HEALTHCARE LEADERSHIP COUNCIL | CONFIDENTIALITY COALITION

July 9, 2025

Cybersecurity in Healthcare:

Defining Private and Public Sector Responsibility

A Strategic Framework from the Healthcare Leadership Council and the Confidentiality Coalition

The Healthcare Leadership Council is the exclusive forum for the nation's healthcare industry leaders to discuss major, sector-wide issues, generate innovative solutions to unleash private sector ingenuity, and advocate for policies to improve our nation's healthcare delivery system. Learn more about HLC's policy priorities on our website at www.hlc.org and follow us on LinkedIn and X/twitter.

The Confidentiality Coalition is a broad alliance of organizations from across the healthcare industry committed to balancing the protection of confidential health information with the need for efficient, interoperable healthcare systems. Organized by HLC, the Coalition is uniquely positioned to shape effective and pragmatic policies to safeguard the privacy of individuals' data and information while facilitating the essential flow of information for the timely and effective delivery of high-quality care and healthcare innovation.

Manatt, Phelps & Phillips, LLP is a leading professional services firm, providing integrated legal and consulting services to a global client base. With offices strategically located in California (Los Angeles, Orange County, San Diego, San Francisco, Sacramento and Silicon Valley), New York (New York City and Albany), Chicago, Washington, D.C., and Boston, the Firm represents sophisticated clients—including Fortune 500, middle-market and emerging companies—across a range of industry sectors such as health care; financial services; entertainment; digital and technology; and energy, environmental and real estate. For more information, visit www.manatt.com.

Executive Summary

Hackers target hospitals and providers, academic medical centers and researchers, insurers, pharmaceutical and medical device manufacturers, community health organizations, and many other organizations across the healthcare ecosystem. Sophisticated cyberattacks endanger patients, disrupt integrated networks, and inflict steep financial costs. In addition to proactively defending against these pervasive threats, healthcare organizations face a labyrinth of complex, overlapping, and burdensome cybersecurity requirements and breach reporting duties.

The Healthcare Leadership Council (HLC)[1] and the Confidentiality Coalition (the Coalition)[2] propose a collaborative approach between the private and public sectors to define and share cybersecurity responsibilities, create mutual accountability to protect patient safety, and support the healthcare systems on which our country relies.

The Current Challenge

Healthcare organizations face persistent, and complex cyberattacks – ranging from ransomware and zero-day exploits to email phishing strikes and insider threats. In fact, 92% of healthcare organizations reported that they experienced a cyberattack last year.[3]

> **92%** of healthcare organizations reported that they **experienced a cyberattack last year**.[3]

The Threat Landscape

These threats spring from a variety of sources, including sophisticated state-sponsored actors, organized international criminal rings, and malicious "insiders."

- *Patient Health.* Most significantly, cyberattacks threaten patients by disrupting clinical care, delaying treatments and surgical procedures, and jeopardizing patient safety.
- *Systemwide Operations.* With technology innovation and adoptions, organizations have become entwined. A cyberattack on one provider can impact payers, affiliated practice groups, and patients, and the downtime can last for months.
- *Operational Costs.* Finally, cyberattacks have a disproportionate financial impact on

---

[1] The Healthcare Leadership Council is the exclusive forum for the nation's healthcare industry leaders to discuss major, sector-wide issues, generate innovative solutions to unleash private sector ingenuity, and advocate for policies to improve our nation's healthcare delivery system.

[2] The Confidentiality Coalition is a broad alliance of organizations from across the healthcare industry committed to balancing the protection of confidential health information with the need for efficient, interoperable healthcare systems. With its diverse and expert membership, the Coalition is uniquely positioned to shape effective and pragmatic policies to safeguard the privacy of individuals' data and information while facilitating the essential flow of information for the timely and effective delivery of high-quality care and healthcare innovation. www.confidentialitycoalition.org

[3] Nathan Eddy, 2025's Biggest Healthcare Cybersecurity Threats, HEALTHTECH MAGAZINE (Jan. 24, 2025) (quoting Proofpoint study), https://healthtechmagazine.net/article/2025/01/healthcare-cybersecurity-threats-2025-perfcon

healthcare operations with the average cost of a healthcare data breach topping the highest of any sector for the 14th year in a row.[4]

The Regulatory Landscape

The U.S. healthcare industry also faces a maze of federal, industry, and state cybersecurity requirements, guidelines, and reporting duties.

- *Cybersecurity Regulations and Guidelines.* A litany of laws, regulations, and guidelines that apply to healthcare entities are enforced and updated by the U.S. Department of Health and Human Services (HHS), the Food and Drug Administration (FDA), the Center for Medicare and Medicaid Services (CMS), the Office of the National Coordinator (ONC).
- *Industry Frameworks:* Many healthcare organizations also must implement general industry frameworks like the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) 2.0, or more specific rules like the Payment Card Industry Data Security Standards (PCI DSS) for credit card transactions.
- *Federal Breach Reporting Requirements.* In addition, healthcare organizations face a dense array of breach reporting laws. Depending on their type of activity, healthcare organizations may be subject to additional federal rules with different timelines and standards that trigger reporting to the U.S. Department of Education, federal bank or financial regulators, the FTC, the Securities and Exchange Commission (SEC), and the Cybersecurity & Infrastructure Security Agency (CISA).
- *State Breach Notification Laws.* In addition, all 50 states and all U.S. territories impose their own breach notification requirements. Some apply specifically to healthcare or insurance companies, while others apply generally to all businesses operating within a jurisdiction.

Proposed Framework

Based on the challenges posed by the current threat and regulatory landscapes, HLC and the Coalition propose the Cybersecurity Framework set forth below. The framework emphasizes a collaborative approach to the current crisis and highlights private and public actions needed before, during, and after a data breach.

[4] IBM and Ponemon Institute, *Cost of a Data Breach Report 2024* 10, https://www.ibm.com/reports/data-breach

Healthcare Leadership Council & Confidentiality Coalition Cybersecurity Framework

PREVENTION: Hygiene and Resilience

Private Sector Commitments

- Maintain an Information Security Program based on an Established Industry Framework
- Conduct Regular Risk Assessments based on an Established Industry Framework
- Implement an Incident Response Plan based on an Established Industry Framework

Public Sector Recommendations

- Promote Law Enforcement and Information-Sharing as International Priorities
- Bolster Public-Private Collaboration over Cybersecurity Prevention Measures
- Enhance Public-Private Information-Sharing

RESPONSE: Restoring and Reporting

Private Sector Commitments

- Investigate and Report Breaches in a Timely Manner
- Promptly Restore Critical and Essential Systems

Public Sector Recommendations

- Harmonize Breach Reporting Requirements
- Improve Real-Time Information-Sharing

RECOVERY: Rebuilding and Learning

Private Sector Commitments

- Update Stakeholders
- Reconnect Efficiently with Trusted Partners
- Embed Lessons Learned in Security Planning

Public Sector Recommendations

- Streamline Recovery Approvals
- Mitigate Liability and Reward Responsible Action
- Fund and Incentivize Cybersecurity Improvements

Introduction

The Importance of Cybersecurity in Healthcare

Cybersecurity breaches constantly disrupt the U.S. healthcare system, afflicting patients and providers, academic medical centers and researchers, insurers, pharmaceutical and medical device manufacturers, community health organizations, and many others. These disruptions impose staggering financial costs on healthcare organizations as they move to respond quickly to attacks, notify victims and regulators, rebuild systems, update business partners, restore connectivity, and bolster already advanced defenses. More importantly, cybersecurity breaches impose a real human cost — disrupting critical supply chains, undermining healthcare delivery, and endangering patients.

Our Position

HLC and the Coalition believe cybersecurity in healthcare is a critical patient safety issue, requiring shared responsibility and collaboration between the private sector and governments to protect patient data and continuity of care. We advocate for a risk-based approach to information security, aligned with nationally and internationally recognized standards, to ensure optimal health outcomes.

