leading to adverse healthcare outcomes and increased mortality rates.²³⁴

The healthcare system is not a single entity. Rather it is a collection of organizations and vendors who must continually interoperate to ensure the delivery of care and patient safety. If any key participants of this ecosystem are impacted, those impacts ripple across the other participants. There is no better example of this than the Change Healthcare incident.

Change Healthcare is a health information exchange that connects insurers, providers, Pharmacy Benefit Managers (PBMs), and hospitals supporting the flow of authorizations, eligibility, claims submission, payments, and statuses. When Change Healthcare was taken down by hackers in February of 2024, these transactions stopped for their customers impacting the entire system – even those who weren't their customers.

¹ [Average cost of healthcare data breach nearly \\$10M in 2024: report | Healthcare Dive](#)

² [AHA Change Healthcare Cyberattack Having Significant Disruptions on Patient Care, Hospital's Finances](#)

³ [Change Healthcare cyberattack impact: Key takeaways from informal AMA follow-up survey](#)

⁴ [The Devastating Impacts of Ransomware Attacks in Healthcare](#)

An American Hospital Association (AHA) survey of hospitals highlights both the financial as well as the patient care impact noting⁵

- 74% of hospitals reported patient difficulty accessing care
- 82% of hospitals reported financial impacts – 33% impacted >50% of revenue and 60% reporting impacts of \$1M+/day

Similarly, the American Medical Association (AMA) reported that in April, 2024,

- 90% of practices continued losing money
- 62% using personal funds for expenses
- 60% of practices reported challenges confirming patient eligibility
- 30% issues with authorizations.

Even though Change Healthcare was the only entity directly attacked, the impacts were felt across the nation. Hackers have noticed this leading AHA's National Advisor on Cybersecurity and Risk, John Riggi to assert "cyber adversaries have mapped our sector" targeting key central services calling it "one-stop hacking". In an interview, he supported programs such as HHS 405(d)⁶ stating "we need to plan regionally for highly disruptive ransomware - incident-response plans cannot be developed in a silo".⁷

You may hear opposing testimony today that current regulations are sufficient and with new regulations overly burdensome. However current regulations are intentionally ambiguous in certain areas and lack prescriptiveness in defining controls. This has led to CISA creating the Cross-Sector Cybersecurity Performance Goals (CPGs), HHS creating the 405(d) Healthcare Organization Goals, and the proposed HIPAA Security Rule currently out for public comment.

Current regulatory processes perpetuate the silos by ignoring the risks driven by the interconnectedness of the healthcare system. As evidenced by the Change Healthcare incident, this siloed approach failed to identify and mitigate system-wide impacts.

In fairness to the regulators, it is impossible for them to identify the threats to the ecosystem and to foresee the impacts of outages. To do so requires active participation of industry stakeholders to assess the system-wide risk, identify essential services, and design for resiliency.

SB 691 takes a proactive approach to securing Maryland's healthcare ecosystem by implementing the following key measures:

- Mandates independent audits based on CISA Cross-Sector Performance Goals for Critical Infrastructure and the NIST framework
- Mandates compiling these audits into a system-wide view to assess the risk to the system as a whole vs silos
- Establishes an industry-led workgroup to review the system-wide audit results and make recommendations regarding cybersecurity controls
- Establishes an industry-led workgroup to
 - Identify essential services across the healthcare ecosystem
 - Recommend necessary steps to ensure the resiliency of these services

The threat is clear. We have empirical evidence of the financial and patient impact as well as a clear example of an attack rippling across the healthcare sector. These are not hypothetical. This will happen again.

I agree with Mr. Riggi. Criminal and Nation State actors understand that they can cripple our healthcare system by attacking common services. An industry-led workgroup to address this vulnerability and a system-wide view of the risks is the only way to drive the resilience of our healthcare system.

Without these actions, Maryland's healthcare system remains dangerously exposed, and its citizens remain at risk. I strongly urge your support for SB 691 to protect patients, providers, and the integrity of our healthcare infrastructure.

Thank you for the opportunity to testify.

⁵ [AHA Change Healthcare Cyberattack Having Significant Disruptions on Patient Care, Hospital's Finances](#)

⁶ [Government should go on offense against healthcare cyberattacks, says AHA | Healthcare IT News](#)

⁷ [Government should go on offense against healthcare cyberattacks, says AHA | Healthcare IT News](#)

AHA-Testimony-for-Energy-and-Commerce-Subcommittee

Uploaded by: Katie Fry Hester

Position: FAV

Testimony

of the

American Hospital Association

for the

Committee on Energy and Commerce

Subcommittee on Health

of the

U.S. House of Representatives

"Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack"

April 16, 2024

Chairman Guthrie, Ranking Member Eshoo and members of the Subcommittee, my name is John Riggi and I am the National Advisor for Cybersecurity and Risk at the American Hospital Association (AHA). Prior to joining the AHA, I spent nearly 30 years working at the FBI, including as a senior executive for the Bureau's Cyber Division.

On behalf of AHA's nearly 5,000 member hospitals, health systems and other health care organizations, our clinician partners — including more than 270,000 affiliated physicians, 2 million nurses and other caregivers — and the 43,000 health care leaders who belong to our professional membership groups, thank you for the opportunity to testify at today's hearing, "Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack." In my testimony, I will provide background regarding the cyberattack on Change Healthcare, give an update on the current state of play, and outline the impacts on hospitals, health systems and patients around the country. I also will highlight proposals for Congress and the Administration to consider going forward, as well as share concerns about proposals that would unfairly penalize hospitals and not improve cybersecurity of the entire health care sector.



HOSPITALS AND HEALTH SYSTEMS ARE COMMITTED TO CYBERSECURITY

Hospitals and health systems have invested billions of dollars and taken many steps to protect patients and defend their networks from cyberattacks that can disrupt patient care and erode privacy by the loss of personal health care data. The AHA has long been committed to helping hospitals and health systems with these efforts, working closely with our federal partners, including the FBI, the Department of Health and Human Services (HHS), National Security Council, Cybersecurity and Infrastructure Security Agency and many others to prevent and mitigate cyberattacks.

As data theft and ransomware attacks targeting health care have increased dramatically over the past several years, the AHA has worked closely with federal agencies and the hospital field to build trusted relationships and channels for the mutual exchange of cyber threat information, risk mitigation practices and resources to implement these practices. The AHA's work in this area was critically important and allowed us to quickly assist members in their response to the Change Healthcare cyberattack.

BACKGROUND ON THE CYBERATTACK AND IMPACT TO HOSPITALS, HEALTH SYSTEMS, COMMUNITIES AND PATIENTS

On Feb. 21, Change Healthcare, a subsidiary of UnitedHealth Group, was the victim of the most significant and consequential cyberattack on the U.S. health care system in American history. Change Healthcare is the predominant source of more than 100 critical functions that keep the health care system operating. Among them, Change Healthcare manages the clinical criteria used to authorize a substantial portion of patient care and coverage, processes billions of claims, supports clinical information exchange, and processes drug prescriptions. Significant portions of Change Healthcare's functionality were incapacitated and are still being brought back online. As a result, patients struggled to get timely access to care and billions of dollars stopped flowing to providers, thereby threatening the solvency of our nation's provider network including hospitals, health systems, physicians, pharmacists and virtually every other type of care provider.

According to Change Healthcare, the company processes 15 billion health care transactions annually and touches 1 in every 3 patient records. These transactions include a range of services that directly affect patient care, including insurance eligibility verifications and pharmacy operations, as well as claims transmittals and payment. Change Healthcare is part of UnitedHealth Group, which is a Fortune 5 company that brought in more than \$370 billion in revenue and \$22 billion in profit in 2023 and has reach throughout the health care sector. When UnitedHealth Group proposed its acquisition of Change Healthcare in 2021, the AHA wrote to the Department of Justice (DOJ) to express its significant concerns about the transaction, explaining that "[t]he acquisition also will concentrate an immense volume of competitively sensitive data in

the hands of the most powerful health insurance company in the United States.”¹ The Department of Justice’s listened to the AHA’s concerns, and during its investigation of the deal, DOJ uncovered internal Change Healthcare documents stating that the “healthcare system, and how payers and providers interact and transact, would not work without Change Healthcare.”² The past two months have shown everyone what Change knew years ago: The health care system did not work without Change Healthcare.

This unprecedented attack against one of America’s largest health care companies imposed significant consequences on patients and the hospitals, health systems and other providers who care for them. In some communities, patients struggled to obtain prescriptions or faced delays in scheduling care or receiving and paying bills. Responses to a March AHA survey representing nearly 1,000 hospitals found that 74% reported direct patient care impact, including delays in authorizations for medically necessary care.³ In addition, hospitals, health systems and other providers have experienced extraordinary reductions in cash flow. In the same survey, 94% of hospitals reported that the Change Healthcare cyberattack was impacting them financially, with more than half reporting the impact as “significant or serious.” Indeed, a third of the survey respondents indicated that the attack disrupted more than half of their revenue.

The staggering loss of revenue has meant that some hospitals and health systems had to seek alternate ways to ensure they could pay salaries for clinicians and other members of the care team, acquire necessary medicines and supplies, and pay for mission critical contract work in areas such as physical security, dietary and environmental services. In addition, replacing previously electronic processes with manual processes has often proved ineffective and is adding considerable administrative costs for providers, as well as diverting team members from other tasks. Nearly all hospitals that responded to AHA’s survey have implemented one or more workarounds with varying degrees of success and at high cost. While 81% of survey respondents have found these workarounds to be “somewhat” effective, nearly half reported that the cost to their organization to implement workarounds was “significant or serious.”

CURRENT STATE OF PLAY

Since the AHA first learned of the attack, we have remained in communication with UnitedHealth Group leadership to lend our support and share our members’ challenges because of the Change Healthcare outage.

¹ <https://www.aha.org/system/files/media/file/2021/03/aha-urges-doj-investigate-unitedhealth-groups-acquisition-change-healthcare-letter-3-18-21.pdf>
<https://www.aha.org/lettercomment/2021-08-04-letter-doj-antitrust-division-unitedhealth-groups-proposed-acquisition>

² <https://www.justice.gov/atr/case-document/file/1476901/dl>, Page 12

³ The AHA issued a survey to all U.S. hospitals on Friday, March 9, 2024. These results reflect responses representing 960 hospitals as of the morning of Tuesday, March 12, 2024.

