

Documents for the Record – 4/16/2024

Majority:

- April 14, 2024 – Statement submitted by the American Association of Nurse Anesthesiology
- April 15, 2024 – Statement submitted by AvaMed
- April 15, 2024 – Statement submitted by the American Dental Association
- April 15, 2024 – Statement submitted by the National Association of Insurance Commissioners
- April 16, 2024 – Document submitted by the Health Sector Coordinating Council, Recommendations for Government Policy and Programs
- April 16, 2024 – Document submitted by the Health Sector Coordinating Council, Strategic Plan
- April 16, 2024 – HITrust Report submitted by Rep. Latta
- April 16, 2024 – Statement submitted by AHIP
- April 16, 2024 – Statement submitted by the Blue Cross Blue Shield Association
- April 16, 2024 – Statement submitted by the Federation of American Hospitals
- April 16, 2024 – Statement submitted by the Healthcare Leadership Council
- April 16, 2024 – Statement submitted by the Medical Group Management Association

Minority:

- April 16, 2024 – Article from the Wall Street Journal, “UnitedHealth Stock Jumps After Earnings Beat Expectations, Despite Cyberattack”
- April 16, 2024 – Statement submitted by the American Medical Association



American Association of
NURSE ANESTHESIOLOGY

The Honorable Brett Guthrie
Chairman
House Committee on Energy and Commerce
Subcommittee on Health
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Anna Eshoo
Ranking Member
House Committee on Energy and Commerce
Subcommittee on Health
2425 Rayburn House Office Building
Washington, D.C., 20515

Chairman Guthrie and Ranking Member Eshoo:

On behalf of the American Association of Nurse Anesthesiology (AANA), I write to you today in light of the Subcommittee's upcoming hearing titled "Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack," to urge the Subcommittee to swiftly take action to prevent similar incidents in the future to maintain patient access to care.

The AANA is the professional association for Certified Registered Nurse Anesthetists (CRNAs), representing over 61,000 CRNAs, representing nearly 90% of nurse anesthetists in the United States. CRNAs are advanced practice registered nurses (APRNs) who administer more than 50 million anesthetics to patients every year, across the nation. CRNAs are also Medicare Part B providers who, since 1989, have billed Medicare directly for 100% of the Medicare Physician Fee Schedule (PFS), as well as commercial payers.

Cybersecurity attacks, like the one on Change Healthcare, can have significant effects on providers, including CRNAs and their patients. A significant share of AANA members work in anesthesia groups, own their own businesses, or work as independent contractors where they may rely on organizations such as Change Healthcare to handle claims processing and provider payment management services. Disruptions to Change Healthcare's services imperils the financial health of healthcare providers, which can lead to patient's access to care.

These effects are being felt most acutely in the healthcare settings that have already been stretched thin, including rural communities and other already underserved populations, where CRNAs are often the only anesthesia providers. Healthcare providers in these communities depend on steady and predictable cash flows to maintain their razor-thin margins in order to continue to provide patients with adequate access to healthcare.

We are appreciative of the efforts that the Department of Health and Human Services and the Centers for Medicare and Medicaid Services have undertaken to secure advance payments to Medicare Part B providers who were impacted by the service outage. However, Congress needs to take additional steps to stop these attacks before they disrupt patient's access to care.

We hope to be a resource to your Subcommittee as they continue this important work. We appreciate your timely, attentive response to this crisis and urge swift action to prevent these kinds of attacks in the future. I encourage Members of the Subcommittee and their staff to contact AANA's Directors of Federal Government Affairs, Matthew Thackston () and Kristina Weger () with any questions. Thank you again for your attention to this important issue.

Sincerely,

Dru Riddle



**Statement for the Record
House Energy and Commerce Committee,
Subcommittee on Health
Hearing, "Examining Health Sector Cybersecurity in the Wake
of the Change Healthcare Attack"
Tuesday, April 16, 2024**

AdvaMed, the medtech association, represents manufacturers of medical devices, diagnostic products, and health information systems that are transforming health care through earlier disease detection, less invasive procedures, and more effective treatments. These members range from the smallest to the largest medical technology innovators and companies. AdvaMed's 450 member companies manufacture the vast majority of all medical technology products sold in the United States. AdvaMed advocates for a legal, regulatory and economic environment that advances global health care by assuring worldwide patient access to beneficial medical technology. We promote policies that foster the highest ethical standards, rapid product approvals, appropriate reimbursement, and access to international markets.

Medical devices are an important component of healthcare ecosystem. This ecosystem includes but is not limited to the users, health care professionals, providers, IT system integrators, health IT developers, IT vendors, medical device manufacturers, and regulators. The entire healthcare ecosystem should be aware of the potential for cybersecurity incidents and share in the commitment to securing these technologies.

Patient safety is the number one priority for the medical technology industry, and so medical device manufacturers take seriously the need to continuously assess the security of their devices in a world where technology constantly evolves. Medical device manufacturers make concerted efforts to address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment, maintenance and disposal of the device and associated data.

The U.S. Food and Drug Administration (FDA) is the primary authority in regulating medical devices, including establishing that they are cybersecure. FDA administers comprehensive regulations and implements guidance that prescribes risk management requirements that medical technology manufacturers must comply with and for which they face severe penalties for failing to follow. FDA's cybersecurity requirements address both pre- and post-market concerns.



The medical device industry developed Medical Device Cybersecurity Foundational Principles (attached) to guide the development of an effective cybersecurity program for the production and deployment of secure medical devices.¹ Originally adopted in 2016, the Foundational Principles were updated in 2023 to be consistent with the Consolidated Appropriations Act for 2023, which included the Food and Drug Omnibus Reform Act (FDORA), with a section, Ensuring Cybersecurity of Devices.

Our industry actively participates in numerous groups and organizations that bring together the healthcare industry to address cybersecurity matters. One such organization is the Health and Healthcare Sector Cybersecurity Coordinating Council (“HSCC”) Joint Cybersecurity Working Group (“JCWG”), which brings together more than 200 domestic industry and government organizations to work together to develop strategies to address emerging and ongoing cybersecurity challenges to the health sector.

Device manufacturers also participate in information-sharing organizations, including the Healthcare Information Sharing and Analysis Center (“H-ISAC”) and the U.S. Department of Homeland Security’s National Cybersecurity and Communications Integration Center, which operates the Computer Emergency Response Team (“US-CERT”), and Industrial Control System CERT (“ICS-CERT”).

Our industry has also engaged in the development of numerous consensus standards that included representatives from medical device manufacturers, independent security experts, academia, and health care delivery organizations. Some of these standards include: (1) AAMI TIR57:2016, Principles for medical device security—Risk management (FDA Recognition Number 13-83); (2) IEC 80001-1 series including ANSI/AAMI/IEC TIR 80001-2-2:2012, Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls (FDA Recognition Number 13-43); (3) HIMSS/NEMA HN 1-2013, Manufacturer Disclosure Statement for Medical Device Security; and (4) AAMI TIR97, Principles for medical device security – Postmarket risk management for device manufacturers.

We are committed to patient safety and continue to work with the FDA, health care providers, the academic community, security experts and other stakeholders on ways to ensure the continued security, safety and effectiveness of medical devices.

¹ <https://www.advamed.org/member-center/resource-library/advamed-medical-device-cybersecurity-foundational-principles-2/>





AdvaMed Medical Device Cybersecurity Foundational Principles

Safety is critical to the medical technology industry, and medical device manufacturers take seriously the need to continuously assess the security of their devices in a world where the risks, no matter how remote, evolve. Medical device manufacturers address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment, maintenance and disposal of the device and associated data. Similarly, manufacturers implement proactive measures to manage medical device cybersecurity, including but not limited to routine device cyber maintenance, assessing postmarket information, employing risk-based approaches to characterizing vulnerabilities, and timely implementation of necessary actions.

This document provides the medical device industry's foundational principles¹ for building a cybersecurity program for the development and deployment of secure medical devices. To be sure, the entire health care ecosystem that uses advanced medical technologies should be aware of the potential for cybersecurity incidents and share in the commitment to securing these technologies. This includes but is not limited to the users, health care professionals, providers, IT system integrators, health IT developers, IT vendors, medical device manufacturers, and regulators. Moreover, security requirements for medical devices must take into account the intended use and use environment of the product. For example, many medical devices are required to be immediately accessible by a physician during an emergency medical procedure, and miniaturized medical devices are often constrained by limited energy storage (e.g., battery life).

The medical device industry commends and supports FDA's efforts to address medical device cybersecurity. We continue to work with the agency, health care providers, the academic community, security experts and other stakeholders on ways to ensure the continued security, safety and effectiveness of medical devices.

The following foundational principles should guide the development of an effective cybersecurity program for the production and deployment of secure medical devices:

1. Medical device development and security risk management. An effective cybersecurity risk management program incorporates both premarket and postmarket lifecycle phases and addresses cybersecurity from medical device conception to disposal.²

Medical device security risks should be addressed through a risk management process that is based on consensus-driven recognized standards and reference documents.³

- A. Manufacturers shall address and document cybersecurity during the design and development of the medical device. As a result, cybersecurity should be fully integrated into manufacturer quality management systems. In addition to patient safety and device effectiveness, product development processes must address privacy concerns as well as the fundamental objectives of secure design: Confidentiality, integrity (including authenticity and non-repudiation), and availability.
- B. Manufacturers should work with health care providers, device users and patients to ensure that risk control measures intended to increase security do not degrade the intended use of the device, including requirements related to emergency access. A risk-benefit analysis may be required in certain situations. In many cases, the therapeutic benefits of a product far outweigh potential security risks.
- C. Manufacturers shall have a process to monitor the ongoing security of their devices and if new vulnerabilities are revealed, they must determine whether additional security risk control measures can be implemented without compromising the safety and effectiveness of the device. These processes should operate with the quality management system creating supporting records and must operate in a timely manner to ensure health care ecosystem cybersecurity risks from vulnerabilities are adequately communicated and managed.
- D. Manufacturers should employ mechanisms to receive relevant cybersecurity-related information from their suppliers.

2. System-level⁴ security. Systems are only as secure as their weakest point. In order to maintain system-level security, all elements of the system must be appropriately managed and secured.⁵

- A. System-level security is a shared responsibility. Device manufacturers play an important role; however, all stakeholders within the larger health care ecosystem must work together to ensure its integrity.

- B. Security incidents should be investigated in a collaborative fashion in order to, as appropriate, uncover facts, appropriately inform stakeholders including patients, health care delivery organizations, and regulators, and to employ additional security risk control measures when appropriate in the context of a device's intended use.

3. Coordinated disclosure. Medical device manufacturers should support a coordinated disclosure process that provides a pathway for researchers and others to submit information, including detected potential vulnerabilities, to the organization.

- A. Coordinated disclosure processes should clearly define the responsibilities of both the manufacturer and researcher.
- B. Manufacturers bear a responsibility to address submitted potential vulnerabilities in a timely and professional manner and to comply with regulatory reporting requirements.
- C. To minimize any potential impact to patient safety, researchers and other third parties should work with and submit as promptly as possible, and prior to public release of such information, potential vulnerabilities to the manufacturer and relevant government body (e.g., FDA or DHS) on a coordinated basis.

4. Information sharing. It is important for manufacturers to continuously manage their device's cybersecurity throughout the product's lifecycle. Part of this process includes the judicious sharing of threat and vulnerability information, which enables organizations to efficiently respond to new threats.

- A. In order to facilitate the exchange of information, manufacturers should consider the use of a single information exchange body, with the understanding that other avenues of information sharing exist. If a new threat is discovered, it should be shared and, once validated, disseminated to the appropriate stakeholders.
- B. Shared vulnerability information must protect the identity and intellectual property of medical device manufacturers and disclosure of the information should not jeopardize the privacy and civil liberties of individuals. Authentication methods, non-disclosure agreements, and restricted access to information should be employed to ensure that only trusted entities receive vulnerability information.
- C. Close cooperation with local, state, and federal law enforcement agencies is necessary to ensure that information sharing does not inadvertently enable a threat source.

5. Software Bill of Materials (SBOM). To ensure medical device users are able to respond to cybersecurity threats, the community must coalesce around a common approach and align with standards to create and share SBOMs to ensure their consistency and usefulness.

- A. Medical device manufacturers, FDA and health care providers should agree to the information that is to be conveyed in the SBOM. Information required in the SBOM should be consistent with industry minimum expectations and standards including CISA minimum elements of an SBOM guidance. Only information that is necessary to support the essential cybersecurity functions of the SBOM recipient, without compromising intellectual property rights or providing information capable of misuse, should be shared.
- B. In order for an SBOM to serve as a meaningful resource, manufacturers should appropriately maintain and update the document when changes are made to the device.
- C. If required by a device manufacturer, SBOM recipients are expected to keep confidential all information shared by the device manufacturer, and the information must not be shared with third parties outside of established confidentiality agreements. Some device manufacturers may choose to provide SBOMs in a less restrictive manner, but until practices mature it is important to establish trust between all stakeholders.

6. Consensus standards, regulatory requirements, and education. The development of consensus standards and regulations should be a collaborative effort between regulators, medical device manufacturers, independent security experts, academia, and health care delivery organizations.

- A. The health care industry should leverage the experiences and expertise of other critical infrastructure sectors and government agencies (e.g., CISA, NIST).
- B. The involvement of academia and independent security experts is a critical factor in ensuring that new standards and regulations are current and reflect best practices.
- C. Manufacturers and health care delivery organizations should leverage principles elaborated in relevant consensus standards and technical reports.
- D. Stakeholders should be educated on the importance of coordinating privacy and security requirements so that they complement each other to further patient safety.

¹ AdvaMed initially approved these principles in 2016 and updated them in 2023 to reflect new FDA authority.

² Device manufacturers are expected to apply FDA's cybersecurity-related guidance documents during the premarket and postmarket lifecycle phases. See *Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act* (Mar. 29, 2023); *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions* (Sept. 26, 2023); *Postmarket Management of Cybersecurity in Medical Devices* (Dec. 27, 2016).

³ For example, manufacturers should address medical device security risks through a risk management process aligned with ISO 14971 Medical devices — Application of risk management to medical devices, and apply the NIST Framework for Improving Critical Infrastructure Cybersecurity in the development and implementation of their cybersecurity program.

⁴ System-level security refers to the architecture, policy and processes that ensure data and system security in systems that contain connected medical devices.

⁵ The ISO/IEC 80001 series of standards and technical reports support the risk management of IT-networks incorporating medical devices, including communication of product-specific security risk control measures that are the responsibility of a health care delivery organization.

April 15, 2024

The Honorable Brett Guthrie
Chair, Health Subcommittee
U.S. House of Representatives
Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Anna Eshoo
Ranking Member, Health Subcommittee
U.S. House of Representatives
Committee on Energy & Commerce
2322A Rayburn House Office Building
Washington, DC 20515

Dear Chair Guthrie and Ranking Member Eshoo,

On behalf of the more than 159,000 dentist members of the American Dental Association (ADA), we are writing to provide insights and recommendations for your hearing on the Change Healthcare cyberattack.

As you are aware, the cyberattack on Change Healthcare, one of the largest healthcare technology companies in the United States, has had significant repercussions for many sectors, including dental practices. The lack of transparency surrounding the financial impact of this incident is concerning and we believe full financial impact assessments by the industry are imperative.

Our members have reported delayed claims, additional expenses incurred due to resorting to physical mailing, and increased office staff time spent on call centers and troubleshooting. In the nearly ten weeks since the cyber-attack, dental services have yet to be fully restored. This means provider credentialing, claims and claim attachments processing and tracking, practice analytics and revenue cycle insights, and automation of business functions (eligibility and benefits verification, payment remittances, etc.) are experiencing ongoing disruptions.

Due to the unprecedented magnitude of this attack, we recommend the below measures that we believe are crucial to ensuring the resilience of our healthcare infrastructure in the face of cyber threats.

1. **Comprehensive Financial Impact Assessments:** Urgently conduct comprehensive financial impact assessments across the industry to ascertain the extent of the damage inflicted by the cyberattack. These assessments should encompass not only direct financial losses, but also indirect costs incurred due to disruptions in practice operations.
2. **Enactment of Prompt Pay Legislation:** The enactment of “prompt pay” laws would mandate insurance companies to promptly reimburse healthcare providers for services rendered. This is pivotal to ensuring the financial stability of systemically important healthcare institutions, which include dental practices, amidst increasing cyber incidents and other emergencies.
3. **Enhanced E-Prescribing Standards:** Strengthen e-prescribing standards implementation and interoperability to ensure seamless continuity of care and medication access for patients during cyber-related disruptions. Standardized e-prescribing and systems to access to Enhanced Prescription Drug Monitoring Program (ePDMP) improve patient safety and alleviate administrative burdens on dental practices.
4. **Health Insurance Portability and Accountability Act (HIPAA) Compliance Enhancement:** HIPAA compliance can help safeguard protected health information from cyber threats. Strengthening HIPAA compliance measures so that health IT vendors that enter in business associate agreements with covered entities are held to the same standards

under HIPAA as covered entities is imperative for protecting patient confidentiality and mitigating cybersecurity risks.


5. **Cybersecurity Support for Dental Practices:** As critical small healthcare businesses, dental practices often lack the resources and expertise to implement robust cybersecurity measures independently. Providing for enhanced cybersecurity support and resources to fortify defenses against cyber threats could include access to cybersecurity training, assistance in implementing cybersecurity frameworks, and other collaboration with cybersecurity experts.
6. **Mitigation of Potential Price Gouging:** Price transparency measures such as price caps and stringent oversight mechanisms are essential to prevent opportunistic pricing practices that could exploit vulnerabilities in the healthcare system.
7. **Payer Responsibility and Collaboration:** Holding payers accountable for facilitating uninterrupted access to reimbursement and financial support for healthcare providers during cyber incidents. Payers should collaborate with providers, industry stakeholders, and government agencies to develop robust contingency plans and expedite claims processing to minimize disruptions.

We believe these proposals can aid policymakers as they seek to take proactive steps towards long-term resilience in the face of future cyber threats to dental practice and the broader health care system. In addition to addressing the immediate aftermath of this cyberattack, we urge the Committee to consider any legislative measures that would improve options for healthcare providers impacted by cyberattacks and that attempt to prevent such incidents in the future. We are particularly interested in policies addressing gaps in cybersecurity regulations and enforcement mechanisms such as measures to enhance penalties for cybercrimes, streamlining transparency on incident reporting requirements, support for contingency planning and facilitating information sharing among law enforcement agencies and healthcare providers.

We appreciate the Committee holding a hearing on this critical issue and would be happy to provide any further information or assistance. The ADA remains committed to collaborating with policymakers to safeguard the integrity and security of our healthcare infrastructure.

The ADA looks forward to continuing to work with you and we would welcome the opportunity to speak with you in more detail and answer any questions you have regarding these comments. Please contact Ms. Natalie Hales at [REDACTED] or [REDACTED] to facilitate further discussion.

Sincerely,



Linda J. Edgar, D.D.S., M.Ed.
President



Raymond A. Cohlma, D.D.S.
Executive Director

LJE:RAC:nh

Cc: Members of the House Energy & Commerce Committee

April 15, 2024

The Honorable Brett Guthrie
Chairman
Subcommittee on Health
Energy and Commerce Committee
United States House of Representatives
Washington, DC 20515

The Honorable Anna Eshoo
Ranking Member
Subcommittee on Health
Energy and Commerce Committee
United States House of Representatives
Washington, DC 20515

The Honorable Larry Bucshon, MD
Vice Chair
Subcommittee on Health
Energy and Commerce Committee
United States House of Representatives
Washington, DC 20515

Dear Chairman Guthrie, Vice Chair Bucshon, and Ranking Member Eshoo:

Thank you for reaching out to the National Association of Insurance Commissioners (NAIC) for comments on the Change Healthcare ransomware attack, and we commend the Committee for examining this important issue. The NAIC represents the lead insurance regulators in the 50 states, the District of Columbia, and 5 United States Territories.

When news broke that Change Healthcare's systems were down due to a cyberattack there was great concern among state regulators, but our concerns only grew as the significance of the event quickly became apparent. What initially seemed to be an incident limited to United Health Group (UHG) soon became a crisis that impacted the operations of insurance companies, providers, and pharmacists - and thus consumers - nationwide. There were also questions about whether private information was obtained by the criminals responsible for this attack. As state regulators collaborated with each other, and engaged UHG and Change Healthcare, we gained an understanding of the growing issue and began reaching out to insurance carriers for more information and encouraged them to provide immediate assistance and flexibilities to providers to ensure care and access to prescription drugs continued without significant delay.

States issued official bulletins and memos to their carriers urging them to take actions to keep funds flowing to providers, allow prior authorization flexibility, and provide timely updates on the status of their various systems.

To be clear, Change Healthcare was the victim of a crime, but also has a responsibility to follow applicable rules and laws of the states for data security that may apply to it. We are currently working to determine the applicability of state rules and laws to Change Healthcare, which itself is not a risk-bearing insurance entity, and determining whether additional protections and contingencies are necessary to ensure consumers receive care and providers receive reimbursement in a timely manner and that regulators have the authority they need to enforce such requirements.

State regulators are now working together to determine if impacted carriers complied with all existing state cybersecurity and consumer protections regulations. For example, the NAIC developed cybersecurity and claims settlement regulations that some states have adopted. You can find those here:

Cybersecurity:

<https://content.naic.org/sites/default/files/inline-files/MDL-668.pdf>

Unfair Claims Settlement:

<https://content.naic.org/sites/default/files/inline-files/MDL-900.pdf>

The NAIC has created a multi-state Steering Group to look at how the cyberattack unfolded, assess how insurance carriers and other impacted entities reacted, and facilitate discussions about the response and recovery efforts with UHG's and Change Healthcare's senior management. The Steering Group, which is in the early stages of their work, can keep the Subcommittee updated on their progress and findings. While corporate protocols, IT security, and appropriate regulatory requirements can minimize the risk of a ransomware attack, we acknowledge that such attacks can and will still occur, and some will be successful. We are committed to examining whether UHG and Change Healthcare lived up to their obligations under the law, communicating with impacted stakeholders, and in the weeks ahead analyzing what we can do better to assist consumers and mitigate the damage from ransomware and cyber security threats to the insurance sector.

As we look forward, state regulators hope to learn from this attack and be more prepared should it happen again. One overarching concern is how an attack on a single entity could impact the delivery and reimbursement of healthcare nationwide. Regulators and policy makers may need to consider the significance of this event and whether additional redundancies or contingency plans need to be developed to prevent such a crisis in the future. Part of our collective work should be to assess whether state and federal regulators have sufficient authority during a cyberattack or comparable emergency to require certain actions by health insurers and healthcare providers. What flexibilities, consumer protections, notifications, liability protections, etc., are necessary to avoid distributions in care? We intend to focus on these important questions, and welcome engagement with this Subcommittee as our work progresses.

We applaud the Subcommittee for holding this hearing and look forward to working with you and other Members of Congress and the Administration to improve the resilience of the health insurance sector for the benefit of its policyholders.

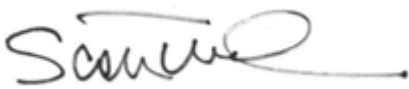
Sincerely,



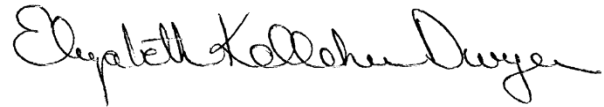
Andrew N. Mais (He/Him/His)
NAIC President
Commissioner
Connecticut Insurance Department



Jon Godfread
NAIC President-Elect
Commissioner
North Dakota Insurance Department



Scott White
NAIC Vice President
Commissioner
Virginia Insurance Department



Elizabeth Kelleher Dwyer
NAIC Secretary-Treasurer
Director
Rhode Island Department of Business
Regulation



Health Sector Coordinating Council
Cybersecurity Working Group



**Manage
Risks**



**Monitor
Threats**



**Respond &
Recover**

Health Industry Cybersecurity -

Recommendations for Government Policy and Programs



OCTOBER 2023

Reprint of April 2023 Edition

Table of Contents

Introduction	3
About the Health Sector Coordinating Council	4
Healthcare Cybersecurity Policy and Program Proposals for Government Consideration	4
<i>Preparedness Support and Information Sharing</i>	4
<i>Financial Support and Incentives</i>	6
<i>Incident Response and Recovery</i>	7
<i>Workforce</i>	8
<i>Regulatory Reform</i>	8
Policy Foundation and Current Developments	9

Introduction

Cyber threats to the healthcare sector are a well-documented reality of modern healthcare delivery. Ransomware attacks against hospitals, clinics, service providers, and other healthcare delivery organizations (HDOs) routinely deny access to patient records, billing systems, and other digital technologies deployed throughout modern healthcare environments. Vulnerabilities discovered in the digital infrastructure relied upon by modern healthcare delivery organizations (HDOs) to deliver quality care pose patient safety and privacy risks that include delay or denial of treatment, data loss, manipulation or corruption of necessary treatment or other digital healthcare data, and the risk of intentionally or unintentionally tampered software, among other potential risks. And the massive and increasing complexity of today's connected healthcare ecosystem gives rise to its own risks: of unanticipated and poorly understood interdependencies; of unknown inherited security weaknesses; of overreliance on vendor solutions; of systems that fail to adequately account for human factors related to cybersecurity controls; and of inconsistencies between software and equipment lifecycles, among others. As a result, we are adopting new technologies faster than we are updating security practices, therefore creating a growing gap between slowly developing security posture and rapidly evolving security threats.

In addition, the healthcare sector itself is evolving through the adoption of digital consumer wellness and fitness technologies, as well as the shift towards remote care models, accelerating consolidation of health systems and new disruptive healthcare business models, which were greatly accelerated by the COVID-19 pandemic and financial pressures. As a result of these drivers, healthcare now frequently occurs outside of hospitals and clinician offices. Telehealth, remote care, and home health are all driving the integration of healthcare technologies with, for example, patients' home networks, and require transmission of data across uncontrolled networks (home, public) and cloud services. Further, valuable data that can be derived from personal lifestyle devices (e.g., fitness trackers, smart watches) can now augment clinical data and decisions. Ensuring that a hospital or clinician's office is "cybersecure" alone is no longer sufficient; modern care delivery requires that all disparate pieces of the evolving healthcare ecosystem be considered, and appropriately secured as well.

This imperative is addressed through both cybersecurity regulation and policy, and voluntary practices implemented across the healthcare ecosystem. It is clear that, given the increasing number and techniques of cyber incidents inflicted on the health system, neither voluntary practices nor government policy have been sufficient to reduce cyber risk and incidents across the sector.

The Health Sector Coordinating Council Cybersecurity Working Group assesses that enhanced governmental programs and policy could offset the cost of existing cybersecurity regulatory requirements with a coordinated and coherent approach to the reduction of cybersecurity risk in the health sector. Particular attention should be paid to smaller health institutions that remain vulnerable targets but do not have the resources or expertise to comply with existing or proposed cybersecurity regulations, or to implement voluntary practices to shore up their cyber defenses, because of increasing financial, workforce and compliance costs associated with clinical priorities.

Accordingly, the HSCC herein offers suggestions and ideas for how government policy and programs might support the health sector's investment in and management of stronger cybersecurity risk reduction. These proposals are neither exhaustive nor rigid in their descriptions. Rather, by focusing more on the "what" than the "how", they are meant to stimulate discussion and creativity within government and with industry around possible initiatives the government can develop. Line numbers are included in the document for easy reference during discussions.

The following sections provide: 1) categorized options for government programs, incentives, and direct support for healthcare cybersecurity beyond regulatory mandate, and 2) a landscape reference of some foundational policy actions over recent years that are aimed specifically at, or implicate, healthcare cybersecurity.

About the Health Sector Coordinating Council

The Healthcare and Public Health Sector Coordinating Council (HSCC) is a coalition of private-sector critical healthcare infrastructure entities organized under the National Infrastructure Protection Plan to partner with and advise the government in the identification and mitigation of strategic threats and vulnerabilities facing the sector's ability to deliver services and assets to the public. The HSCC Cybersecurity Working Group (CWG) is the largest HSCC working group of more than 400 healthcare providers, pharmaceutical and medtech companies, payers and health IT entities partnering with government to identify and mitigate cyber threats to health data and research, systems, manufacturing and patient care. The CWG membership collaboratively develops and publishes freely-available healthcare cybersecurity best practices and policy recommendations, and produces outreach and communications programs emphasizing the imperative that cyber safety is patient safety.