Collaboration between the private sector and government is essential to strengthening cybersecurity in healthcare. Policies should prioritize information-sharing among international, governmental, and private industry stakeholders and harmonize reporting related to breach incidents.

While the private sector must innovate and implement strong security measures, the government should recognize existing industry standards and provide incentives and assistance to strengthen our collective cyber defenses. Together, we must work to combat growing cyberattacks that pose a threat not only to healthcare organizations but to individual patient health.

The Current Challenge

The Threat Landscape

Healthcare systems are increasingly targeted by a variety of malicious cyberattacks that pose significant risks to patient care and healthcare security. Ransomware attacks, which encrypt or steal critical data and demand a ransom for its return, have been particularly devastating, often leading to the disruption of hospital and other essential healthcare services. Zero-day exploits, which take advantage of previously unknown vulnerabilities, allow attackers to infiltrate systems undetected and cause extensive damage before any patches can be applied. Business email compromises (BEC) and other phishing attacks deceive employees into revealing sensitive information or transferring funds, exploiting human error as a weak link in cybersecurity defenses. Insider threats, where individuals within the organization misuse their access to compromise data or systems, add another layer of complexity to the cybersecurity landscape.

The volume and sophistication of these cyberattacks on healthcare systems have grown at an alarming rate. In 2024, Check Point Research reported a 30% year-over-year increase in cyberattacks globally,[5] and a separate Proofpoint study found that 92% of healthcare organizations reported that they experienced a cyberattack last year.[6] Overall, the global cost of cybercrime is projected to reach $23 trillion by 2027, a 175% increase from 2022.[7]

> In 2024, Check Point Research reported a **30% increase in cyberattacks globally.**[5]

Technology – both old and new – can add to the risk faced by healthcare organizations. Many hospitals operate legacy devices that cannot be easily patched or protected, increasing the risk to the hospital and other devices on the same network. Meanwhile, the integration of artificial intelligence (AI) by malicious actors has further threatened healthcare systems, enabling more sophisticated phishing and malware attacks. State-sponsored threat actors are also targeting healthcare systems, exploiting geopolitical tensions, and disrupting critical infrastructure.

Collectively, these threats compromise patient safety, disrupt healthcare delivery, undermine intellectual property, impede innovation, and inflict significant financial costs on healthcare organizations that could be better spent improving health.

The Impact of Data Breaches on Patient Health

Cyber disruptions often have their greatest impact on healthcare delivery and patient services. Ambulances may need to be diverted from emergency rooms. Life-saving medical devices may go dark. Research may be corrupted or interrupted. Electronic health records may become inaccessible. Doctors and nurses may need to resort to paper forms and charts. Insurance claims or payments may be delayed. Providers and their staff may go unpaid, and pharmacy prescriptions may be delayed.

U.S. researchers found that hospital volumes decreased by 17% to 26% during the first week following a ransomware attack, and among patients already admitted to the hospital during an attack, in-hospital mortality increased by 35% to 41%.[8] A separate 2021 study found that data breaches increased the rate and lowered the survivability of cardiac arrests, even among hospitals that were untargeted but "adjacent" to an healthcare organization suffering a ransomware attack.[9]

> U.S. researchers found hospital volumes **decreased by 17%** during the first **week following a ransomware attack.**[8]

Finally, a well-documented 2024 attack on a British medical lab offered sobering proof of the potential clinical impact of a cyber incident. In the first 17 days after the lab incident, two London hospital systems had to postpone 2,194 outpatient appointments and 1,134 elective procedures,

---

[5] Checkpoint, *Check Point Research Reports Highest Increase of Global Cyber Attacks seen in last two years – a 30% Increase in Q2 2024 Global Cyber Attacks* (July 16, 2024), https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/

[6] Eddy, *supra,* note 3.

[7] Sentinel One, *Key Cybersecurity Statistics for 2025* (Sept. 12, 2024), https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/

[8] Claire McGlave, Hanna Neprash & Sayeh Nikpay, *Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients*, SSRN (Oct. 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4579292

[9] Thaidan Pham et al., *Ransomware Cyberattack Associated with Cardiac Arrest Incidence and Outcomes at Untargeted, Adjacent Hospitals*, CRITICAL CARE EXPLORATIONS 6(4):p e1079 (April 2024), https://journals.lww.com/ccejournal/fulltext/2024/04000/ransomware_cyberattack_associated_with_cardiac.15.aspx

including 184 cancer treatments. Sixty-four organs had to be diverted to other hospitals for transplants.[10]

In short, attacks do not just impose technical or financial hardship; they can hinder access to vital healthcare services and pose real risks to patient safety.

The Impact of Data Breaches on Systemwide Operations

The impact of a data breach does not fall solely on the organization targeted by attackers. Lost connections to systems and data can have a ripple effect across the entire healthcare industry. This is especially true given the health industry's move toward software-as-a-service (SaaS), cloud computing and storage, cross-border research collaborations, and relationships with international partners and vendors. The complex web of healthcare connections expands the "attack surface" that criminals can target and increases the potential impact of any given incident.

For example, in many ransomware attacks, vital data may become encrypted or inaccessible within the targeted organization. At the same time, trusted connections between healthcare partners may be severed, either because the attacker has disabled servers or because the original victim of an attack has deliberately shut down its networks to contain the attack and prevent its spread to others.[11] Therefore, a cyberattack executed on a healthcare provider may impact downstream service providers, healthcare payers contracted with the provider, affiliated practice groups, and patients. Similarly, when one provider must limit or discontinue new admissions or curtail services during a cyberattack, volumes frequently increase at other local facilities, placing additional strain on nearby providers and contributing to systemwide capacity issues. Overall, the downtime caused by cyberattacks can last for months while the impacted organization completes its investigation and restores its systems. Even in cases where the organization pays a ransom to the threat actors, it can take weeks to decrypt affected systems and resume full services.[12]

Because Change Healthcare processes approximately 15 billion healthcare transactions annually, the impact was widespread when it fell victim to a breach in 2024. HHS reported that the attack not only affected Change Healthcare, but it also "impacted payments to hospitals, physicians, pharmacists, and other health care providers across the country."[13] At the individual level, Change Healthcare reported that approximately 190 million people were affected.[14]

The Impact of Data Breaches on Operating Costs

Data breaches have a disproportionate financial impact on healthcare compared to other sectors. Since 2011, healthcare has incurred the highest data breach costs of any sector.

---

[10] NHS England, *Update on cyber incident: clinical impact in South East London* (Jun.20, 20024), https://www.england.nhs.uk/london/2024/06/20/update-on-cyber-incident-clinical-impact-in-south-east-london-thursday-20-june/