During the early days and weeks of the event, it was very difficult to obtain clear information from UnitedHealth Group. Initially, there was little communication and a minimization of the impact this event was having on the ability to process medical claims. While this event had disparate impacts on providers, ultimately all communities felt the effects in some way. Change Healthcare's loss of functionality due to the cyberattack prevented most payers' ability to process claims and complete other critical functions for the delivery and payment of care. According to Kodiak Solutions, a revenue cycle data analytics firm, the value of claims submitted dropped \$6.3 billion for their 1,850 hospital and 250,000 physician clients alone.⁴

While much of the claims and payment system functionality has been restored, it remains unclear as to how long it will take for all operations to return to normal. This is because reconnecting is not the only step to recovery. Providers will need to work through the backlog of claims, reprocess denials received during this time, reconcile payments to accounts, and bill patients, among other tasks. Therefore, hospitals, physicians and patients are continuing to experience financial and operational impacts. In the AHA's March survey, 60% of hospitals reported they expect it would take between two weeks and three months to resume normal operations once Change Healthcare's full prior functionality is established, and some expect impacts to linger for even longer.

The burden — financial and workload — has been immense. While some hospitals were able to access Medicare's advance and accelerated payments (AAP) and UnitedHealth Group's temporary financial assistance program, many had to pull from reserves or take out private loans to continue providing 24/7 care for their communities. In the meantime, UnitedHealth Group and other insurers have held on to premium dollars, collecting as-yet unknown amounts of interest on what they have not paid out to providers. What we do know, however, is that UnitedHealth Group reported to the Securities and Exchange Commission on March 21 that, "the Company has not determined the incident is reasonably likely to materially impact the Company's financial condition or results of operations,"⁵ even as it has harmed providers across the country.

It is unclear what other impacts may emerge over the coming weeks and months, and we urge Congress and the Administration to continue oversight of the aftermath of the attack.

While we will continue to work with UnitedHealth Group and other payers as this situation evolves to communicate the state of the field and ensure support for our members and the patients they serve, all options for assistance must be explored so that the health care field can continue to care for patients and communities.

⁴ <https://www.hcinnovationgroup.com/cybersecurity/news/53099257/cyberattack-costing-hospitals-2-billion-a-week-in-cash-flow-report-shows>

⁵ <https://www.sec.gov/ix?doc=/Archives/edgar/data/731766/000073176624000085/unh-20240221.htm>

ACTION BY DEPARTMENT OF HEALTH AND HUMAN SERVICES AND RECOMMENDATIONS TO ASSIST HOSPITALS AND HEALTH SYSTEMS

On day 18 of the initial event, the Centers for Medicare & Medicaid Services (CMS) issued a [notice](#) formally announcing terms for hospitals, physicians and other providers impacted by the Change Healthcare cyberattack to apply for AAPs. The agency stated that it would provide a maximum of a 30-day payment amount, with repayment in full required 90 days after the date that the AAP is issued. However, we are close to completing the second month of disruption from this attack, so hospitals and health systems will need additional support. **Specifically, we urge Congress and CMS to consider supporting legislation to expand these programs to help providers access necessary support in future events. AHA would support allowing providers to access up to 90 days of payment, as well as an extension of the recoupment terms. Currently, payback begins immediately at 100%; AHA would support a delay and a reduced recoupment amount, such as 25% or 50%. In addition, interest rates are at prevailing Treasury rates, which is over 12%. During COVID-19, Congress reduced that amount to 4%. The AHA would support Congress taking similar action to reduce the interest rates. For this event, needed flexibilities were not immediately available, which threatened the viability of our nation's provider network. Additional authority for the AAP would allow CMS to expand these programs to make them more responsive to the needs of providers during an emergency going forward.**

The AHA welcomed the [letter](#) sent on March 10 to all providers from HHS and the Department of Labor recognizing the unprecedented nature of the Change Healthcare cyberattack and its far-reaching impacts on hospitals, physicians and the health care sector. We appreciated the letter asked for greater transparency from UnitedHealth Group and expedited payments to impacted providers so that they can continue timely care for patients. The departments also urged other commercial insurance companies and payers to make interim payments to providers, ease administrative burdens, and pause prior authorizations, requirements on timely billing and other utilization management requirements. It is critical that all payers help providers during this incident to ensure patient care is not compromised. **We urge payers to broadly adopt waivers of timely filing requirements for new claims and appealing denied claims within a 45-day window of the attack (Feb. 21, 2024) and its full resolution, as well as waivers of prior authorization for a shorter window (e.g., within 14 days of the cyberattack until the point of full resolution).**

We recognize that the federal government does not have statutory authority to require private payers to take all the actions that may be needed, and, therefore, Congress may need to take specific steps to ensure that payers do not penalize providers and patients. We will continue to work with Congress and policymakers as the impacts from the cyberattack persist.

REACTION TO HHS OFFICE FOR CIVIL RIGHTS INVESTIGATION

In a March 13 [letter](#), the HHS Office for Civil Rights (OCR) notified stakeholders it was initiating an investigation into the Change Healthcare cyberattack that will focus on whether a breach of protected health information occurred, as well as Change Healthcare and UnitedHealth Group's compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security and Breach Notification Rules. The AHA is grateful that OCR recognizes that the cyberattack "is disrupting health care and billing information systems nationwide" and "poses a direct threat to critically needed patient care and essential operations of the health care industry." **While OCR is not prioritizing investigations of health care providers, the AHA remains concerned providers may be required to make breach notifications to HHS and affected individuals if it is later determined that a breach occurred.**

The AHA has requested OCR provide additional clarification that hospitals and other providers do not have to make additional notifications if UnitedHealth Group and Change Healthcare are doing so already. Providing duplicative notifications is inconsistent with Change Healthcare's regulatory obligations. **Given the scope and scale of the cyberattack on Change Healthcare, without a unified notification process, patients could possibly face multiple notifications of this same breach, which could unnecessarily increase public confusion and misunderstandings. We ask Congress to reinforce this important message with OCR and HHS, urging those agencies to take steps to protect patients and providers from these needless consequences.**

COMMENTS ON CYBERSECURITY PROPOSALS

The AHA supports voluntary consensus-based cybersecurity practices, such as those [announced](#) in January by HHS. These cybersecurity performance goals (CPGs) are targeted at defending against the most common tactics used by cyber adversaries to attack health care and related third parties, such as exploitation of known technical vulnerabilities, phishing emails and stolen credentials.

The AHA was meaningfully involved in the development of the CPGs and will continue to work collaboratively with HHS, the Healthcare Sector Coordinating Council and other federal partners to enhance cybersecurity efforts for the entire health care field, including hospitals and health systems, technology providers, payers, pharmacists and other vendors, to ensure we are all protected against the primary source of cyber risk – criminal and nation state-supported cyber adversaries.

Hospitals and health systems are not the primary source of cyber risk exposure facing the health care sector. A review of the top data breaches in 2023 shows that over 95% of the most significant health sector data breaches, defined by those where over 1 million records were exposed, were related to "business associates" and other non-hospital health care entities, including CMS, which had a breach included in the top 20 largest data breaches last year. Any proposals that unfairly focus on one part of the

health care sector will ultimately not address cyber-risk in a comprehensive, strategic manner.

For example, the President's fiscal year (FY) 2025 budget recommends new penalties for hospitals and health systems for not meeting what the Administration defines as essential cybersecurity practices. Beginning in FY 2029, the Administration proposes to enforce adoption of essential practices with hospitals failing to meet these standards facing penalties of up to 100% of the annual market basket increase and, beginning in FY 2031, potential additional penalties of up to 1% off the base payment. Critical access hospitals that fail to adopt the essential practices would incur a payment reduction of up to 1%, but their total penalty is capped. While it is coupled with funding purported to assist hospitals in defending against cyberattacks, the per hospital benefit would be extremely limited.

The AHA opposes proposals for mandatory cybersecurity requirements being levied on hospitals as if they were at fault for the success of hackers in perpetrating a crime. The now well-documented source of cybersecurity risk in the health care sector, including the Change Healthcare cyberattack, is from vulnerabilities in third-party technology, not hospitals' primary systems. No organization, including federal agencies, is or can be immune from cyberattacks. Imposing fines or cutting Medicare payments would diminish hospital resources needed to combat cybercrime and would be counterproductive to our shared goal of preventing cyberattacks. These proposals for hospitals are misguided and will not improve the overall cybersecurity posture of the health care sector.

To make meaningful progress in the war on cybercrime, Congress and the Administration should focus on the entire health care sector and not just hospitals. Furthermore, for any defensive strategy imposed on the health care sector, Congress should call on federal agencies to protect hospitals and health systems — and the patients they care for — by deploying a strong and sustained offensive cyber strategy to combat this ongoing and unresolved national security threat. Health care is a top critical infrastructure sector with direct impact to public health and safety and must be protected. Any cyberattack on the health care sector that disrupts or delays patient care creates a risk to patient safety and crosses the line from an economic crime to a threat-to-life crime. These attacks should be aggressively pursued and prosecuted as such by the federal government. We use the term “prosecuted” in all sense of the definition related to the totality of the government's capabilities and authorities, including intelligence and military authorities.

Imposing swift and certain consequences upon cyber adversaries, who are often provided safe harbor in non-cooperative foreign jurisdictions, such as Russia, China, Iran and North Korea, is essential to reducing the cyber threats targeting health care and the nation.

CONGRESSIONAL REQUEST

The AHA recommends that Congress consider any statutory limitations that exist for an adequate response from CMS and HHS to help minimize further fallout from the Change Healthcare cyberattack and for future incidents. The

Administration has limited tools available, particularly because the government is not operating under a declared Public Health Emergency and National Emergency. While CMS has offered payments under the AAP, the agency only has authority to do so for limited time periods and amounts and with very high interest rates after repayments are due.

We also urge Congress to put forward policies that would alleviate administrative requirements imposed by payers, including Medicare Advantage and other commercial payers. Without relief from these payers in the form of waivers of prior authorization and timely filing requirements, providers, including hospitals and health systems, will likely see significant denials of care as a result of the shutdown of Change Healthcare. **In addition, we ask Congress to urge OCR to relieve providers from the burden of making duplicative breach notifications based on the outcome of their investigation to reduce any further confusion and unnecessary costs from this cyberattack.**

CONCLUSION

We must address the outstanding issues resulting from the cyberattack on Change Healthcare for the wellbeing of our patients and communities. These include ensuring providers are reconnected to services, are able to process claims and appeal denials, have the information needed to reconcile payments and issue patient bills, and are able to access needed financial support to mitigate the considerable costs incurred by hospitals and health systems as a result of the cyberattack. We stand ready to work with Congress, Change Healthcare and its corporate ownership to ensure hospitals and health systems have the resources they need to continue serving their patients and communities. At the same time, we also must enact policies that bolster support for the entire health care system's efforts to protect health care services, data and patients from cyberattacks.