Healthcare Cybersecurity Policy and Program Proposals for Government Consideration

The following compilation of policy and programmatic considerations are offered for HHS, CISA, Congress and other Federal agencies to support healthcare cybersecurity. If implemented under existing or new statutory authorities, these concepts could help reduce risk across the sector through incentive- or grant-based financial assistance and operational support, particularly to under-resourced health systems, including small practice, critical access, safety net and rural emergency hospitals.

The recommendations are grouped into the following topical categories, linked here to their location in the document: 1) [Preparedness Support and Information Sharing](#); 2) [Financial Support and Incentives](#); 3) [Incident Response and Recovery](#); 4) [Workforce](#); and 5) [Regulatory Reform](#).

The second section of this paper provides as foundational reference a brief overview of [recent policy developments](#) affecting healthcare cybersecurity management and compliance.

Preparedness Support and Information Sharing

- HHS should fund a national marketing and outreach campaign to the health provider community about the imperative of cyber security as a patient safety issue. This begins with a coherent website and communications strategy featuring the joint Health Sector Coordinating Council- 405(d) Program's Health Industry Cybersecurity Practices (HICP) as the primary recognized cybersecurity practices recommended by HHS and P.L. 116-321 for U.S. health providers. This includes the 405(d) Knowledge on Demand resources and other relevant joint HHS-HSCC cybersecurity publications, as well as resources developed by the Health-ISAC and HSCC as official critical infrastructure industry partners to the government.

- Consider applying the review and approval procedures of the HHS 405(d) program to additional joint publications by HHS and the HSCC Cybersecurity Working Group. As the 405(d) Program has a successful track record of partnership with HSCC, this model should continue with consideration of options for how it may be enhanced with continued industry-driven leadership.
- Boost funding for HHS Health Sector Cyber Coordination Center (HC3) to be a primary knowledge sharing and analysis resource within HHS to support healthcare cybersecurity in coordination with CISA. Congress should make HC3 an appropriated line item.
- Remove potential regulatory or legal barriers (eg., antitrust, Stark law, etc) to the formation of a health provider consortium that would develop and promote uniform minimum cybersecurity program requirements for any entity that sells hardware, software or services to a health system. This could be modeled on, for example, a FEDRAMP-type govt conduit to 3rd party cyber risk management requirements using a version of the HSCC Model Contract - <https://healthsectorcouncil.org/model-contract-language-for-medtech-cybersecurity-mc2>.
- Assign an office within HHS, (similar to a “Bureau of Census” for healthcare cybersecurity) in partnership with industry, to develop a program to measure cybersecurity performance in the health provider sector.
- For legislative consideration: In the reauthorization Pandemic and All Hazards Preparedness Act (PAHPA):
 - Designate high impact cyber and ransomware attacks, which result in the disruption and delay of health care delivery at one or more critical access, safety net and rural emergency hospitals, as “all hazards” incidents to activate FEMA and other government response support services;
 - Fund and provide support for the appropriate federal agencies to help hospitals and health systems enhance their emergency preparedness, response, resiliency and recovery capabilities related to cyberattacks (one of the recommendations included in the landmark report to Congress issued by the 2017 Health Care Industry Cybersecurity Task Force established under the Cybersecurity Act of 2015); and
 - Fund the appropriate federal agencies to provide emergency response for high impact cyberattacks targeting hospitals and health systems and provide human, technical and financial support to the victim organizations to minimize harm to public health and safety.
- HHS and CISA should coordinate with major cyber insurance carriers and their state regulatory agencies to encourage the reference of HICP into cyber insurance policy requirements, similar to the incentive codified in P.L. 116-321. This can include participation in the Health-ISAC or other information sharing and analysis organizations as one element of good practice that would improve premiums and coverage. Such a coordination process could build on the past DHS initiative of the Cyber Incident Data and Analysis Working Group (CIDAWG).
- Presently, cyber liability carriers have varying and inconsistent cybersecurity control requirements for determining premiums and coverage. Consistency in expectations for insurance will scale for providers’ investments in risk management programs.
- Protect health delivery organizations from class action lawsuits if they can demonstrate that they implement NIST CSF, HICP, or other recognized cybersecurity practices. This could incentivize more robust adoption and implementation of security controls.

- Continue development, outreach and provision of innovative CISA support programs, such as the Cyber Hygiene (CyHy) program, the Joint Cyber Defense Collaborative and table-top cyber exercises, that can be tailored, in close consultation with HHS, to healthcare entities.
- With respect to ongoing threat monitoring and analysis, timely and actionable government sharing of cyber threat and incident information is frequently inadequate for private sector needs. When developing threat and remediation advisories for the health sector, CISA, HHS and law enforcement should, as a matter of protocol under MOU, consult with designated industry sector leaders through Health-ISAC and HSCC with credible – and as appropriate, global - threat intelligence and analysis that can be compared and reconciled with government intelligence ahead of release of any advisories. This would ensure that both industry and government leaders are generally aligned before publication to the broader community about the accuracy of the intelligence, its relevance to and impact on the sector, and appropriate remediation procedures.
- Tailor a classified information sharing program involving health sector-designated liaison representatives, CISA, HC3, and law enforcement agencies, so that the liaison representatives can provide consideration and feedback to federal threat analysts on what is most relevant and actionable to the Sector.
- Consider incentives, support and protections for health systems working with government in various forms of proactive operational collaboration against threats and attacks, impending or in-process.

Financial Support and Incentives

- CMS reimbursement incentives: If an institution demonstrates implementation of HICP, the NIST CSF, or other recognized security practices as incentivized in P.L. 116-321 as mitigation for HIPAA-enforcement liability following a data breach, CMS similarly can offer additional reimbursement under a concept of “meaningful protection.” This could include additional CMS reimbursement to HDO’s participating in the Health-ISAC or other ISAO’s, implementation of active legacy medical technology cyber security management and replacement programs, and cybersecurity being included among performance goals overseen by hospital boards. Such incentive programs could be phased-in, measuring progress over time, alignment with HICP or other recognized security practices, and tying incentives to the cost/difficulty/scale of particular control frameworks and other cybersecurity investments in the clinical environment.
- HHS should establish needs-based grant, subsidy and incentive programs to help under-resourced health systems wanting to improve situational awareness by participating in the Health-ISAC or other information and sharing and analysis organizations.
- CISA and HHS should encourage state insurance regulatory agencies to work with insurance companies to tie reduced premiums and/or improved coverage for cyber insurance to participation in the Health-ISAC and other information sharing and analysis organizations as one element of an appropriate cybersecurity risk management program.
- HHS should provide funding support and/or technical assistance for critical access, safety net and rural emergency hospitals to remediate urgent vulnerabilities or mitigate threats. Many organizations struggle to take advantage of information made available via various channels including agencies, information sharing organizations, product vendors, etc. Local and regional FBI and CISA offices can enhance health sector outreach and communications channels to under-resourced health systems.

- Add specified cybersecurity tools and services as an allowable expense under the FCC Health Connect Fund subsidy of the Universal Service Administrative Company (USAC). This would leverage the purchasing power of under-resourced systems to supplement the current and more narrow WAN/Core Network investment expense.
- HHS should compile a reference of federal subsidies and grants across the government that fund cybersecurity services, tools, and education for health providers.

Incident Response and Recovery

- When responding to an incident, timely and actionable government sharing of cyber threat and incident information is frequently inadequate for private sector needs. When developing threat and remediation advisories for the health sector, CISA, HHS and law enforcement should, as a matter of protocol under MOU, consult with designated industry sector leaders through Health-ISAC and HSCC with credible – and as appropriate, global - threat intelligence and analysis that can be compared and reconciled with government intelligence ahead of release of any advisories. This would ensure that both industry and government leaders are generally aligned before publication to the broader community about the accuracy of the intelligence, its relevance to and impact on the sector, and appropriate remediation procedures.
- CISA should clearly articulate and rapidly-deliver actionable intelligence when implementing its cyber incident reporting collection and analysis authorities under CIRCIA 2022.
- Implementation should include consideration of waivers from victim reporting requirements while the incident response is underway in the early stages of discovery and operational triage.
- Provide federal-sponsored incident response support for organizations that are experiencing security incidents and need assistance getting through and recovering from the breach.
- Fund a federally-sponsored cyber incident insurance modeled after FEMA to compensate for the retraction of private insurance carriers from the cyber insurance market.
- Expand innovative law enforcement disruption initiatives against threat groups (e.g., botnet takedowns) to reduce ecosystem risk creating the most harm to hospitals.
- Incident reporting timeframes and methodologies should be standardized across government regulatory entities - e.g., CISA, SEC, OCR, etc. Health systems are burdened with multiple differing report forms and overlapping agency requirements for the same incident.
- The same civil, regulatory, FOIA and anti-trust protections provided under CISA 2015 for cyber threat information sharing with the federal government should be provided for: 1) victim organizations that have implemented recognized cybersecurity practices, as defined under PL 116-321 and 2) discussions with government to determine impact of attack on public health and safety. This in effect is a “safe harbor” incentive: if you report and you’re following NIST CSF/HICP then you’re “safe”
- Provide Military, State, or National Guard cyber/medical personnel, equipment and services support for providers meeting specific need thresholds after an attack (incident response and recovery), with appropriate reimbursement from HHS/CISA.
- HHS, CISA, and FBI should consider negotiating a pre-approved template for “request for technical assistance” from a health system struggling to respond to and remediate the effects of a cyber attack, such that the request can be processed quickly across the interagency to provide timely assistance to the victim

organization. This would be modeled after a similar RTA negotiated between the financial sector and the government.

Workforce

- HHS can administer a healthcare cybersecurity workforce development and cyber training program with assistance from NIST, CISA, and/or Veterans Administration. A program could include access to free cyber training, assistance to providers under an expanded Regional Extension Centers program, and student loan forgiveness programs modeled after physician loan forgiveness programs, or the National Science Foundation's CyberCorps(R) Scholarship for Service (SFS) program. This program provides a full scholarship plus stipend for undergraduate and master's degrees in cybersecurity and requires two years of government service.
- Consider authorizing a funded, subsidized "civilian cyber health corp". This could take the form of loan forgiveness; i.e., a Federal program pays / helps pay for a cyber education in exchange for a minimum number of years served, modeled after a uniformed health corp - see: <https://www.usphs.gov/> and <https://www.hhs.gov/surgeongeneral/corps/index.html>. Also suggest establishing career pathways that do not require full 4 years of college (i.e. certificate programs and associates).
- In addition to funding Electronic Health Record investment, the HITECH Act under the American Recovery and Reinvestment Act of 2009 funded workforce programs. See: <https://www.healthit.gov/data/quickstats/hitech-workforce-development-programs>, and possibly look at these as examples for short-term training programs.
- Consider mapping the NICE Framework's Work Roles and Job Descriptions to HICP to bring better and clarity and uniformity to matching skills with job descriptions - <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf>.

Regulatory Reform

- As recommended in the 2017 Health Care Industry Cybersecurity Task Force report, HHS should work across the regulatory OpDivs (OCR, ONC, CMS, FDA) and other other cyber- and data-regulating government entities involving cyber and privacy (FTC, SEC, etc) to cross-map and harmonize regulatory requirements on health systems that duplicate or conflict. A holistic, coherent cyber policy strategy is essential for a healthcare environment where clinical operations, medical devices, electronic health record technology, patient data, and IT systems are all interconnected but subject to differing regulatory structures and authorities.
- Enhance CMS Fraud protection programs to reduce the value and thus demand of stolen ePHI and other data, and thus attempts at cyber exploitation.

Policy Foundation and Current Developments

The following partial list of legislative, regulatory or executive actions taken over the past 2-3 years illustrates the range of potential policy shifts that healthcare organizations may consider as part of their cyber and enterprise risk management strategies. Likewise, this overview may stimulate discussion between industry and government partners about how to synthesize disparate initiatives into a coherent national critical infrastructure protection strategy.

- **Omnibus Appropriations Act Section 3305**, p. 1374 (December 2022): requires medical device manufacturers to ensure that their devices meet select minimum cybersecurity requirements, supported by device manufacturers and health delivery organizations;
- **National Cybersecurity Strategy, The White House** (March 2023): with an emphasis on protection of and minimum controls for critical infrastructure industries
- Policy options paper **“Cybersecurity is Patient Safety”** released by Senator Mark Warner (D-VA) (November 2022)
- **Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)** (March 2022): Require (p. 127) critical infrastructure owners and operators to report to the Cybersecurity and Infrastructure Security Agency within 72 hours of a substantial cyberattack or within 24 hours of a ransomware payment. Rulemaking process will take up to 3.5 years.
- **S. 3904 Healthcare Cybersecurity Act of 2022** (March 2022): - proposes closer collaboration between the Department of Health and Human Services and the Cybersecurity and Infrastructure Security Agency, with the goal of strengthening cybersecurity in the health and public health sectors.
- **Securities and Exchange Commission proposed rules** (March 2022) aimed at bolstering the cybersecurity-related disclosures of regulated public companies that would require covered public companies to, among other things:
 - Report material cybersecurity incidents on Form 8-K within four business days of a materiality determination.
 - Routinely update investors on such incidents in quarterly and annual reports.
 - Analyze whether individually immaterial cybersecurity incidents are material in the aggregate and report those in quarterly and annual reports.
 - Make periodic disclosures regarding the company’s cyber-related risk management policies and procedures.
 - Periodically disclose cyber-related governance information, including the board’s oversight and management’s implementation of cyber-related risk management policies and procedures.
 - Make periodic disclosures regarding board-level expertise in cybersecurity.
- **Federal Trade Commission policy statement** (September 2021) directing health apps and connected device companies to comply with the Health Breach Notification Rule. Under the Rule’s requirements, vendors of personal health records (“PHR”) and PHR-related entities must notify U.S. consumers and the FTC, and, in some cases, the media, if there has been a breach of unsecured identifiable health information or face civil penalties for violations. The Rule also covers service providers to these entities.

- **Class action lawsuits** (June 2021) against Scripps Health in State and Fed Courts re ransomware effect on violation of California Confidentiality of Medical Information Act, Federal Trade Commission unfair trade practice regulations and the HIPAA privacy and security rules.
- **Government Accountability Office report** (June 2021) on the need for enhanced HHS Industry Partnership responsibilities.
- **HHS OIG Report** on Lack of CMS Cybersecurity Oversight of Networked Medical Devices in Hospitals (June 2021).
- **Executive 14028 Order on Improving the Nation’s Cybersecurity** (May 2021): Section 4 encompasses medical technology security by specifying procurement requirements for Software Bills of Materials and agency guidance on purchasing systems with software defined as “critical software” for purposes of ensuring appropriate security before purchasing or deploying.
- **P.L. 116-321 (HR 7898) HITECH Act Amendment** (January 2021) requires OCR to consider mitigating fines and audit during a data breach enforcement if it determines that a breached entity has implemented recognized cybersecurity practices, such as NIST CSF and 405(d) Health Industry Cybersecurity Practices over the previous year.
- **FY ’21 NDAA Section 9002** (p. 3383), January 1, 2021– which codified Sector-Specific Agencies (SSAs), previously defined in Presidential Policy Directive 21 (PPD-21), as Sector Risk Management Agencies (SRMAs), and defined how DHS and SRMAs should work with each other to protect critical infrastructure.
- **Cybersecurity Act of 2015** (pp. 104-108): §405c directed HHS to establish the Health Care Industry Cybersecurity Task Force and §405d directed HHS to convene an industry partnership program that eventually joined the HSCC Cybersecurity Working Group and produced the Health Industry Cybersecurity Practices.

##



Health Sector Coordinating Council Cybersecurity Working Group



**Monitor
Threats**



**Manage
Risks**



**Respond &
Recover**



**Measure
Effectiveness**

Health Industry Cybersecurity – Strategic Plan (2024–2029)



FEBRUARY 2024

Table of Contents

I. Background on the Health Industry Cybersecurity Strategic Plan	3
A. Why the need for an industry Strategic Plan?	3
B. About the Health Sector Coordinating Council	6
C. How the Health Industry Cybersecurity Strategic Plan Was Developed	7
II. What will Industry cyber resilience Targeted Future State look like?	8
III. Principles and Structures of the Strategic Plan	8
IV. Industry Trends (T) Impacting Cybersecurity	9
V. Cybersecurity Goals (G) based on Industry Trends	15
VI. Objectives (O) and Measurable Outcomes	19
VII. Mobilizing the Strategic Plan	28
A. Appendix A Development of the Health Industry Cybersecurity Strategic Plan	29
B. Appendix B Context on Goals	32
C. Appendix C Call to Action: Public-Private Partnership Mobilization (I)	35
D. Appendix D Goals to Objectives Mapping	37
E. Appendix E Acknowledgements	42

I. Background on the Health Industry Cybersecurity Strategic Plan

A. Why the need for an industry Strategic Plan?

Cyber threats to the healthcare sector are a well-documented reality of modern healthcare delivery. Unrelenting cyber-attacks impact all subsectors of health industry, including direct patient care, medical technology and devices, pharmaceuticals and labs, plans and payers, health IT, and public health. These attacks, occurring because of increasingly connected and remote use of digital health technology, widely distributed portability of health data, and shortages of qualified healthcare cybersecurity professionals, among other factors, present significant risks to patient safety, clinical operations, manufacturing operations, research & development (R&D), public health organizations, and other business operations.

Ransomware attacks against hospitals, clinics, service providers, and other healthcare delivery organizations (HDOs) deny access to patient records, billing systems, and other digital technologies deployed throughout modern healthcare environments. Vulnerabilities discovered in the digital infrastructure relied upon by modern HDOs to deliver quality care pose patient safety and privacy risks that include delay or denial of treatment, data loss, manipulation or corruption of necessary treatment, among other potential risks. The sprawling and increased complexity of today's connected healthcare ecosystem gives rise to its own risks of: i) unanticipated and poorly understood interdependencies; ii) unknown inherited security weaknesses; iii) overreliance on vendor solutions; iv) systems that fail to adequately account for human factors related to cybersecurity controls; and v) inconsistencies between software and equipment lifecycles, among others. More recently, attacks against public health organizations have interrupted disease surveillance and other vital public health processes that protect the health of populations. The fast pace of new technology adoption is creating a growing gap between slowly developing security posture and rapidly evolving security threats.

In addition, the health sector itself is evolving through the adoption of digital consumer wellness and fitness technologies, as well as the shift towards remote care models, consolidation of health systems, and new disruptive healthcare business models, which were greatly accelerated by the COVID-19 pandemic and financial pressures. As a result of these drivers,

healthcare now frequently occurs outside of hospitals and clinician offices. Telehealth, remote care, and home health are all driving the integration of healthcare technologies with, for example, patients' home networks and transmission of data across uncontrolled home and public networks and cloud services. Further, valuable data that can be derived from personal lifestyle devices such as fitness trackers and smart watches can now augment clinical data and support decisions. Ensuring that a hospital or clinician's office is "cybersecure" alone is no longer sufficient; modern care delivery requires that all disparate pieces of the evolving healthcare ecosystem be considered, and appropriately secured as well.

Cyber threats extend to the entire regulated and unregulated value chain in the healthcare ecosystem. Pharmaceutical and other life science companies must be concerned about protecting their intellectual property and research data from cyber theft. Medical device companies must pay close attention to product security and the vulnerability of network-connected operational technology on the factory floor. Public health institutions depend on accurate research and surveillance data to make informed predictions and decisions about emerging diseases. Payers not only maintain and transmit thousands of terabytes of information about patients, treatments, and insurance claims, but they are subject to extensive cybersecurity regulatory compliance obligations focused on liquidity and maintaining public confidence in the nation's financial services system.

The imperative of protecting the health sector is a shared responsibility across all interdependent subsectors of the ecosystem. This imperative – and associated recommendations for addressing cybersecurity challenges – is guided by the Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG), which is a government-recognized critical infrastructure sector council of more than 400 healthcare providers, pharmaceutical and med-tech companies, payers and health IT entities partnering with government to identify and mitigate cyber threats to health and research data, critical systems, manufacturing, patient care, and public health. The CWG membership collaboratively develops and publishes freely available healthcare cybersecurity best practices and policy recommendations and produces outreach and communication programs emphasizing the imperative that cyber safety is patient safety. See <https://HealthSectorCouncil.org>.

The HSCC CWG has over the past five-years developed a wide range of publicly available cyber toolkits and documented best practices useful to the healthcare and public health

sectors for meeting the cybersecurity challenge. Much of that work since 2018 has focused on addressing the many recommendations of a joint HHS-health sector cybersecurity task force report - "[Report On Improving Cybersecurity In The Health Care Industry](#)." The report determined that health sector cybersecurity was in "critical condition" and prescribed six major imperatives and 105 action items for the sector and government to address the growing threat. Those recommendations guided initiatives across the health sector and in government to strengthen its security and resiliency, and ultimately, patient safety.

Now, given emerging trends in an increasingly complex and distributed health system and the associated cybersecurity threats, the HSCC CWG has prepared a forward-looking five-year Health Industry Cybersecurity (HIC) - Strategic Plan (SP) that:

- Projects major clinical, business, policy and technology trends in the health sector over the next five-plus years;
- Assesses how those trends may present continued or emerging cybersecurity challenges to the health sector; and
- Recommends how the sector and government should prepare for those changes with broad cybersecurity principles and specific actions.

The result is a forward-looking and measurable HIC-SP that all healthcare, public health, and life science-related entities can implement to improve security and resiliency across the ecosystem.

The HSCC CWG, our government, and health sector partners are united in our call to action to coalesce around the principle that *cyber safety is patient safety* and make the appropriate investments in the people, processes, technology, and partnerships to strengthen the sector against – and weaken the effectiveness of – cyber threats. In 2017, cyber threats and attacks reached a critical point in their impact on the health sector, and five-years later the impact is greater than ever.

The intent of this document is to guide C-suite executives, information technology and security leaders, and other relevant stakeholders toward investment and implementation of strategic cybersecurity principles which, if adopted, will measurably reduce risks to patient safety, data privacy, and care operations which can cause significant financial, legal, regulatory, and reputational impact. This strategic plan, as applied to public health organizations at

the state, local, tribal and territorial levels, can mitigate risk, protect the nation's public health infrastructure and safeguard the interoperable movement of essential data that ensures the public health of entire populations.

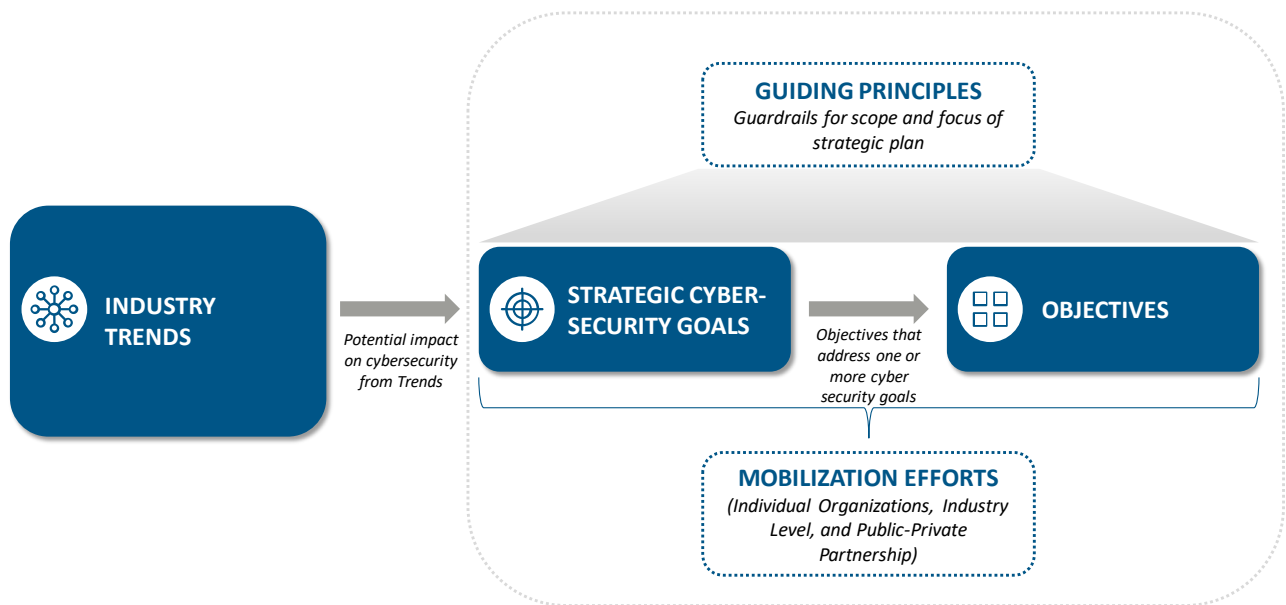
To facilitate sector-wide achievement of this strategic plan, the HSCC membership and our government partners will collaborate year after year to raise awareness of this imperative, through promulgation of sound practices, workshops and exercises, webinars and conferences, positive policy incentives, and other support.

B. About the Health Sector Coordinating Council

The Healthcare and Public Health Sector Coordinating Council (HSCC) is a coalition of private-sector critical healthcare infrastructure entities organized under the National Infrastructure Protection Plan to partner with and advise the government in the identification and mitigation of strategic threats and vulnerabilities facing the sector's ability to deliver services and assets to the public. At the time of the publication of this strategic plan in February 2024, the [HSCC Cybersecurity Working Group \(CWG\)](#) is composed of more than 400 healthcare providers, pharmaceutical and medtech companies, payers and health IT entities partnering with government to identify and mitigate cyber threats to health data and research, systems, manufacturing and patient care. The CWG membership collaboratively develops and publishes freely available healthcare cybersecurity best practices and policy recommendations and produces outreach and communications programs emphasizing the imperative that cyber safety is patient safety.

C. How the Health Industry Cybersecurity Strategic Plan Was Developed

The Health Industry Cybersecurity Strategic Plan (HIC-SP) is the result of extensive and multiple consultations among at least 175 industry and government organizations across the spectrum represented by senior cybersecurity and clinical executives and subject matter experts over a period of over 20 months. See illustration below on high-level process, as well as more details in [Appendix A](#).



II. What will Industry cyber resilience Targeted Future State look like?

While specific goals, objectives, and potential actions are in the latter section of this plan, the following represent the future state of healthcare cybersecurity in 2029:

- Healthcare cybersecurity – both practiced and regulated – is reflexive, evolving, accessible, documented and implemented for practitioners and patients.
- Secure design and implementation of technology and services across the healthcare ecosystem is a shared and collaborative responsibility.
- The healthcare C-Suite embraces accountability for cybersecurity as enterprise risk and a technology imperative.
- A Cyber Safety Net in the form of financial, policy and technical assistance ensures cyber equity across the ecosystem.
- Workforce cybersecurity learning and application is an infrastructure wellness continuum.
- A “911 Cyber Civil Defense” capability ensures that early warning, incident response and recovery are reflexive, collaborative, and always on.

III. Principles and Structures of the Strategic Plan

Guiding Principles

The following operational and governance principles guided the development of the strategic plan:

- **Cyber Safety is Patient Safety** - Patient safety is core, and cybersecurity is a critical element to enable patient safety;
- **Shared Responsibility** - Cybersecurity objectives involve all interdependent healthcare and public health subsectors. Every organization should be able to “see themselves” and what actions they can take or influence to achieve one or more objectives of the strategic plan;
- **Symbiotic Security and Interoperability** - Protection of sensitive data, trademarks, and intellectual property is symbiotic with the promotion of data sharing and interoperability to enable informed care delivery;

- **Mutually-enabling Privacy and Security** – Cybersecurity supports data privacy and privacy requirements integrate with cybersecurity objectives;
- **Cybersecurity Business Enabler** – Cybersecurity requirements should foster innovation and evolving healthcare business needs;
- **U.S-Framework Globally Adaptable** – Cybersecurity strategic objectives should focus first on the U.S. healthcare and public health ecosystem and be adaptable to global healthcare cybersecurity and resilience imperatives; and
- **Culture of Cybersecurity** - Cybersecurity goals constitute a lifetime wellness plan that should not be limited by tactical constraints of habit or myopia.

Structure

The **Table** below provides a legend for definition of terms used in this section of the document:

Table 1: Definitions

Section	Ref ID	Definition
Key Industry Trends	T	Business/industry macro-level trends that currently are or will continue to impact the health sector through 2029 and beyond
Cybersecurity Goals	G	Vision statements focused on addressing what the cybersecurity-enabled future in the health sector end state will look like by 2029
Objectives	O	The cybersecurity functions that will enable the achievement of the cybersecurity goals
Measurable Outcomes	M	How progress towards achieving the objectives can be measured or an outcome that will help support it

IV. Industry Trends (T) Impacting Cybersecurity

The first step in developing the strategy was to identify business, technology, clinical, and policy trends that will affect most of the health sector over the next five years and beyond. Many significant sector trends emerged during facilitated deliberations among a broad cross-section of cybersecurity and technology leaders across the HSCC membership in November 2022, and April and July 2023. The intent of this trends analysis, as compiled in **Table 2** below, was to identify what cybersecurity challenges could be presented by one or more of the trends and consider the types of cybersecurity investments and programs that should scale

across the sector. Additional consideration was given to concerns about cybersecurity as a health equity issue for small, rural, critical access hospitals, Federally Qualified Health Centers, and healthcare delivery organizations that support underprivileged population areas that are “target-rich, cyber-poor” and need focused support from government and community efforts.