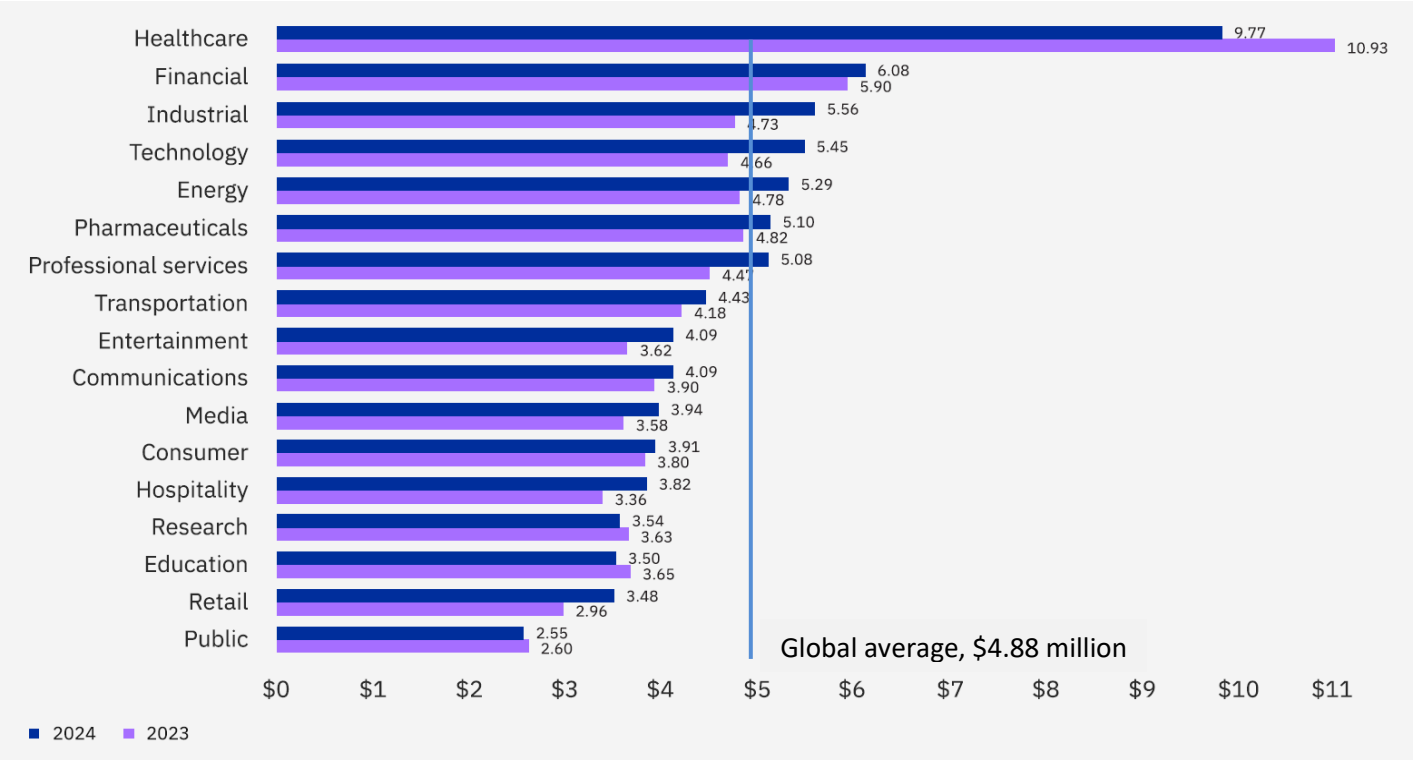
[11] Genevieve Kanter, James Rekowski & Joseph Kannarkat, *Lessons from the Change Healthcare Ransomware Attack*, JAMA HEALTH FORUM. 2024;5(9), https://jamanetwork.com/journals/jama-health-forum/fullarticle/2823757

[12] *Id.*

[13] HHS Sec'y Xavier Becerra, *Letter to Health Care Leaders on Cyberattack on Change Healthcare* (Mar. 10, 2024), https://www.hhs.gov/about/news/2024/03/10/letter-to-health-care-leaders-on-cyberattack-on-change-healthcare.html (archived).

[14] Emily Olsen, *UnitedHealth hikes number of Change cyberattack breach victims to 190M*, CYBERSECURITY DIVE (Jan. 27, 2025), https://www.cybersecuritydive.com/news/change-healthcare-attack-affects-190-million/738369/

Figure 1 – Cost of a Data Breach by Industry



(globally, in millions)

According to the 2024 IBM/Ponemon annual global survey, last year's average cost of a data breach in the healthcare sector was $9.77 million. As shown in Figure 1, this cost was more than double the global, cross-industry average of $4.88 million.[15]

The industry with the next costliest average – the financial sector – averaged just $6.09 million per breach.[16] The impact in this country may be even more stark, given that the study included information from around the world, and data breaches in the U.S. are estimated to be twice as costly compared to those in other industrialized nations like Canada, the U.K., Italy, France, and Japan.[17]

The financial cost of a data breach falls heavily on healthcare organizations, and these costs are borne both immediately and also over a lengthy recovery period. Immediately following an intrusion, organizations typically must organize an internal response team, execute downtime procedures where necessary, and retain experienced outside counsel, forensic experts, and crisis communicators. After days or weeks of intense investigation, healthcare organizations then face the daunting and expensive task of notifying regulators, affected individuals, and business partners. In addition to the cost of notification letters, breached organizations may need to purchase credit monitoring and identity theft protection services, establish call centers, respond to regulators, incur fines, and defend lengthy class-action litigation. Meanwhile, servers, databases, and individual workstations need to be remediated, rebuilt, and scanned for malicious software before being brought back online.

---

[15] IBM and Ponemon Institute, *supra,* note 4 at 10.
[16] *Id.*
[17] The average cost of a data breach across all sectors in the U.S. was $9.36 million in 2024, versus Italy ($4.73M), Canada ($4.66M), the U.K. ($4.53M), Japan ($4.19M) and France ($4.17M). *Id.* at 9.

Recent U.S. breaches announced in 2024 demonstrate just how significant the financial impact can be on a single healthcare organization. For example, UnitedHealth Group announced that the cyberattack against its subsidiary Change Healthcare would cost the company an estimated $3.1 billion.[18]

The Regulatory Landscape

The U.S. healthcare industry faces a labyrinth of cybersecurity laws and regulations in addition to the technical threat of cyberattacks. The U.S. healthcare system is not governed by a single cybersecurity law or standard. Instead, healthcare organizations must navigate a maze of complex state and federal laws, regulations, and best practices related to cybersecurity prevention measures and breach reporting obligations.

Cybersecurity Regulations and Guidelines: HHS and Beyond

Most hospitals, providers, healthcare insurers, exchanges, and their vendors must adhere to the HIPAA Security Rule. As "covered entities" or "business associates," they must follow dozens of specific administrative, technical, and physical controls designed to safeguard information about a person's physical or mental health and any related provision of healthcare or payment. This data, known as electronic "protected health information" or PHI, can be disclosed only for specific authorized purposes under the separate HIPAA Privacy Rule. HHS periodically issues guidance regarding these regulations, and the Department recently proposed an overhaul of the entire Security Rule itself.[19]

Separately, HHS has encouraged the adoption of Cybersecurity Performance Goals (CPGs), which are voluntary standards, guidelines, best practices, methodologies, procedures, and processes to protect PHI. However, if a company falls victim to a large data breach, HHS often determines potential penalties based on yet another security standard called the Health Industry Cybersecurity Practices (HICP), also known as the "405(d) Program."[20]

As explained on its web page called the HHS Cyber Gateway, the Department also embeds cybersecurity requirements in several other offices or initiatives. For example, the FDA considers cybersecurity features when evaluating medical devices.[21] CMS promotes cybersecurity through their Conditions of Participation (CoPs) and Conditions for Coverage (CfCs) that healthcare organizations must meet to participate in the Medicare and Medicaid programs,[22] and ONC certifies and issues security requirements for health information technology (HIT) systems.[23]

If healthcare companies' activities fall outside the ambit of HHS, then different or additional cybersecurity requirements may apply. For example, organizations that offer patient payment plans

---

[18] Emily Olsen, *supra,* note 14.
[19] HHS, *HIPAA Security Rule Notice of Proposed Rulemaking to Strengthen Cybersecurity for Electronic Protected Health Information*, https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/factsheet/index.html
[20] The HICP was developed under Section 405(d) of the Cybersecurity Act of 2015, which called for a more coordinated approach to cybersecurity in the healthcare industry. An organization can mitigate its potential fine if it can show HHS that "reasonable security practices" like the HICP were in place during the twelve months preceding a breach. *See* Public Law 116-321, 134 Stat. 5072 (2021).
[21] *See e.g.*, FDA, *Cybersecurity*, https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity
[22] *See* CMS, *Conditions for Coverage (CfCs) & Conditions of Participation (CoPs),* https://www.cms.gov/medicare/health-safety-standards/conditions-coverage-participation
[23] Asst. Sec'y for Tech. Policy (ASTP), *ONC Health IT Certification Program*, HEALTHIT.GOV https://www.healthit.gov/topic/certification-ehrs/certification-health-it

or other financial or consumer services may fall under the Gramm-Leach-Bliley Act or FTC regulations.[24]

Outside the federal sphere, while most U.S. states and territories generally require "reasonable" security controls around personal information, a few states – such as Massachusetts and New York – impose more detailed cybersecurity programs related to personal information.[25] In addition, several states impose more specific consent requirements related to the collection or disclosure of private health information,[26] and New York has adopted detailed cybersecurity and reporting regulations just for hospitals.[27]

Industry Frameworks

In addition to the statutes and regulations described above, many healthcare organizations and their Chief Information Security Officers (CISOs) must implement nationally recognized cybersecurity "frameworks" published by government agencies, standard-setting bodies, or trade associations. These robust frameworks help establish security controls around health data as well as other types of confidential and valuable information, including employment records, internal financial reports, strategic plans, trade secrets, and privileged legal documents. Many healthcare companies implement these frameworks, not just because they are consistent with cybersecurity "best practices," but also because they appear as requirements in customer or government contracts.