Other State Regulations - Hospital Cybersecurity.p

Uploaded by: Katie Fry Hester

Position: FAV

New York: Mandatory Cybersecurity Regulations for Hospitals

New York has taken a prescriptive approach to hospital cybersecurity by implementing strict regulatory requirements. The state is developing a regulation that mandates hospitals to establish and maintain comprehensive cybersecurity programs. These regulations outline substantial and specific actions hospitals must take to protect sensitive patient data and critical healthcare infrastructure.

The associated regulatory impact statement acknowledges the significant financial burden this may place on hospitals, with many expected to incur costs in the millions to comply. While this approach ensures a standardized and enforceable cybersecurity framework, it may pose challenges for smaller hospitals with limited resources. However, state regulators argue that the long-term benefits—protecting patient safety, ensuring continuity of care, and reducing financial losses from cyberattacks—justify the investment.¹

Oklahoma: Incentivizing Cybersecurity Through Legal Protections

In contrast to New York's mandatory regulations, Oklahoma has opted for an incentive-based approach. In 2023, the state passed legislation designed to encourage hospitals to develop robust cybersecurity programs by offering legal protections rather than imposing direct requirements. Specifically, the law establishes an affirmative defense to negligence lawsuits arising from cybersecurity breaches.

To qualify for this defense, hospitals must implement a cybersecurity program that meets specific criteria outlined in the legislation. This approach aims to balance regulatory oversight with flexibility, allowing hospitals to tailor their cybersecurity efforts while providing a strong incentive to meet industry best practices. By reducing potential liability, Oklahoma hopes to encourage widespread adoption of effective cybersecurity measures without imposing costly mandates.²

¹ New York State Department of Health. (2024). *Hospital Cybersecurity Requirements (Proposed Regulations)*. Retrieved from

<https://regs.health.ny.gov/sites/default/files/proposed-regulations/Hospital%20Cybersecurity%20Requirements.pdf>

² Oklahoma State Legislature. (2024). *House Bill 2790 (Enrolled)*. Retrieved from http://webserver1.lsb.state.ok.us/cf_pdf/2023-24%20ENR/hB/HB2790%20ENR.PDF

Review of National and State-Level Data Relating t

Uploaded by: Katie Fry Hester

Position: FAV

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..... | 3 |
| II. | Maryland-specific analysis..... | 6 |
| III. | Sampling of regulations and legislation being pursued in other states..... | 8 |
| IV. | Current cybersecurity posture of the healthcare industry | 10 |
| V. | Information on costs of cyber incidents..... | 14 |
| | Works Cited | 18 |

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

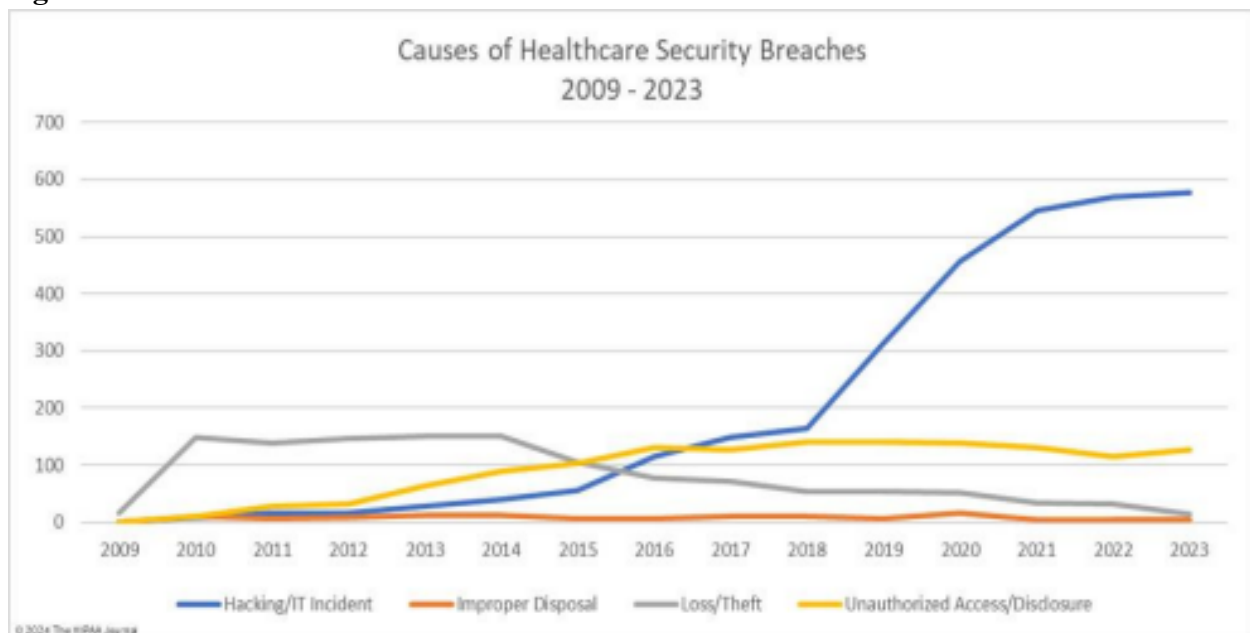
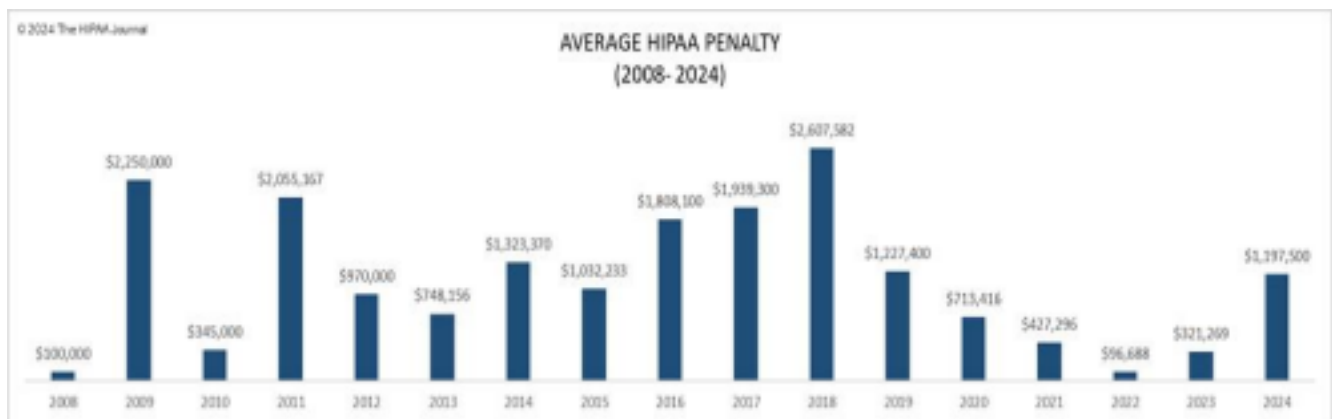


Figure 2



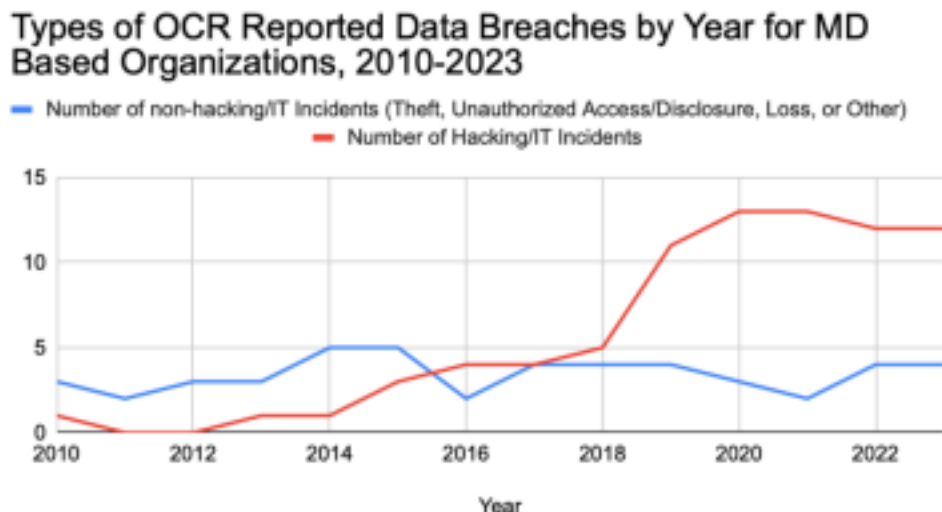
Figure 3



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

| 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 |
| <i>Notes: US population data obtained from US Census Bureau; physician and hospital data obtained from Kaiser Family Foundation.</i> | | | | | | |

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/>

- 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

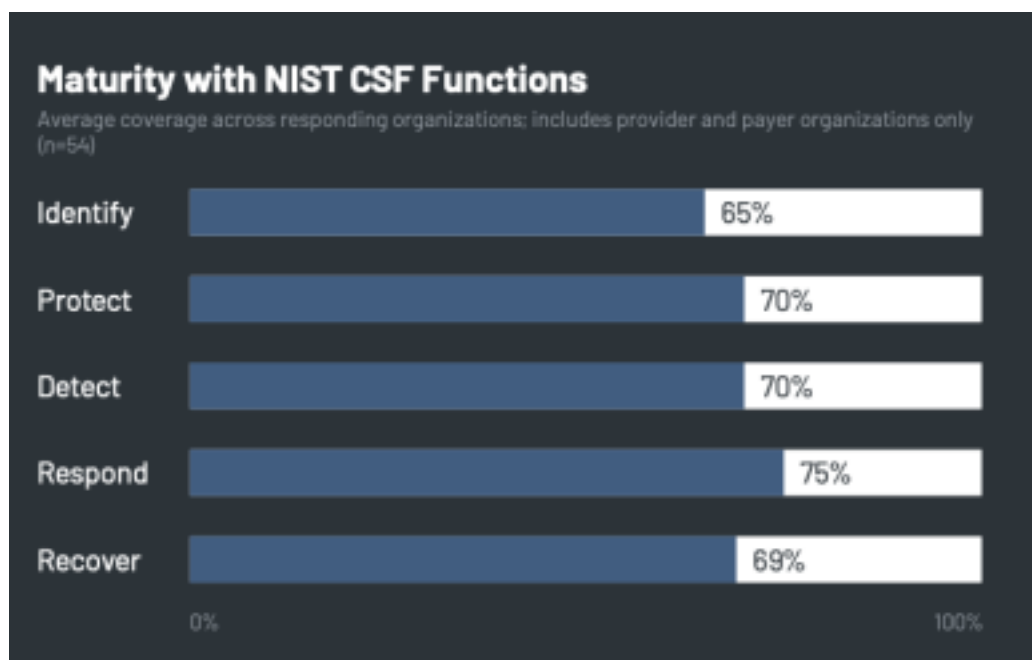
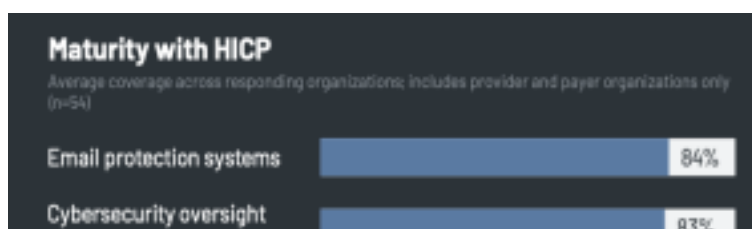