Table 2: Industry Trends

ID	Key Industry Trends (Current & Future)	Description
T1	Methods of care delivery will continue to shift and evolve	<p>The health delivery sector is seeing a rapid rise in implementation and use of technologies to enable the practice of delivering healthcare services and consultations remotely, such as:</p> <ul style="list-style-type: none"> • Ongoing chronic care • Hospital at home care • Consumer-Driven <ul style="list-style-type: none"> ○ Wellness care (consumer drives the need / desire of care) ○ Direct to consumer lab tests, and ○ Software as a medical device at home <p>The level and sophistication of remote care will continue to evolve beyond current telemedicine and consultation type care. An upward trend is being seen in remote and home-based care, more telehealth technologies for an individual, and more data sources (pull and push) to leverage in care coordination. Due to cost pressures and changing consumer needs, there will be more transformations in the delivery of care outside of traditional physical locations such as hospitals and clinics.</p> <p>A change in the model of healthcare delivery will be enabled by software and hardware consumer devices and services. Non-traditional healthcare providers like large technology companies will reach consumers directly with diagnostics, analytics, educational materials, and personal health records. This will enable the healthcare consumer to overcome the limitations of traditional healthcare providers and put more power in the hands of the healthcare consumer to diagnose, understand, and manage their conditions. Novel and secure data sharing, privacy, and cybersecurity models will be needed to govern this new ecosystem.</p>
T2	Adoption of emerging and disruptive technologies will accelerate	<p>There is an increase in pace of innovation and accelerated adoption of emerging technologies to deliver wellness and care differently, drive operational efficiencies, gain deeper insights, and reduce costs. Specific categories of trends include:</p>

ID	Key Industry Trends (Current & Future)	Description
		<p>Data Analytics (Data Driven Insights / Decision Support):</p> <p>Collection and use of data continue to evolve and expand at a rapid pace within the healthcare ecosystem. The growth of data access and analytics is shifting us from a world of limited, contained and point-in-time data to robust, real-time data and continuous computing, allowing for earlier diagnostics and intervention. Data are being generated, stored and transmitted across devices such as wearable and implanted devices, Internet of Things (IoT) devices, and connected medical devices. Portable health data flows across organization boundaries to different health institutions, non-traditional healthcare organizations, and even across national borders. Post-COVID-19 public health surveillance is also driving the growth in volume/velocity of data collection, analysis, and interpretation to yield rapid actionable results.</p> <p>Accelerated Adoption of Artificial Intelligence:</p> <p>Artificial Intelligence (AI), including generative AI, is in the early stages of its use for improving business, medical diagnosis, and clinical outcomes across the health ecosystem. Examples include:</p> <ul style="list-style-type: none"> • Improved provider and clinician productivity and quality of care • Enhanced patient engagement • Streamlined patient access to care • Accelerated pharmaceutical research and development with reduced cost • Broader and deeper data insights that improve efficiency, cost savings, and improved decision-making capabilities • Enhanced patient outcomes <p>Adoption of Emerging Technologies:</p> <p>Health sector organizations looking for competitive advantage through improved operational efficiency and enhanced patient experiences are increasingly experimenting with emerging technologies such as Internet of Things (IoT), Robotics, Virtual and Augmented Reality, quantum computing and 3D bioprinting, among other unforeseen innovations.</p> <p>Novel Digital Biomarkers of Health and Disease:</p> <p>Novel use of digital assets like geolocation and environmental conditions (e.g., temperature and pollution) coupled with wearable sensors (accurate consumer physiologic and metabolic markers) will provide novel data streams to gain insights into how to prevent conditions, identify high risk groups, and provide individualized risk and mitigation strategies in an on-going, continuous model. In the same way that consumers</p>

ID	Key Industry Trends (Current & Future)	Description
		<p>are continuously notified of changes in their credit score, the consumer will have access to personalized information related to their dynamic health status and have visibility into how changes in behavior and environment can help manage risk.</p> <p>Digital Transformation:</p> <p>Digital transformation enables new care delivery models and process changes to meet the well-being needs of consumers. For example, health plans are undergoing digital transformation by “digitizing and cloudifying” environments to enhance their members’ engagement, simplify claims processing, and improve care coordination. In the med tech sector, digital transformation entails incorporating IoT devices, wearable sensors, and data analytics to enable remote patient monitoring, real-time data collection, and proactive intervention. Pharmaceutical companies are embracing digital transformation to enhance drug discovery, clinical trials, and patient engagement.</p> <p>In the realm of public health, the Centers for Disease Control and Prevention (CDC) has undertaken an important data modernization initiative to “get better, faster, actionable insights for decision-making at all levels of public health in response to COVID-19 pandemic.”</p> <p>Many organizations will continue to drive digital transformations to improve operational efficiency, enhance patient engagement, empower individuals to actively participate in their health, and drive better business outcomes.</p>
T3	The business of healthcare will continue to change and adapt	<p>The health sector is experiencing rapid change in business models, driven by:</p> <ul style="list-style-type: none"> • Acute cost pressures in sub-sectors like hospital systems; • Anticipated disruptions from new / non-traditional health sector entrants; • Advances in technologies; and • Evolving expectations of health consumers. <p>Organizations are adapting to this change by adopting new technologies, business practices, strategic partnerships, and exploring efficiencies through consolidations, continued mergers, acquisitions, and divestitures (MA&D) activities.</p>
T4	Acute Financial Distress will not abate	<p>Costs to care delivery continue to increase at an unsustainable level. While all subsectors are feeling cost pressures, healthcare delivery organizations are facing:</p>

ID	Key Industry Trends (Current & Future)	Description
		<ul style="list-style-type: none"> • Increasing operating costs such as inflation and labor shortages; • Impact of cybersecurity events such as ransomware and data breaches; • Continued downward pressure on hospital, physician practice, and smaller health delivery organization reimbursements; and • Push from “Fee for Service” to “Value-Based” contracts. <p>These factors in turn drive:</p> <ul style="list-style-type: none"> ○ Increased mergers, acquisitions, & divestitures (MA&D) and consolidation activities; ○ Focus on cost reduction; ○ Closures / reduced options for health services, especially in rural areas; and ○ Increase in out-of-data / out-of-support vulnerable technologies. <p>Similarly, other healthcare sub-sectors like medical device and pharmaceutical manufacturers respond to increasing operational costs and regulatory pressures by shifting some operations offshore.</p>
T5	Workforce recruitment and talent management will face competitive pressures from supply and demand pressures	<p>As experienced by other industries, talent (in terms of quantity and skillsets) is limited relative to global demand. This is due to rapidly evolving technological, operational, and business trends in the health sector, which are causing challenges in attracting, training, and retaining individuals with relevant skillsets. For example, healthcare delivery organizations are seeing a rising rate of nursing and physician shortages due to burnout from supporting patient care and increasing legal and regulatory responsibilities, which may increase cybersecurity risks due to lack of focus.</p> <p>In addition, while often being a necessary enterprise cost reduction strategy, increased reliance on outsourced services can dilute workforce unity and morale and add to third-party resource management costs and risk.</p> <p>The public health sector is facing workforce shortages that were exacerbated by the COVID-19 pandemic which could increase cyber risks to this health sector.</p>
T6	Governments will be challenged to develop coordinated and coherent policies for a rapidly evolving and	Health sector organizations face increased attention/pressure from State, Federal, and International regulatory bodies to address risks to patient safety, business resiliency, product security, and unregulated technology deployment and implementation (e.g., AI). An unpredictable regulatory landscape in an already complex patch work of regulatory

ID	Key Industry Trends (Current & Future)	Description
	complex health system	requirements within the United States and other countries is driving increased compliance costs and, in some cases, counterproductive results.
T7	Global instability, climate change and downstream effects will increase pressure on the healthcare supply chain	Global instability, climate change, and the associated potential for new emerging infectious diseases with pandemic potential will increase pressure on the health system. The US has the largest life sciences related research & development (R&D) capability in the world that provides a pipeline of products; however, global instability can impede protection of trade secrets and intellectual property. Risk to the global healthcare supply chain will also increase as geopolitical instability can impede access to critical healthcare raw materials and technologies. Finally, severe and catastrophic weather events resulting from climate change will impact care delivery and manufacturing (i.e., plan, source, make, deliver).

V. Cybersecurity Goals (G) based on Industry Trends

Based on the projected sector trends, specific cybersecurity goals are identified to address potential impact from sector trends. Please refer to [Appendix B](#) for additional context and clarification on the intent and scope of each cybersecurity goal. See [Appendix D](#) for mapping of Goals to Cybersecurity Objectives (O) that is covered later in this document in Section VI. The following [Table](#) maps the goals that address identified industry trends and aligns the mapping to the *targeted Future States* of healthcare cybersecurity in 2029.

Table 3: Cybersecurity Goals

Ref ID	Cybersecurity Goals What does this cybersecurity-enabled end state look like?	Industry Trends						
		Shifts in care delivery	Accelerated use of emerging technologies	Pace of Change	Acute Financial Distress	Managing Talent / Workforce	Evolving Regulatory Requirements	Global Instability and Climate Change
		T1	T2	T3	T4	T5	T6	T7
TARGET FUTURE STATES								
<ul style="list-style-type: none"> Healthcare cybersecurity - both practiced and regulated - is reflexive, evolving, accessible, documented and implemented for practitioners and patients Workforce cybersecurity learning and application is an infrastructure wellness continuum 								
G1	Healthcare and wellness delivery services are user-friendly, accessible, safe, secure, and compliant	✓	✓	✓	✓	✓	✓	
G2	Cybersecurity and privacy practices and responsibilities are understandable to healthcare technology consumers and practitioners	✓	✓			✓	✓	

Ref ID	Cybersecurity Goals What does this cybersecurity-enabled end state look like?	Industry Trends						
		Shifts in care delivery	Accelerated use of emerging technologies	Pace of Change	Acute Financial Distress	Managing Talent / Workforce	Evolving Regulatory Requirements	Global Instability and Climate Change
		T1	T2	T3	T4	T5	T6	T7
G3	Cybersecurity requirements are readily available, harmonized, understandable, and feasible for implementation across all relevant healthcare and public health subsectors		✓				✓	
TARGET FUTURE STATE								
Secure design and implementation of technology and services across the healthcare ecosystem is a shared and collaborative responsibility								
G4	Health, commercially sensitive research, and intellectual property data are reliable and accurate, protected, and private while supporting interoperability requirements	✓	✓				✓	
G5	Emerging technology is rapidly and routinely assessed for cybersecurity risk, and protected to ensure its safe, secure, and timely use	✓	✓	✓	✓			

Ref ID	Cybersecurity Goals What does this cybersecurity-enabled end state look like?	Industry Trends						
		Shifts in care delivery	Accelerated use of emerging technologies	Pace of Change	Acute Financial Distress	Managing Talent / Workforce	Evolving Regulatory Requirements	Global Instability and Climate Change
		T1	T2	T3	T4	T5	T6	T7
G6	Healthcare technology used inside and outside of the organizational boundaries is secure-by-design and secure-by-default while reducing the burden and cost on technology users to maintain an effective security posture	✓	✓	✓				
G7	A trusted healthcare delivery ecosystem is sustained with active partnership and representation between critical and significant technology partners and suppliers, including non-traditional health and life science entities	✓	✓			✓		✓
TARGET FUTURE STATE								
A Cyber Safety Net ensures cyber equity across the ecosystem								
G8	Foundational resources and capabilities are available to support cybersecurity needs across all healthcare stakeholders regardless of size, location, and financial standing	✓	✓		✓	✓	✓	

Ref ID	Cybersecurity Goals What does this cybersecurity-enabled end state look like?	Industry Trends						
		Shifts in care delivery	Accelerated use of emerging technologies	Pace of Change	Acute Financial Distress	Managing Talent / Workforce	Evolving Regulatory Requirements	Global Instability and Climate Change
		T1	T2	T3	T4	T5	T6	T7
TARGET FUTURE STATE								
A “911 Cyber Civil Defense” capability ensures that early warning, incident response and recovery are reflexive and always on								
G9	The health and public health sector has established and implemented preparedness response and resilience strategies to enable uninterrupted access to healthcare technology and services	✓		✓	✓			✓
TARGET FUTURE STATE								
The Healthcare C-Suite Embraces Accountability for Cybersecurity as Enterprise Risk and a Technology Imperative								
G10	Organizations across the health sector have strong cybersecurity and privacy cultures that permeate down from the highest levels within each organization	✓	✓	✓	✓	✓	✓	

VI. Objectives (O) and Measurable Outcomes

The following cybersecurity objectives and related sample measurable outcomes in **Table 4** below are intended to implement the proposed cybersecurity goals in Section **V** that address the identified healthcare trends. These objectives constitute a cybersecurity wellness plan for organizations individually and collectively to improve the security and resiliency of healthcare data, operations, and patient care. Each identified objective is applicable to one or more health sector stakeholders (described below), in terms of primary responsibility for leading or initiating certain activities to help address the objective:

- **Health Delivery:** Organizations directly involved in patient wellness and care – often referred to as healthcare providers, such as hospital systems and clinics.
- **Health Insurer:** Organizations that support the financing and payment of care – referred to as payors, such as health insurance companies and the federal Centers for Medicare and Medicaid Services (CMS).
- **Service Provider:** Organizations that provide any type of support to core health sector organizations like hospitals and insurance companies, such as outsourced claims processing, health information exchanges (HIEs), IT operations, payroll, SaaS solutions, etc.
- **Health Software / Device Manufacturer:** Technology and Life Science organizations that develop software, devices, diagnostics and therapeutics used by health systems and patients for wellness and care delivery, such as pharmaceutical, labs, and medical technology companies.
- **Industry Group:** Industry groups that represent and support one or more healthcare subsectors or specialties.
- **Government:** Various federal, state, local, tribal or territorial agencies that support the health sector and public health in their cybersecurity-related missions.

Table 4: Objectives and Measures

ID	Objectives	Applicable To?	Cybersecurity Goal Mapping	Sample Measurable Outcomes
O1	Develop, adopt and demand safety and resilience requirements for products and services offered, from business to business, as well as health systems to patients, with the concept of secure-by-design and secure-by-default	<input checked="" type="checkbox"/> Health Delivery <input checked="" type="checkbox"/> Health Insurer <input checked="" type="checkbox"/> Service Provider <input checked="" type="checkbox"/> Health Software / Device Manufacturer <input type="checkbox"/> Industry Group <input checked="" type="checkbox"/> Government	G2, G4, G5, G6	<ul style="list-style-type: none"> • Collaboration among product vendors for seamless end-to-end security integration • Products with validated security posture • Security as a standardized critical requirement by health sector organizations for products and services • Development and adoption of processes related to security communication (e.g., safety issue alerts to patients) • Development, knowledge, and use of security practices by common use case / reference architecture, including resilience (e.g., secure architecture design for medical device at home) • Development and use of monitoring processes to ensure the reliability and integrity of services and data in remote patient care, including health monitoring of connections to patient devices, regular backup testing, and disaster recovery tests • Utilization of the Health Industry Cybersecurity Practices (HICP) or the HHS HPH Cyber Performance Goals, or a standardized framework (without introducing a new framework), to assess an organization's resilience score. This score would

ID	Objectives	Applicable To?	Cybersecurity Goal Mapping	Sample Measurable Outcomes
				<p>gauge their capabilities in various aspects, including backup procedures, ransomware preparedness, incident response capabilities, business continuity, IT disaster recovery, and testing protocols</p>
<p>O2</p>	<p>Simplify access to resources and implementation approaches related to the adoption of controls and practices aligned with regulatory and sector standards for securing devices, services, and data</p>	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Health Delivery <input checked="" type="checkbox"/> Health Insurer <input checked="" type="checkbox"/> Service Provider <input checked="" type="checkbox"/> Health Software / Device Manufacturer <input checked="" type="checkbox"/> Industry Group <input checked="" type="checkbox"/> Government 	<p>G1, G3, G4, G5, G6, G7, G8, G9</p>	<ul style="list-style-type: none"> • Development and use of standardized enterprise and product security practices for consumers, manufacturers, health delivery organizations, etc. • Collaboration among vendor partners and industry peers to periodically communicate the top vulnerabilities • Existence of a centralized repository for security best practices and an analogous repository for patient-facing information. Also, an effective harmonization between these two repositories to promote development and use of standardized enterprise and product security practices, including Mergers, Acquisitions & Divestitures, data integrity, etc. • Development of clear privacy policies for patients • Development of a national healthcare cybersecurity implementation, software bill of materials (SBOM), and patient cyber-vulnerability database (Cyber Wikipedia) • Incorporation of simple quick training for patient when creating sign-on (through patient/member portal /

ID	Objectives	Applicable To?	Cybersecurity Goal Mapping	Sample Measurable Outcomes
				Electronic Health Record (EHR system)
O3	Develop and adopt practical and uniform privacy standards to protect personal information and promote fair and ethical data practices while sharing the data in a consensual ecosystem	<input type="checkbox"/> Health Delivery <input type="checkbox"/> Health Insurer <input type="checkbox"/> Service Provider <input type="checkbox"/> Health Software / Device Manufacturer <input checked="" type="checkbox"/> Industry Group <input checked="" type="checkbox"/> Government	G2, G3, G4, G10	<ul style="list-style-type: none"> Updated regulatory requirements related to privacy for consistent expectations to promote data sharing with appropriate guardrails Development of consistent legal / contractual requirements for data sharing Existence of educational initiatives or awareness campaigns to elucidate the methods and purposes of data collection and utilization
O4	Increase new partnerships with public/private entities on the front edge of evaluating and responding to emerging technology issues to enable safe, secure, and faster adoption of emerging technologies	<input checked="" type="checkbox"/> Health Delivery <input checked="" type="checkbox"/> Health Insurer <input checked="" type="checkbox"/> Service Provider <input checked="" type="checkbox"/> Health Software / Device Manufacturer <input checked="" type="checkbox"/> Industry Group <input checked="" type="checkbox"/> Government	G2, G4, G5, G6, G7, G9	<ul style="list-style-type: none"> Creation and use of collaboration and research forums for medical device manufacturers, health providers and information technology suppliers to understand emerging tech and how it is applied to healthcare Increased sector adoption of the National Institute of Standards and Technology (NIST) Artificial Intelligence (AI) Risk Management Framework to protect against adversarial AI manipulation and abuse Established standards and sector strategy for adoption of verifiable quantum-safe products Development and use of training programs focused on ensuring the safe and secure delivery of emerging technologies Active participation in cross-industry forums and watch groups conducted annually,

ID	Objectives	Applicable To?	Cybersecurity Goal Mapping	Sample Measurable Outcomes
				<p>inclusive of government entities and small/medium Healthcare Delivery Organizations (HDOs); these forums should facilitate the exchange of insights, best practices, and requirements between the healthcare and technology industries</p>
<p>O5</p>	<p>Enhance health sector senior leadership and board knowledge of cybersecurity and their accountability to create a culture of security within their organizations</p>	<p><input checked="" type="checkbox"/> Health Delivery</p> <p><input checked="" type="checkbox"/> Health Insurer</p> <p><input checked="" type="checkbox"/> Service Provider</p> <p><input checked="" type="checkbox"/> Health Software / Device Manufacturer</p> <p><input type="checkbox"/> Industry Group</p> <p><input type="checkbox"/> Government</p>	<p>G7, G8, G10</p>	<ul style="list-style-type: none"> • Development and use of training programs targeting select non-cyber groups. • Adoption of key performance indicators (KPIs) by business that include security • Develop, distribute, and measure use of educational materials targeting board accountability for security • Include cyber as part of enterprise risk management • Enhanced awareness of cyber risks among senior leadership and the board by making the threat personal and tangible, emphasizing the shift from considering "if" a cyber incident occurs to acknowledging "when" it may happen • Inclusion of cyber in job and board descriptions • Expansion of standard metrics beyond IT for effective decision making • NACD standard of practices for healthcare cybersecurity • Inclusion of cybersecurity in Enterprise Risk Management (ERM) frameworks

ID	Objectives	Applicable To?	Cybersecurity Goal Mapping	Sample Measurable Outcomes
O6	Increase utilization of cybersecurity practices / resources / capabilities by public health, physician practices and smaller health delivery organizations (e.g., rural health)	<input checked="" type="checkbox"/> Health Delivery <input type="checkbox"/> Health Insurer <input type="checkbox"/> Service Provider <input type="checkbox"/> Health Software / Device Manufacturer <input checked="" type="checkbox"/> Industry Group <input checked="" type="checkbox"/> Government	G8, G9	<ul style="list-style-type: none"> Existence of regulatory and legal “safe-harbor” to promote peer collaboration and partnerships for cybersecurity Existence of funding, positive incentives, technical assistance and other programs to support public health, physician practices and smaller health delivery organizations Government technology program to subsidize cybersecurity technology investments, bringing all hospitals, physician practices and smaller health delivery organizations to a minimum technology baseline Increase in the adoption of the Health Industry Cybersecurity Practices (HICP) and HHS HPH Cybersecurity Performance Goals (CPGs), specifically within rural health settings Implementation of training programs for office managers to enhance their oversight capabilities concerning IT subcontractors
O7	Increase incentives, development and promotion of health care cybersecurity-focused education and certification programs	<input checked="" type="checkbox"/> Health Delivery <input checked="" type="checkbox"/> Health Insurer <input checked="" type="checkbox"/> Service Provider <input checked="" type="checkbox"/> Health Software / Device Manufacturer <input checked="" type="checkbox"/> Industry Group <input checked="" type="checkbox"/> Government	G2, G8, G10	<ul style="list-style-type: none"> Increase in education certification and degree programs with healthcare and cyber focus Number of/increase in certified cybersecurity professionals in the healthcare workforce A healthcare Cyber Corps for student training into health service and a branch of civilian

ID	Objectives	Applicable To?	Cybersecurity Goal Mapping	Sample Measurable Outcomes
				<p data-bbox="1057 264 1419 331">mutual assistance for incident response</p> <ul data-bbox="1016 352 1435 1808" style="list-style-type: none"> <li data-bbox="1016 352 1435 604">• Government initiatives that will positively incentivize or subsidize cybersecurity training for physician practices and smaller health delivery organizations that support under-privileged communities <li data-bbox="1016 625 1435 730">• Peer-peer sharing of cybersecurity practices and other materials <li data-bbox="1016 751 1435 1035">• 90 percent of health providers are implementing HICP and HPH CPGs; CMS and private insurance incentive bonus reimbursement, and cyber insurance risk assessments for healthcare market are based on HICP controls <li data-bbox="1016 1056 1435 1234">• Marketing programs by broad and subsector-based industry groups promote 405(d) HICP, and relevant HSCC leading practices publications <li data-bbox="1016 1255 1435 1360">• Ability to use billing code for time spent on education by health providers <li data-bbox="1016 1381 1435 1444">• Addition of cyber course for medical oriented degrees <li data-bbox="1016 1465 1435 1612">• Health insurance payers and cyber insurance industry drive requirements for cyber proficiency <li data-bbox="1016 1633 1435 1808">• Leverage local workforce development boards (CHW - community health workers - State level and National Level) to drive education

ID	Objectives	Applicable To?	Cybersecurity Goal Mapping	Sample Measurable Outcomes
O8	Increase utilization of automation and emerging technologies like AI to drive efficiencies in cybersecurity processes	<input type="checkbox"/> Health Delivery <input type="checkbox"/> Health Insurer <input type="checkbox"/> Service Provider <input type="checkbox"/> Health Software / Device Manufacturer <input checked="" type="checkbox"/> Industry Group <input checked="" type="checkbox"/> Government	G5, G6, G8	<ul style="list-style-type: none"> Increased sharing of knowledgebase and use cases for automation to enrich the current talent pool Government technology initiatives that will positively incentivize or subsidize cybersecurity technology Government investments in use cases for AI to augment / enhance cyber resilience Development of risk-based best practices and periodic measurement of adoption of these practices to enhance risk management effectiveness
O9	Develop health sub-sector specific integrated cybersecurity profile aligned with regulatory requirements	<input checked="" type="checkbox"/> Health Delivery <input checked="" type="checkbox"/> Health Insurer <input checked="" type="checkbox"/> Service Provider <input checked="" type="checkbox"/> Health Software / Device Manufacturer <input checked="" type="checkbox"/> Industry Group <input checked="" type="checkbox"/> Government	G2, G3, G4, G8, G9	<ul style="list-style-type: none"> Development and adoption of key security practices in context of risk and sub-sector business requirements
O10	Develop meaningful cross-sector third-party risk management strategies for evaluating, monitoring, and responding to supply chain and third-party provider cybersecurity risks	<input checked="" type="checkbox"/> Health Delivery <input checked="" type="checkbox"/> Health Insurer <input checked="" type="checkbox"/> Service Provider <input checked="" type="checkbox"/> Health Software / Device Manufacturer <input checked="" type="checkbox"/> Industry Group <input checked="" type="checkbox"/> Government	G1, G2, G4, G7, G9	<ul style="list-style-type: none"> Development and communication of consistent approach for assessing third parties Sector level sharing of information and data on security posture of third parties based on consistent and adopted standards Existence of regulatory and legal “safe-harbor” to promote peer collaboration and partnerships for cybersecurity

ID	Objectives	Applicable To?	Cybersecurity Goal Mapping	Sample Measurable Outcomes
O11	Increase meaningful and timely information sharing of cyber related disruptions to improve sector readiness	<input checked="" type="checkbox"/> Health Delivery <input checked="" type="checkbox"/> Health Insurer <input checked="" type="checkbox"/> Service Provider <input checked="" type="checkbox"/> Health Software / Device Manufacturer <input checked="" type="checkbox"/> Industry Group <input checked="" type="checkbox"/> Government	G8, G9	<ul style="list-style-type: none"> Increased sharing of information related to cyber disruptions through centralized and formalized channels Protection and education of organizations about legal or regulatory consequences when sharing information Standard protocol (e.g., FHIR) for threat and vulnerability data Increased number of physician practices and smaller health sector delivery organizations participating in healthcare sector information sharing organizations ISAO-tracked and aggregated measures of membership/industry response and recovery times following cyber incidents.
O12	Develop mechanisms to enable “mutual aid” support across sector stakeholders to allow for timely and effective response to cybersecurity incidents	<input type="checkbox"/> Health Delivery <input type="checkbox"/> Health Insurer <input type="checkbox"/> Service Provider <input type="checkbox"/> Health Software / Device Manufacturer <input checked="" type="checkbox"/> Industry Group <input checked="" type="checkbox"/> Government	G8, G9	<ul style="list-style-type: none"> Reduction in regulatory or legal barriers (real or perceived), e.g., antitrust, Stark law, Anti-Kickback Statute (AKS), liability concerns, etc., to health sector peer support for cybersecurity incident response Indemnify organizations that donate cyber technology and other capabilities, and make this clear in AKS and Stark policies Availability of Federal funding such as from CMS and FEMA to reimburse expenses for any mutual support such as travel expenses, tool licenses, etc.

ID	Objectives	Applicable To?	Cybersecurity Goal Mapping	Sample Measurable Outcomes
				<ul style="list-style-type: none"> FEMA/mobile “tiger team” type on-site available rapid incident response support

VII. Mobilizing the Strategic Plan

Moving the needle on cyber industry resilience requires organizations to take action to achieve the identified goals and objectives. The sample measurable outcomes can be used as a starting point to think about specific actions and related success measures. Each organization is encouraged to use the objectives and think of implementation through three approaches explained in **Table 5** below:

Table 5: Mobilization Strategy

Individual Organization Action(s)	<ul style="list-style-type: none"> Identify objectives where specific actions can be taken by the organization on its own and may not be dependent on specific industry or government support. An example of that could be Objective 1 (Develop, adopt and demand safety and resilience requirements for products and services offered (i.e., from business to business, as well as health systems to patients) with the concept of secure-by-design and secure-by-default) for instance. Develop / update the organization’s cyber strategic plan using this industry level strategic plan as an input for its own objectives.
Active Industry Participation	<ul style="list-style-type: none"> Identify objectives and associated action(s) that require industry level collaboration where the organization will want to actively participate and contribute time/resource(s) to. This could be through HSCC as well as other industry groups.
Inform Government Policy	<ul style="list-style-type: none"> Identify any public-private partnership related strategies or tactics that the organization wants to pursue and influence. Some of these are listed below in Appendix C of this document.
Conduct an executive briefing of the strategic plan with relevant business executives for support on action(s) the organization may want to take based on the above suggested lens	

From a measurement standpoint, specific collaboration will be needed from the industry on “what and how” we measure with micro and macro level metrics for assessing progress against the strategic plan (i.e., measurement will be needed at both the individual organization as well as industry level).