One commonly referenced standard is the NIST Cybersecurity Framework (NIST CSF) 2.0, which sets forth five distinct categories and over 100 specific controls designed to address cyber risks.[28] A list of notable cybersecurity industry frameworks includes:

- NIST CSF 2.0[29]
- International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) Directives, 27001:2022 (ISO 27001)[30]
- HITRUST Cybersecurity Framework (HITRUST CSF)[31]
- Center for Internet Security (CIS) Critical Security Controls (CSC),[32] and the
- American Institute of Certified Public Accountants (AICPA) System and Organizational Controls 2 Type II Framework (AICPA SOC2 Type II).[33]

Other more specific industry standards may be imposed by contract. For example, organizations that accept credit cards as payment for health services must follow PCI DSS. These standards set forth

---

[24] 15 U.S.C.A. § 6801, *et seq.* ; 16 CFR § 314, *et seq.*
[25] 23 NYCRR § 500; N.Y. Gen. Bus. Law § 899-aa, 899-bb; 201 C.M.R. 17.00 *et seq.*
[26] WA ST 19.373.005, *et seq.*
[27] 10 NYCRR § 405.46
[28] NIST, *The NIST Cybersecurity Framework (CSF) 2.0, NIST Cybersecurity White Paper*, NIST CSWP 29 (Feb. 26, 2024), https://doi.org/10.6028/NIST.CSWP.29
[29] *Id.*
[30] ISO/IEC, *ISO/IEC 27001:2022, Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements* (3d ed. 2022), https://www.iso.org/standard/27001
[31] HITRUST, *HITRUST CSF Version 11.5.0* (2024), https://hitrustalliance.net/hitrust-framework
[32] CIS, *CIS Critical Security Controls® Version 8* (2021), https://www.cisecurity.org/controls
[33] AICPA & Chartered Inst. of Mgmt. Accts., *SOC 2® – SOC for Service Organizations: Trust Services Criteria, AICPA & CIMA*, https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2

12 categories and over 300 specific cybersecurity requirements ranging from access controls around card holder data to security awareness training for employees.[34]

Federal Breach Reporting Requirements

The complexity and cost of cybersecurity compliance rises significantly when healthcare organizations fall victim to a breach because healthcare organizations then face daunting reporting requirements.

When a hacker or unauthorized party gains access to unsecured PHI from a vendor, this business associate must report the breach up the chain to hospitals, health plans or other covered entities that are their customers. Under the HIPAA Breach Notification Rule,[35] these covered entities then must report the vendor compromise or their breach to HHS's Office for Civil Rights (HHS OCR) and affected individuals, unless a multi-factor assessment can show there is a low probability that PHI was actually compromised. If this exception does not apply and 500 or more individuals were affected, then covered entities must report the breach to individual victims and HHS OCR "without unreasonable delay" and no later than 60 days after discovering the compromise. HHS OCR then publishes these reports on its public website.[36]

At the same time, covered entities generally must post media notices in the geographic areas where victims are likely to reside. If fewer than 500 victims are affected, covered entities can report data breaches in an annual update to HHS OCR, but in any case, if they cannot locate current addresses for 10 or more individuals, covered entities must post a "substitute notice" on their website and maintain that site for 90 days.

The FTC enforces a similar Health Breach Notification Rule[37] that applies to organizations not covered by HIPAA, including platforms that allow consumers to access or manage personal health records from multiple sources. Any compromise of personal health records must be reported to impacted individuals within 60 days, and to the FTC within 60 days if at least 500 individuals were affected. Like HIPAA, the FTC rule requires local media notices for breaches that involve 500 or more residents in any state or U.S. territory.

For its part, CMS regulations present a maze of requirements for an impacted organization to follow to receive relief after a cybersecurity incident. CMS oversees over 26 quality reporting programs and initiatives, each with detailed requirements that are often tied to payment withholdings or penalties for noncompliance. If a data breach prevents healthcare organizations (providers, payers, etc.) from meeting these reporting deadlines, the impacted organizations must seek relief from CMS by submitting detailed applications for each program and activity in which they are participating. For large health systems, this often means completing dozens of different applications across various CMS compliance programs, with competing deadlines, paperwork requirements, and CMS decisionmakers. As states increasingly adopt their own quality reporting programs, organizations impacted by cybersecurity incidents also must seek relief from state-mandated requirements or risk severe financial penalties.

Depending on their activities, some healthcare organizations must adhere to additional federal requirements aimed at other sectors. For example, large academic medical centers that participate

---

[34] PCI Sec. Standards Council, *Payment Card Industry Data Security Standard: Requirements and Testing Procedures*, v4.0.1 (June 2024), https://www.pcisecuritystandards.org
[35] 45 CFR § 164.400-414.
[36] HHS, *Office for Civil Rights Breach Portal*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
[37] 16 C.F.R. pt. 318 and FTC, *Health Breach Notification Rule*, https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule

in federal loan programs for their medical students may have to report compromises of financial aid data to students and the U.S. Department of Education under federal financial aid contracts and must internally document any unauthorized disclosures of student data under the Family Educational Rights Protection Act (FERPA).[38] In some cases, reporting a breach of educational financial aid data to the government must occur on the *same day* that the breach is detected or suspected.[39]

Other healthcare organizations may fall under the Gramm-Leach-Bliley Act based on their financial activity. Those engaging in banking activities may need to report to federal bank regulators within 36 hours of determining that a reportable computer-security incident has occurred.[40] Other organizations that offer payment and financing options to patients may count as non-bank financial institutions that need to report breaches involving 500 or more financial customers to the FTC within 30 days under the Safeguards Rule.[41]

Separately, publicly traded companies must report data breaches through filings with the SEC within four business days of determining that a cybersecurity incident is "material."[42]

Finally, currently proposed rules from CISA would require any critical infrastructure entity to notify the government of a "substantial" data breach within 72 hours and any ransomware payment within 24 hours. Under these proposed regulations, "critical infrastructure" would include entities in the healthcare and public health sectors.[43]

State Breach Notification Requirements: Health Data and Unauthorized Access Laws

Adding to this complex web of federal laws or regulations, all 50 states and all U.S. territories have breach notification requirements. In the midst of a crisis, healthcare organizations must navigate through numerous variations in these state laws, as described below.