Figure 10



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 1/3 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

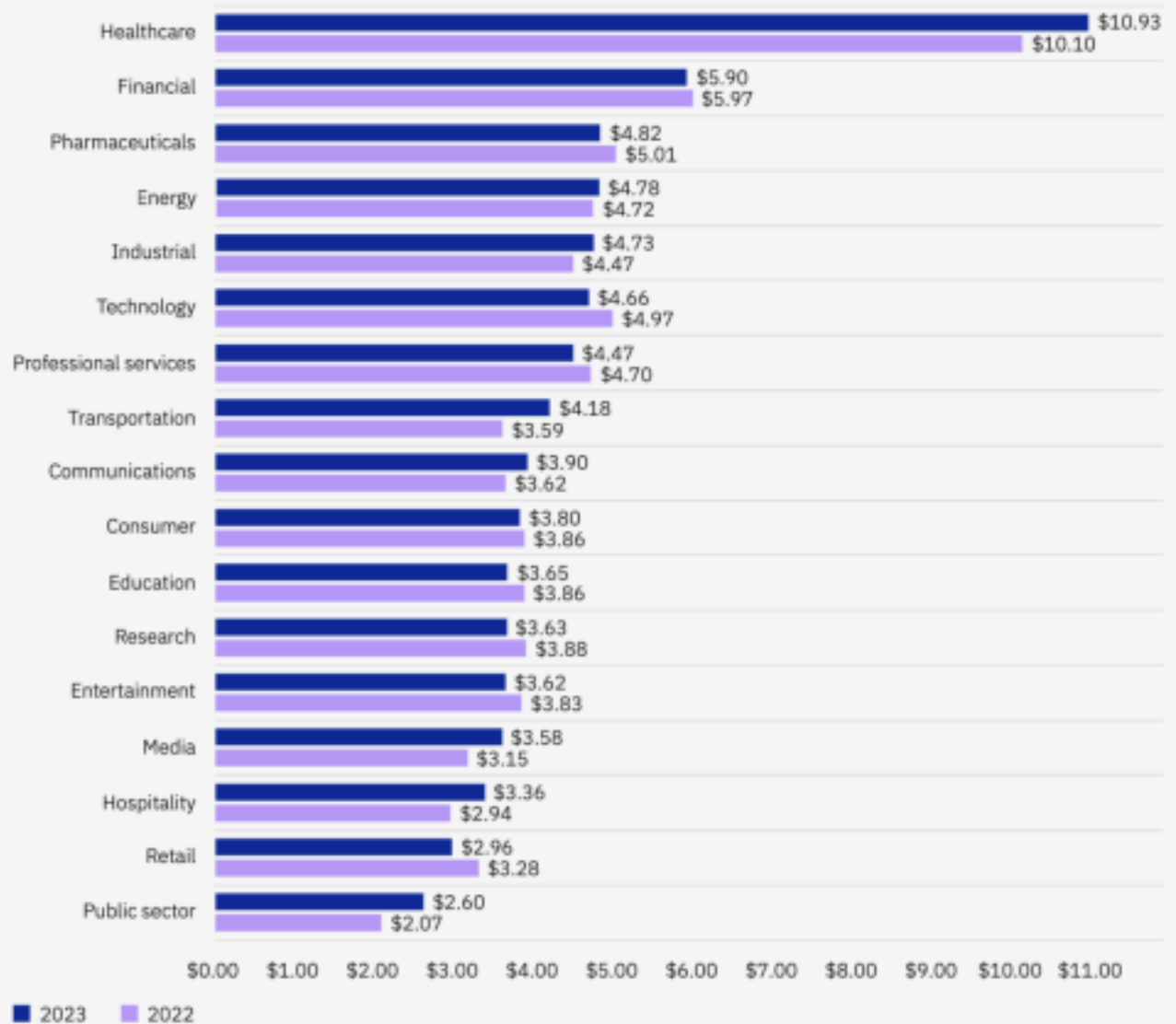
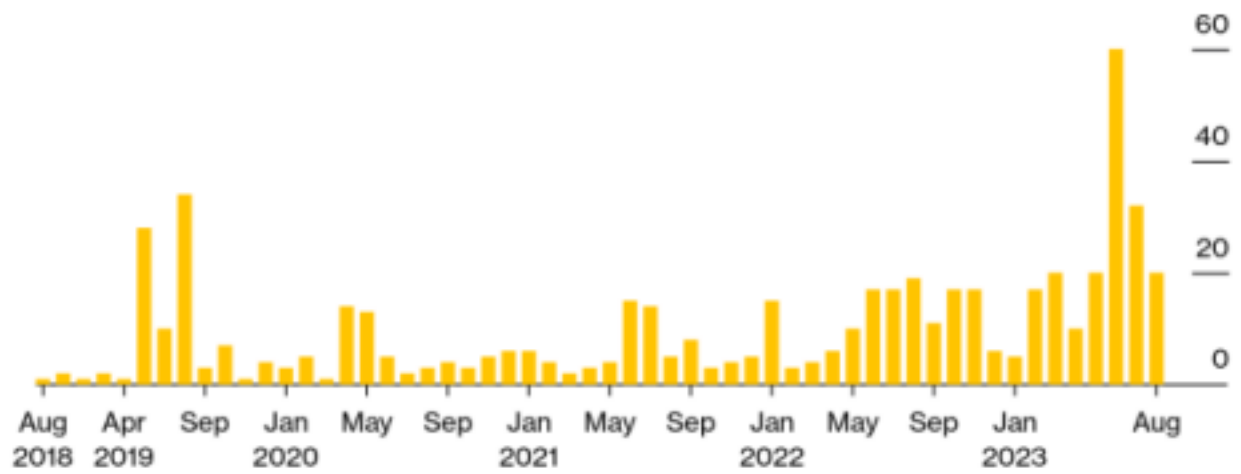


Figure 12

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 visited 19 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_Breach_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_regulations_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.

SB 691 Hester Testimony (1).pdf

Uploaded by: Katie Fry Hester

Position: FAV



THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

Testimony in Support of SB 691 - Cybersecurity - Healthcare Ecosystem

February 27, 2025

Chair Feldman, Vice-Chair Kagan, and Members of the Education, Energy, and the Environment Committee:

Thank you for your consideration of **SB 691 - Cybersecurity - Healthcare Ecosystem**, a critical piece of legislation aimed at protecting Maryland's healthcare system from escalating cyber threats.

Cyberattacks on healthcare are a serious threat to public safety, with the FBI and DOJ labeling them as "threat to life" crimes. The National Security Council has identified healthcare as one of the top three sectors that urgently need stronger cybersecurity.¹ Cybercriminals, often backed by hostile nations, target hospitals knowing that any disruption can put lives at risk.

Healthcare is a prime target due to its valuable data and urgency of ransom payments. Hacking-related breaches have surged 256% in five years, and in 2023, the FBI identified healthcare as the most targeted critical sector for ransomware. Maryland alone has seen 84 major breaches since 2010, affecting over 3.5 million residents in 2023 alone.²

Cyberattacks are not just IT issues—they disrupt patient care. A recent Ponemon study found:³

- 92% of healthcare organizations faced cyberattacks last year.
- 28% reported increased patient mortality.
- 59% saw delays in procedures, leading to poor health outcomes.
- 46% had to transfer or divert patients.

¹ The White House. (2024). *Fact sheet: National Cybersecurity Strategy Implementation Plan Version 2*. National Security Council. Retrieved from <https://bidenwhitehouse.archives.gov/oncd/briefing-room/2024/05/07/fact-sheet-ncsip-version-2/>

² From Chris Hart (2024). *Review of National and State-Level Data Relating to Cyber Incidents and Cybersecurity at Healthcare Organizations*. Research supported by the Center for Health and Homeland Security at the University of Maryland, Baltimore.

³ Ponemon Institute. (2024). *2024 Ponemon Healthcare Cybersecurity Report*. Proofpoint. Retrieved from <https://www.proofpoint.com/us/resources/threat-reports/ponemon-healthcare-cybersecurity-report>

Cyberattacks are taking a severe toll on hospitals' finances, with 94% reporting financial losses and 60% losing over \$1 million per day.⁴ The 2024 Change Healthcare attack underscores the financial strain caused by these cyber disruptions. A significant 82% of hospitals are experiencing major cash flow issues, making it increasingly difficult to keep operations running and pay for essential services. At the same time, 67% of hospitals are struggling to switch clearinghouses, adding another layer of complexity to restoring billing and reimbursement processes. To make matters worse, 20% of hospitals are still uncertain about the full extent of the financial damage, leaving them in a vulnerable position as they continue to deal with the disruptions.

SB 691 follows the approach established in HB 969 (2023), which provided cybersecurity standards for utilities. It requires:

- MDEM, MIA, and MHCC to enforce stronger cybersecurity standards and adopt a zero-trust model.
- Biennial third-party audits starting in 2026, with findings reported to the State CISO.
- A healthcare cybersecurity workgroup to improve resilience, define essential functions, and coordinate incident response.
- Real-time cyber incident reporting to enhance state situational awareness.