Potential sample public-private partnership mobilization ideas that will need further collaboration have been included in [Appendix C](#).

A. Appendix A

Development of the Health Industry Cybersecurity Strategic Plan

The Health Industry Cybersecurity Strategic Plan (HIC-SP) is the result of extensive and multiple consultations among at least 175 industry and government organizations across the spectrum represented by senior cybersecurity and clinical executives and subject matter experts. The timeline below illustrates how the Council facilitated the vision and consensus among these industry leaders during regularly and specially scheduled sessions around the trends, goals and strategies that will shape healthcare cybersecurity policy and practice by 2029:

- Much of the development of the HIC-SP was conducted in partnership with the U.S. Department of Health and Human Services, the DHS Cybersecurity and Infrastructure Security Agency and other agencies under the auspices of the Critical Infrastructure Partnership Advisory Council (CIPAC) designation required for joint industry-government deliberation and planning for critical infrastructure protection. For more information, see the CISA CIPAC Charter.
- The strategic plan initiative involved extensive labor and time to convene industry leadership and facilitate, capture and draft input into consensus recommendations, which in turn required structured, professional capability that the HSCC funded through member donations. The leadership selected Deloitte & Touche from a number of bids to serve as our facilitator, with generous cross-sector donations from:
 - Abbott
 - Deloitte
 - HCA Healthcare
 - Health Care Service Corporation (HCSC)
 - Intermountain Health
 - Mayo Clinic
 - McKesson
 - Medtronic
 - Merck
 - Pfizer
 - Premera Blue Cross

- The Five-Year Plan Task Group kicked off at the April 2022 All-Hands membership meeting in Chicago. Initial brainstorming during that session helped shape the dialogue and process for the strategic plan, which would begin with an assessment throughout the Summer and Fall of how we have addressed the many recommendations in the 2017 Health Care Industry Cybersecurity (HCIC) Task Force report. The HCIC report served as our primary compass for our work over the past 5 years, and the assessment of our progress – what we have reasonably addressed and what remains a relevant challenge – informed the starting point for our strategic planning sessions.
- The November 2022 All-Hands membership meeting in Washington DC involved intensive subsector-based breakout sessions – Providers, Medical Device Manufacturers, Pharmaceuticals, Payers, Health IT and Digital Health – to project major trends in the health industry, the cybersecurity challenges posed by those trends and how those challenges should be addressed through technology, clinical, business and policy imperatives. The results of those breakout sessions laid the substantive foundation for structuring a forward-looking plan that is both measurable and achievable across the healthcare industry.
- At the All-Hands membership meeting in April 2023 in Minneapolis, breakout sessions further refined predictions and priorities.
- During July 11-12, 2023, a newly convened senior-level Strategic Plan Steering Committee of 40 health industry representatives, advisors and government officials met virtually to capture and prioritize inputs from the previous All-Hands sessions to forge consensus around projected trends and associated cybersecurity challenges and objectives.

Since the July Steering Committee meeting, the Five-Year Plan (5YP) Task Group Leads and writing team worked weekly to further refine the content, capturing as much input and consensus as possible from the Steering Committee and previous workshop sessions. This strategic plan represents that consensus.

B. Appendix B

Context on Goals

Table 6 below provides more context in terms of intent and scope on the cybersecurity goals (G) identified in Section V.

Table 6: Cybersecurity Goals Clarification

Cybersecurity Goals	Context / Clarifications
<p>G1 - Healthcare and wellness delivery services are user-friendly, accessible, safe, secure, and compliant</p>	<p>The intent of this objective is to make information security to patients and care givers (e.g., doctors, nurses, and medical assistants) easily understandable and simple to implement or configure in context of remote and wellness services (i.e., outside of traditional hospital and clinical setting – remote care). User friendly implies:</p> <ul style="list-style-type: none"> • Security integration works seamlessly across different products that may support remote health and wellness care, and • Interactions with security services (e.g., authentication process) is frictionless and not overly complicated
<p>G2 - Cybersecurity and privacy practices and responsibilities are understandable to healthcare technology consumers and practitioners</p>	<p>The intent of this objective is to make information security easily understandable and simple to implement or configure by the user, regardless of who has “developed or manufactured” the product, and where it is used. “User” could be clinical workers operating medical devices, patients accessing application(s) for remote health support, or information technology related staff responsible for configuring systems securely. While this objective is similar to objective G1, this objective is broader in scope in terms of who, as well as the types of devices and technology, it applies to.</p>
<p>G3 - Cybersecurity requirements are readily available, harmonized, understandable, and feasible for implementation across all relevant health and public health sub-sectors</p>	<p>The intent of this objective is to have integrated and harmonized security requirements by sub-sector, and perhaps by reference architecture (e.g., applicable security requirements for a certain category of medical device, Cloud Infrastructure, PHI Application, etc., and/or integrated security framework for Health Delivery Organization versus Health Plan versus MedTech).</p>

Cybersecurity Goals	Context / Clarifications
<p>G4 - Health, commercially sensitive research, and intellectual property data are reliable and accurate, protected, and private while supporting interoperability requirements</p>	<p>The intent of this objective is to accomplish the following:</p> <ul style="list-style-type: none"> Remove the ambiguity and complexity driven from the patchwork of Federal and State level privacy and data protection laws as well as other legal aspects to make sharing of health data easier while maintaining the necessary protection to foster collaboration, research and innovation, and deliver efficient and effective care. Support the necessary restrictions and protections of trade secrets, intellectual property, and other commercially sensitive research information.
<p>G5 - Emerging technology is rapidly and routinely assessed for cybersecurity risk, and protected to ensure its safe, secure, and timely use</p>	<p>The intent of this objective is to enable the business to quickly adopt emerging technologies while managing cybersecurity risks. The objective is to have processes or capabilities to quickly analyze and understand risks and identify control strategies or requirements to mitigate risks of emerging technologies in an agile manner.</p>
<p>G6 - Healthcare technology used inside and outside of the organizational boundaries is secure-by-design, and secure-by-default while reducing the burden and cost on technology users to maintain an effective security posture.</p>	<p>The intent of this objective is to establish requirements and accountability of product developers for “secure by-design” products.</p>
<p>G7 - A trusted healthcare delivery ecosystem is sustained with active partnership and representation between critical and significant technology partners and suppliers (including non-traditional health and life science entities)</p>	<p>The intent of this objective is to foster proactive collaboration market-leading technology vendors and other non-traditional health organizations / vendors that are serving healthcare organizations and/or developing healthcare products for sector security.</p>
<p>G8 - Foundational resources and capabilities are available to support cybersecurity needs across all healthcare stakeholders regardless of size, location, and financial standing</p>	<p>Foundational resources can be considered minimum baseline requirements that organizations must deploy to enable reasonable commercially viable security. Resources include people, process, and technologies. The intent of this objectives to make available foundational tools for all health sector organizations, including those organizations that are resource constrained.</p>

Cybersecurity Goals	Context / Clarifications
<p>G9 - The health and public health sector has established and implemented response and resilience strategies to enable uninterrupted access to healthcare technology and services</p>	<p>The intent of this objective is to look at resilience holistically for sustaining critical business and patient care operations and its safety. This includes:</p> <ul style="list-style-type: none"> • Traditional business continuity and recovery capabilities • Supply chain security (e.g., service providers) • Skillsets and financial resources • Relevant and meaningful intelligence, vulnerability and incident data in easy to consume manner
<p>G10 – Organizations across the health and public health sector have strong cybersecurity and privacy cultures that permeate down from the highest levels within each organization</p>	<p>The intent of this objective is to drive cybersecurity and privacy awareness and appreciation outside of the traditional approach of “one-size fits all” cybersecurity awareness. This includes at the leadership and board level as well as business and clinical staff.</p>

C. Appendix C

Call to Action: Public-Private Partnership Mobilization (I)

One of the guiding principles of this Strategic Plan is that cybersecurity responsibility in the health sector is a *shared responsibility*. In that spirit, if the industry is to achieve the ambitious goals and objectives that will deliver us to the Targeted Future State that we envision, it will take the collective and collaborative efforts of all private sector and government stakeholders. This means not just investing in, demanding, implementing, and incentivizing the many cybersecurity practices in this wellness plan. It also means actively promoting and advocating the enablers of “*Cyber Safety is Patient*” across the ecosystem in a sustained and proactive national campaign that draws on successes of similar efforts by the U.S. Department of Homeland Security (“If you see something say something”) and the annual National Cyber Security Awareness Month. **Table 7** below offers a variety of policy, operational, public awareness, and coalition actions that can help cultivate a culture of cybersecurity and upgrade our national healthcare cybersecurity condition from “critical” as diagnosed in 2017 to “stable” in 2029.

Table 7: Public-Private Partnership Mobilization Examples

Ref ID	Public-Private Partnership (P ³) Initiative Examples
I1	Collaborate with sector peers and healthcare domain experts to develop sector-aligned cybersecurity guidelines for emerging technologies and other practices
I2	Create guidelines and frameworks for healthcare providers and technology vendors for developing and implementing secure solutions, including compatibility
I3	Collaborate with sector and subsector peers to support resource sharing models (e.g., operating model, cost structure)
I4	Collaborate with sector and subsector peers and healthcare domain experts to develop and share practices related to automation and proactive risk insights
I5	Influence collaboration mechanisms among various agencies and private organizations for the sharing and timely dissemination of vulnerabilities, threats, and controls related to emerging technologies
I6	Promote inter-government collaboration to increase consistent security and privacy practices
I7	Health sector and government stakeholders collaborate to design and administer recurring national surveys to measure trends in health sector cybersecurity performance

Ref ID	Public-Private Partnership (P ³) Initiative Examples
I18	Develop and share a concise educational resource on essential security measures with key stakeholders.
I19	Influence regulatory bodies for policies that incentivize product vendors to implement “security and privacy-by-design” protocols in product development lifecycles
I10	Collaborate with sector legal peers and regulators to identify and address any impediments for sharing of resources; Influence legal / regulatory mechanisms to foster collaboration and sharing of cyber knowledge and resources
I11	Establish open communication and collaboration with regulatory agencies to gain insights into upcoming changes and participate in the development of regulations that consider the sector’s challenges
I12	Influence regulatory bodies for clear and practical privacy requirements that don’t impede collaboration for seamless product integration in a multi-party environment
I13	Identify government investment programs that will incentivize the cyber healthcare workforce pipeline
I14	Influence and enact policies to fund cybersecurity capabilities and replacement of obsolete technology in smaller health delivery systems
I15	Influence hospital accreditation organizations to enhance review of hospital cybersecurity administrative and technical controls
I16	Promote education and awareness of applying risk-based, automation, and other efficient methodology in cybersecurity practices
I17	Influence collaboration mechanisms among various private organizations, such as EMR user groups for education about cybersecurity imperatives
I18	Collaborate with sector peers and select higher education centers for updating / creating additional educational focus paths
I19	Develop approach to educate patients / non-tech individuals on basic cybersecurity considerations when leveraging remote care and wellness options
I20	Explore options to develop more user friendly and clear privacy policies for remote patients
I21	Establish a cross-sector council of C-Suite business leaders to provide strategic insights, guidance, and support for cybersecurity efforts across the healthcare sector

D. Appendix D

Goals to Objectives Mapping

Table 8: Goals to Objectives Mapping

Ref ID Cybersecurity Goals What does this cybersecurity-enabled end state look like?	Objective(s) that address the Goal
G1 Healthcare and wellness delivery services are user-friendly, accessible, safe, secure, and compliant	<ul style="list-style-type: none"> • O2. Simplify access to resources and implementation approaches related to the adoption of controls and practices aligned with regulatory and sector standards for securing devices, services, and data • O10. Develop meaningful cross-sector third-party risk management strategies for evaluating, monitoring, and responding to supply chain and third-party provider cybersecurity risks
G2 Cybersecurity and privacy practices and responsibilities are understandable to healthcare technology consumers and practitioners	<ul style="list-style-type: none"> • O1. Develop, adopt and demand safety and resilience requirements for products and services offered (i.e., from business to business, as well as health systems to patients) with the concept of secure-by-design and secure-by-default • O3. Develop and adopt practical and uniform privacy standards to protect personal information and promote fair and ethical data practices while sharing the data in a consensual eco-system • O4. Increase new partnerships with public/private entities on the front edge of evaluating and responding to emerging technology issues to enable safe, secure, and faster adoption of emerging technologies • O7. Increase incentives, development and promotion of health care cybersecurity-focused education and certification programs • O9. Develop health sub-sector specific integrated cybersecurity profile aligned with regulatory requirements • O10. Develop meaningful cross-sector third-party risk management strategies for evaluating, monitoring, and responding to supply chain and third-party provider cybersecurity risks

RefID Cybersecurity Goals What does this cybersecurity-enabled end state look like?	Objective(s) that address the Goal
G3 Cybersecurity requirements are readily available, harmonized, understandable, and feasible for implementation across all relevant healthcare and public health sub-sectors	<ul style="list-style-type: none"> • O2. Simplify access to resources and implementation approaches related to the adoption of controls and practices aligned with regulatory and sector standards for securing devices, services, and data • O3. Develop and adopt practical and uniform privacy standards to protect personal information and promote fair and ethical data practices while sharing the data in a consensual eco-system • O9. Develop health sub-sector specific integrated cybersecurity profile aligned with regulatory requirements
G4 Health, commercially sensitive research, and intellectual property data are reliable and accurate, protected, and private while supporting interoperability requirements	<ul style="list-style-type: none"> • O1. Develop, adopt and demand safety and resilience requirements for products and services offered (i.e., from business to business, as well as health systems to patients) with the concept of secure-by-design and secure-by-default • O2. Simplify access to resources and implementation approaches related to the adoption of controls and practices aligned with regulatory and sector standards for securing devices, services, and data • O3. Develop and adopt practical and uniform privacy standards to protect personal information and promote fair and ethical data practices while sharing the data in a consensual eco-system • O4. Increase new partnerships with public/private entities on the front edge of evaluating and responding to emerging technology issues to enable safe, secure, and faster adoption of emerging technologies • O9. Develop health sub-sector specific integrated cybersecurity profile aligned with regulatory requirements • O10. Develop meaningful cross-sector third-party risk management strategies for evaluating, monitoring, and responding to supply chain and third-party provider cybersecurity risks

RefID Cybersecurity Goals What does this cybersecurity-enabled end state look like?	Objective(s) that address the Goal
G5 Emerging technology is rapidly and routinely assessed for cybersecurity risk, and protected to ensure its safe, secure, and timely use	<ul style="list-style-type: none"> • O1. Develop, adopt and demand safety and resilience requirements for products and services offered (i.e., from business to business, as well as health systems to patients) with the concept of secure-by-design and secure-by-default • O2. Simplify access to resources and implementation approaches related to the adoption of controls and practices aligned with regulatory and sector standards for securing devices, services, and data • O4. Increase new partnerships with public/private entities on the front edge of evaluating and responding to emerging technology issues to enable safe, secure, and faster adoption of emerging technologies • O8. Increase utilization of automation and emerging technologies like AI to drive efficiencies in cybersecurity processes
G6 Healthcare technology used inside and outside of the organizational boundaries is secure-by-design and secure-by-default while reducing the burden and cost on technology users to maintain an effective security posture	<ul style="list-style-type: none"> • O1. Develop, adopt and demand safety and resilience requirements for products and services offered (i.e., from business to business, as well as health systems to patients) with the concept of secure-by-design and secure-by-default • O2. Simplify access to resources and implementation approaches related to the adoption of controls and practices aligned with regulatory and sector standards for securing devices, services, and data • O4. Increase new partnerships with public/private entities on the front edge of evaluating and responding to emerging technology issues to enable safe, secure, and faster adoption of emerging technologies • O8. Increase utilization of automation and emerging technologies like AI to drive efficiencies in cybersecurity processes

RefID Cybersecurity Goals What does this cybersecurity-enabled end state look like?	Objective(s) that address the Goal
G7 A trusted healthcare delivery ecosystem is sustained with active partnership and representation between critical and significant technology partners and suppliers, including non-traditional health and life science entities	<ul style="list-style-type: none"> • O2. Simplify access to resources and implementation approaches related to the adoption of controls and practices aligned with regulatory and sector standards for securing devices, services, and data • O4. Increase new partnerships with public/private entities on the front edge of evaluating and responding to emerging technology issues to enable safe, secure, and faster adoption of emerging technologies • O5. Enhance health sector senior leadership and board knowledge of cybersecurity and their accountability to create a culture of security within their organizations • O10. Develop meaningful cross-sector third-party risk management strategies for evaluating, monitoring, and responding to supply chain and third-party provider cybersecurity risks
G8 Foundational resources and capabilities are available to support cybersecurity needs across all healthcare stakeholders regardless of size, location, and financial standing	<ul style="list-style-type: none"> • O2. Simplify access to resources and implementation approaches related to the adoption of controls and practices aligned with regulatory and sector standards for securing devices, services, and data • O5. Enhance health sector senior leadership and board knowledge of cybersecurity and their accountability to create a culture of security within their organizations • O6. Increase utilization of cybersecurity practices / resources / capabilities by public health, physician practices and smaller health delivery organizations (e.g., rural health) • O7. Increase incentives, development and promotion of health care cybersecurity-focused education and certification programs • O8. Increase utilization of automation and emerging technologies like AI to drive efficiencies in cybersecurity processes • O9. Develop health sub-sector specific integrated cybersecurity profile aligned with regulatory requirements • O11. Increase meaningful and timely information sharing of cyber related disruptions to improve sector readiness • O12. Develop mechanisms to enable “mutual aid” support across sector stakeholders to allow for timely and effective response to cybersecurity incidents

RefID Cybersecurity Goals What does this cybersecurity-enabled end state look like?	Objective(s) that address the Goal
G9 The health and public health sector has established and implemented preparedness response and resilience strategies to enable uninterrupted access to healthcare technology and services	<ul style="list-style-type: none"> • O2. Simplify access to resources and implementation approaches related to the adoption of controls and practices aligned with regulatory and sector standards for securing devices, services, and data • O4. Increase new partnerships with public/private entities on the front edge of evaluating and responding to emerging technology issues to enable safe, secure, and faster adoption of emerging technologies • O6. Increase utilization of cybersecurity practices / resources / capabilities by public health, physician practices and smaller health delivery organizations (e.g., rural health) • O9. Develop health sub-sector specific integrated cybersecurity profile aligned with regulatory requirements • O10. Develop meaningful cross-sector third-party risk management strategies for evaluating, monitoring, and responding to supply chain and third-party provider cybersecurity risks • O11. Increase meaningful and timely information sharing of cyber related disruptions to improve sector readiness • O12. Develop mechanisms to enable “mutual aid” support across sector stakeholders to allow for timely and effective response to cybersecurity incidents
G10 Organizations across the health and public health sector have strong cybersecurity and privacy cultures that permeate down from the highest levels within each organization	<ul style="list-style-type: none"> • O3. Develop and adopt practical and uniform privacy standards to protect personal information and promote fair and ethical data practices while sharing the data in a consensual eco-system • O5. Enhance health sector senior leadership and board knowledge of cybersecurity and their accountability to create a culture of security within their organizations • O7. Increase incentives, development and promotion of health care cybersecurity-focused education and certification programs

E. Appendix E

Acknowledgements

This 18-month project is the result of hundreds of hours of collective thought and effort by senior and subject matter executives across the healthcare spectrum. The organizational and personnel members of the Health Sector Coordinating Council Cybersecurity Working are far too numerous to list, but certain key contributors must be recognized:

- Deloitte for donating substantial staff resources to helping manage the process and frame the plan, facilitate the discussions, capture the content and hold the pen for drafting the plan.
- Funding Members:
 - Abbott
 - Deloitte
 - HCA Healthcare
 - Health Care Service Corporation (HCSC)
 - Intermountain Health
 - Mayo Clinic
 - McKesson
 - Medtronic
 - Merck
 - Pfizer
 - Premera Blue Cross
- The HSCC 2022-23 Cybersecurity Working Group Executive Committee:
 - Intermountain Health (Chair)
 - Abbott (Vice Chair)
 - Mass General Brigham
 - McLaren Healthcare
 - USC Center for Body Computing
 - Organon
 - The University of Texas Austin Public Health Program
 - Health Information Sharing and Analysis Center
 - Fresenius Medical Care North America

- Premera Blue Cross
 - CommonSpirit Health
- Members of the 2016-17 [HHS Health Care Industry Cybersecurity Task Force](#)
- HSCC Members of the Strategic Plan Steering Committee (includes those above):
 - Becton Dickinson
 - Centura Health
 - Medtronic
 - Northwell Health
 - Premier, Inc
 - University of Chicago Medicine
- HSCC Advisor Members of the Strategic Plan Steering Committee
 - Censinet
 - First Health Advisory
 - Fortified Health Security
- Government Partners to the HSCC Joint Cybersecurity Working Group
 - U.S. Department of Health and Human Services
 - U.S. Department of Homeland Security – Cybersecurity and Infrastructure Security Agency



TRUST REPORT

Navigating the Landscape
of Trust in Information Assurance

HITRUST®

Table of Contents

- Message from Leadership**3
- Executive Summary: Navigating the Landscape of Trust in Information Assurance** 4
- HITRUST’s Commitment to a High-Quality Assurance Process**7
 - Transparency..... 10
 - Scalability.....13
 - Consistency..... 16
 - Accuracy..... 18
 - Integrity..... 20
 - Efficiency..... 23
- Demonstrating Cyber Resilience**..... 26
 - Data security breaches..... 27
 - Annual progress on Corrective Action Plans (CAPs)..... 27
 - Significant changes..... 28
- The HITRUST MyCSF Platform** 29
 - Assessment Workflow.....31
 - Assurance Intelligence Engine..... 32
 - Inheritance..... 32
 - Results Distribution System (RDS)..... 33
- Looking Ahead** 34
 - Plus Reporting & Insight Reports..... 36
 - HITRUST Artificial Intelligence (AI) Assurance Program..... 36

Message From Leadership

Welcome to our first Trust Report.

When we started HITRUST seventeen years ago, our goal was to address the information compliance and security needs of the healthcare industry including those embodied in HIPAA. What we've built since then extends far beyond that initial scope. Today, HITRUST offers a comprehensive suite of security, compliance, and risk management solutions that serve a wide array of industries, not just healthcare. Our offerings are designed to be accessible, scalable, and suitable for organizations of any size, from small startups to large enterprises, enabling trust in digital systems both internally and between parties.

The breadth of our certifications, from essential to rigorous levels, reflects our understanding that there is no one-size-fits-all in information security. Our approach allows for a pragmatic journey through our traversable portfolio, ensuring that organizations can find a pathway that fits their unique needs and grows with them.

These past few years, we've observed a significant increase in the demand for our certifications. This trend suggests a shift in the industry's mindset: merely checking compliance boxes is no longer sufficient. Organizations are increasingly seeking ways to genuinely lower their risks while providing reliable evidence of their security posture. It's clear that there's a growing recognition of the value in a complete and comprehensive solution that involves the entire ecosystem—something only HITRUST provides.

Our commitment is to establish trust in the security, privacy, and compliance of computing infrastructures. To do this we build upon two dimensions, relevance and reliability. Relevant meaning, are the requirements we set forth relevant to the current threat landscape and the reality of the organization and its relationships? And reliability, based on the six principles of Transparency, Scalability, Consistency, Accuracy, Integrity, and Efficiency. We believe these are essential for an assurance program to be relied upon. We believe that any assurance solution that does not address these sufficiently should be questioned. These aren't just ideals. They are the necessary foundation for any trusted assurance system in today's world of escalating cyber threats and increasing personal liability for security breaches.

As we look to the future, including expanding our assurances to emerging technologies such as AI, our focus remains on providing the necessary tools and certifications that support your cyber risk management and compliance objectives.

Finally, we also feel that those relying on our assurances should have visibility into the checks and balances in place and the effectiveness of our program, which this report that will be issued on an annual cadence aims to address.

Thank you to our customers, partners, employees, and other stakeholders who have helped make this company what it is. I am more optimistic than ever in HITRUST's future and the importance of the work we are doing together.

Sincerely,



Daniel Nutkis
Founder and Chief Executive Officer
HITRUST

Executive Summary:

Navigating the Landscape of Trust in Information Assurance

In today's rapidly evolving digital landscape, where threats loom large and compliance complexities grow, the question of trust in assurance mechanisms becomes paramount. How can organizations be certain that the assurance reports they depend on are not merely symbolic gestures but vital instruments of trust and reliability? Amidst the myriad of compliance frameworks and assurance reports, distinguishing between superficial validation and genuine security assurance is a challenge that demands urgent attention.

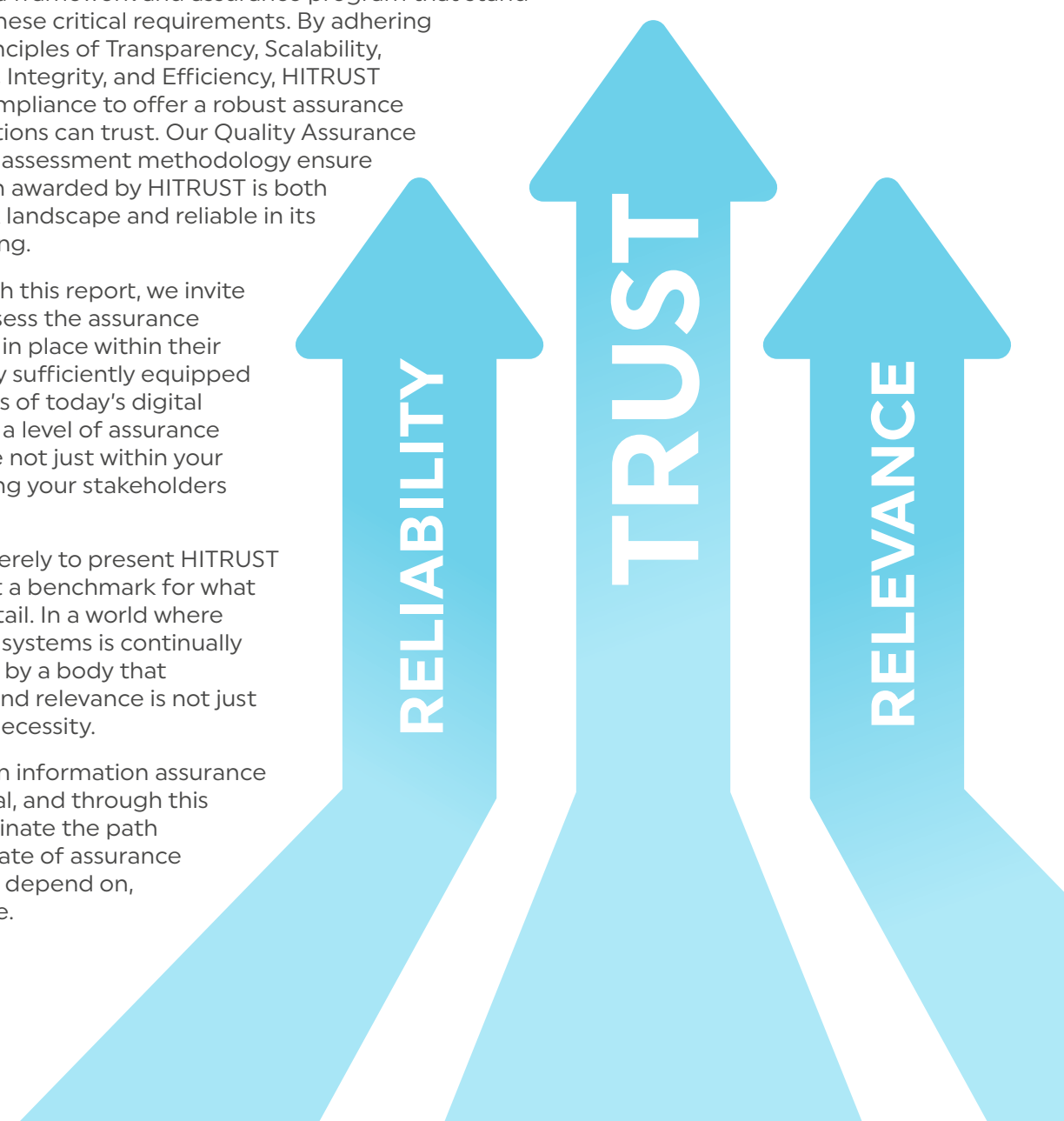
The HITRUST 2024 Trust Report seeks to address this crucial concern by presenting a comprehensive evaluation of assurance mechanisms within the context of a constantly shifting threat landscape and regulatory environment. We understand that for trust to be established, it needs to rest on two fundamental pillars: relevance and reliability. An assurance mechanism must not only resonate with the current threat environment and regulatory requirements but also demonstrate an unwavering commitment to precision, consistency, and integrity.