State Data Breach Notifications Laws

- **Breach definitions** – States and territories vary in their definitions of a breach. Most define a breach as the unauthorized "acquisition" of personal data, whereas a handful of states follow the HIPAA example and define a breach as unauthorized "access" to personal information.
- **Federal exemptions** – Forty U.S. state or territorial laws provide exemptions for organizations that follow the notice requirements of HIPAA; however, these exemptions vary in their applicability and breadth. Some states provide a broad "status" exemption for organizations that fall under HIPAA's ambit, while other states only provide "data" exemptions for notices related to PHI. Therefore, other types of compromised personal information (e.g., an unrelated driver's license number) may still be governed by state law. Moreover, some states allow an exemption only if the

---

[38] *See* U.S. Dept. of Education, *Data Breach guidance*, https://studentprivacy.ed.gov/topic/data-breach
[39] The "same day" requirement appears in the Student Aid Internet Gateway (SAIG) Agreement that academic institutions must sign to participate in federal financial aid programs. *See* Nat'l Ass'n of Student Fin. Aid Administrators, *Frequently Asked Cybersecurity Compliance*, https://askregs.nasfaa.org/uploads/resources/ED_Cybersecurity_FAQ.pdf
[40] *Joint Rule on Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers*, 12 CFR Part 53 (Treasury), 12 CFR Part 225 (Fed. Reserve), 12 CFR Part 304 (FDIC) , https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211118a1.pdf
[41] FTC, *FTC Safeguards Rule: What Your Business Needs to Know*, https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know
[42] SEC, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Final Rule*, 17 CFR Parts 229, 232, 239, 240, and 249, https://www.sec.gov/files/rules/final/2023/33-11216.pdf
[43] These regulations were promulgated under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). *See* DHS CISA, *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, Proposed Rule*, 89 FR 23644 (Apr. 4, 2024), https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements

organization's security is deemed "reasonable," and others still require notice to the state Attorney General if the breach affected a threshold number of local residents.

- **Covered personal information** – States also differ in the types of personal information that, if compromised, trigger a duty to notify victims. About half of the jurisdictions require notice if medical data, health information, or health insurance numbers are compromised. All states and territories require notice if Social Security Numbers (SSNs) or state IDs are compromised, and many require notice if financial account numbers and passwords are compromised. Yet, an assortment of other notification "triggers" also applies, including the compromise of biometric or genetic information, email or online account passwords, mother's maiden names, dates of birth, tribal IDs, or even "data collected through the use or operation of an automated license plate recognition system."[44]
- **Form and content of notices** – State laws lack uniformity regarding the breach information that consumers should receive and in what form. All states and territories require organizations to send out hard-copy letters via U.S. mail unless special circumstances trigger "substitute notice" via emails, web site postings, and press releases. One state prohibits telling individual victims about "the nature of the breach … or the number of residents … affected," whereas other regulators require more details including the number of residents affected, and then they publish such reports online. Some states provide little or no guidance about the content of notification letters, while others specify detailed information that must be included in breach notifications, such as: i) paragraph headings, ii) the type of data compromised, iii) steps taken to address the breach, iv) the telephone or toll-free number victims may call for assistance, v) victims' rights to obtain police reports, credit reports, and credit freezes, and vi) contact information for the FTC or state Attorney General. Most state and territorial regulators expect organizations to provide victims with credit monitoring and identity theft protection, especially where SSNs are involved, but only four states actually mandate such monitoring by statute. The required length of such monitoring varies by jurisdiction.
- **Reporting thresholds and authorities** – Whether organizations need to report a breach to regulators or credit bureaus depends on different thresholds set by state law. Some states have no such reporting requirements, while others are "one-and-done" states that require notice to the state Attorney General if even one state resident is affected. Other jurisdictions require notice to regulators if thresholds ranging from 50 to 1,000 victims have been reached and require notice to the major credit bureaus if 500 to 10,000 individuals have been affected. Deadlines for filing reports with regulators and credit bureaus usually follow the timing for individual notices, but one state requires notice to credit bureaus within 48 hours, and two states require reporting to the regulators *first,* before individual letters are sent. Finally, *which regulator* should receive notice also differs. Most states require reporting to the state Attorney General, but some mandate filing with the state police, consumer affairs office, or department of financial affairs.
- **Deadlines** – All states require notification "without unreasonable delay," and some allow for delays if law enforcement is involved. However, many states set more specific deadlines for notifications to affected individuals and regulators. Only four states follow HIPAA's pattern of requiring notice within 60 days; the other states with specific deadlines require faster notice – within 10 to 45 days of discovering a data incident.

[44] Cal. Civ. Code § 1798.82.

State Unauthorized Access Laws for Healthcare Entities

Apart from state data breach notification rules that apply generally within each jurisdiction, healthcare organizations face more specific breach reporting requirements in different industry sectors. For example, California requires clinics, health facilities, home health agencies, or hospice services to "report any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information to the [Department of Public Health] within 15 business days" of the incident.[45] In addition, 26 states have passed the National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law.[46] Under this law, licensed health plans must report any "unauthorized access to," as well as any "disruption or misuse of," their information systems or any information stored on those systems. In most states, reporting to the insurance commissioner must occur within 72 hours of the cyber disruption.

[45] California Health and Safety Code § 1280.15 (2024), https://law.justia.com/codes/california/code-hsc/division-2/chapter-2/article-3/section-1280-15/
[46] NAIC, *State Legislative Brief* (May 2025), https://content.naic.org/sites/default/files/government-affairs-brief-data-security-model-law.pdf

Proposed Framework: Private and Public Sector Responsibilities

The persistent threats posed by cyber criminals, along with these cumbersome regulations, mean that the time is ripe for new thinking within the healthcare sector. Therefore, adhering to applicable industry standards, HLC and the Coalition have developed and endorsed a Cybersecurity Framework that contains a set of private and public sector commitments designed to shore up cybersecurity across the healthcare sector and preserve vital access to care.

This Cybersecurity Framework is not intended to serve as yet another set of regulations or requirements in a crowded field. Instead, HLC and the Coalition hope the Framework will cut through the noise and highlight the critical areas where private and public commitments can have the greatest impact.

To cover the range of commitments needed from private and public partners, we have divided the Cybersecurity Framework into three parts, covering actions needed before to prevent, during to respond, and after to recover from a breach, as described below.

PREVENTION: Hygiene and Resilience

RESPONSE: Restoring and Reporting

RECOVERY: Rebuilding and Learning

Private Sector Commitments

HLC and the Coalition advocate for a risk-based cybersecurity strategy aligned with nationally recognized standards. Therefore, the following responsibilities are derived, not only from the expertise of our members and their respective CISOs, but also from established industry regulations, frameworks, and guidance, including but not limited to HHS's HIPAA Security Rule, its Cybersecurity Performance Goals, and the NIST CSF 2.0.

PREVENTION: Hygiene and Resilience

- **Maintain an Information Security Program based on an Established Industry Framework**

  Our members are committed to maintaining a formal written Information Security Program based on an established industry framework such as NIST CSF, HITRUST CSF, AICPA SOC2 Type II, CIS CSC, or ISO 27001. Rather than taking an ad hoc approach, members already implement one or more of these frameworks because each incorporates years of industry experience and provides a structured and comprehensive approach to managing cybersecurity risks. Different healthcare organizations may adopt different industry frameworks based on their size and needs, but by implementing at least one such framework and following its specific requirements, a healthcare organization can significantly enhance its security posture, not only around patient information but also regarding other personal information and sensitive business data. The breadth and rigor of the framework also can help the organization meet its regulatory requirements and build trust with patients and stakeholders.

  Within each framework, security work begins by identifying, classifying, and encrypting sensitive data. Healthcare organizations must be able to accurately identify and classify PHI and other data based on their sensitivity and criticality to ensure that appropriate security measures are applied. Encryption is then a vital control that can help protect data both at rest and in transit, making it unreadable to unauthorized individuals. Collaborating with software and device vendors is also important to ensure that systems are deployed securely and patched regularly, replacing legacy systems with modern "security by design" systems whenever possible. By adopting a defense-in-depth strategy, entities can create a layered security posture that can effectively thwart cyberattacks.

  Under each framework, our members also implement robust access controls, such as multi-factor authentication (MFA) where appropriate and possible. Many members are also moving toward Zero-Trust architecture, which applies strict identity verification to every person and device trying to access an IT system, regardless of whether they are within or outside the network perimeter. These access controls ensure that only authorized personnel have access to sensitive data, thereby reducing the risk of data breaches and enhancing the organization's overall security posture.