We repeatedly attempted to work with the Maryland Hospital Association (MHA) over the interim to discuss this bill and a path forward, but engagement was minimal and responses were delayed. Legislative action is necessary to ensure cybersecurity in healthcare across the ecosystem is proactively addressed and prioritized.

I urge this committee to take decisive action to protect Maryland's healthcare infrastructure by implementing the safeguards outlined in this bill. **Cybersecurity in healthcare is not optional—it is a matter of life and death.**

For these reasons, I respectfully request a favorable report on SB 691.

Sincerely,




Senator Katie Fry Hester
Howard and Montgomery Counties

⁴ American Hospital Association. (2024). *AHA survey: Change Healthcare cyberattack having significant disruptions to patient care, hospitals' finances*. Retrieved from <https://www.aha.org/news/news/2024-03-15-aha-survey-change-healthcare-cyberattack-having-significant-disruptions-patient-care-hospitals-finances>

SB691_CyberEcosystemSlides

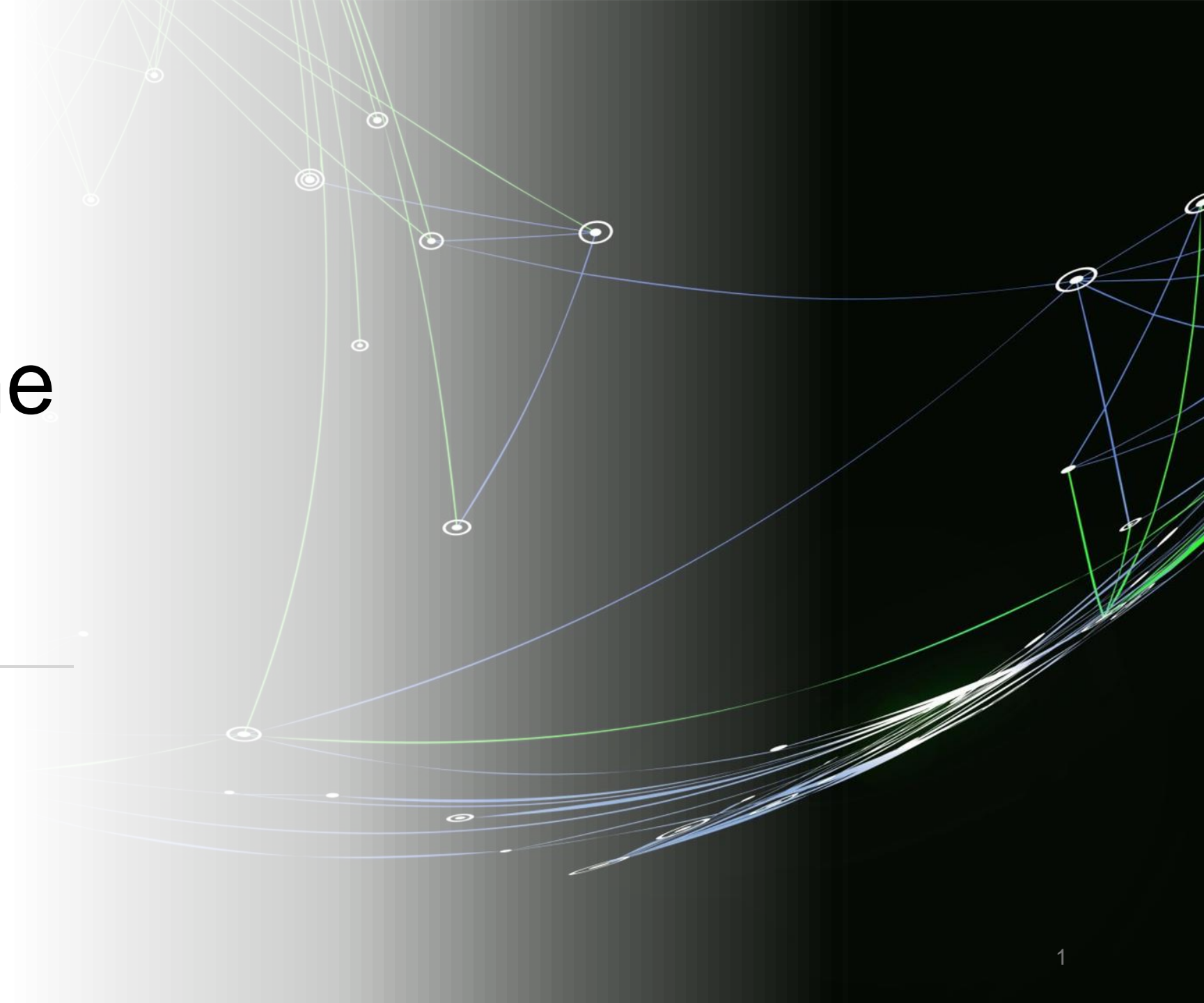
Uploaded by: Katie Fry Hester

Position: FAV



Cyber Threats to the Healthcare Ecosystem

HB333/SB691



Why Healthcare is a Target



Valuable Data: Healthcare organizations possess a wealth of sensitive data, which is highly valuable to cybercriminals and nation-state actors.



High Financial Rewards: Stolen records sell 10 times more than stolen credit card numbers on the dark web, with costs to remediate breaches also being significantly higher than in other industries.

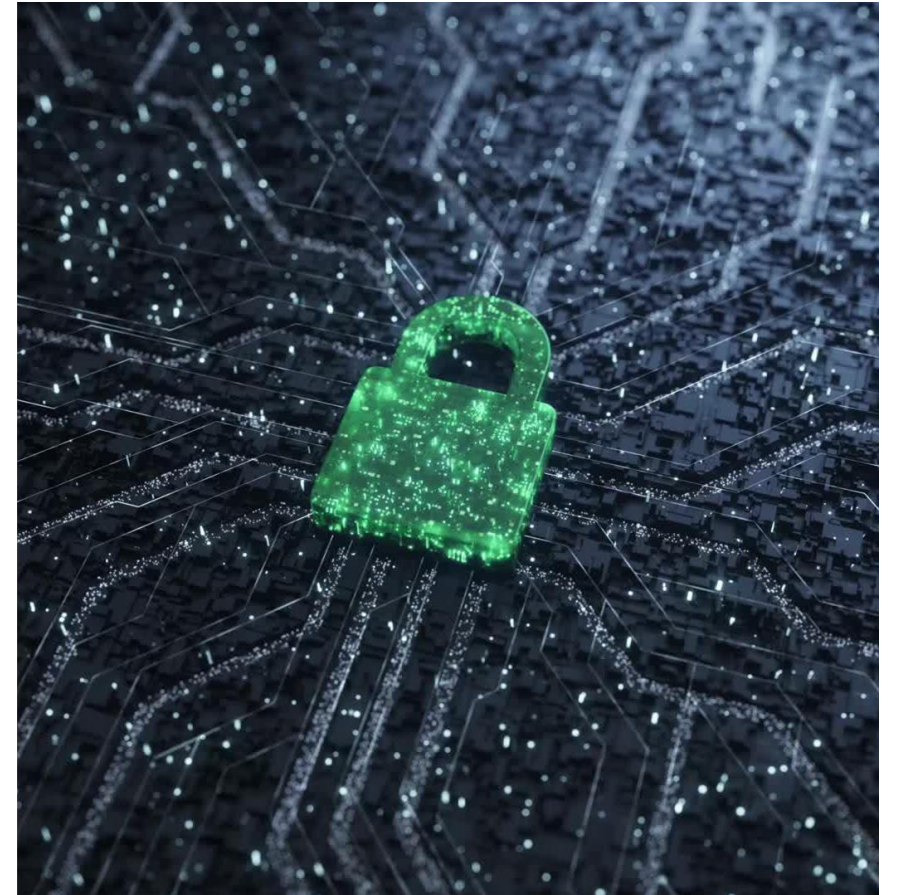


Disruption Drives Immediacy: Disruptions to healthcare lead to proven negative impact on patient outcomes, meaning the pressure is high to pay ransoms to cybercriminals.

National Threat Landscape

- Health-related privacy breaches have gone up 256% over the past five years (OCR).
- Ransomware attacks on healthcare related organizations is up 264%. (OCR)
- "Healthcare and Public Health" was the most affected critical infrastructure industry from ransomware attacks. (FBI Internet Crime Complaint Center)

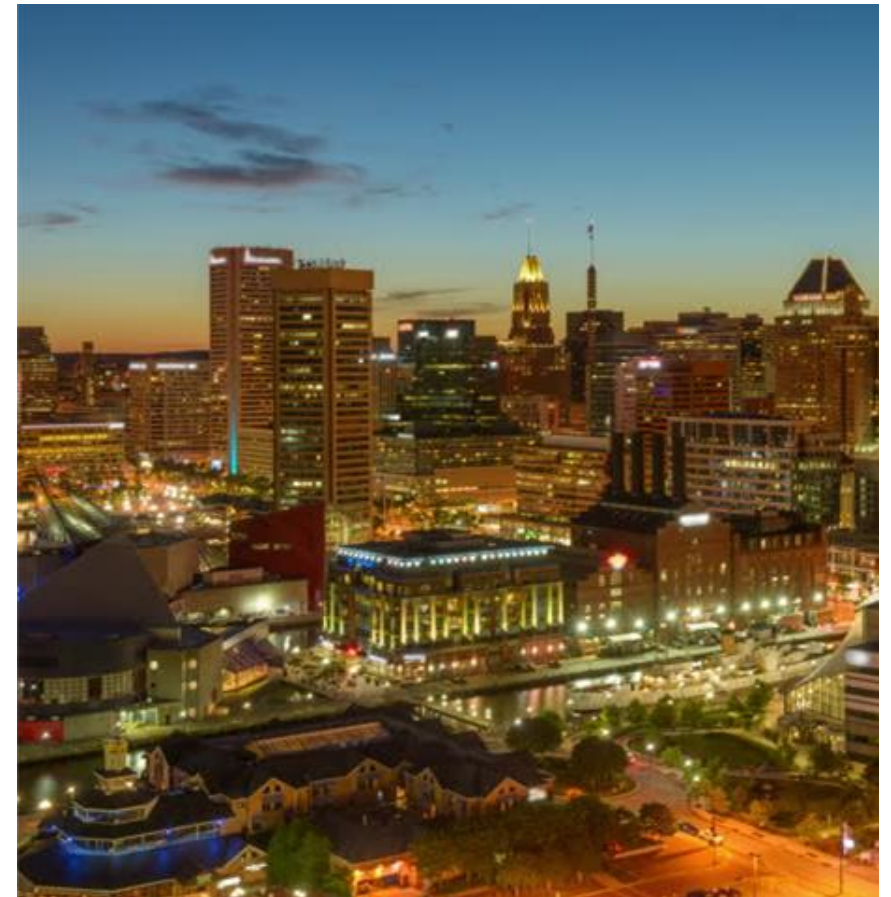
From Chris Hart (2024). Review of National and State-Level Data Relating to Cyber Incidents and Cybersecurity at Healthcare Organizations. Research supported by the Center for Health and Homeland Security at the University of Maryland, Baltimore.