This report delves into how HITRUST, through 17 years of dedicated effort, has developed a framework and assurance program that stand at the confluence of these critical requirements. By adhering to the six essential principles of Transparency, Scalability, Consistency, Accuracy, Integrity, and Efficiency, HITRUST goes beyond mere compliance to offer a robust assurance solution that organizations can trust. Our Quality Assurance program and rigorous assessment methodology ensure that every certification awarded by HITRUST is both relevant to today's risk landscape and reliable in its evaluation and reporting.

As we navigate through this report, we invite readers to critically assess the assurance mechanisms currently in place within their organizations. Are they sufficiently equipped to address the nuances of today's digital threats? Do they offer a level of assurance that instills confidence not just within your organization but among your stakeholders and customers?

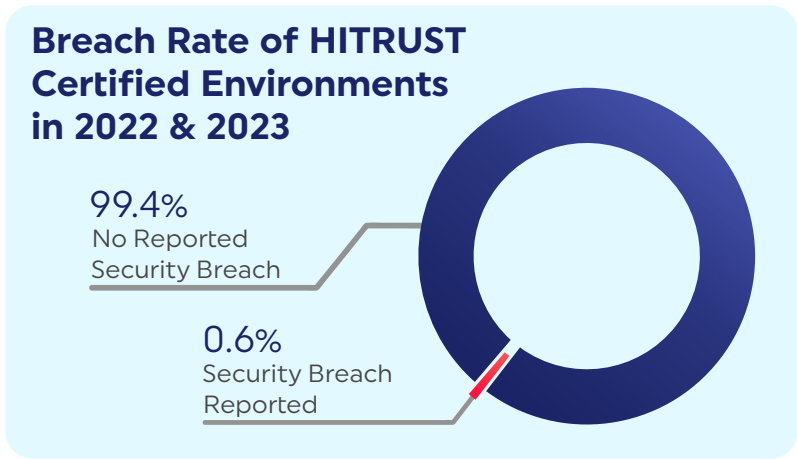
Our objective is not merely to present HITRUST as a solution but to set a benchmark for what digital trust should entail. In a world where the integrity of digital systems is continually tested, being certified by a body that epitomizes reliability and relevance is not just an advantage—it is a necessity.

We believe that trust in information assurance systems is foundational, and through this report, we aim to illuminate the path towards achieving a state of assurance that organizations can depend on, today and in the future.

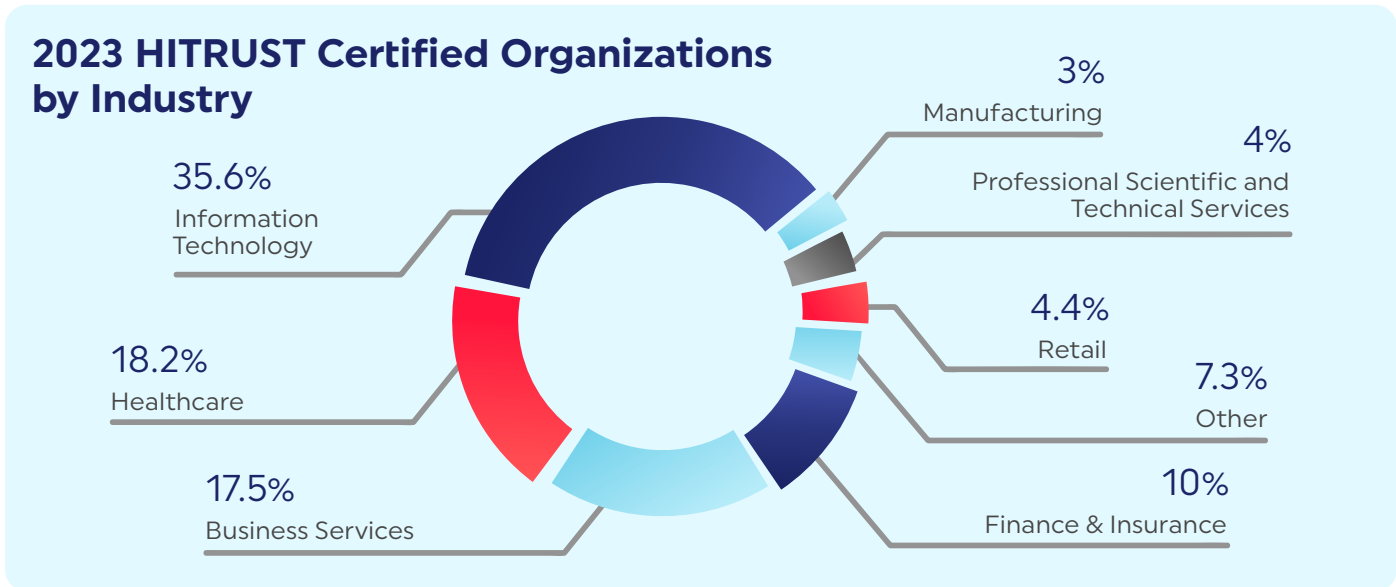


Report Highlights

97%
of all threat indicators
in MITRE ATT&CK are
covered in CSF version 11.2



HITRUST CSF
version 11.2 incorporates
44
standards, frameworks,
and regulations



100% of submitted assessments go through **HITRUST Quality Review**

HITRUST'S COMMITMENT TO A HIGH-QUALITY ASSURANCE PROCESS



HITRUST'S COMMITMENT TO A HIGH-QUALITY ASSURANCE PROCESS

Establishing trust in assurance mechanisms is challenging because many organizations do not know how to properly assess the options available. HITRUST has observed that organizations often develop a false sense of security from compliance reports and certifications that fail to offer the accurate, necessary assurances. As a result, these organizations are still vulnerable to significant information security threats.

In this report, we provide expectations that you can use to evaluate whether an assurance mechanism is both **reliable** and **relevant**.

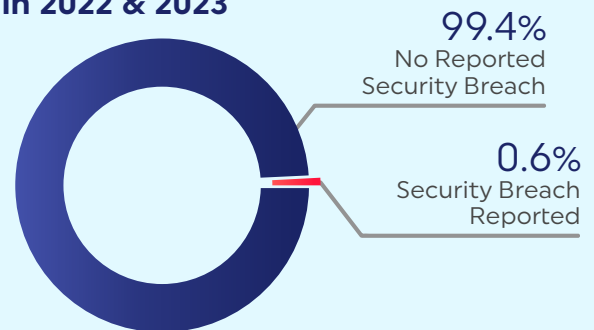
HITRUST's **reliable** assurances are built on the six essential principles of *Transparency, Scalability, Consistency, Accuracy, Integrity, and Efficiency*. HITRUST assessments encompass each of these principles and demonstrate HITRUST's commitment to a high-quality assurance process. We evolved our program to provide appropriate and transparent levels of assurance that organizations can trust. This includes incorporating a HITRUST Quality Assurance program to govern the assessment submission and report issuance processes. All assessments submitted to HITRUST must undergo a comprehensive quality review prior to achieving certification.

Relevant assurances must allow an organization to demonstrate their cyber resilience, which includes the ability to detect, protect, respond and recover from cybersecurity incidents, to a user of the report. HITRUST assessments are based upon

the HITRUST CSF, which is cyber threat adaptive to ensure organizations have controls in place that address current threats, such as ransomware.

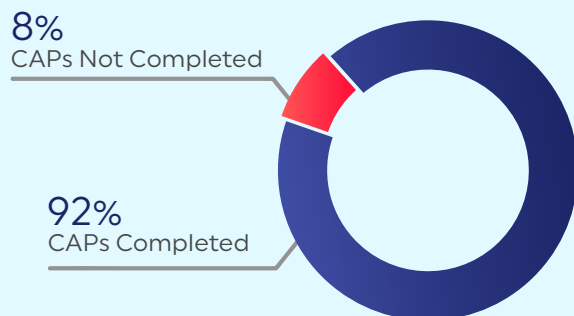
Being cyber threat adaptive means the HITRUST CSF consumes threat intelligence data from a leading threat intelligence provider, maps threats to the MITRE ATT&CK framework, and utilizes that data to identify controls within the CSF framework that are needed in an assessment. As cyber threats evolve over time, so does the HITRUST CSF, which is reviewed and enhanced to ensure new and emerging threats are mitigated.

Breach Rate of HITRUST Certified Environments in 2022 & 2023



Through relevant and reliable assurances, HITRUST has the ability to provide assurance to the organization that it is adequately protecting and improving its information security posture over time. HITRUST believes organizations that achieve a HITRUST certification reduce their risk of a data security breach, as **less than 1% of organizations with a HITRUST certification have reported security breaches to HITRUST over 2022 and 2023**. In addition, HITRUST expects organizations to continuously improve their maturity level, even after achieving certification. In 2024, HITRUST identified that **HITRUST r2 certified organizations remediated 92% of controls that did not fully address the HITRUST CSF framework requirements within one year of achieving their certification**.

Corrective Action Plan (CAP) Progress* in 2023



*As of an organization's one-year anniversary of its r2 certification

HITRUST's commitment to a high-quality assurance process starts at the top with a foundation of governance. This governance model drives continuous quality improvements within the HITRUST Quality Assurance Program, CSF control framework, and HITRUST assessment methodology. In this report, we'll further explore how each piece of the assurance process contributes to achievement of the six essential principles of *Transparency, Scalability, Consistency, Accuracy, Integrity, and Efficiency*.

HITRUST Assurance

HITRUST Governance

HITRUST Quality
Advisory Committee

MyCSF
Quality Reporting

Continuous Quality
Monitoring

HITRUST Quality Assurance Program

Assurance
Intelligence
Engine Review

HITRUST QA Analyst
Pre-submission
Review

HITRUST QA Analyst
Post-submission
Review

Escalated
QA Review

Report
Quality Review

External Assessor
Training

QA Analyst
Training

HITRUST CSF Control Framework

Threat-Adaptive

Risk-Scalable

Authoritative
Source Mappings

HITRUST Assessment Methodology

PRISMA
Maturity Model
& Scoring Rubric

Assessment
Workflow

HITRUST
Assessment
Handbook

In addition to highlighting HITRUST's performance against each of the six essential principles, we will provide the expected components which drive reliable and relevant assurances. HITRUST believes that while other assurance providers offer assessments and frameworks that include elements supporting each principle, they are not able to offer the same high-quality assurance process that exists with HITRUST.

Principle	HITRUST Expected Components		HITRUST Performance
Transparency	Control Framework Source	A control framework must include visibility into its requirements, including the basis for the framework.	✓
	Published Assessment Methodology	A published process must exist for the assessment approach, requirements, and scoring methodology.	✓
Scalability	Tailorable Control Framework	The control framework must be customizable based on organization's needs.	✓
	Relevant Control Framework	The framework must provide controls that address the current threat landscape and adapt to the scope of the assessment.	✓
Consistency	Formal Assessor Program	There must be a mechanism to ensure a consistent approach for the firms and individuals evaluating the results.	✓
	Centralized Quality Assurance	The assurance provider must ensure consistency in its Quality Assurance process to minimize variances and inconsistencies in the report and results.	✓
Accuracy	Control Maturity Model	The assessment must be able to report the state of the organization's information protection program clearly and accurately.	✓
	Assessment Scoring Methodology	There must be a mechanism to facilitate the accurate evaluation and scoring of the organization's implemented controls.	✓
Integrity	Quality Assurance Program	A process must be in place to ensure the assessment was conducted faithfully and results reported truthfully.	✓
Efficiency	Harmonized Control Framework	The control framework must be harmonized to avoid unnecessary or redundant requirements.	✓
	Streamlined Assessment & Reporting Process	The assurance provider must be able to support an efficient assessment process and timely report issuance.	✓
	Multi-use Reporting	The reports must satisfy multiple stakeholders for multiple purposes.	✓

"Organizations must be able to receive relevant information they can rely on. We have identified the mechanisms needed in an assurance process to deliver that relevance and reliability. Our commitment to this assurance process is what uniquely defines the value of a HITRUST certification."

– Vincent Bennekers, HITRUST Vice President of Quality

Transparency

Transparency requires an assurance provider to set clear expectations of the controls necessary to achieve certification along with the certification's corresponding evaluation and scoring model. This is needed for both the organization and its report recipients to clearly understand how controls were selected, evaluated, and scored.

Control Framework Source

In the case of HITRUST validated assessment reports, the HITRUST CSF control framework is used to determine if an organization can achieve certification. This framework provides the structure, transparency, guidance, and cross-references to authoritative sources that organizations globally need to be certain of their data protection compliance. Within the CSF framework, HITRUST maintains the requirements that an organization needs to achieve to obtain certification.

HITRUST CSF version 11.2 is publicly available and incorporates 44 relevant standards, best practice frameworks, and regulations. Utilizing such a large universe of potential controls is what makes the HITRUST CSF suitable for organizations of all types and sizes, regardless of industry. With each additional version of the CSF, HITRUST continues to expand this body of authoritative sources, which demonstrates its commitment to maintaining a comprehensive control framework.

HITRUST Authoritative Sources (as of CSF v11.2)		
16 CFR Part 681 – FTC "Red Flag" Identity Theft Rules [16 CFR 681]	Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements [OCR Guidance for Unsecured PHI]	ISO/IEC 27002:2022: Information Security, Cybersecurity and Privacy Protection – Information Security Controls ISO/IEC 27002:2022]
201 CMR 17.00 – State of Massachusetts Data Protection Act: Standards for the Protection of Personal Information of Residents of the Commonwealth [201 CMR 17.00]	Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook – Information Security, September 2016 [FFIEC IS]	ISO/IEC 27799:2016: Health Informatics – Information Security Management in Health using ISO/IEC 27002 [ISO/IEC 27799:2016]
American Institute of Certified Public Accountants (AICPA) Trust Services Principles and Criteria: Security, Confidentiality and Availability, 2017 [AICPA TSP 100]	Federal Risk and Authorization Management Program (FedRAMP) [FedRAMP]	ISO/IEC 29100:2011: Information Technology – Security Techniques – Privacy Framework [ISO/IEC 29100:2011]
Asia-Pacific Economic Cooperation (APEC) Cross Border Rules for the APEC Privacy Framework, 2005 [APEC]	Health Industry Cybersecurity Practices (HICP)	ISO 31000: Risk management – Guidelines [ISO 31000:2018]
California Consumer Privacy Act (CCPA) [CCPA 1798]	Health Information Trust Alliance (HITRUST) De-Identification (De-ID) Framework: De-identification Controls Assessment (DCA) [HITRUST De-ID Framework v1]	Joint Commission Standards, The Joint Commission (formerly the Joint Commission on the Accreditation of Healthcare Organizations) [TJC]

Center for Internet Security (CIS) Critical Security Controls (CSC) v7.1: Critical Security Controls for Effective Cyber Defense [CIS Controls v7.1]	HIPAA – Federal Register 45 CFR Part 164, Subpart C: HIPAA Administrative Simplification: Security Standards for the Protection of Electronic Protected Health Information (Security Rule) [45 CFR HIPAA.SR]	Minimum Acceptable Risk Standards for Exchanges (MARS-E) v2.2: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges [MARS-E v2.2]
CMS Information Security ARS 2013 v3.1: CMS Minimum Security Requirements for High Impact Data [CMS ARS v3.1]	HIPAA – Federal Register 45 CFR Part 164, Subpart D: HIPAA Administrative Simplification: Notification in the Case of Breach of Unsecured Protected Health Information (Breach Notification Rule) [45 CFR HIPAA.BN]	New York State Department of Financial Services – Title 23 NYCRR Part 500 [23 NYCRR 500]
COBIT 5: Deliver and Support Section 5 – Ensure Systems Security [COBIT 5]	HIPAA – Federal Register 45 CFR Part 164, Subpart E: HIPAA Administrative Simplification: Privacy of Individually Identifiable Health Information (Privacy Rule) [45 CFR HIPAA.PR]	NIST Artificial Intelligence Risk Management Framework [NIST AI RMF 1.0]
Electronic Health Network Accreditation Commission (EHNAC) [EHNAC]	IRS Publication 1075 v2021: Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for protecting Federal Tax Returns and Return Information [IRS Pub 1075 (2021)]	NIST Framework for Improving Critical Infrastructure Cybersecurity v1.1 [NIST Cybersecurity Framework v1.1]
Federal Register 21 CFR Part 11: Electronic Records; Electronic Signatures, 2003 [21 CFR 11]	ISO/IEC 23894: Information technology – Artificial intelligence – Guidance on risk management [ISO/IEC 23894:2023]	NIST Special Publication 800-53 Revision 4 (Final), including Appendix J – Privacy Control Catalog: Security Controls for Federal Information Systems and Organizations [NIST SP 800-53 R4]
General Data Protection Regulation (GDPR) European Union [EU GDPR]	ISO/IEC 27001:2022: Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements [ISO/IEC 27001:2022]]	NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations [NIST SP 800-53 R5]
NIST Special Publication 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations [NIST SP 800-171 R2]	Organisation for Economic Co-operation and Development (OECD) Privacy Framework, 2013 [OECD Privacy Framework]	Ontario, Canada Personal Health Information Protection Act, 2004 Chapter 3 [PHIPA]
NRS: Chapter 603A – State of Nevada: Security and Privacy of Personal Information [NRS 603A]	Payment Card Industry (PCI) Data Security Standard Version 3.2.1: Information Management (IM) Standards, Elements of Performance, and Scoring [PCI DSS v3.2.1]	South Carolina Insurance Data Security Act (SCIDSA) – Title 38, Chapter 99 [SCIDSA 4655]
NY DOH Office of Health Insurance Programs SSP v5.0 [NY OHIP Moderate-Plus Security Baseline v5.0]	Personal Data Protection Act 2012 (PDPA) [PDPA]	Title 1 Texas Administrative Code § 390.2 – State of Texas: Standards Relating to the Electronic Exchange of Health Information [1 TAC 15 390.2]
Office of Civil Rights (OCR) Audit Protocol April 2016 – HIPAA Security Rule [OCR Audit Protocol (2016)]	VA Directive 6500 VA Cybersecurity Program [VA Directive 6500]	

Published Assessment Methodology

HITRUST's robust assessment approach, control maturity and scoring methodology, and related assurance requirements are also clearly articulated in the publicly available [HITRUST Assessment Handbook](#). The HITRUST Assessment Handbook defines the requirements for those organizations assessing their information protection programs against the HITRUST CSF through a readiness or validated assessment. On April 4, 2023, HITRUST released an exposure draft of the HITRUST Assessment Handbook. Prior to final release of the Assessment Handbook, HITRUST received and reviewed feedback from 17 External Assessor firms

and other organizations. **The HITRUST Assessment Handbook (version 1.0) was published in final on October 16, 2023 and contains 401 total criteria across 15 Chapters.** It consolidates and replaces six other guidance documents HITRUST previously released.

HITRUST provides a support desk for organizations to reach out to when they have questions related to the CSF control framework, assessment approach or related assurance guidance. **In 2023, HITRUST Assurance and Quality teams resolved over 400 support tickets and provided recurring guidance to over 15 External Assessor firms.**

Assurance Provider Considerations

Do other Assurance Providers and Frameworks have the necessary components of Transparency?



Control Framework Source

A control framework must include visibility into its requirements, including the basis for the framework.

- ✓ HITRUST provides a published framework with the ability for an organization to cross-reference any requirement with its corresponding authoritative source.

Published Assessment Methodology

A published process must exist for the assessment approach, requirements, and scoring methodology.

- ✓ HITRUST maintains the publicly available [HITRUST Assessment Handbook](#) which describes the process, requirements, and scoring methodology for all HITRUST assessments.

Scalability

Scalability refers to the ability for an assurance provider to tailor its assessment approach based on organizational needs and risks. The assurance provider should also maintain a process that ensures the control framework remains relevant to the current threat landscape.

Tailorable Control Framework

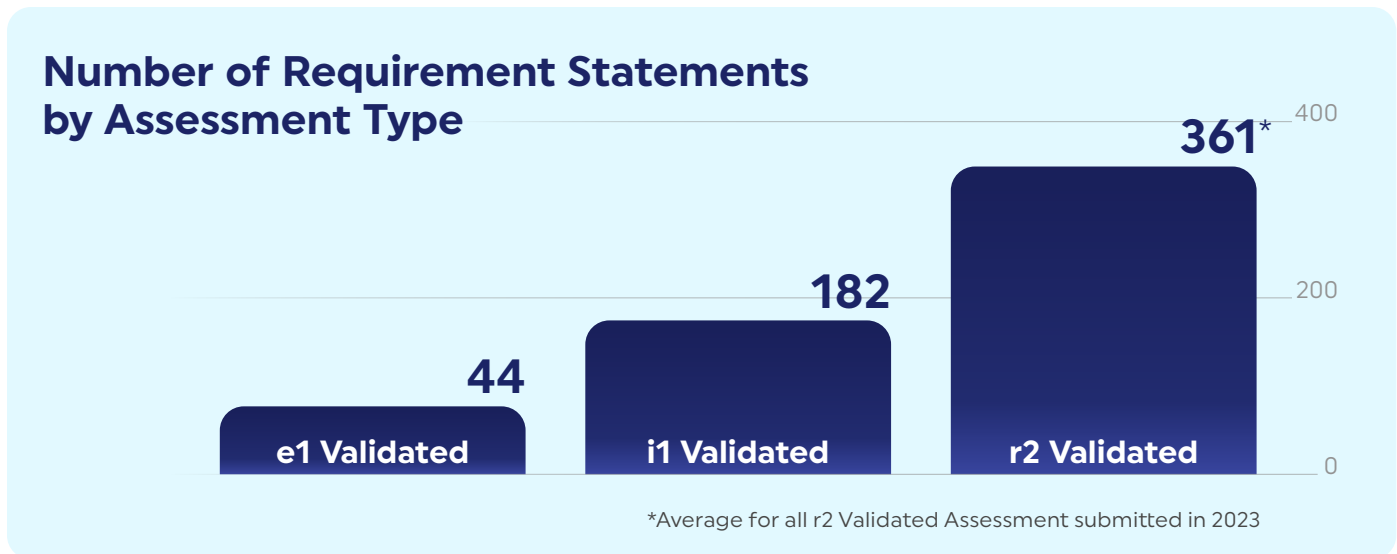
HITRUST provides three assessment types for organizations:

- HITRUST Essentials, 1-year (e1) Assessment: Foundational Cybersecurity
- HITRUST Implemented, 1-year (i1) Assessment: Leading Practices
- HITRUST Risk-based, 2-year (r2) Assessment: Expanded Practices

The e1 provides entry-level assurance focused on the most critical cybersecurity controls to demonstrate that essential cybersecurity hygiene is in place. **It focuses on a curated set of 44 core requirement statements, which encompass those fundamental cybersecurity practices.** These practices have been shown to represent the core controls that any organization must apply to provide a basic level of trust.

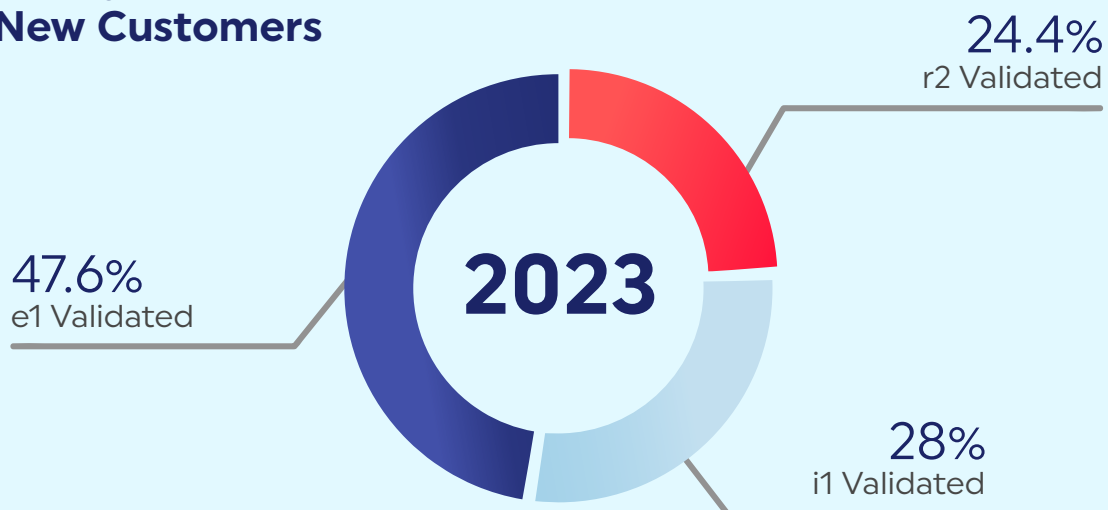
The i1 builds on those 44 requirements in the e1 by adding 138 requirement statements, which address a broader range of cyber threats. The i1 provides a moderate level of assurance through the inclusion of controls that are generally recognized as leading cybersecurity practices.

The r2 is a risk-based and tailorable assessment that provides the highest level of assurance for situations with greater risk exposure due to data volumes, regulatory compliance, or other risk factors. The r2 includes all 182 core requirements from the i1 as a baseline along with additional requirement statements based on the risk analysis HITRUST performs when an organization prepares for an r2 assessment. **In 2023, HITRUST noted that an r2 validated assessment averaged approximately 361 requirements.**



In response to changes in market dynamics and expanded organization needs to apply HITRUST, HITRUST expanded its portfolio to meet various risk profiles. HITRUST introduced a nested portfolio across the e1, i1, and r2 on January 18, 2023 with version 11.0 of the HITRUST CSF control framework. In 2023, most new customers chose to start their HITRUST journey with the HITRUST Essentials (e1) assessment, demonstrating the market need for this type of scalability.

Assessment Types Chosen by 2023 New Customers



This market need for scalability was also represented through the increase in i1 and e1 submissions across 2023. **HITRUST noted a 187% increase in i1 validated assessment submissions from 2022 to 2023.** For the e1, HITRUST continued to see an increase in submissions quarter over quarter in 2023, including a 113% increase from Q2 to Q3 and a 58.8% increase from Q3 to Q4 2023.

Relevant Control Framework

The HITRUST CSF control framework is threat adaptive, allowing changes to the framework as the threat landscape evolves. HITRUST analyzes cyber threat data on a regular basis, comparing it to the HITRUST baseline requirements to ensure the framework includes controls to address all relevant practices and evolving cyber threats. **The i1 and r2 baseline requirements for CSF version 11.2 cover 97% of all threat indicators present in the most recent threat analysis.** Those threats not addressed in the HITRUST CSF framework cannot be mitigated (as determined by the MITRE ATT&CK framework).