  Regular vulnerability scans are another critical component of an effective Information Security Program. Our members conduct these scans and prioritize patching based on accepted vulnerability scores to help identify and remediate security weaknesses before attackers can exploit them. In addition, other proven strategies for cyber resilience are used, such as leveraging cloud-based security infrastructure and integrating AI into security workflows to enhance readiness against attacks.

  Finally, within their industry frameworks, our members recognize the importance of securing their supply chain because vulnerabilities among vendors and subcontractors can be their "weakest

link." Managing this risk requires not only implementing stringent third-party controls but also using contractual requirements to ensure that fourth- and fifth-level subcontractors adhere to the member's high standards of security.

- **Conduct Regular Risk Assessments based on an Established Industry Framework**

  Conducting security assessments based on an established industry framework is a critical component of a comprehensive Information Security Program. These assessments can take various forms, including: i) an internal or external penetration ("pen") test that simulates hacker tactics to identify network vulnerabilities, or ii) comprehensive security evaluations that scrutinize key security controls under established frameworks like NIST CSF.[47] Such assessments not only provide valuable insights into potential security gaps but also ensure that organizations are adhering to best practices and regulatory requirements. For healthcare organizations covered by HIPAA, conducting these assessments is not just a good idea — it is mandated under the HIPAA Security Rule.[48]

- **Implement an Incident Response Plan based on an Established Industry Framework**

  Our members believe that drafting and implementing a robust Incident Response Plan (IRP) is essential for any comprehensive Information Security Program. An effective IRP is an essential component of every industry framework and ensures that an organization can swiftly and efficiently address and mitigate the impact of security breaches or cyberattacks, minimizing potential damage and facilitating a quicker recovery.[49]

  A successful IRP defines a dedicated response team drawn from different offices and functions across the organization and from trusted outside advisors. Figure 2 depicts one such team for a hospital. The IRP also should define specific roles and responsibilities to establish clear accountability and ensure all team members know their specific duties during an incident. This clarity helps reduce confusion, and it speeds up the response time during a crisis.

  Finally, HLC and the Coalition members understand that team members and even board members and executives must train to use their IRP effectively through tabletop exercises and other simulations. These exercises should mimic real-world attack scenarios, allowing an organization to evaluate the effectiveness of its IRP, identify weaknesses, and improve overall preparedness. Regular practice through these drills ensures that the response team remains sharp, knowledgeable, and ready to act calmly and decisively in the heat of the moment during an actual incident.

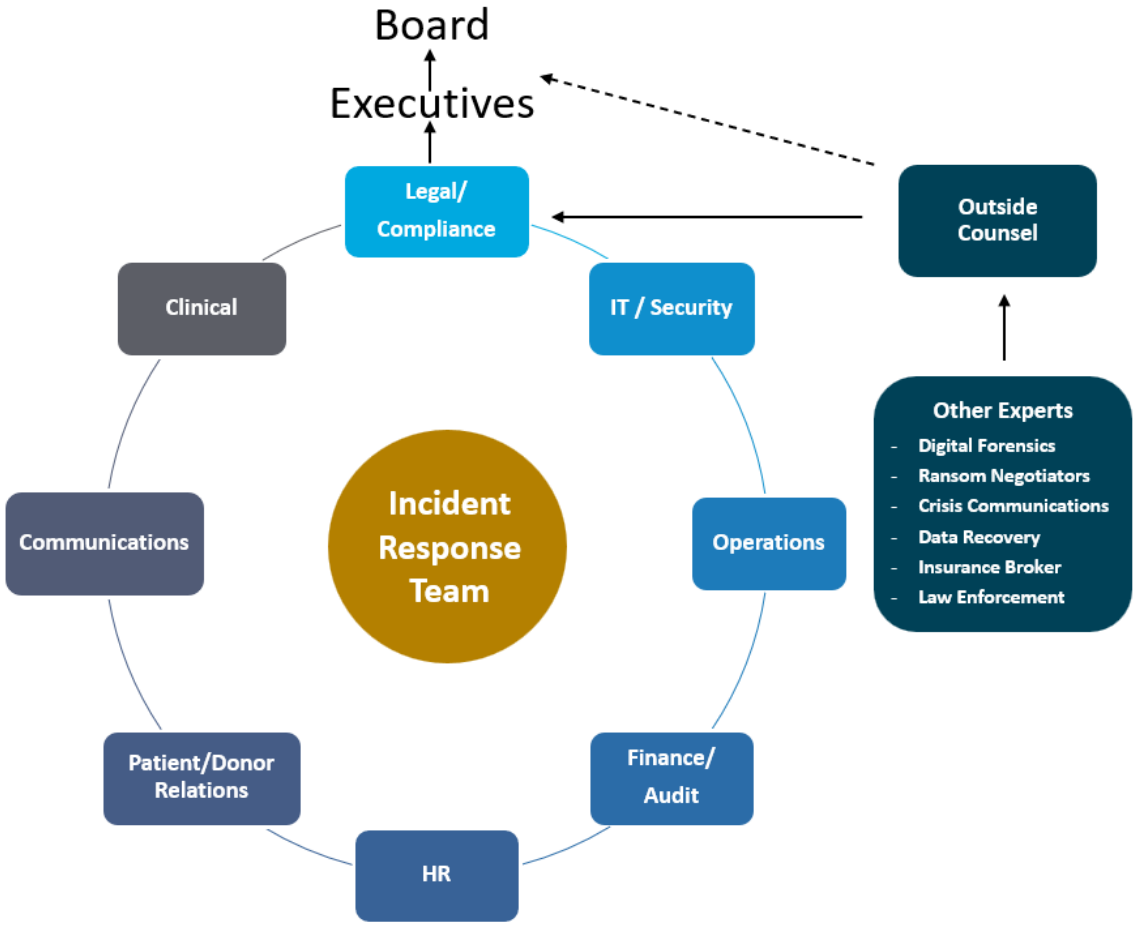
---

[47] Different examples of NIST assessment tools can be found at NIST, *Assessment and Auditing Resources*, https://www.nist.gov/cyberframework/assessment-auditing-resources

[48] *See* 45 CFR § 164.308.

[49] IGW Staff, *The Importance of a Robust Cybersecurity Incident Response Plan*, INFOGOV WORLD (Apr. 9, 2025) at https://infogovworld.com/the-importance-of-a-robust-cybersecurity-incident-response-plan-2/

Figure 2 – Example Incident Response Team



RESPONSE: Restoring and Reporting

- **Investigate and Report Breaches in a Timely Manner**

  To minimize the damage from cyberattacks, HLC and the Coalition members are committed to conducting efficient and effective investigations of such events, following a robust IRP as described above. Each investigation should include a thorough examination of the root cause behind the attack, including forensic analysis where needed. Timely investigation and reporting are crucial because they help identify vulnerabilities and prevent future incidents. Most importantly, a timely and thorough investigation can help mitigate losses and provide assurances to individual victims, business partners, and regulators that an organization is safe to resume operations.

  Following a thorough investigation, our members are committed to providing timely information about the incident to both regulators and affected individuals as required by law. Prompt reporting ensures that affected parties can take additional actions to protect themselves, such as changing passwords or monitoring their accounts for suspicious activity. In addition, timely disclosures help organizations comply with legal and regulatory requirements, thereby avoiding potentially costly fines.

- **Promptly Restore Critical and Essential Systems**

  Effective breach response must not only investigate the nature of an attack but also must restore critical systems as quickly as possible. This is especially important in healthcare, where so many parties operate in an interconnected environment, and a single data incident can affect the entire industry. Therefore, HLC and the Coalition members are committed to identifying impacted systems and rebuilding or restoring them as quickly and safely as possible on a priority basis.