Maryland Threat Landscape

- Since 2010, Maryland healthcare organizations have suffered 84 breaches categorized as “hacking/IT incidents” affecting more than 500 people. (OCR)
- In 2023, over 3.5 million people were impacted by hacking/IT incidents of Maryland organizations, a significant increase from previous years.
- According to a 2021 Maryland Healthcare Commission report, from 2018-2020 Maryland had the highest number of breaches per-capita among 7 states with similar per-capita hospital inpatient rates.

From Chris Hart (2024). Review of National and State-Level Data Relating to Cyber Incidents and Cybersecurity at Healthcare Organizations. Research supported by the Center for Health and Homeland Security at the University of Maryland, Baltimore.



Kinetic Impacts

- According to a [2024 Ponemon study](#):
 - **92%** of all hospitals experienced a cyber incident in 2023
 - Average cost of single most expensive attack was **\$4.7 million**
 - Hospitals suffering a cyber incident lost an average of **\$1.47 million** due to disruptions to normal healthcare operations

Financial Impacts

- According to a [2023 study](#), of the 68% of hospitals surveyed that experienced a ransomware attack:
 - 28% reported an increase in the mortality rate
 - 59% reported delays in procedures and tests have resulted in poor outcomes
 - 44% reported an increase in complications from medical procedures
 - 48% reported longer length of stay
 - 46% reported an increase in patients transferred or diverted to other facilities

Change Healthcare



Widespread Impact- Change Healthcare was attacked, impacting the entire U.S. healthcare system.

Critical Role- Processes billing and insurance for hospitals, pharmacies, and medical practices.

Massive Data Breach- 190 million patient records were compromised.

Key Functions Impacted:

- ☐ **Eligibility Checks** – Verifies patient coverage and costs.
- ☐ **Claims Submissions** – Sends claims to insurers.
- ☐ **Claims Status** – Tracks claim progress and rejections.
- ☐ **Prior Authorizations** – Approves high-cost services before treatment.

HB333/SB 691

No Need to Reinvent the Wheel

- SB 691 adopts the same approach to healthcare cybersecurity and protections that the General Assembly codified in HB 969 (2023), sponsored by Delegate Qi. This provided protections for utilities, with common provisions including:
 - Expanded regulator responsibility for the agencies commensurate with the threat
 - Incorporation of NIST frameworks and guidance

On April 3, 2024 Senator Hester sent a letter to MHA:

KATIE FRY HESTER
Legislative District 9
Howard and Montgomery Counties

Education, Energy, and
Environment Committee

Chair, Joint Committee on
Cybersecurity, Information Technology
and Biotechnology



Annapolis Office
James Senate Office Building
11 Bladen Street, Room 304
Annapolis, Maryland 21401
410-841-3671 • 301-858-3671
800-492-7122 Ext. 3671
KatieFry.Hester@senate.state.md.us

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

April 3, 2024

Pegeen Townsend, Vice President, Government Affairs
Jake Whitaker, Director, Government Affairs
Maryland Hospital Association
6820 Deerpath Road
Elkridge, MD, 21075

Dear Vice President Townsend and Director Whitaker,

Thank you for meeting with me on February 14 to discuss [HB 1123](#) and our shared interest in cybersecurity. In 2023, [16 breaches compromised more than 2 million patient records each](#), more than five times the number of the previous year. We must do everything we can in response.

This letter is to confirm that the Maryland Hospital Association is willing to collaborate with the Maryland Cybersecurity Council in the interim to ensure Maryland hospitals are as prepared as possible to address the threat of increased cybersecurity attacks in the industry. I would appreciate your suggestions on a few representatives to include within an interim workgroup from both large and small institutions in urban and rural settings to ensure a diversity of perspectives. Key issues for the working group to explore include:

- Minimum cybersecurity standards
- Third-party assessments
- Reporting of cybersecurity incidents
- Designation of Chief Information Security Officers (CISOs)
- Legislation in other states related to the topic

I have copied Greg Von Lehman, staff to the Maryland Cybersecurity Council, and Secretary Strickland, who chairs the Critical Infrastructure Subcommittee. I look forward to finding a suitable time for our first conversation in May.

Many thanks!

A handwritten signature in black ink that reads "Katie Fry Hester".

Senator Katie Fry Hester
Chair of the Joint Committee on Cybersecurity, Information Technology and Biotechnology

Conclusion

“The increasing incidence of ransomware attacks and proliferating cyberthreats require a coordinated approach led by government, in partnership with private sector efforts to innovate on cyber protections and distributed data systems that limit damage after an intrusion”¹

HB 333/SB 691 answers the call

1. Genevieve P Kantor, et al (2024), [Lessons From the Change Healthcare Ransomware Attack](#). Journal of the American Medical Association.

von Lehmen__SB 691__Favorable_.pdf

Uploaded by: Greg Lehmen

Position: FWA

TESTIMONY PRESENTED TO THE
SENATE FINANCE COMMITTEE

SB 691
CYBERSECURITY - HEALTHCARE ECOSYSTEM

DR. GREG VON LEHMEN
February 27, 2025

Madam Chair, Mr. Vice Chair, and members of the committee, good afternoon and thank you for the opportunity to testify in favor of SB 691. I am Dr. Greg von Lehmen, special assistant for cybersecurity at UMGC and staff to the Maryland Cybersecurity Council. My comments today in support of the bill are my own and are not intended to represent the views of these organizations.

Given the testimony today, I would say the question is not so much whether to act but what action to take. This question will become more urgent as new technologies, like AI, are increasingly incorporated into the attacker toolbox, reducing attacker costs and turbocharging the scale and effectiveness of attacks.¹

The bill has two significant virtues.

First, it recognizes the complexity of the problem and puts in place a deliberate process to address it. Healthcare cybersecurity of course starts with the cybersecurity of the individual members. The bill has provisions that aim to enhance the general security posture of the individual ecosystem members. That is foundational. It helps mitigate the problem.

But it is not enough. Addressing the vulnerability that stems from the interconnectedness of the ecosystem is critical. Representatives of all entities involved have to be brought together to identify what especially needs to be protected and to work out the business continuity arrangements *between* the ecosystem members to provide essential patient services in an emergency.

The bill recognizes this need for such a convening by providing for it by design. Not as a one-time event but as an ongoing practice to pace with the threat while

¹ See for example, Heikkeliä, M (2024, May 21). [Five ways criminals are using AI](#) MIT Technology Review, and MIT Technology Review Insights (2021). [Preparing for AI-enabled cyberattacks](#).

including the relevant State government agencies and departments with their particular roles and strengths.

Second, the fact that SB 691 would use a tried and true regulatory model to address the cybersecurity of its healthcare sector is a significant benefit. If you subtract out from the bill the provisions that are particular to the subject matter—the definitions of the healthcare ecosystem, “essential capabilities”, MHCC and MIA as the agencies involved, and so forth—what you are left with is Maryland’s Critical Infrastructure Act of 2023 that concerned the PSC and utilities serving Maryland. The provisions pertaining to cybersecurity requirements, the staffing support for the agencies, and the various processes described in SB 691 are all carried over from that Critical Infrastructure Act.

What is the benefit of this? I served both on the workgroup that helped inform the 2023 statute and also participated in the cybersecurity working group that the PSC convened to inform its rulemaking under the statute. I would very much expect that lessons learned from that process would be of value to the agencies and the stakeholders involved in the implementation of SB 691.

Like electricity, healthcare is critical to Maryland residents. The General Assembly has acted with respect to the former. It should now address the latter. I urge a favorable report.

Thank you.

CA-2025-SB691-TESTIMONY-FWA.docx.pdf

Uploaded by: John Fiastro

Position: FWA



10440 Little Patuxent Pkwy
Floor 12
Columbia, MD 21044
+443-853-1970
info@cyber-association.com
www.cyber-association.com

SB 691 – Cybersecurity – Healthcare Ecosystem
Senate Finance Committee
February 27, 2025
Favorable with Amendment

Dear Chair Beidle and Members of the Senate Finance Committee,

My name is Tasha Cornish, and I am writing on behalf of the Cybersecurity Association, Inc. (CA), a nonprofit 501(c)(6) organization dedicated to strengthening Maryland's cybersecurity industry. Our association represents over 600 businesses ranging from small enterprises to large corporations employing nearly 100,000 Marylanders. We appreciate the opportunity to offer testimony on Senate Bill 691, which seeks to enhance cybersecurity standards for healthcare ecosystem entities.

The Cybersecurity Association supports SB 691 with amendments to ensure the legislation aligns with best practices in cybersecurity law while balancing security requirements with reasonable compliance expectations for healthcare facilities. We commend the bill's incorporation of national cybersecurity frameworks, such as those outlined by the National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA). However, we suggest two key improvements to enhance its effectiveness:

Ensuring Alignment with Federal Standards and Regular Updates

The legislation correctly references federal cybersecurity standards, including those set forth by HIPAA. However, cybersecurity is an evolving field, and federal guidelines are subject to change. To maintain consistency with federal regulations, we recommend an amendment requiring periodic review and updates to Maryland's cybersecurity requirements to reflect changes in federal standards. This approach will ensure that Maryland healthcare facilities remain in compliance without unnecessary disruptions or inconsistencies in security practices.

Safe Harbor Protection for Healthcare Facilities

SB 691 should include a safe harbor provision similar to the **Oklahoma Hospital Cybersecurity Protection Act of 2023 (HB 2790)**. The Oklahoma law grants affirmative defense in tort actions for healthcare entities that implement and maintain reasonable cybersecurity measures based on recognized industry standards. This approach incentivizes compliance while protecting hospitals and other covered entities from undue liability when they make good-faith efforts to secure sensitive information.