Each r2 assessment is also independently scalable through the risk analysis that HITRUST performs prior to generating the requirement statements that must be evaluated in the organization's assessment. The risk analysis uses factors to customize the assessment based on size, complexity, geography, technology, information,

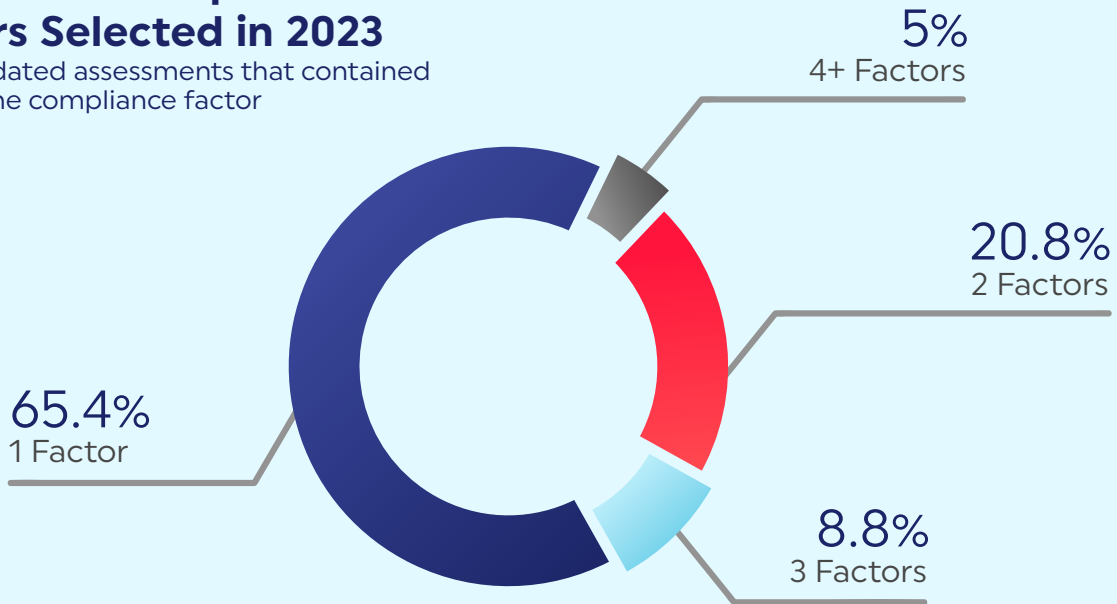
and regulatory requirements. The compliance factors within an assessment allow organizations to scale the assessment based on specific risks by integrating and harmonizing requirements from the relevant standards, best practice frameworks, and regulations. **Throughout 2023, over 60% of organizations selected at least one compliance factor when performing an r2 validated assessment with HIPAA being the most commonly selected factor.** For organizations that selected at least one compliance factor, over one-third selected more than one factor.

97%

of all threat indicators in MITRE ATT&CK are covered in CSF version 11.2

Number of Compliance Factors Selected in 2023

for r2 validated assessments that contained at least one compliance factor



Assurance Provider Considerations

Do other Assurance Providers and Frameworks have the necessary components of Scalability?



Tailorable Control Framework

The assurance provider must be able to customize the control framework based on organization's needs.

- ✓ HITRUST provides three assessment types whether the organization is ready to assess its scope against Foundational Security (e1), Leading Practices (i1), or Expanded Practices (r2).

Relevant Control Framework

The framework must provide controls that address the current threat landscape and adapt to the scope of the assessment.

- ✓ The threat-adaptive nature of the CSF framework allows HITRUST to maintain a continuous process for reviewing and updating its framework as threats evolve. When an organization approaches an r2 assessment, the assessment requirements are based on a risk analysis that incorporates size, complexity, geography, technology, information, and regulatory requirements.

Consistency

For an assessment to be reliable, the results must be consistent regardless of the professional or professional services firm performing the review. As a result, each assurance provider must have a process to ensure that individuals performing the work are evaluating and documenting their findings consistently. The assurance provider must also maintain an approach that minimizes variance and inconsistencies in the assessment report and results.

Formal Assessor Program

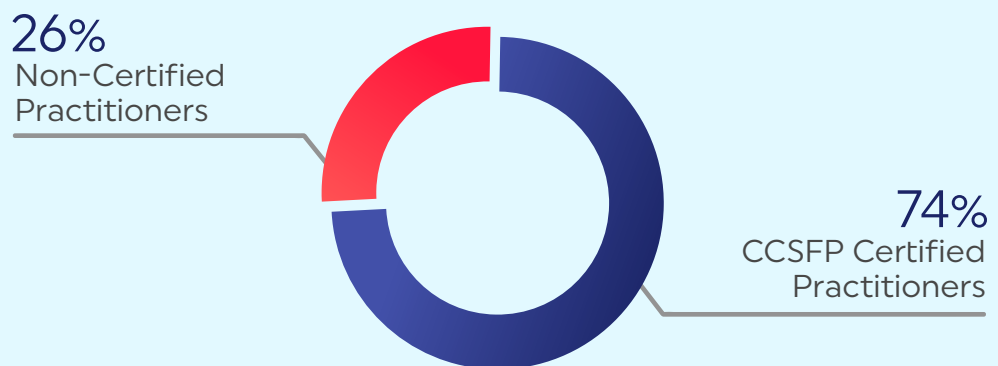
With the HITRUST system, all organizations must engage with a HITRUST-authorized External Assessor to perform validation procedures prior to completing and submitting a HITRUST validated assessment. **HITRUST's External Assessor Program is supported by a pool of independent HITRUST Authorized External Assessor Organizations ranging from large global professional services firms to small boutique consultancies.** This program has also proven itself extremely capable of supporting the wide and varied needs of industry as demand for HITRUST CSF Validated Assessment Reports has continued to grow over the past decade. Each of those External Assessor firms is vetted by HITRUST and required to utilize professionals who are trained and certified in the application of HITRUST's prescriptive assessment and assurance methodologies on every engagement.

HITRUST offers two certifications for individuals to demonstrate their understanding of the HITRUST CSF framework and its information protection principles: Certified CSF Practitioner (CCSFP) and Certified HITRUST Quality Professional (CHQP). The CCSFP is intended for individuals in organizations that plan to leverage the

HITRUST CSF framework and process internally or External Assessors who are performing HITRUST assessments, while the CHQP provides guidance to practitioners expected to perform independent quality assurance (QA) reviews of validated assessment results. Once an individual has achieved the CCSFP designation, he/she must attend an annual refresher course to maintain the designation. **Each organization that would like to become an authorized HITRUST External Assessor must perform a minimum of 140 hours of HITRUST-specific training prior to receiving the designation.** In 2023, HITRUST provided over 37,000 hours of training to individuals through its HITRUST Academy department.

External Assessors firms within the HITRUST External Assessor Program must maintain a minimum of five practitioners with the CCSFP designation and two practitioners with the CHQP designation. For each submitted validated assessment, at least 50% of all engagement hours must be performed by practitioners with a CCSFP to ensure the team has an appropriate understanding of the HITRUST CSF and HITRUST Assurance Program methodologies and tools. Additionally, the assessment quality assurance

HITRUST Assessment Hours Incurred by CCSFP Certified vs. Non-Certified Practitioners in 2023



reviewer must hold both a CCSFP and CHQP designation. That individual may not perform any other duty on the assessment to help ensure the pre-submission quality review was performed with objectivity. **In 2023, over 70% of hours on each submitted validated assessment were performed by an individual with a CCSFP designation.**

Centralized Quality Assurance

HITRUST utilizes a multi-faceted approach throughout the assurance program to drive consistency in its QA process and report issuance. This includes the use of the Assurance Intelligence Engine to drive over 150 automated quality checks, along with HITRUST quality inspection through the HITRUST Assurance department.

The HITRUST Assurance department employs Analysts who perform Quality Assurance (QA) reviews on all validated assessments submitted to HITRUST. The QA Analyst is responsible for reviewing that assessments submitted to HITRUST meet HITRUST requirements prior to issuing a report and/or certification. Each HITRUST QA Analyst is expected to attend relevant training on an annual basis to maintain appropriate knowledge

for their position. **In 2023, each HITRUST QA Analyst attended an average of 85 hours of training including internal HITRUST training and corresponding CPE (Continuing Professional Education) credits.**

During the QA review, the QA Analyst will open tasks when they have questions or feedback for the organization or External Assessor. **To ensure consistency in feedback across HITRUST QA Analysts, the HITRUST Quality department reviews all HITRUST QA Analysts on a monthly basis.** During the review, the HITRUST Quality team ensures the HITRUST QA Analyst provided and closed all necessary feedback and tasks to the organization or External Assessor prior to issuing its report and/or certification.

Assurance Provider Considerations

Do other Assurance Providers and Frameworks have the necessary components of Consistency?



Formal Assessor Program

There must be a mechanism to ensure a consistent approach for the firms and individuals evaluating the results.

- ✓ HITRUST maintains a formal External Assessor program which vets all firms prior to becoming an External Assessor and requires HITRUST-specific training for each individual on an annual basis. Assessments submitted to HITRUST require a minimum percentage of hours on each assessment performed and reviewed by those individuals with HITRUST designations.

Centralized Quality Assurance

The assurance provider must ensure consistency in its Quality Assurance process to minimize variances and inconsistencies in the report and results.

- ✓ HITRUST uses a combination of automated quality checks and manual HITRUST quality inspection as part of a centralized Quality Assurance function to drive consistency in its QA process and report issuance.

Accuracy

Organizations expect that assessment results accurately reflect the state of controls implemented in an organization's environment. As a result, assurance providers must have mechanisms in place to facilitate the accurate evaluation and scoring of implemented controls.

Control Maturity Model

HITRUST provides the only assessment report that clearly articulates control maturity using an innovative PRISMA-based control maturity and scoring model, which provides a level of accuracy not achievable by traditional assessment approaches. For an r2 assessment, the status of an organization's information security policies, procedures, and controls implementation must be assessed as part of the maturity model. **This provides a higher level of assurance because it is based on direct rather than circumstantial evidence** and therefore is more indicative of the actual level of protection the organization provides to sensitive information, making it the most accurate method of measuring the performance of an organization's controls. For e1 and i1 assessments, the control maturity is only scored based on the organization's information security controls implementation.

Assessment Scoring Methodology

To help assessors score control maturity in a consistent, accurate, and repeatable way, HITRUST developed a scoring rubric to be used in their scoring evaluations. **100% of validated assessments submitted to HITRUST in 2023 utilized the HITRUST scoring rubric to evaluate the organization's control maturity.**

The rubric provides guidance on scoring a requirement statement based on an evaluation of strength and coverage where strength and coverage are defined as:

- *Strength*: The rigor with which the Assessed Entity has implemented the requirement within its organization.
- *Coverage*: Percentage of the requirement where the Assessed Entity is compliant.

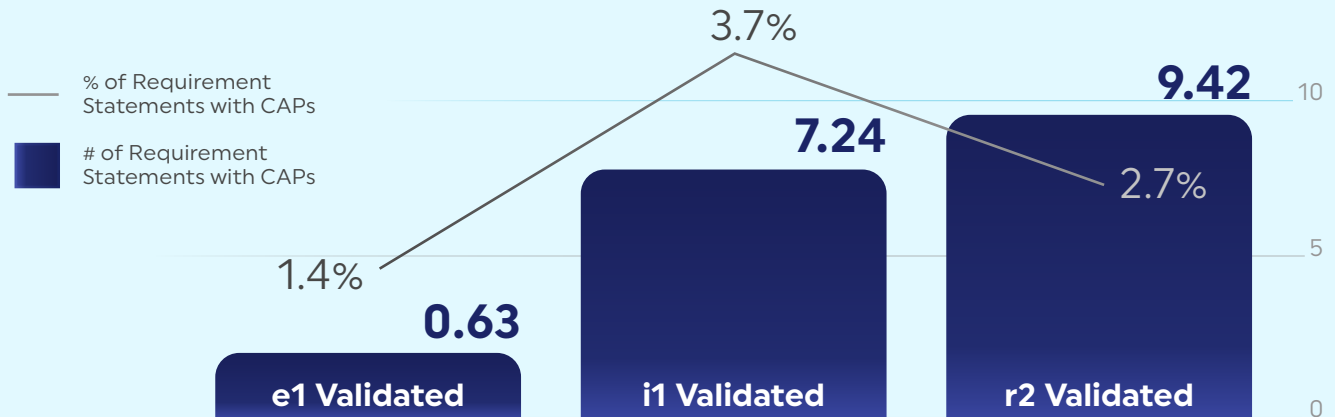
When an entity has not fully implemented a HITRUST requirement within the scope of its assessment, or when deficiencies in the operation of those controls are identified, the control maturity scores are lowered based upon the HITRUST scoring rubric. In order to achieve a HITRUST certification, each HITRUST domain must achieve a score that meets or exceeds the certification threshold for the assessment type selected. In the table below, HITRUST identified the most difficult domains for organizations to achieve maturity based on the lowest scores by assessment type.

Assessment Type	Lowest Scoring Domain
HITRUST r2 Validated Assessment	10: Password Management
HITRUST i1 Validated Assessment	19: Data Protection & Privacy
HITRUST e1 Validated Assessment	11: Access Control

If an organization's HITRUST requirement statement scores less than fully compliant and reaches a specific threshold (based on assessment type), the organization is required to define a Corrective Action Plan (CAP). The CAP must include a description of the planned corrective action that is specific, measurable, and clear enough to provide value to readers of the HITRUST report. All deficient levels and evaluative elements must be addressed by the corrective action plan. HITRUST requires CAPs so that an organization continues improving its control maturity, even if it has achieved the necessary score for certification.

HITRUST identified the average number of requirement statements along with the ratio of average number of CAPs per requirement statement for each assessment type in 2023. As the HITRUST e1 assessment is considered a cybersecurity essentials assessment, it is not surprising that it recorded the lowest average number of CAPs and CAP to requirement statement ratio. While there are more CAPs on average in an r2 validated assessment, the i1 maintained a higher CAP to requirement statement ratio across all validated assessments submitted to HITRUST in 2023. **Based on this, organizations performing an i1 average more deficiencies to remediate on a per requirement basis than those performing an e1 or r2.**

Average Number of Requirement Statements with CAPS by Assessment Type in 2023



Assurance Provider Considerations

Do other Assurance Providers and Frameworks have the necessary components of Accuracy?



Control Maturity Model

The assessment must be able to report the state of the organization's information protection program clearly and accurately.

- ✓ HITRUST provides the only assessment report that clearly articulates control maturity using an innovative PRISMA-based control maturity and scoring model, which provides a level of accuracy not achievable by traditional assessment approaches.

Assessment Scoring Methodology

There must be a mechanism to facilitate the accurate evaluation and scoring of the organization's implemented controls.

- ✓ HITRUST has developed and published a scoring rubric which assessors must use to evaluate control maturity in a consistent, accurate, and repeatable way.

Integrity

Integrity is the heart of an assessment process. Without it, an assurance provider's report cannot be trusted even if all other essential principles are in place. An assurance provider must have processes in place to ensure the assessor conducted the assessment faithfully and the results were reported truthfully.

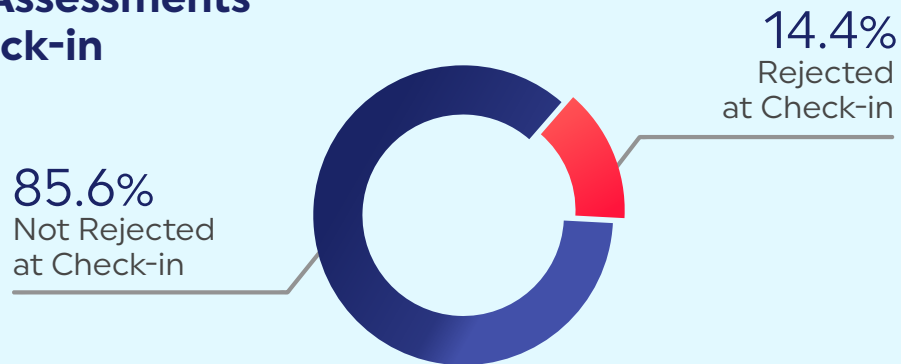
Quality Assurance Program

HITRUST has focused its assurance and quality processes to ensure the highest level of integrity and confidence in a HITRUST certification. The HITRUST Assurance Program provides a granular level of oversight through a quality control process that reviews each assessment and the resulting report it produces. The key components of the quality control process include pre-submission checks, post-submission QA reviews, report quality reviews, and continuous quality monitoring.

Pre-submission checks

Utilizing the HITRUST Assurance Intelligence Engine (AIE), each submitted assessment undergoes over 150 automated quality checks to identify and address assessment errors and omissions. The Assurance Intelligence Engine proactively identifies potential issues by performing a real-time analysis against thousands of data points across the body of documentation for an assessment. Through the MyCSF platform, the Assurance Intelligence Engine provides detailed descriptions for potential quality issues, the triggering data point(s), and recommended remedial actions. Upon submission, HITRUST reviews the potential quality issues identified by the AIE and determines whether to accept the submission or return the submission to the External Assessor for remediation.

2023 Validated Assessments Rejected at Check-in



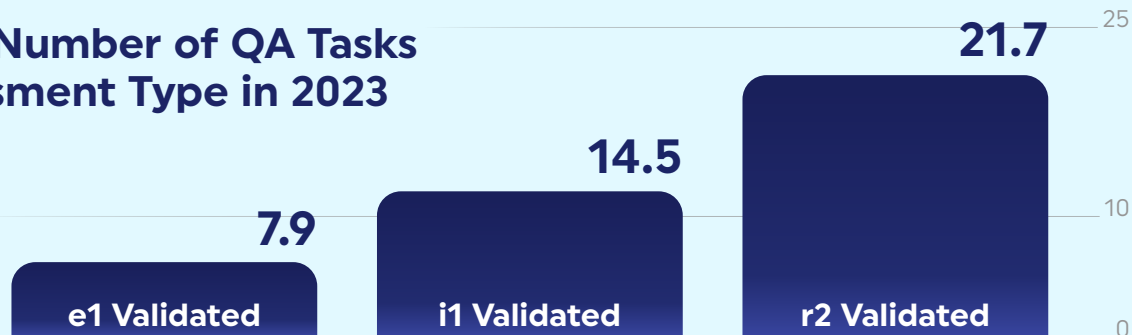
Post-submission QA reviews

Each validated assessment must undergo a detailed Quality Assurance (QA) review after it has been submitted to HITRUST. The QA review uses a risk-based approach to determine the required level of review for each assessment. The appropriate QA risk level for each assessment is identified through a set of analytics that HITRUST runs on the assessment upon submission. After determining the QA risk level, a HITRUST QA Analyst will perform the QA review.

During the QA review, the HITRUST QA Analyst

will review each potential quality issue, ensure the assessment information meets HITRUST criteria defined in the Assessment Handbook, and perform an in-depth review of the testing performed by the External Assessor for a sample of requirement statements. The HITRUST QA Analyst will create QA tasks in the MyCSF platform, assigned to the organization or External Assessor, when questions or concerns are identified. **In 2023, HITRUST QA Analysts spent over 14,550 hours performing QA reviews on validated assessment submissions.**

Average Number of QA Tasks by Assessment Type in 2023

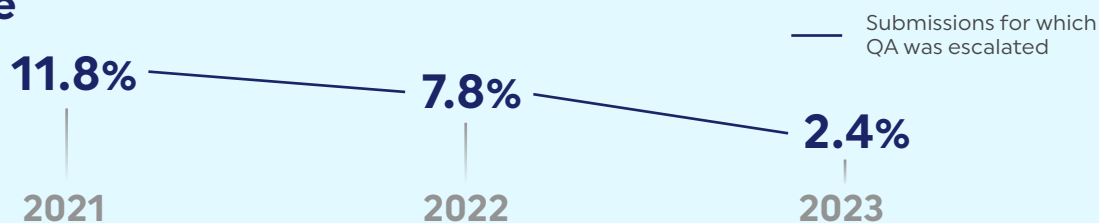


HITRUST maintains an Escalated QA (EQA) process for those assessments where the HITRUST QA Analyst has identified a higher volume and/or severity of concerns than typically expected. An assessment only enters EQA if HITRUST believes that the nature of the concerns may be pervasive enough to affect scoring across the validated assessment. In EQA, the HITRUST Quality team attempts to understand the procedures performed by the External Assessor during fieldwork to validate the assessment scoring. The EQA team will communicate and meet with the External Assessor at least two times to attempt to resolve HITRUST's questions and concerns. At the end of EQA, HITRUST will either return the validated assessment back to normal QA or provide options to remediate

the assessment which may include lowering scores, providing additional evidence or performing a new validated assessment. If a validated assessment re-enters EQA a second time after remediation, and the External Assessor is unable to resolve HITRUST's concerns, it will be considered a failed QA.

HITRUST noted a decrease in the percentage of submitted validated assessments entering EQA from 2022 (7.8%) to 2023 (2.4%). HITRUST believes the significant reduction can be attributed to the increased communication between the HITRUST Assurance and Quality teams with the External Assessor community, along with an increased understanding in the HITRUST community of validated assessment expectations.

Assessments Entering Escalated QA Over Time



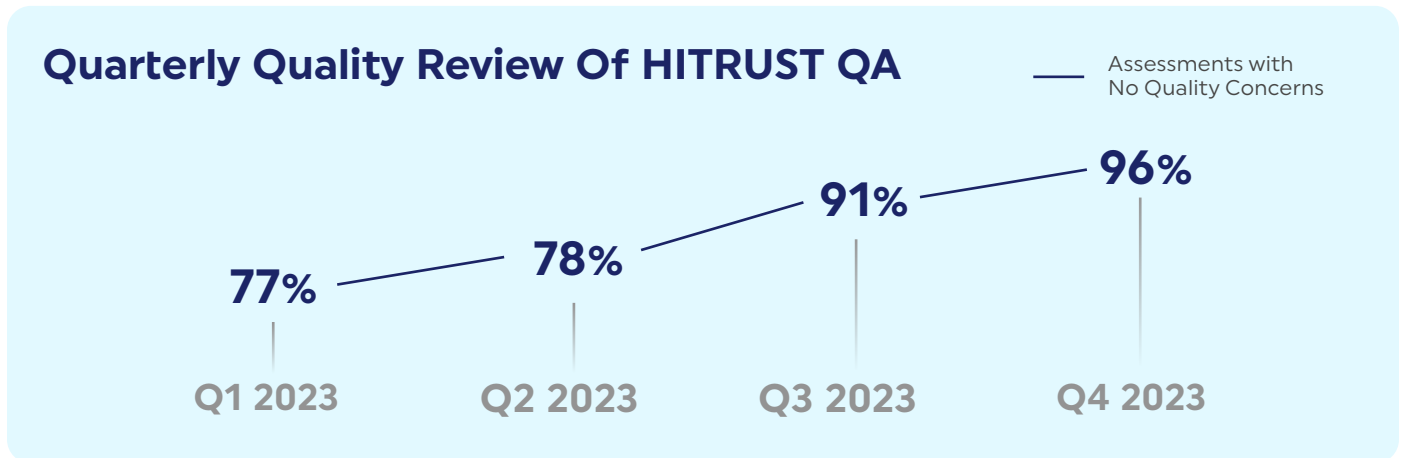
Report quality reviews

Reports are initially prepared by HITRUST analysts with the assistance of the HITRUST AIE and reviewed by two levels of HITRUST management prior to issuance. After the HITRUST QA Analyst prepares the draft report, it is reviewed by assurance management and then sent to the HITRUST Quality team for a second management review. Upon approval from the HITRUST Quality team, the draft report is released in MyCSF to the organization for its review and final approval.

Continuous internal quality monitoring

Quality performance is continuously monitored and audited by the HITRUST Quality department, with quality metrics reported quarterly to the Quality Assurance Advisory committee and HITRUST CEO.

To ensure consistency in feedback across HITRUST QA Analysts, the HITRUST Quality department reviews all HITRUST QA Analysts monthly. During its review, the HITRUST Quality team ensures the HITRUST QA Analyst provided and closed all necessary feedback and tasks to the organization or External Assessor prior to issuing its report and/or certification. HITRUST saw improvement in the QA Analyst's performance throughout 2023 as it went from 77% of assessments with no quality concerns to 96% by the end of 2023.



The HITRUST Quality Assurance Advisory committee was formed to provide additional governance and oversight of the HITRUST Assurance Program. **The role of the HITRUST Quality Assurance Advisory committee is to independently review the processes HITRUST has in place to ensure quality and consistency across the entire program.** This includes reviewing metrics used by HITRUST to measure quality at every level of the process, providing feedback where changes are required, and making recommendations for process improvements when appropriate.

Assurance Provider Considerations

Do other Assurance Providers and Frameworks have the necessary components of Integrity?



Quality Assurance Program

A process must be in place to ensure the assessment was conducted faithfully and results reported truthfully.

- ✓ The HITRUST Quality Assurance Program provides a granular level of oversight through a multi-layered quality control process that reviews each assessment and the resulting report it produces.

Efficiency

For a report to be efficient, assessments and their associated reports should satisfy multiple stakeholders for multiple purposes. Assurance providers should develop an assessment report that can be used by multiple relying parties. Additionally, the assessment process itself should not be burdensome with report issuance performed on a timely basis after completion.

Harmonized Control Framework

HITRUST has aligned various relevant information risk and compliance frameworks, best practices, and regulations into a single set of harmonized control requirements. In 2023, HITRUST was able to reduce the expected number of requirement statements to achieve an i1 or r2 certification through both control rationalization and control alignment with the latest cyber threat intelligence. **For an i1 assessment, CSF version 11 reduced the number of requirement statements by 17% (from 219 to 182).** For an r2 assessment, the number of requirement statements vary based on the inherent risks present in the assessed environment (such as whether the scoped system is accessible from the internet), and the optional inclusion of compliance factors. However, HITRUST modeling of CSF version 11 projected an average requirement statement reduction of 5%.

Streamlined Assessment & Reporting Process

The MyCSF platform enables HITRUST's ability to provide an efficient approach through streamlining the assessment and reporting processes. Two key functionalities within MyCSF that support this efficiency are Inheritance and the QA Reservation System.

Inheritance

The vast majority of IT platforms built today use service providers to support various components within the platform. To adequately address the risks posed by those service providers, an organization's assessment should encompass the control performance of those providers. As a result, HITRUST developed an automated process for relying on another HITRUST validated assessment through the use of Inheritance. Inheritance allows organizations to import requirement scores from one HITRUST validated assessment into another validated assessment within the MyCSF platform. The Inheritance functionality is a simple mechanism that can be used by a service provider to share scores with users that are attempting to obtain a HITRUST certification, or it can be used by an organization to share scores across separate business units or entities. Inheritance reduces and,

in some cases, eliminates the need for duplicative control assessment testing by organizations during a HITRUST assessment.

Inheritance is only possible as a result of the system of trust HITRUST has built around its assessment process. These automated reliance capabilities enable the delivery of a comprehensive assessment that addresses the risks posed by service providers.

In 2023, over two-thirds (68%) of r2 validated assessments utilized External Inheritance, while 64% of i1 validated assessments, and 58% of e1 validated assessments used External Inheritance.

These organizations utilizing inheritance see both lower certification costs and faster times to achieve HITRUST certification.

Average Number of External Inheritance Requests in a Validated Assessment in 2023

for validated assessments which contained at least one inheritance request



QA Reservation System

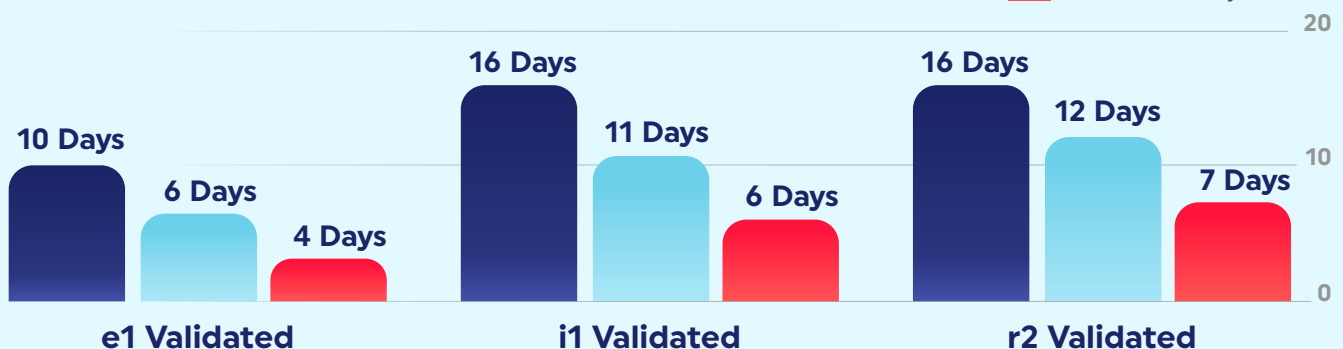
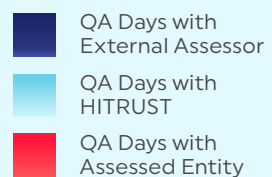
HITRUST uses an automated Reservation System within the MyCSF platform to streamline the QA process. The Reservation System requires organizations to schedule the start of their QA procedures prior to submitting a HITRUST validated assessment. The Reservation System is designed to:

- Eliminate the uncertainty around when HITRUST's QA procedures will begin
- Allow organizations and their External Assessor to schedule resources to respond to HITRUST's QA feedback
- Provide the opportunity for QA to occur closer to the submission date

Since implementation of the Reservation System on July 1, 2021, HITRUST has observed a substantial decrease in the number of days after submission when an organization will receive their HITRUST report and/or certification. As the MyCSF platform automatically records the amount of time a validated assessment resides within each phase of the workflow, **HITRUST identified the average number of days from QA start to draft report for an r2 validated assessment in 2023 was 35 days.**

For i1 and e1 assessments, HITRUST has established a post-submission Service Level Agreement (SLA). The SLA commits that the HITRUST time from QA to draft report is not greater than 45 business days. If HITRUST does not meet the SLA, the organization's next i1 or e1 validated assessment report credit is complimentary. In 2023, HITRUST did not exceed this SLA threshold for any i1 or e1 assessments

Average QA Days with HITRUST, External Assessor, and Assessed Entity for a Validated Assessment



Multi-use Reporting

HITRUST's control framework incorporates 44 (CSF version 11.2) relevant standards, best practice frameworks, and regulations which allows it to deliver comprehensive assessment reports that can provide appropriate assurances for multiple requesting parties, saving organizations significant time and money—an approach HITRUST calls *Assess Once, Report Many*.