RECOVERY: Rebuilding and Learning

- **Update Stakeholders**

  For healthcare organizations, updating stakeholders promptly and transparently after a data breach is crucial to maintaining trust and restoring patient services. Transparent communications, not only with individual victims and regulators as required by law, but also with other stakeholders (e.g., donors, business partners, and vendors), help mitigate the impact of a breach. By providing accurate and timely information about what happened, what steps are being taken to address the issue, and how the incident affects other parties, an organization can foster the trust needed to reconnect and restart its business activities with others. This responsibility also extends to internal stakeholders such as employees, management, and board directors who need to know about the current cybersecurity threat and risk mitigation plans. Transparent communications help prevent misinformation and rumors, which can exacerbate the fallout from a breach and damage an organization's reputation. In fact, many stakeholders judge the corporate victim of a healthcare breach, not so much by the incident itself, but by the organization's responsible action when recovering from the breach. Therefore, HLC and the Coalition members are committed to updating stakeholders with timely information, reassuring them that the organization is handling the situation responsibly and proactively.[50]

- **Reconnect Efficiently with Trusted Partners**

  Understanding that the healthcare system depends on numerous interconnected participants to deliver medicine and patient services, HLC and the Coalition members are committed to reconnecting with trusted partners as quickly as possible. This involves timely and transparent communications about the incident's impact, as described above, in addition to providing information about *unaffected* systems or those that have been remediated, tested, and "cleared." Requests for "assurance letters" have exploded in recent years[51] and have contributed to costs, anxiety, and delays related data breach reporting. Therefore, HLC members support the development of a voluntary industry initiative to create a standard "assurance" notice that provides crucial information in a widely accepted format, thereby minimizing the need for dozens of one-off responses.

---

[50] For an example of the importance of transparency in the work place, see Andrew Rahman, *The Case for Transparency in the Workplace, and Its Impact on Organizational Performance*, FORBES (June 16, 2023), https://www.forbes.com/councils/forbesbusinesscouncil/2023/06/16/the-case-for-transparency-in-the-workplace-and-its-impact-on-organizational-performance/

[51] Matt Burgess, *Red Tape Is Making Hospital Ransomware Attacks Worse*, WIRED (Jun. 24, 2024), https://www.wired.com/story/ransomware-health-care-assurance-letters/

- **Embed Lessons Learned in Security Planning**

  Our members also commit to conducting "lessons learned" sessions after a data breach because they are essential to improve security management and planning. Post-event evaluations allow organizations to thoroughly analyze the breach, identify its root causes, and understand the effectiveness of their response measures. This process helps pinpoint areas where existing security defenses could be improved and where policies and procedures should be updated. Lessons learned may also provide a valuable foundation for industry-wide action and feedback on regulatory reforms. By taking time to evaluate a previous breach, healthcare companies can strengthen their defenses against future attacks and ensure that their security measures evolve in response to emerging threats. In fact, several established cybersecurity frameworks incorporate “lessons learned” into their models, such as the recently released revision to the NIST Incident Response Life Cycle Model.[52]

  In addition, *ongoing* training and vigilance are needed to maintain a robust security posture. Regular updates to cybersecurity policies and training programs – based on an organization’s own breach or recent incidents across the healthcare industry – help keep staff informed about the latest security practices and threats. This continuous education fosters a culture of caution and preparedness, enabling employees to recognize and respond to potential security issues more effectively. By embedding lessons learned into their security planning, healthcare organizations can enhance their resilience and better protect patient data.

Public Sector Recommendations

HLC and the Coalition members have made strong commitments to cybersecurity, as described above, but they cannot protect patients by themselves. They need the help of the public sector before, during, and after a data breach. The following recommendations highlight areas where the government can work more collaboratively with private industry to build mutual trust, support healthcare organizations, safeguard patient data, and promote public health.

PREVENTION: Hygiene and Resilience

- **Promote Law Enforcement and Information-Sharing as International Priorities**

  To address the growing problem of cybercrime, public officials need to look beyond our own borders. While the U.S. certainly has its own cybercriminals, a significant percentage of ransomware attacks have been attributed to Russian-affiliated threat groups. Other significant cyberattacks have originated from state-sponsored hackers in China and North Korea. Individual healthcare entities find themselves outgunned by state actors or well-organized crime syndicates operating with impunity behind foreign protectors. Against such disproportionate firepower, our members support a push by the U.S. government to make cybersecurity an international priority in diplomatic relations.

  A whole-of-government approach is necessary to tackle the problem of international cybercrime, requiring coordination across agencies such as the U.S. State Department, Department of Defense (DOD), Department of Homeland Security (DHS) and CISA, the

[52] NIST, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management*, NIST SP 800-61r3 (Apr. 2025), https://doi.org/10.6028/NIST.SP.800-61r3

Treasury Department's Office of Foreign Assets Control (OFAC), the Federal Bureau of Investigation (FBI), and others. By leveraging their diverse strengths and expertise, these agencies can work with other governments and non-governmental organizations (NGOs) on two important goals: i) enforcing the laws and norms that criminalize hacking and cyber fraud, and ii) improving the exchange of information between trusted allies in order to bring cybercriminals to justice and thwart emerging cyber threats.

In this regard, U.S. officials can build on successes like the expansion of the International Financial Fraud Kill Chain (FFKC). Coordinated through the FBI and the Internet Crime Complaint Center (IC3.gov), this partnership of law enforcement and financial entities works to freeze fraudulent funds wired by victims of phishing emails and other frauds. Originally focused on recovering funds through U.S. financial institutions, the FFKC increasingly recovers funds through overseas partners as well.[53]

Such international cooperation is needed to ensure that healthcare and other vulnerable sectors can survive and thrive in the face of evolving cyber threats.

- **Bolster Public-Private Collaboration over Cybersecurity Prevention Measures**

  As another valuable tool to combat cybersecurity threats, HLC and the Coalition members support closer collaboration over cybersecurity prevention measures. In particular, we advocate against a one-size-fits-all approach to cybersecurity in favor of a system that recognizes the validity of the nationally and internationally recognized industry frameworks discussed above (e.g., NIST CSF, HITRUST CSF, ISO 27001, etc.). This would allow healthcare organizations to take a more flexible, risk-based approach to cybersecurity while still requiring rigor and implementation of trusted standards.

- **Enhance Public-Private Information-Sharing**

  HLC and the Coalition also support closer collaboration and information-sharing related to cyber threats. Information Sharing and Analysis Centers already exist for the health (Health-ISAC) and biomedical (Bio–ISAC) fields, but cybersecurity could be enhanced through increased participation, wider industry real-time alerts, advanced technology (like AI), and more training opportunities for healthcare organizations. HLC and the Coalition also support the adoption of modern technology and incentives that promote prevention and resilience. Such incentives would help the industry take a more proactive approach to cybersecurity while supporting post-incident and post-breach efforts.

RESPONSE: Restoring and Reporting

- **Harmonize Breach Reporting Requirements**

  Current reporting laws need to be harmonized to speed up response times and reduce the burden of reporting a data incident. As described above, the current patchwork of state and federal laws creates significant challenges and forces healthcare organizations to navigate through inconsistent definitions about what constitutes a breach, what types of personal data trigger reporting, who needs notice, and how fast notice must be provided. This complexity not only increases administrative costs but also delays the timely reporting of breaches, potentially exacerbating the impact on affected patients and other individuals. Therefore, we would support a

[53] *See* FBI, *International Kill Chain Process*, https://www.justice.gov/elderjustice/media/1364056/dl?inline

federal data breach notification law aimed at streamlining these processes, preempting overlapping state laws, and standardizing key elements to ensure more consistent and efficient responses to data breaches.