To incorporate this principle into SB 691, we propose the following amendment:

Proposed Amendment Language – Safe Harbor Provision

Article – Health – General

19–113.1. Safe Harbor for Cybersecurity Compliance

(A) A healthcare ecosystem entity that implements and maintains a cybersecurity program that reasonably conforms to one or more recognized cybersecurity frameworks, including but not limited to:

1. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule (45 CFR Part 164 Subpart C);
2. The Health Information Technology for Economic and Clinical Health (HITECH) Act;
3. The National Institute of Standards and Technology (NIST) Cybersecurity Framework; or
4. Any successor regulations or frameworks recognized by the Maryland Health Care Commission.

shall be entitled to an affirmative defense in any cause of action sounding in tort alleging that a failure to implement reasonable information security controls resulted in a data breach concerning personal or restricted healthcare information.

(B) If any framework referenced in subsection (A) is updated or amended, a healthcare ecosystem entity shall conform to the updated framework within one (1) year of its effective date to maintain safe harbor protections.

(C) The Maryland Health Care Commission shall adopt regulations governing the verification and certification of compliance with this safe harbor provision.

Conclusion

By incorporating these amendments, SB 691 will create a cybersecurity framework that is both robust and practical. Aligning with federal standards ensures consistency and compliance while adopting a safe harbor provision will encourage healthcare providers to enhance their security posture without fear of excessive liability.

We urge the committee to issue a favorable report on SB 691 with these proposed amendments. Thank you for your time and consideration. I am happy to answer any questions the committee may have.

Sincerely,

Tasha Cornish
Executive Director
Cybersecurity Association, Inc.

DOCS-#238938-v1-SB_691_League_FWA.pdf

Uploaded by: Matthew Celentano

Position: FWA



15 School Street, Suite 200
Annapolis, Maryland 21401
410-269-1554

February 27, 2025

The Honorable Pam Beidle
Chair, Senate Finance Committee
3 East
Miller Senate Office Building
Annapolis, MD 21401

Senate Bill 691– Cybersecurity – Healthcare Ecosystem

Dear Chair Beidle,

The League of Life and Health Insurers of Maryland, Inc. *supports* **Senate Bill 691 – Cybersecurity – Healthcare Ecosystem** with amendments.

We applaud the important goal of this bill as cyber events are a reality in this technologically interwoven, dependent, and increasingly connected universe. While we certainly understand the broad reach of Senate Bill 691 to ensure stakeholders in the health care universe have documented and well-developed approaches to cybersecurity, we believe the catchment is misguided. Insurance carriers are already required to have significant cyber protections and function, as well as an omnibus piece of legislation that the committee passed in 2023 to address data breaches, protections, and security.

These protections came at great cost to implement for carriers, but those protections will pay off in the long term. Yes, there will be cost to implement mandated protections, but in this ever-complicated world it is money well spent. Carriers already regularly conduct security audits, implement multi-factor authorization, encrypt sensitive data, require frequent password changes, and establish an incident response plan.

Carriers have a variety of approaches, but as the world evolves and the threats expand, many have established support networks that include the Cybersecurity & Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) to help broaden insight into potential threats and accelerate the response to vulnerabilities. Carriers outline their cybersecurity requirements and incorporate them into their partners' contractual obligations. Carriers are committed to prioritizing cybersecurity to ensure the confidentiality and integrity of data, allowing people to focus on their top priorities: access to affordable, equitable, high-quality healthcare.

We most certainly believe that all stakeholders and entities in the health care continuum should be required to have formal security policy, and frankly, there is really only one major stakeholder that has not been

required to have a formal policy in the last decade. While many entities must have protections for Maryland consumers, Maryland's hospitals are not one of the health care organizations that have yet to have mandated protections for consumers. We believe that should change and the bill should be amended to just require Maryland hospitals that get the benefit of entities they do business with to implement protections but have none of their own.

For these reasons, the League urges the committee to give Senate Bill 691 a favorable with amendment report.

Very truly yours,

A handwritten signature in black ink, appearing to read "Matthew Celentano", with a long horizontal flourish extending to the right.

Matthew Celentano
Executive Director

cc: Members, Senate Finance Committee

SB691 Cybersecurity - Healthcare Ecosystem_HOPKINS

Uploaded by: Brandon Floyd

Position: UNF

TO: The Honorable Pamela Beidle, Chair
Finance

SB691
Unfavorable

FROM: Brandon Floyd
Associate Director, Maryland Government Affairs

DATE: February 27, 2025

RE: SB691 Cybersecurity - Healthcare Ecosystem

Johns Hopkins opposes **SB691 Cybersecurity - Healthcare Ecosystem**. This bill requires hospitals every two years to undergo third party evaluation of cyber practices and resources. It also requires the Maryland Health Care Commission (MHCC) submit a report, providing a general overview of cybersecurity and technologies used by hospitals. The bill also requires the MHCC to establish a process for hospitals to report cyber incidents to adopt regulations to implement cybersecurity standards.

Johns Hopkins is an international organization that cares for patients and educates millions of people. It is paramount that all who come in contact with Johns Hopkins Health System receive proper care and proper patient protections. To ensure these protections, Johns Hopkins, like many other hospitals, must remain in compliance with numerous cyber standards. The National Institute of Standards and Technology (NIST), whose mission is to promote innovation, security, and industrial competitiveness, provides cyber and privacy frameworks for organizations to remain in compliance. Hopkins is current with other frameworks and regulations including federal HIPAA and American Hospital Association (AHA) security rules. The cyber requirements in this bill would duplicate the existing cyber safety measures.

We are very concerned with the bill provisions subjecting hospitals to an audit and requiring hospitals to report on the outcome of the audit. The information disclosed during an audit is highly proprietary and would require the State to have the proper safeguards to guarantee hospital inner workings are not being exposed. Providing the actual output of the audit may open the door for unintended consequences like sharing infrastructural vulnerabilities with cyber criminals and other bad actors.

Johns Hopkins spends over \$20M annually in cyber, information technology, and information system protections. These protections are to ensure patient data and other confidential important information is secure. As written, hospitals must undergo a bi-annual audit which would be incredibly costly for hospitals and do not advance protections for hospitals. Without clear financial and operational support, this bill risks creating more challenges in the ongoing effort to strengthen cybersecurity.

The bill includes third-party cybersecurity vendors into the aforementioned hospital auditing process. Cybersecurity vendors, by nature, generate revenue by providing cyber service lines and products to organizations. Bill language like “zero-trust” is ambiguous terminology that supports cyber vendors business efforts who have a financial interest in providing services to hospitals. It is unclear why a third-party vendor would need to be a part of this process, when their motives cannot be guaranteed.

Furthermore, the bill shifts control from in-house experts to external vendors. This approach does not reflect the nuanced needs of individual hospitals, with varying infrastructure. Hospitals must have the flexibility to determine the most effective protections based on their risk assessments, rather than being required to implement vendor-driven solutions that may not address their unique threats.

Cybersecurity is an evolving industry, this bill places unnecessary obstacles on hospitals are prioritizing patients – virtually and in person – every day. Accordingly, Johns Hopkins respectfully requests an **UNFAVORABLE** committee report on SB691.

SB0691_UNF_LifeSpan_Cybersecurity - Healthcare Eco

Uploaded by: Danna Kauffman

Position: UNF



*Keeping You Connected...Expanding Your Potential...
In Senior Care and Services*

Senate Finance Committee
Senate Education, Energy, and the Environment Committee
February 27, 2025
Senate Bill 691 – *Cybersecurity – Healthcare Ecosystem*
POSITION: OPPOSE

On behalf of the LifeSpan Network, a senior care provider association in Maryland representing nursing facilities, assisted living providers, continuing care retirement communities, medical adult day care centers, senior housing communities, and other home and community-based services, we oppose Senate Bill 691, which among other provisions, requires a healthcare ecosystem to adopt specific cybersecurity standards and to undergo a third-party audit to evaluate the entity's cybersecurity practices and resources.

While the bill defines specified entities as a "healthcare ecosystem," it also uses a catch-all phrase of "an entity identified by the Commission in regulations to be included in the healthcare ecosystem." (page 4, lines 1-2; page 4, lines 3-4; page 11, lines 7-9). Granting the Maryland Health Care Commission the authority to identify entities not explicitly listed in the bill makes it impossible to evaluate the effect of this bill on non-listed entities that may ultimately be required to comply. If the bill moves forward, we request that this language be removed.

For more information, contact:

Danna Kauffman
Christine Krone
410-244-7000

SB 691- Cybersecurity-Healthcare Ecosystem.pdf

Uploaded by: Jake Whitaker

Position: UNF



Senate Bill 691 - Cybersecurity - Healthcare Ecosystem

Position: *Oppose*

February 27, 2025

Senate Finance Committee

MHA Position:

On behalf of the Maryland Hospital Association (MHA) and our member hospitals and health systems across the state, we appreciate the opportunity to comment in opposition to Senate Bill 691. Maryland hospitals and health systems are committed to upholding the highest cybersecurity standards and safeguarding patient data. SB 691 mandates strict state-level cyber security standards and audit procedures that fail to account for the realities of data sharing across multiple states and constantly evolving technological standards.

Health care cybersecurity involves a complex, interconnected network of stakeholders—hospitals, insurers, health information exchanges, and other third parties—many of whom operate across multiple states. Several Maryland hospitals and health systems also have facilities outside the state. State-specific regulations risk creating conflicting or duplicative requirements, increasing administrative burdens, and potentially weakening cybersecurity efforts. Moreover, cyber threats are not confined by state lines.

Maryland hospitals already comply with rigorous federal cybersecurity standards designed to protect patient data and safeguard systems. The HIPAA Security Rule mandates administrative, physical, and technical safeguards to protect electronic protected health information (ePHI). Further, on Dec. 27, 2024, the U.S. Department of Health and Human Services proposed updates to HIPAA cybersecurity requirements, including mandates for written documentation of all cybersecurity policies and maintaining a comprehensive technology asset inventory. Hospitals also adhere to the National Institute of Standards and Technology (NIST) cybersecurity framework, which includes guidance on risk assessments to identify and mitigate cybersecurity threats and outlines security guidelines for access control, incident response, authentication, auditing, and cybersecurity training.

Additionally, Maryland hospitals conduct regular cybersecurity audits to identify vulnerabilities and ensure compliance. Federal regulations require ongoing HIPAA risk assessments, and hospitals proactively engage in third-party evaluations to maintain the highest cybersecurity standards. SB 691's broad incident reporting requirements could lead to excessive and unnecessary reporting of minor cybersecurity events, overwhelming state agencies and diverting attention from



truly critical threats. Over-reporting could create administrative inefficiencies that hinder timely responses to serious cyberattacks.