HITRUST continued to enhance its capabilities to *Assess Once, Report Many* through the introduction of Insight Reports in 2023. HITRUST Insight Reports are assurance reports that provide easy-to-understand, reliable compliance reporting

over specific authoritative sources. These optional add-on reports can be produced for those organizations that have completed a HITRUST r2 validated assessment using the corresponding authoritative source. Organizations can share the reports with either internal or external stakeholders to provide its compliance posture on an authoritative source. **In November 2023, HITRUST launched the first Insight Report which includes the ability to provide insights into an organization's HIPAA compliance.** HITRUST will continue to expand its offerings in this area into 2024 to provide additional information security insights for organizations.

Assurance Provider Considerations

Do other Assurance Providers and Frameworks have the necessary components of Efficiency?



Harmonized Control Framework

The control framework must be harmonized to avoid unnecessary or redundant requirements.

- ✓ HITRUST has aligned various relevant information risk and compliance frameworks, best practices, and regulations into a single set of harmonized control requirements for each assessment type.

Streamlined Assessment & Reporting Process

The assurance provider must be able to support an efficient assessment process and timely report issuance.

- ✓ HITRUST developed the MyCSF platform to allow organizations to manage and coordinate their assessment and certification processes with assessors, service providers, relying parties and HITRUST. The Inheritance and QA Reservation System functionalities within MyCSF enable the efficient completion of an assessment and timely issuance of reports.

Multi-use Reporting

The reports must satisfy multiple stakeholders for multiple purposes.

- ✓ HITRUST's control framework incorporates 44 (CSF version 11.2) relevant standards, best practice frameworks, and regulations allowing it to deliver comprehensive assessment reports that can provide appropriate assurances for multiple requesting parties.

DEMONSTRATING CYBER RESILIENCE



DEMONSTRATING CYBER RESILIENCE

For an assurance mechanism to be relevant, it must allow the organization to demonstrate it has the necessary cyber resilience capabilities. These cyber resilience capabilities are necessary to allow organizations to continuously support their business operations regardless of the nature of the cyber attack.

The HITRUST CSF framework drives cyber resilience so that organizations are able to detect, protect, respond, and recover from cyber incidents. A HITRUST certification allows an organization to demonstrate it has achieved a high level of cyber resilience.

When an organization achieves HITRUST certification it remains valid from the date of certification for a specific amount of time into the future; two years for an r2 certification, and one year for an i1 or e1 certification as long as certain conditions are met during that period. These conditions include:

- No data security breach reportable to a federal or state agency by law or regulation has occurred within or affecting the assessed environment.
- Annual progress is made on areas identified in the Corrective Action Plan(s) (CAPs).
- No significant changes in the business or security policies, practices, controls, and processes have occurred that might impact its ability to meet the certification criteria.

These conditions are in place to ensure that organizations continue to meet and exceed their assessed levels of cyber resilience.

Data Security Breaches

Cyber resilience not only expects organizations are appropriately protected from cyber threats, but that when it occurs, they can detect, respond and recover from a particular security incident.

When an organization achieves a HITRUST r2 certification, it has demonstrated that the organization's security program has achieved compliance with the most rigorous cybersecurity requirements that HITRUST publishes. However, no organization can fully eliminate all risks of a security breach due to the various types of threats along with weaknesses that can be exposed.

When an organization encounters a security breach, HITRUST works with the organization to understand the nature, cause, and impact of the cyber attack in relation to the scope

of its assessment. HITRUST uses the reported security breach information to enhance the CSF framework as part of its cyber threat adaptability program.

While not all risks can be fully eliminated, HITRUST believes that achieving a HITRUST certification significantly reduces the risk of a data security breach. When a HITRUST-certified organization has a security breach in the certified environment, its agreement with HITRUST requires them to notify HITRUST. **Over 2022 and 2023, only 0.64% of organizations that received HITRUST certifications reported a security breach to HITRUST in their certified environment over that same period.**

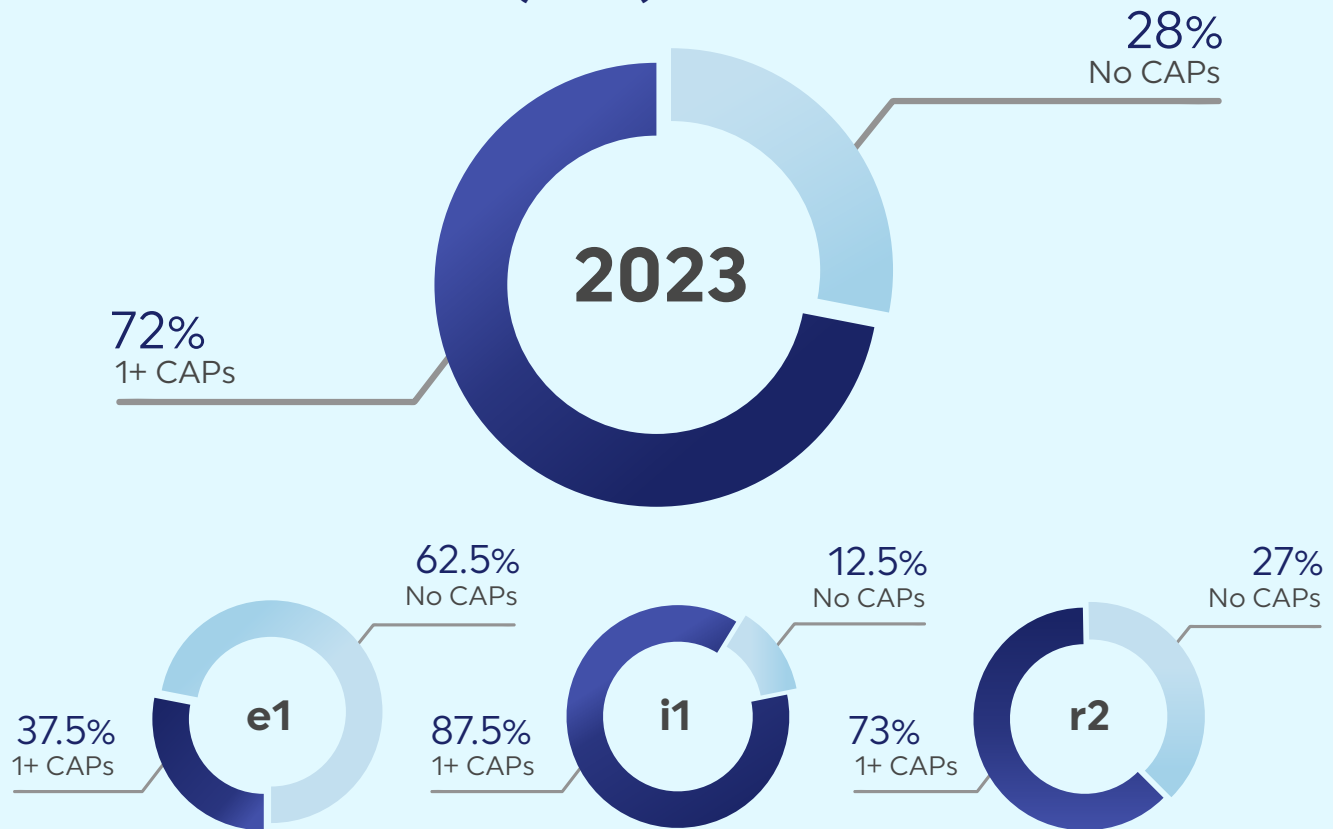
Annual Progress on Corrective Action Plans (CAPs)

HITRUST expects organizations to make annual progress on CAPs so they are not only meeting the assessed level of cyber resilience, but continuing to increase their cyber resilience capabilities. If an organization's HITRUST requirement statement scores are below a specific threshold (based on assessment type), it is required to define a CAP to improve its control maturity in that domain. This causes those organizations that have achieved a HITRUST

certification to more regularly improve their security posture than those that haven't achieved a HITRUST certification.

In 2023, HITRUST identified that 28% of all validated assessments did not require a CAP to be defined. For r2 assessments with CAPs, **92% of those CAPs were closed, on average**, by the interim assessment which occurs on the one-year anniversary of a certification.

2023 Validated Assessments with Corrective Action Plans (CAPs)



Significant Changes

A HITRUST certification is only valid for the environment included in-scope of the organization's assessment and the corresponding certification letter and validated report. However, HITRUST understands that Assessed Entities may have fast-changing environments that still require maintaining a continuous HITRUST certification. As a result, HITRUST has a collaborative process that enables Assessed Entities to

maintain their certification when they have identified developments that may impact their current certification. **In 2023, 2.1% of certified organizations reported a significant change to HITRUST.** HITRUST provided guidance for each of those entities on the steps and testing necessary for their HITRUST certifications to remain in compliance.

"Organizations have discovered that HITRUST assessments are the gold standard in information protection assurances because of the comprehensiveness of control requirements, depth of quality review, and consistency of oversight. The tools and methodologies used by organizations to complete HITRUST certification allow them to assess and report against multiple sets of requirements – assess once, report many, as we say – making our certification assurances efficient, transparent, and thorough."

– Bimal Sheth, HITRUST Executive Vice President, Standards Development & Assurance Operations

THE HITRUST MYCSF PLATFORM



THE HITRUST MYCSF PLATFORM

HITRUST developed the MyCSF platform to integrate all stakeholders into the system of trust that HITRUST has built. The HITRUST MyCSF platform allows an organization to manage its assessment and certification through coordination with its assessor, service providers, relying parties, and HITRUST. MyCSF has become the central repository where customers work to document, communicate, and improve their information security performance.

As a result of the capabilities of MyCSF, HITRUST is uniquely positioned to understand each organization's true information security maturity

and provide the reporting that each organization requires. MyCSF allows organizations to perform high-quality assessments against the HITRUST CSF framework utilizing functionality that incorporates the essential principles for a reliable and accurate assessment report including:

- Assessment Workflow
- Assurance Intelligence Engine
- Inheritance
- Results Distribution System (RDS)

"Our innovation and investment into MyCSF enables organizations to use HITRUST as a centralized platform for managing and monitoring their information security performance and risks. We will continue to develop and streamline our assurance processes providing organizations with numerous quality advantages over other assurance programs and certifying bodies."

– Jeremy Huval, HITRUST Chief Innovation Officer

Assurance Provider Considerations

Do other Assurance Providers and Frameworks have platforms that allow organizations to manage and coordinate their assessments and certifications?

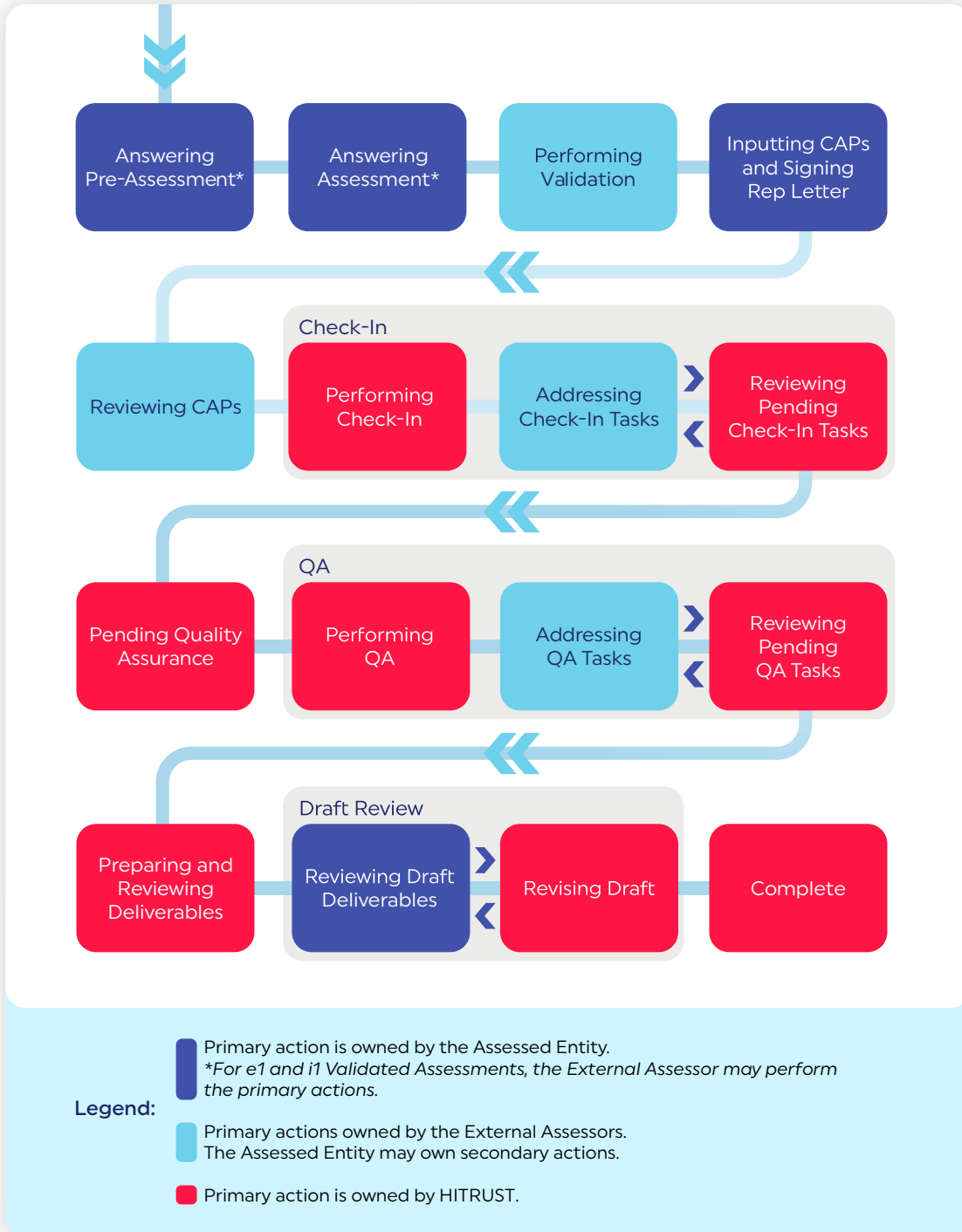


The HITRUST MyCSF platform allows an organization to manage and coordinate its assessment and certification processes with assessors, service providers, relying parties, and HITRUST.

Assessment Workflow

The workflow for any HITRUST assessment consists of multiple workflow phases with each phase owned by either HITRUST, the organization being assessed, or the External Assessor. MyCSF automates the entire workflow and submission process for these assessments. When a workflow phase is complete, the entity owning the phase is able to submit the assessment into the next phase of the workflow. When entering a new phase, entities will receive notifications that the assessment has moved into the next phase in the workflow.

HITRUST Validated Assessment Workflow Phases



The MyCSF platform also includes a Kanban-style dashboard allowing all participants of the assessment to track and view the assessment status at any time. The Kanban view contains a column for each phase of the Validated Assessment Workflow, and each accessible Validated Assessment is displayed as a card. The view includes key details of each Validated Assessment, including:

- Colored, circle badges depicting responsible parties for action items
- Summary of open items per organization
- Time elapsed in current phase
- HITRUST-assigned point of contact

Assurance Intelligence Engine

MyCSF also includes the Assurance Intelligence Engine (AIE) to drive efficiency and elevate quality. The AIE analyzes assessment documentation for oversights, inconsistencies, and errors throughout the information security and privacy assessment process. It adds efficiency to the HITRUST assessment quality review process by adding a layer of automated checks that complement existing, manual reviews to identify potential issues in assessment submissions that might otherwise jeopardize the integrity, accuracy, or consistency of information.

Impact of the Assurance Intelligence Engine™ on the HITRUST CSF Assurance Program

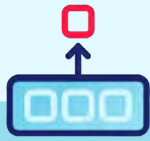


Prior to an assessment moving into the next workflow phase, the AIE will notify the participant of errors (or potential errors) in the corresponding information entered into MyCSF. The AIE brings awareness for early remediation of quality issues and this awareness also helps to avoid their recurrence. It adds efficiency to the entire assurance lifecycle by reducing the likelihood of surprises during quality assurance reviews of completed assessments. The impacts are mutually beneficial for HITRUST, organizations, and External Assessors.

Inheritance

Inheritance is a unique capability available in MyCSF that delivers a high-efficiency solution to streamline the process and expense of managing information protection assurance assessments. Inheritance can be used internally to import control testing results and scores from an organization's HITRUST validated assessment, or externally from a third-party HITRUST-certified cloud or other service provider who shares responsibility for protecting an organization's data.

Key Inheritance Benefits



Reduces the need for duplicative and redundant direct controls testing that is covered and obtained under a prior valid assessment.



Identifies control mappings and leverages assessment results within one system to efficiently process inheritance information exchange.



Provides the transparency and visibility needed to fully understand and effectively inherit existing controls assessment data.



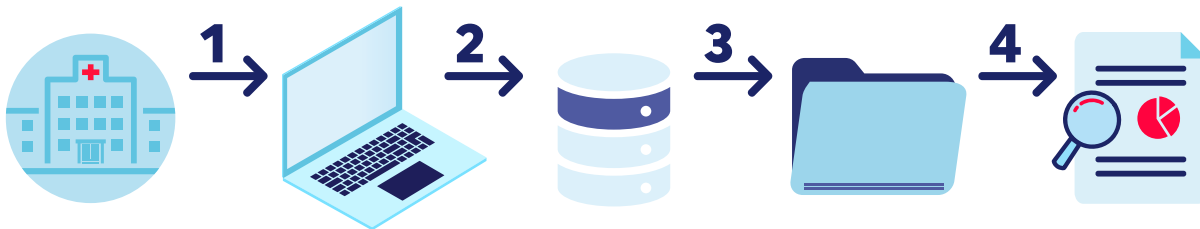
The industry's only inheritance capability for third-party assurances, especially well-suited for shared cloud-based control environments.

The MyCSF platform works in determining what controls are inheritable, validating the applicability of Inheritance requests to the scope of the assessment, orchestrating the exchange, and managing the process. This dramatically reduces the level of effort for all involved. By working with a participating service provider, customers can reduce the required testing and associated costs for inherited controls in a fully automated manner.

With external inheritance, organizations of all sizes and levels now have the ability to leverage cloud platforms to their utmost potential because HITRUST has worked with service providers to accept full or partial responsibility for delivering on many security control objectives on behalf of their customers. This gives customers and service providers a complete understanding of which parties are responsible for which controls.

Results Distribution System (RDS)

RDS makes it possible for assessed entities to share results from their HITRUST assessments securely and electronically with any relying party. Those recipients can then manage and review essential information—such as assessment date, scope, control requirements, scores, corrective action plans (CAPs), and more—using the API (Application Programming Interface) and their own TPRM (Third-party Risk Management) solution. This automation adds efficiency and saves time by eliminating the multiple back-and-forth communications that are common between parties during the annual vendor review process. Whether relying parties manage hundreds or thousands of vendors, RDS delivers game-changing innovation and efficiencies.



Results Distribution System Reliant Party Ecosystem

1. Reliant party requests Assessment Data through API from HITRUST
2. Reliant party granted access to Supplier Assessment Data
3. Reliant party enhances current data in their VRM/TPRM/GRC solution
4. Reliant party manages residual risk associated with entire supply chain through enhancement of supplier assessment data

LOOKING AHEAD

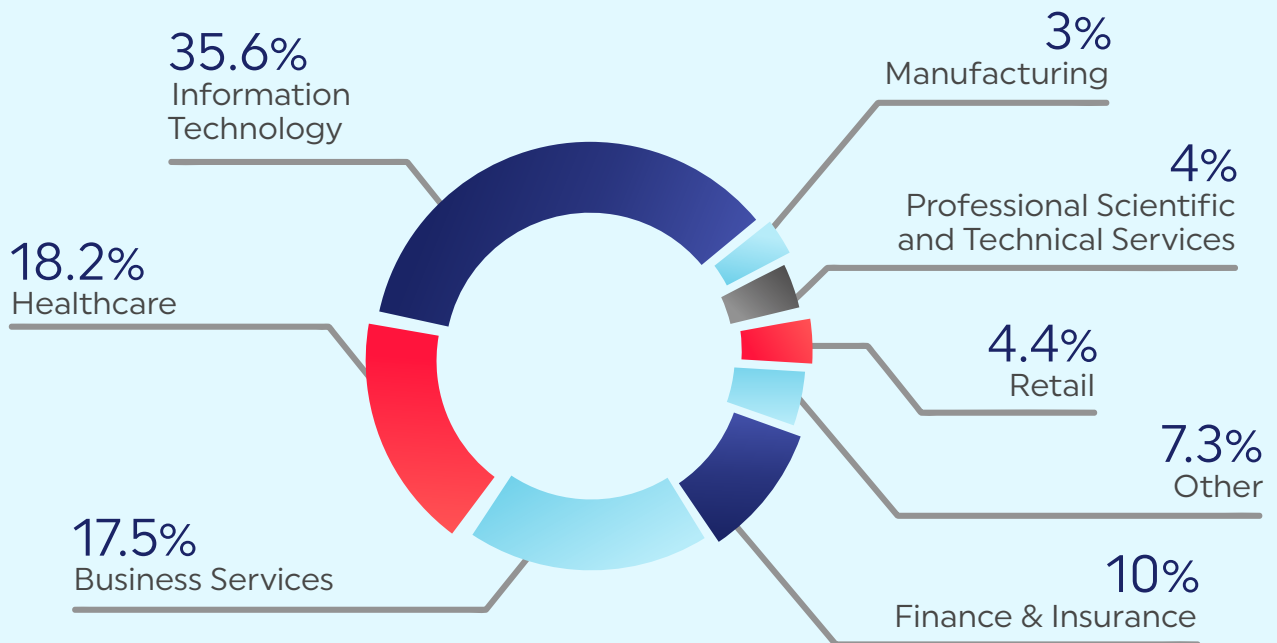


LOOKING AHEAD

Since it was founded in 2007, HITRUST has championed programs that safeguard sensitive information and manage information risk for global organizations across all industries and throughout the third-party supply chain. HITRUST continuously broadens the ability for organizations of all sizes and industries to utilize and benefit from a HITRUST assessment. In 2023, HITRUST noted the top five industry sectors that obtained a HITRUST certification were:

- Information Technology
- Healthcare
- Business Services
- Finance & Insurance
- Retail

2023 HITRUST Certified Organizations by Industry



HITRUST expects to continue to broaden its industry base in 2024 through additional initiatives to enhance the ability for organizations to leverage a HITRUST report.

PLUS Reporting & Insight Reports

In 2024, HITRUST will expand the scope of available validated assessments through the ability to select, or tailor, additional authoritative sources for validation on top of the HITRUST e1 Essentials and HITRUST i1 Implemented assessments. These "e1 PLUS" and "i1 PLUS" reports will expand the e1 and i1 reports with the same tailoring logic used by the HITRUST r2 Risk-based assessment—providing increased flexibility and value for organizations with multiple security and compliance requirements—all with the same transparency, scalability, consistency, accuracy, and integrity provided with all HITRUST assurance reports.

In order to support the new and increased flexibility and relevance available for all HITRUST assurance reports, HITRUST will release a series of Insight Reports throughout 2024. These reports will extend

the Insight Reports concept beyond the three HIPAA Insight Reports available today to a portfolio that allows organizations that have completed e1 PLUS, i1 PLUS, or r2 validated assessments to understand and report on their coverage and conformity with the many authoritative sources available through the HITRUST framework.

The scalability and flexibility of these reports will support customers from many different industries across the globe. All PLUS Reports and Insight Reports will build on the HITRUST pillars of relevance and reliability. These new assurance mechanisms will continue to be backed by an industry leading Quality Assurance Program and the nested approach to assurance reporting that supports an organization's needs both today and throughout their security and compliance journey.

HITRUST Artificial Intelligence (AI) Assurance Program

AI, and more specifically, Generative AI, made popular by OpenAI's ChatGPT, is unleashing a technological wave of innovation with transformative economic and societal potential. Goldman Sachs Research predicts that Generative AI could raise global GDP by **7% over the next 10 years**. Organizations are eager to transform their operations and boost productivity across business functions ranging from customer relationship management (CRM) to software development in order to unlock new layers of value through a growing evolution of enterprise AI use cases. However, any new disruptive technology also inherently delivers new risks, and Generative AI is no different.

AI foundational models now available from cloud service providers and other leading organizations allow organizations to scale AI across industry use cases and specific enterprise needs. But the opaque nature of these deep neural networks introduces data privacy and security challenges that must be met with transparency and accountability. It is critical for organizations offering AI solutions to understand their responsibilities and ensure that they have reliable assurances for their service and solution providers.

As a result, HITRUST is launching the AI Assurance Program: the first and only assurance program

able to demonstrate and enable sharing of security control assurances for Generative AI and other emerging AI model applications.

HITRUST began prioritizing AI Risk Management as a foundational consideration with the release of HITRUST CSF version 11.2 in October 2023. In this release, HITRUST included an "Artificial Intelligence Risk Management" compliance factor which included mappings to the following authoritative sources:

- NIST AI Risk Management Framework (RMF) v1.0,
- ISO/IEC 23894 (AI Risk Management Guidelines), and
- ISO 31000

This provides an important foundation that AI system providers and users can use to consider and identify risks and negative outcomes in their AI systems with regular updates available as new controls and standards are identified and harmonized in the framework and available through HITRUST assurance reports.

HITRUST will add an AI certification so that organizations can address AI risks through a common, reliable, and proven approach.

This will allow organizations that are implementing AI systems and the AI model and service providers to understand the risks associated and reliably demonstrate their adherence with AI risk management principles with the same transparency, consistency, accuracy, and quality available through all HITRUST reports.

AI certifications will be supported on top of the HITRUST e1, i1, and r2 reports. This allows organizations to provide assurances that they have considered risks from their adoption and use of AI while also demonstrating the maturity of the underlying system that supports the AI platform.

HITRUST Compliance Insight Reports will also be available to support organizations that wish to

demonstrate the breadth, coverage, and quality of their AI Risk Management efforts to relying parties, including customers, that are seeking to understand efforts that the organization has undertaken to understand and manage AI risks and to govern their AI systems in a trustworthy, responsible, and reliable manner.

The use of existing and proven HITRUST reports and the HITRUST assurance system will demonstrate that the security of the underlying technology systems supporting the AI system has also been considered including transparency around the identification and documentation of risks, consistency in assessment results, and independent verification and quality assurance of the testing.

“Trustworthy AI requires understanding of how controls are implemented by all parties and shared and a practical, scalable, recognized, and proven approach for an AI system to inherit the right controls from their service providers. We are building AI Assurances on a proven system that will provide the needed scalability and inspire confidence from all relying parties, including regulators, that care about a trustworthy foundation for AI implementations.”

– Robert Booker, HITRUST Chief Strategy Officer



601 Pennsylvania Avenue, NW T 202.778.3200
South Building, Suite 500 F 202.331.7487
Washington, D.C. 20004 ahip.org

**Statement for Hearing on
“Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack”**

House Committee on Energy and Commerce

April 16, 2024

AHIP is the national association that represents health plans that provide coverage services, and solutions for millions of Americans. Collectively, we represent 128 member plans that provide access to health care for over 205 million people covered by employer-sponsored insurance, the individual insurance market, and public programs such as Medicare and Medicaid.

We welcome the opportunity to update policymakers on health plans’ response to the cyberattack on Change Healthcare and what measures can be taken to protect against such attacks in the future.

AHIP and our members share the Committee’s dedication to ensuring that all patients receive access to care without disruption despite cyberattacks like that perpetrated on Change Healthcare earlier this year. We are committed to supporting patients, providers, and the broader health care system during this unprecedented attack on the nation’s health care infrastructure. Health insurance plans invest significant resources and expertise to keep their enrollees’ data safe and secure and to ensure continuity of service in response to cyberattacks or other disruptions to health care information and critical administrative processes. Criminals and nation-state actors, however, are increasingly targeting the U.S. health care system as a critical infrastructure sector. Given the scale and scope of the ongoing cyberattacks, we believe stakeholders and policymakers must work together across the federal government, states, and the health care system to better protect Americans going forward.