Consistent with a single reporting law, our members would support the establishment of a common reporting portal to replace over seventy-five different state or federal reporting procedures currently in play. We also would support permitting notices to be provided to individuals via email, rather than through hardcopy letters sent via U.S. mail. In large breaches, this single change could save healthcare organizations millions of dollars and shave weeks off the average reporting time because manually collecting, looking up, and verifying current postal addresses of victims often takes longer than the initial breach investigation itself. Such measures would enhance efficiency, speed up notices, and boost public confidence in government agencies and healthcare organizations charged with protecting patient data.

- **Improve Real-Time Information Sharing**

HLC and the Coalition members support improvements in real-time information sharing in the wake of a data breach, both with the government and across private industry stakeholders. In this regard, we advocate for an expansion of protections in the Cybersecurity Information Sharing Act of 2015. This law provides businesses with protections related to liability, confidentiality, antitrust, and privilege issues, encouraging corporate breach victims to share cyber threat indicators and defensive measures with the government without fear of legal repercussions.[54] In particular, we would support broadening the definition of cyber threat indicators that can be exchanged, expanding the number of government agencies that could receive such information (e.g., HHS, FDA, and CMS) and affording similar protections for the exchange of cyber threat indicators and defensive measures with vendors and business partners. This would help provide the assurance consistently sought by stakeholders, regulators, and law enforcement and would enable quicker reconnections after a breach, enhancing overall cybersecurity resilience.

Additionally, HLC and the Coalition members see a need to enhance local and regional emergency networks, so they are better equipped to exchange information and transfer patients during cyberattacks, not just natural disasters. Strengthening these networks would involve working with existing emergency networks to improve communications and operational capabilities among healthcare facilities, emergency responders, and government agencies. By ensuring that these networks are robust and well-coordinated, healthcare organizations can maintain continuity of care and protect patient safety even in the face of cyber threats.

Finally, our members applaud and encourage continued cooperation with federal law enforcement during cyberattacks. The FBI and other federal agencies provide invaluable insights into the tactics, techniques, and procedures (TTPs) of specific ransomware gangs and other threat groups. We recommend additional collaboration aimed at improving updates for attack victims about ongoing investigations and speeding up the delivery of threat alerts related to new types of attacks.

---

[54] *See* DHS & U.S. Dept. of Justice, *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015* (Oct. 2020) 16-18, https://www.cisa.gov/sites/default/files/publications/Non-Federal Entity Sharing Guidance under the Cybersecurity Information Sharing Act of 2015_1.pdf

RECOVERY: Rebuilding and Learning

- **Streamline Recovery Approvals**

  With responsibility for the oversight and operation of dozens of quality reporting programs, CMS is a primary stakeholder in recovery efforts after a cyberattack, and the agency acts as a gatekeeper for organizations seeking relief from onerous and costly mandatory reporting programs. As a result of downtime procedures after cybersecurity incidents, healthcare organizations often lack the ability or even underlying data to meet reporting requirements that span provider type (inpatient hospital, home health, skilled nursing, etc.) and program area (Merit-based Incentive Payment System, Medicare Shared Savings Program, etc.) Failure to receive an exception or exemption from such requirements during a data breach can place millions of Medicare dollars at risk, and in certain cases subject the reporting organization to compliance actions.

  CMS has made strides to reduce the burden of seeking exceptions from these reporting requirements through its Extreme and Uncontrollable Circumstances (EUC) Exceptions process. However, CMS procedures and underlying regulations remain heavily focused on traditional emergencies (such as hurricanes, fires, etc.) and only offer automatic exceptions in the case of specific disasters, such as a Federal Emergency Management Agency (FEMA)- designated major disaster. In other cases, regulations are outdated and place geographic bounds on the scope of emergencies, which are largely inapplicable to cybersecurity incidents.

  HLC and the Coalition members encourage CMS to update and harmonize its regulations to clearly recognize cybersecurity incidents as disasters eligible for relief under its various quality reporting programs. Moreover, the identification of a single “cybersecurity response ombudsman” at the agency would greatly aid organizations seeking to request various exceptions as they navigate the maze of otherwise conflicting requirements.

- **Mitigate Liability and Reward Responsible Action**

  Healthcare organizations live under a constant, impossible, and costly mandate to prevent all data intrusions, losses, or accidental disclosures, while hackers only need to succeed once to penetrate a network and cause a data breach. Recognizing this dynamic, U.S. regulators should offer incentives for healthcare organizations to build stronger defenses, rewarding such proactive measures and mitigating liability for healthcare organizations that build robust cybersecurity programs.

  Therefore, HLC and the Coalition seek deeper recognition of the substantial cybersecurity programs built and maintained by its members. For example, as described above, HHS considers whether to mitigate fines if an organization has implemented 405(d) measures in the year before a breach. However, showing such compliance often involves tediously "cross-walking" numerous policies and program activities into the 405(d) rubric. Instead, there should be more direct approval of implemented industry frameworks like the NIST CSF. Recognizing these trusted industry frameworks would streamline compliance efforts and acknowledge the rigorous standards already being met by healthcare organizations.

  Furthermore, healthcare organizations that implement comprehensive cybersecurity programs under an approved framework should be granted a "safe harbor" that exempts them from liability or mitigates potential fines and damages flowing from regulatory or private actions. Providing such incentives and relief is crucial and would not only enhance cybersecurity resilience but also

would ensure that healthcare organizations can focus on delivering quality services and care without the constant threat of punitive actions.

- **Fund and Incentivize Cybersecurity Improvements**

  Combating current and future cybersecurity threats will require additional government funding and support, particularly for small, rural, or less mature providers that face cost constraints and staffing shortages. These organizations often struggle to hire sophisticated cybersecurity experts or even IT professionals. Therefore, our members support government assistance in the form of grants, direct cybersecurity training, or penetration and security testing. Such support could be modeled after services already offered by DHS and CISA to state, local, tribal, and territorial governments. For example, in 2024, DHS offered 839 grants to these governments to develop cybersecurity policies, hire cybersecurity contractors, upgrade equipment, and implement multi-factor authentication. A recent GAO audit found that such projects were "essential to identifying risks, protecting systems, detecting events, and responding to and recovering from incidents."[55]

  In addition to such training and education, HLC and the Coalition members would support private, academic, and government partnerships to expand cybersecurity opportunities at all career stages in healthcare. More than 500,000 cybersecurity jobs remain unfilled across all sectors in the U.S.,[56] and this workforce gap has a severe impact on healthcare organizations' ability to thwart cyberattacks and protect patients.

  HLC and the Coalition members also encourage the government to consider a national insurance fund to cover companies facing cyberattacks. Many healthcare organizations find that private cybersecurity insurance is unaffordable, limited, or unavailable to meet their needs. Therefore, we support the exploration of a publicly backed insurance fund, patterned after models used to address terrorism or floods. This fund would offer coverage for catastrophic cyber incidents while providing incentives to organizations to adopt best practices in cybersecurity. By providing a safety net, the national cyber insurance fund would help mitigate catastrophic losses from cyberattacks and help build a more resilient healthcare industry.

Conclusion

Data breaches have caused widespread and disproportionate harm by endangering patients, undermining the delivery of care, disrupting critical supply chains, and forcing systemwide outages. Collaboration between private healthcare organizations and the government is crucial to safeguarding patients, access to services, and a functioning healthcare system.

Mutual accountability is essential. As the private sector innovates and implements robust security measures designed to protect healthcare systems and data, the government should provide a risk-based regulatory framework that aligns with established industry standards, promotes international and local cooperation, harmonizes breach notice requirements, streamlines operational reporting, and offers incentives and assistance to healthcare organizations to meet persistent and growing cybersecurity threats.

---

[55] U.S. Gov't Accountability Off., *Cybersecurity: DHS Implemented a Grant Program to Enable State, Local, Tribal, and Territorial Governments to Improve Security,* GAO-25-107313 (Apr. 25, 2025), https://www.gao.gov/products/gao-25-107313

[56] CyberSeek, *Cybersecurity Supply/Demand Heat Map*, https://www.cyberseek.org/heatmap.html