Since January 2020, Maryland hospitals have faced significant financial challenges, with operating expenses rising sharply. More than half of Maryland hospital systems have reported negative operating margins in most quarters over the past three years. In the third quarter of 2024, Maryland hospital system operating margins averaged just 0.3%, far below the 3% margin that experts consider necessary to sustain nonprofit health care systems. Over the past 11 years, Maryland hospital system margins have averaged only 1.6%, significantly lagging behind hospitals nationwide. Maryland's unique rate setting system limits hospitals' ability to cover unplanned costs. Mandating substantial new cybersecurity investments without a funding mechanism places additional financial strain on hospitals.

Given these concerns, MHA urges caution in adopting costly, unfunded cybersecurity mandates and advocates for a more strategic, federally aligned approach to health care cybersecurity.

For these reasons, we request an unfavorable report on SB 691.

For more information, please contact:

Jake Whitaker, Assistant Vice President, Government Affairs & Policy

Jwhitaker@mhaonline.org

2025 Legislation-MHCC-SB 691 -Cybersecurity Ecosys

Uploaded by: David Sharp

Position: INFO



February 27, 2025

The Honorable Pamela Beidle
Chair, Senate Finance Committee
3 East Miller Senate Office Building
Annapolis, MD 21401

Re: SB 691 – Cybersecurity - Healthcare Ecosystem – Letter of Information

Dear Chair Beidle and Committee Members,

The Maryland Health Care Commission (MHCC) is submitting this letter of Information on *SB 691 – Cybersecurity - Healthcare Ecosystem*. The bill requires MHCC to implement certain cybersecurity requirements for the health care ecosystem entities (entities). This includes adopting cybersecurity standards and requiring select entities to undergo third-party cybersecurity audits and report certain information to MHCC. The bill requires MHCC to hire at least one cybersecurity expert to carry out specific functions and collaborate with the State Security Operations Center in the Department of Information Technology and Maryland Department of Emergency Management.

The MHCC is required by law to establish regulations that protect the privacy and security of electronic protected health information,¹ The regulations build on the federal requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).² Approximately 29 EHNs and 16 HIEs submit to annual audits that evaluate the strength of their security measures, including data encryption, access controls, and network protections against unauthorized access or breaches. The audits also assess the effectiveness of disaster recovery and incident response plans in the event of a cyberattack. The MHCC believes these named technology entities are already meeting stringent third-party audit requirements outlined in the bill, while other named provider entities minimally comply with HIPAA.

Cybersecurity is an enormous and complex issue. The risk to the health system and patients is substantial from a variety of external threats. The MHCC believes that the State government has an appropriate oversight role to play if a thoughtful program of oversight can be developed. However, the MHCC is not financially able to take on a new program such as this, given our FY 2026 proposed budget. Our projected 2026 funding has already been stretched to the limit of our authority to assess the regulated industries.³ The MHCC can assess from regulated health entities a maximum of \$20 million under our current law. The proposed MHCC operating budget for FY 2026 is \$21.6 million. The \$1.6 million difference between the proposed budget of \$21.6 million and the \$20 million to be assessed from the

¹ Chapters 534 and 535 (SB 723 | HB 535) of the 2011 laws of Maryland.

² U.S. Department of Health and Human Services, Summary of the HIPAA Security Rule available at: www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

³ The MHCC is a Special Fund agency through annual assessments on hospitals (39%), payers (26%), nursing homes (19%), and health occupation boards (16%). The Department of Budget Management requires that Special Fund agencies maintain a 10% reserve in their non-lapsing fund, which for MHCC would be about \$2 million.

regulated health care entities will be withdrawn from the MHCC's fund reserve which totals just \$3.6 million.

While MHCC fully supports the intent of SB 691, given the current budget and the spending limit anchored in statute, MHCC is not in a position to take on this initiative at this time. The MHCC would be pleased to work with the legislature to develop a program of oversight after our funding issue can be resolved.

We appreciate your consideration. If you have any questions, please do not hesitate to contact me at dsharp@maryland.gov or Ms. Tracey DeShields, Director of Policy Development and External Affairs, at tracey.deshields2@maryland.gov or 410-764-3588.

Sincerely,

A handwritten signature in black ink, appearing to read 'D. Sharp', with a stylized flourish at the end.

David Sharp,
Acting Executive Director

SB 691 - MIA - LOI.pdf

Uploaded by: Marie Grant

Position: INFO

WES MOORE
Governor

ARUNA MILLER
Lt. Governor

MARIE GRANT
Acting Commissioner

JOY Y. HATCHETTE
Deputy Commissioner



200 St. Paul Place, Suite 2700, Baltimore, Maryland 21202
Direct Dial: 410-468-2471 Fax: 410-468-2020
1-800-492-6116 TTY: 1-800-735-2258
www.insurance.maryland.gov

Date: February 27, 2025

Bill # / Title: Senate Bill 691 - Cybersecurity – Healthcare Ecosystem

Committee: Senate Finance Committee

Position: Letter of Information

The Maryland Insurance Administration (MIA) appreciates the opportunity to provide information regarding Senate Bill 691.

The MIA currently regulates cybersecurity of Maryland carriers under Title 33 of the Insurance Article, which requires carriers to adopt a security plan that meets specific requirements and requires notification to the MIA in the event of a breach that significantly affects Marylanders. However, this oversight is limited to the entities which the MIA regulates - authorized insurers, nonprofit health service plans, health maintenance organizations, dental organizations, managed general agents, and third-party administrators. Additionally, pursuant to § 33-106, a carrier “that is subject to, governed by, and compliant with the privacy, security and breach notification rules” of the Health Insurance Portability and Accountability Act (HIPAA) is deemed in compliance with the information security and breach investigation requirements of Title 33, but is still obligated to comply with the notification requirements of the Title.

Senate Bill 691 requires the Maryland Health Care Commission and the MIA to each employ a cybersecurity expert and to submit reports on the cybersecurity practices of healthcare ecosystem entities to the State Chief Information Security Officer. In the case of the MIA, the additional requirements for cybersecurity regulation are specifically health insurers and pharmaceutical benefit managers. The bill also mandates that healthcare ecosystem entities adopt cybersecurity standards, undergo third-party audits, and report cybersecurity incidents to the State Security Operations Center. Additionally, the bill authorizes the Maryland Health Care Commission to convene a workgroup to review and make recommendations to improve cybersecurity in the healthcare ecosystem.

The MIA notes that the requirements placed on the Agency in the bill are unable to be executed with current staff due to lack of technical expertise, and would necessitate the hiring of at least

one full time staff member with cybersecurity experience. However, the MIA is committed to enhancing cybersecurity oversight for the entities we regulate, and looks forward to continuing a dialogue with the sponsor to refine amendments to address the ability of the MIA to implement provisions of the bill.

Thank you for the opportunity to provide this letter of information. The MIA is available to provide additional information and assistance to the Committee.

Senate Bill 691 - DoIT Written Testimony.docx.pdf

Uploaded by: Sara Elalamy

Position: INFO



Wes Moore | Governor
Aruna Miller | Lt. Governor
Katie Savage | Secretary

TO: Senate Education, Energy, and the Environment Committee
FROM: Department of Information Technology
RE: Senate Bill 691- Cybersecurity - Healthcare Ecosystem
DATE: February 27, 2025
POSITION: Letter of Information

The Honorable Pamela Beidle
Senate Finance Committee
3 East Miller Senate Office Building
Annapolis, Maryland 21401

Dear Chairwoman Beidle,

The Department of Information Technology (DoIT) appreciates the opportunity to provide information regarding Senate Bill 691- Cybersecurity - Healthcare Ecosystem, which aims to enhance cybersecurity measures across Maryland's healthcare ecosystem. We recognize the importance of improving cybersecurity resilience and ensuring the protection of sensitive healthcare data. After reviewing the bill's provisions, we would like to offer insights and considerations for committee members.

SB 691 appropriately emphasizes the need for adopting Zero-Trust (ZT) principles, which align with industry best practices. However, it is critical to recognize that ZT is not an immediate solution but a long-term framework requiring incremental implementation. Rushing ZT adoption may inadvertently introduce vulnerabilities rather than strengthening cybersecurity. We recommend that the bill require a structured implementation plan with key milestones, incorporating tailored audits at each stage to assess the evolving security posture.

The bill's reporting requirements present an opportunity to enhance Maryland's cybersecurity intelligence. Presently, the Office of Security Management (OSM) has limited ability to derive actionable insights from such reports. To maximize the value of this data, we suggest incorporating language that suggests consulting with the Chief Data Officer when developing a centralized repository for cybersecurity reports. This would ensure data is utilized effectively for improved threat detection and response.

The bill's reporting requirements closely align with the Critical Infrastructure Cybersecurity Act of 2023. However, challenges arose with that legislation, as utility companies successfully

contested OSM's minimum reporting standards before the Public Service Commission (PSC). To avoid similar obstacles, HB 333 should explicitly affirm the authority of the State Chief Information Security Officer (SCISO) in defining and enforcing reporting standards upon publication. Alternatively, resolving prior challenges with the PSC before implementation could provide a more stable foundation for enforcing cybersecurity regulations.

SB 691 assigns the Maryland Department of Emergency Management (MDEM) a role in providing guidance on cybersecurity regulatory standards for healthcare ecosystem entities. However, governance, risk, and compliance (GRC) functions typically fall within the purview of regulatory and cybersecurity agencies such as DoIT. We recommend revising this provision to ensure regulatory oversight aligns with the appropriate agency's expertise.

The bill references multiple cybersecurity frameworks, including NIST 800-207, NIST 800-207A, NIST 800-53A, the NIST Cybersecurity Framework, and the Health Industry Cybersecurity Practices (HICP). While each framework offers valuable guidance, inconsistencies may arise if different healthcare entities adopt conflicting standards. A clearer approach may be to align the bill's requirements with a single overarching cybersecurity framework, such as the NIST Cybersecurity Framework or the Cybersecurity and Infrastructure Security Agency's (CISA) Cyber Performance Goals (CPGs), to ensure uniformity across the ecosystem.

The Department of Information Technology supports the overarching goals of SB 691 and its intent to strengthen cybersecurity protections within Maryland's healthcare ecosystem. We believe that refining the bill's approach to Zero-Trust implementation, aggregate reporting, MD-SOC authority, regulatory oversight, and cybersecurity framework alignment will enhance its effectiveness and ensure its successful implementation. We appreciate the opportunity to provide these insights and welcome further discussion on these critical cybersecurity matters.

Best,

Melissa Leaman
Acting Secretary
Department of Information Technology