AHIP appreciates the House Committee on Energy and Commerce’s efforts to consider what steps could be taken to better secure the nation’s health care system. AHIP’s members work every day to ensure that Americans have access to high-quality, affordable care, which could be disrupted by cybersecurity attacks on any of the various components of the health care sector. We look forward to working with the Committee and other stakeholders to support a strong, secure, and resilient health system that ensures high quality and affordable care.

Health Plan Impact and Response

Proactive Cybersecurity Protections

Protecting the privacy, security, and cybersecurity of consumer data is a top priority for our industry, as articulated by AHIP’s Board of Directors and the Chief Medical Officers of our

members.^{1,2} Health plans employ physical, technical, and administrative safeguards to protect members' personal information. These security practices are multi-dimensional and frequently incorporate existing guidance, industry practices, vendor and software recommendations, legal and regulatory requirements, practical experiences, and a host of physical, technical, and administrative features that are built into systems architecture, policies, procedures, and business practices.

Our members remain steadfast in protecting the consumers they serve and diligently work to stay ahead of trends as they face these real-life situations and potential consequences. Health plans employ a variety of tools, depending on the environment, to ensure security practices are in use through various lines of defense, including but not limited to ongoing risk management assessment and analyses, internal audits, standards controls, and ongoing risk assessments. The National Institute of Standards and Technology (NIST) cybersecurity framework provides foundational guidance and serves as the basis for the Department of Health and Human Services's (HHS) cybersecurity goals. In addition to private sector cybersecurity programs and certifications offered by HITRUST, the Electronic Health Network Accreditation Commission (EHNAC), MITRE ATTACK, and others help protect and align industry practices.

Response to the Change Healthcare Cyberattack

The cyberattack on Change Healthcare had and continues to have a significant impact on the U.S. health care system. However, the specific scale and scope of an individual organization's disruption was and continues to be highly dependent on whether the health plan and its provider partners were customers of Change Healthcare and, if so, which services they utilized. Upon learning of the breach, AHIP's affected members took immediate steps to sever connections to impacted Change Healthcare applications, assess impacts to their business processes, implement business continuity plans, and begin notifying network providers. Broadly, the business processes that members reported being impacted and for which alternatives have been implemented include:

- Enrollment,
- Eligibility,
- Prior authorization,
- Claims processing,
- Generation of Explanation of Benefits,
- Chart abstraction, and
- Quality measurement submission.

Based on the degree of disruption and information available at the time, AHIP members prioritized temporary workarounds, implemented alternative solutions, and created tailored assistance programs for their provider partners to ensure patients continue to have access to the medical care and prescriptions they need. Our members reported that patient issues were limited

¹ <https://www.ahip.org/resources/ahip-chief-medical-officers-roadmap-for-protecting-americans-privacy-confidentiality-and-cybersecurity-of-health-information-and-data>

² <https://www.ahip.org/resources/ahip-board-of-directors-guiding-priorities-for-protecting-americans-privacy-confidentiality-and-cybersecurity-of-health-information-and-data-2>

to the first few days. Health plans took decisive action based on contingency plans that were highly customized to their situations and that of individual provider partners such as:

- Increasing call center staff and providing up-to-date guidance on how to assist consumers and providers;
- Hastening the processing of electronic claims that were received prior to the outage to enhance provider cash flow;
- Clearing existing paper claim loads to both enhance provider cash flow and prepare to be ready to accept an influx of new paper claims;
- Re-routing patient eligibility checks via phone;
- Accepting prior authorization requests when impacted through phone, fax, and electronic portals;
- Educating providers on the situation, alternative options, and how plans could help;
- Connecting to new clearinghouses and claim payment services while assisting providers that were doing the same; and
- Providing targeted advance payments to providers for whom cash flow is problematic.

From March 25 - April 10, 2024, AHIP conducted a member survey on the Change Healthcare cybersecurity incident. Responses were provided by health plans with a total major medical enrollment of 143 million lives. As of April 10, 94% of medical claims and 99.3% of pharmacy claims were flowing compared to what they would expect to receive under normal operations. The claims volume is expected to continue to improve over time as systems get fully up and running. For example, additional systems have come online since that survey was conducted. Thirteen percent of respondents indicated their prior authorization processes had been impacted. Of those, 100% of impacted respondents indicated their organizations temporarily waived or modified their prior authorization requirements following the cybersecurity incident.

We are encouraged by the progress being made and are committed to doing our part until the final stage of recovery is complete – and then to collaborating with policymakers and stakeholders to both prevent and prepare for future cyberattacks. All involved should focus on completing the “last mile” of recovery and on taking the actions needed to protect the system and patients in the future. We are looking ahead to what can be done to protect the system from widespread disruption, such as establishing clearer lines of communication across the private and public sectors. Steps also need to be taken to create resiliency and redundancy in operations to ensure an attack on a single entity does not disrupt the entire system.

As our members have consistently demonstrated, we remain focused on serving patients and provider partners to fully restore operations as well as maintaining clear lines of communication across the private and public sectors. The cyberattack on Change Healthcare reinforced the interconnectedness of the health system and the importance of robust cybersecurity emergency preparedness and business continuity planning. It is vital that all stakeholders – health plans, physicians, facilities, pharmacies, and others – adapt, prepare, and invest in the capabilities to minimize disruptions in the first place and to respond quickly in the face of disruptions when they occur so that we can work together to maintain a resilient health care system for patients.

Policy Changes to Boost Health Care Sector Response and Resilience

AHIP and our members have identified specific areas for which Congress can support the health care sector through additional policy, direction to federal agencies, and target support. In addition, our industry welcomes the opportunity to work with the Committee to promote a more secure health care system to prevent and respond to cyber incidents.

Comprehensive Approach

AHIP supports a comprehensive approach to cybersecurity. This approach should include collaboration with private sector stakeholders and coordination across federal government agencies in the education, emergency preparedness planning, mitigation, and response phases of a cybersecurity incident. Effective and timely responses can include the need for federal health care programs to provide emergency relief and authority for extensions and adjustments to timelines for statutory and regulatory measurement and reporting requirements. Waiver authority is often used to provide flexibility in public health and other emergency situations.

We appreciate the Department of Justice (DOJ) and Federal Trade Commission (FTC) statement on the antitrust treatment of cyber information sharing. We believe there are additional steps these agencies could take to support timely and efficient responses to such large-scale and widespread attacks.³ The nature of responding to such attacks inevitably involves forward planning, as participants work to remedy the attack and avoid similar attacks in the future. The mere possibility that working together with other entities could be construed as impermissible sharing of future business plans can chill this urgent work when timely sharing of information is vital. While a framework of analysis provided is useful, when dealing with an ongoing cyberattack it is challenging, and time consuming, to apply that framework to an ongoing situation in a manner that makes entities comfortable with risk. We recommend that the agencies provide more specific guidance and assurances to entities that their good faith efforts to deal with cyber issues will not raise antitrust risks. Minutes matter in responding to a cyberattack, and it is critical that the agencies reduce the time that is spent addressing potential antitrust risk for responsive efforts. We concur with the Health Care and Public Health Sector Coordinating Council's (HSCC) recommendation in its Cybersecurity Strategic Plan that a temporary reduction in regulatory or legal barriers (real or perceived) such as antitrust, Stark law, Anti-Kickback Statute, liability concerns, etc., under such emergency circumstances would support health sector peer support for cybersecurity incident response.⁴

Recommendations:

- Congress should consider legislation that would permit the Centers for Medicare & Medicaid Services and other agencies to temporarily waive statutory requirements to ensure that sufficient health care items and services are available to meet the needs of affected patients during large-scale cybersecurity events.
- Congress should consider potential policies to support smaller and less well-resourced providers and health delivery systems in efforts to ensure robust protections and planning. Potential options include federal funding for cybersecurity capabilities, the

³ <https://www.justice.gov/opa/pr/justice-department-federal-trade-commission-issue-antitrust-policy-statement-sharing#:~:text=The%20Department%20of%20Justice%20and,nation's%20networks%20of%20information%20and>

⁴ <https://healthsectorcouncil.org/wp-content/uploads/2024/02/Health-Industry-Cybersecurity-Strategic-Plan-2024-2029.pdf>

replacement of obsolete technologies, and promoting additional education, awareness, and continuity planning.

- Congress should direct the Department of Justice and the Federal Trade Commission to update the Antitrust Policy Statement on Sharing of Cybersecurity Information to reduce antitrust obstacles to effective responses to cyberattacks, including by more clearly permitting information sharing during cyberattacks.

Streamlining Reporting Requirements to Benefit Enrollees and Focus Resources

Congress can also further work with appropriate federal agencies to improve and streamline the cyber incident reporting process and avoid duplicative reporting requirements. Health care entities covered under HIPAA are required to notify the HHS Office for Civil Rights (OCR), consumers, and the media in the event of a significant cyber data breach. Navigating the applicable reporting requirements will be complex, as Change Healthcare served as both a HIPAA Covered Entity in its role as a clearinghouse and a HIPAA Business Associate in providing a range of technology applications (e.g., HEDIS reporting, analytics for value-based payment contracts, electronic prescribing tools, etc.). Such entities are often also required to report such incidents under state law. Yet, the Department of Homeland Security (DHS) Notice of Proposed Rulemaking on Cyber Incident Reporting for Critical Infrastructure Act would require additional reporting for most health care organizations as critical infrastructure sector entities. AHIP and its member plans are committed to ensuring that timely incident reporting and breach notification protocols are in place when a cyberattack occurs.

Recommendation:

- Congress should work with OCR to streamline reporting for this large-scale event to conserve resources and ensure consumers do not get confusing duplicative notifications.
- Congress should consider changes to the Cyber Incident Reporting for Critical Infrastructure Act to streamline reporting for HIPAA covered entities, making the HIPAA Privacy and Security Rules the central source of requirements for covered entities.

Enhanced Sector Support Through Information Sharing and Resources

While there is existing law that directly addresses the interaction of the federal government and the health care industry (Section 405 of the Cybersecurity Act of 2015), this law is due for updating to reflect the current cybersecurity environment. Congress should consider the next iteration of education, resources, and support, including for rapid and on-going incident response, needed to assist health care organizations in navigating an increasingly hostile cyber threat environment.

AHIP is an active participant in the Health Care and Public Health Sector Coordinating Council's (HSCC) Cyber Working Group (CWG), recognized by HHS as the critical infrastructure industry partner for coordinating strategic, policy, and operational approaches to prepare for, respond to, and recover from significant cyberattacks. Through the CWG, AHIP engages in key initiatives to ensure the health care sector has access to resources, best practices,

and opportunities to engage with key decision makers from across the federal government.⁵

Efficient and timely cyber incident responses depend on access to real-time, actionable cyber threat information. Generally, cyber threat information is made available through separate communications channels from multiple government and private sector sources including DHS, the Federal Bureau of Investigation (FBI), HHS's Health Sector Cybersecurity Coordination Center (HC3), the Health Information Sharing and Analysis Center (H-ISAC), and independent cybersecurity firms, among others. Based on the experience of the Change Healthcare cyberattack, impacted parties needed more information from the federal cybersecurity agencies and law enforcement and could have benefited from unified communications, including communications to organizations beyond ISAC dues-paying members.

Recommendations:

- Congress should work with HHS to leverage public-private partnerships for information sharing and to design and administer recurring national surveys to measure trends in health sector cybersecurity performance.
- Congress should ensure federal agencies can share certain relevant information with private sector organizations such as the timely dissemination of vulnerabilities, threats, and controls related to emerging technologies, such as artificial intelligence (AI).
- Congress should continue, when engaged in lawmaking, to permit flexibility for health sector entities that would allow for technology-neutral, scalable solutions based on an entity's business operations, risk assessment, available resources, and new developments that promote better detection, response, and remediation.

Workforce Development and Training

The health sector is only as strong and resilient as its workforce. The front line of any cyber defense is the people – the cybersecurity professionals – who are developing the cyber risk management policies, monitoring networks for suspicious activity, interpreting threat intelligence, and making critical, real-time decisions in response to active cyber threats. Cybersecurity professionals also play a critical role in training and upskilling the health care workforce at large to improve cyber hygiene and situational awareness. Staffing shortages throughout the health care industry and rapidly evolving technology only increase the cybersecurity risks to the sector.

Recommendation:

- Congress should consider policies to specifically invest in the cyber health care workforce pipeline, promote cybersecurity-focused education, and utilize existing workforce development programs, such as those administered by the Health Resources and Services Administration.

Policy Changes Promoting Trust in Cybersecurity

Independent Security Attestations

⁵ <https://healthsectorcouncil.org/about/organizational-members/>

Trust plays a foundational role in the restoration process for technology applications impacted by cyberattacks. Once an impacted system goes through a robust process of rebuilding, restoration, and testing, a health care organization will have the option to reconnect that product to their network. During this process, third-party security firms are often retained to assess and provide independent attestations that it is safe for an organization to reconnect. Independent attestations are a critical part of the restoration process as health plans and other impacted health care organizations often need verification to satisfy internal and external security policies and insurance requirements necessary to ensure protection of patient information.

The role of independent security attestations in rebuilding trust and restoring services after a cyberattack should be an area of focus for industry cybersecurity risk management frameworks and guidance.

Recommendation:

- Congress should consider policies moving forward to ensure third-party attestations are part of cybersecurity standards for large-scale events.

Patient Trust

Cyberattacks on health care organizations have grown significantly as the sector has become increasingly digital, automated, and connected through digital health technologies, next-generation medical devices, third-party health applications, and other mechanisms by which data moves outside the four walls of traditional health care data holders, such as those covered under the HIPAA Privacy and Security Rules. With that in mind, a health care system in which data flows seamlessly where it is needed would better coordinate care, improve health outcomes, and reduce costs.

This goal is predicated on patients trusting that their information will be safeguarded no matter who holds the data. As we have seen with this event, even the highly regulated health care industry faces challenges with this, let alone the countless organizations that hold health care data but are not subject to the HIPAA privacy and security rules.

Recommendation:

- Congress should fill the gap in the national privacy framework with a comprehensive solution that preempts duplicative state privacy laws, including with respect to oversight of entities outside of HIPAA.

Advancing Interoperability

After the cyberattack on Change Healthcare, AHIP health plan members worked to identify alternate technology solutions that could be deployed to mitigate disruptions in claims processing, enrollment, eligibility determinations, clinical authorizations, and other services. This required a patchwork of solutions with varying implementation timelines guided by legal and data use agreements that facilitated the rerouting of data through new systems. These legal and data use agreements served as a rudimentary “trusted exchange.”

As directed in the 21st Century Cures Act, the Office of the National Coordinator for Health IT has developed a Trusted Exchange Framework and Common Agreement (TEFCA) intended to scale health information exchange nationwide. TEFCA has the potential to create efficiencies and simplify connectivity by establishing standardized rules and technical approaches to exchange under one Common Agreement.

As the health sector reflects on lessons learned after the cyberattack on Change Healthcare, and strategies to improve future cyber incident response, TEFCA presents a promising opportunity to utilize an established trust framework to efficiently (and rapidly) implement technology alternatives where and when necessary, based on an existing agreement. Utilizing TEFCA to reroute data to alternative solutions in the event of a cyberattack would support the critical need for redundancies in business continuity planning. However, TEFCA is currently primarily focused on provider exchange and not health plans.

Recommendation:

- Congress should work with the Office of the National Coordinator (ONC) to ensure that use cases are created that provide value to health plans and include standard operating procedures that would enable rerouting of data connections in the event of a cyberattack or other emergency.

Conclusion

AHIP and our members remain in close contact with federal and state government officials and health care stakeholder groups throughout this ongoing incident. While significant progress has been made to mitigate the impacts of this cyberattack, health plans remain committed to supporting providers, particularly small and independent providers, still dealing with these last effects of response and recovery.

AHIP looks forwards to working with the Committee to improve the health sector's resilience and strengthen against any future cyberattacks.



750 9th Street NW
Washington, D.C. 20001-4524
202.626.4800
www.BCBS.com

Statement for the Record
Submitted to U.S. House Committee on Energy and Commerce
Subcommittee on Health
“Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack”
April 16, 2024
By: David Merritt, Senior Vice President of Policy and Advocacy

The Blue Cross Blue Shield Association (BCBSA) believes everyone should have access to affordable health care, no matter who you are or where you live. We commend Chairman Brett Guthrie and Ranking Member Anna Eshoo for holding this important hearing to examine cybersecurity in the health care sector.

BCBSA is a national federation of independent, community-based and locally operated Blue Cross and Blue Shield (BCBS) companies (Plans). Our Plans collectively cover, serve and support 1 in 3 Americans in every ZIP code across all 50 states, Puerto Rico and Washington, D.C. BCBS Plans contract with 96% of hospitals and 95% of doctors across the country and serve those who are covered through Medicare, Medicaid, an employer or purchase coverage on their own.

The Change Healthcare cyberattack caused significant disruption for the entire health care industry, including patients, health care providers and health plans that rely on Change Healthcare for claims processing and other functions. The security of patients’ data is a critical priority. BCBS Plans acted quickly to disconnect from Change Healthcare systems, monitor their own systems to verify that the attack was isolated to Change and support our patients and provider partners. The impact of this attack has not been uniform across the country, depending on the size, service locations, financial health of providers and reliance on Change Healthcare’s technology. In some states, service areas and lines of business, there has been little disruption to patients or providers, while in others the consequences were felt much more.

We understand the consequences this disruption has caused many health care providers. Their ability to deliver care is essential for BCBS Plans to fulfill our core mission of ensuring affordable access to high-quality health care for the 1 in 3 Americans we serve. That’s why BCBS Plans across the country took immediate action to support our provider partners in need by:

- Facilitating the transition from Change Healthcare to nearly 50 different alternative

clearinghouses and local claims submission portals, working closely with providers — including direct support with multiple IT departments — to get processes back up and running as quickly as possible.

- Proactively educating and reaching out to those providers that had not filed claims nor had been reimbursed so they knew we were there to help.
- Providing advanced payments and other flexibilities so those impacted providers without reserves or limited cash on hand would have the revenue they need to continue to deliver quality care.

Our data shows that these actions have made a difference. With limited exceptions, claims volumes for BCBS Plans across the country are above, at or near normal levels for all lines of business. Claims are being efficiently processed and adjudicated, with no Blue Plan reporting delays or backlogs due to Change Healthcare. That means that the overwhelming majority of BCBS network providers are providing care, filing claims and being reimbursed.

Experience on the ground confirms this as well. Few providers have asked for advanced payments, filing extensions or additional flexibilities. This progress does not diminish the needs of the providers that still face challenges. When they do, BCBS Plans are assisting. We continue to prioritize outreach, engagement and support for any network provider in need and remain committed to helping providers affected by Change Healthcare solve their challenges.

In addition to partnering on claims processing and payment, another critical priority that payers and providers share is strong, independent attestations that Change Healthcare's systems and environments are safe and secure. While some BCBS Plans are in the process of reconnecting to individual Change applications, others are not — citing a lack of engagement or direction from Change Healthcare as well as the lack of detailed, independent attestations that each system they bring back online is safe for reconnection. For those that are reconnecting to the limited applications that Change Healthcare has brought back online, BCBS Plans are closely monitoring progress, particularly for backlogged or duplicate claims that have since been paid through alternative processing solutions.

Another critical component of this incident is the privacy of patient data. At this time, we do not have any information from Change as to the extent of any Blue member information being impacted. As we wait for Change to disclose more details on the scope of the impacted data, it is important to note that under the current notification rules, there is the real potential that patients could become inundated with conflicting information, confusing updates and multiple notifications. That is the likely result if they were to receive numerous notifications from the many entities that were likely affected, including Change, care providers, payers, pharmacies and the many other companies that health care stakeholders partner with. If notifications are done the wrong way, individuals could receive multiple notifications, leaving them confused, burdened and/or immune to the information. If done the right way, patients will be notified in a streamlined, effective and easy-to-understand manner. It is critical that Change and regulators work closely together to clearly define notification obligations in a way that limits the potential for additional

disruption.

This incident is a clear call for everyone in health care to take the necessary steps to strengthen their security so that we are collectively better prepared and protected against future attacks. We are evaluating steps that could be taken to improve communication across the private and public sectors and create resiliency and redundancy in operations. If done properly across the industry, we can be more confident that an attack on a single entity does not create mass disruption for the entire system.

More broadly, BCBSA and BCBS companies embrace the goals of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCA) to ensure that significant cyber incidents are reported in a timely and meaningful fashion and that relevant cyber intelligence is broadly shared. These steps are foundational to being able to react and respond as effectively as possible, reducing disruptions and protecting patients. As we work with regulators on the implementation of this law, we hope the rules will reflect the unique needs of the health care sector and build on the established regulatory structures and mature information-sharing institutions and practices that have been developed over many years. The harmonization with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and other foundational privacy, security and data sharing requirements is essential to the effective evolution of cybersecurity in health care.

Conclusion

We appreciate your leadership and partnership to address cybersecurity challenges so that we are all better prepared and protected from future threats. If you have any questions or would like additional information, please contact me or Keysha Brooks-Coley, vice president of advocacy, at [REDACTED].

David Merritt



Senior Vice President, Policy & Advocacy
Blue Cross Blue Shield Association



President and CEO

Charles N. Kahn III

**STATEMENT
of the
Federation of American Hospitals
to the
U.S. House of Representatives
Committee on Energy and Commerce
Subcommittee on Health
Re: “Examining Health Sector Cybersecurity in the Wake of the Change Healthcare
Attack”
April 16, 2024**

The Federation of American Hospitals (FAH) submits the following statement for the record in advance of the House Committee on Energy and Commerce Subcommittee on Health’s hearing entitled “Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack.” We appreciate the Committee’s attention to this critical issue and its efforts to address the cybersecurity challenges facing the healthcare sector.

The FAH is the national representative of more than 1,000 leading tax-paying hospitals and health systems throughout the United States. FAH members provide patients and communities with access to high-quality, affordable care in both urban and rural areas across 46 states, plus Washington, DC and Puerto Rico. Our members include teaching, acute, inpatient rehabilitation, behavioral health, and long-term care hospitals and provide a wide range of inpatient, ambulatory, post-acute, emergency, children’s, and cancer services. Tax-paying hospitals account for approximately 20 percent of community hospitals nationally.

The Change Healthcare cyberattack paralyzed a core engine of our healthcare system and disrupted critical electronic connections between patients, providers, and insurance companies. Despite this, hospitals and healthcare providers have continued to provide high-quality care 24/7/365 to all patients who come through our doors. The FAH believes cybersecurity is a shared responsibility and efforts to combat future cyberattacks should prioritize safeguarding patient data, protecting scarce hospital resources, and ensuring patient access to health care services.

Ongoing Impact of Change Healthcare Cyberattack

Providers continue to grapple with the profound repercussions of the Change Healthcare cyberattack. Hospitals have worked diligently to find workarounds using alternative clearinghouses to submit claims to insurers and replace other critical lost functions. Even with these efforts, the restoration of the normal flow of claims submission, receipt of payment, and resolution of claim rejections and denials will take months. The complexities of adjusting to a new clearinghouse leads to significantly higher rates of claim rejections and denials. As rejections and denials proliferate, the burden falls on providers to identify for each claim the specific reason for the rejection/denial, communicate with the

insurer, and re-bill the claim and/or appeal it in a timely manner. These factors all amount to additional burdens on providers already struggling to adapt and already operating on strained resources.

As the health care system navigates the aftermath of the attack, the focus must be on supporting providers as they work through the administrative backlog and recover from financial strains caused by this unprecedented attack. Insurers must also be held accountable for ensuring timely payments and reducing administrative burdens, such as temporary suspension of requirements for prior authorization, timely filing, and appeals deadlines to facilitate recovery.

Increasing Cybersecurity

The FAH recognizes the critical importance of cybersecurity in healthcare delivery. FAH members are committed to protecting patient data and ensuring the integrity of healthcare services. Challenges persist in the face of evolving cyber threats and no organization, including the federal government, has immunity from cyberattacks. The FAH believes that any effort to enhance cybersecurity in the healthcare sector should prioritize preserving patients' access to care.

Hospitals are leaders in proactive cybersecurity efforts. In fact, according to the 2023 Department of Health and Human Services (HHS) Hospital Resiliency Landscape Analysis, hospitals' cybersecurity measures include encryption mechanisms, consumption of threat intelligence from other organizations, 24/7/365 security operations and incident response centers, vendor risk assessments, segmentation of medical devices on specialized network segments, comprehensive access management, regular system updates to mitigate risks of data breaches and cyberattacks, and other activities.¹

Increased cybersecurity standards should not impose burdensome mandates on hospitals or fail to consider the shared responsibility of cybersecurity and address system-wide vulnerabilities. Instead, efforts should encourage collaboration between hospitals, government agencies, and other entities to develop innovative cybersecurity solutions which promote shared learning, resource pooling, and proactive threat mitigation strategies.

The FAH stands ready to collaborate on advancing cybersecurity policies that uphold patient care and provider resilience. We thank you for your focus on the Change Healthcare cyberattack and look forward to working with the Committee on these critical issues.

¹ United States Department of Health and Human Services. (n.d.). Hospital cyber resiliency initiative landscape analysis. Hospital Resiliency Landscape Analysis. <https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf>



HEALTHCARE LEADERSHIP COUNCIL

April 16, 2024

The Honorable Brett Guthrie
Chairman
Energy and Commerce Committee
Subcommittee on Health
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Anna Eshoo
Ranking Member
Energy and Commerce Committee
Subcommittee on Health
U.S. House of Representatives
Washington, D.C. 20515

RE: April 16th “Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack” Hearing

Dear Chair Guthrie and Ranking Member Eshoo:

The Healthcare Leadership Council (HLC) thanks you and other members of the U.S. House Energy and Commerce Committee’s Health Subcommittee for holding the hearing, “Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack.” Recent events have brought much needed attention to the risks at stake as the healthcare sector defends itself from an unprecedented number of ransomware and other cybersecurity attacks. Criminals who attack one segment of the healthcare sector cause cross-sector disruption and jeopardize patient safety. These bad actors require a unified and strong industry wide response, and our members are committed to collectively safeguarding patients and protecting their data.

HLC is a coalition of chief executives from all disciplines within American healthcare. It is the exclusive forum for the nation’s healthcare leaders to jointly develop policies, plans, and programs to achieve their vision of a 21st century healthcare system that makes affordable high-quality care accessible to all Americans. Members of HLC – hospitals, academic health centers, health plans, pharmaceutical companies, medical device manufacturers, laboratories, biotech firms, health product distributors, post-acute care providers, homecare providers, group purchasing organizations, and information technology companies – advocate for measures to increase the quality and efficiency of healthcare through a patient-centered approach.

The Administration took swift action to help mitigate the impact of the Change Healthcare cyberattack by accelerating payments to Medicare Part A providers and announcing Medicare Part B advanced payments. However, the impact on providers, payers and patients remains significant. As the frequency of healthcare data breaches continues to increase at a staggering rate, already doubling over the last five years to more than 720 breaks annually, a standard predictable response would ensure that patients can continue to receive the necessary care, and physicians are able to be compensated, even when systems are compromised.¹

¹ See <https://www.hipaajournal.com/security-breaches-in-healthcare/>

Congress and federal agencies must focus further cybersecurity efforts on actions that will offer clear guidance and needed support, rather than punishing legally operating businesses victimized by criminal bad actors. While organizations that violate HIPAA or mismanage data should be held accountable, vilifying healthcare companies compromised by a security hack will only further stress critical infrastructure. We have identified the following areas that are ripe for government action:

- Ransomware Response – Healthcare organizations need guidance when facing ransomware attacks, including recommendations for appropriate responses. While the FBI advises not paying, there are often life-threatening consequences that result from such a stance which necessitate additional consideration.
- Data Breaches and Protections – Congress should consider expanding the protections established under the January 2020 HITECH Act, to offer organizations that implement a comprehensive cybersecurity program full safe harbor protection in the event of cyber incidents beyond their control. This will encourage disclosure and mutual support, a far more constructive and effective mechanism for combatting cyberattacks in the healthcare sector than the current public reporting process.
- Leadership and Coordination – There are many organizations and officials whose duties and missions involve health sector cybersecurity at some level including the Healthcare Sector Cybersecurity Coordinated Center, the Health Sector Coordination Council, and the Office of the National Cyber Director. While there is clearly a great deal of constructive activity and focus on cybersecurity among all these groups, their overlapping roles and the lack of a single dedicated office focused on health sector cybersecurity issues will slow progress in an area, and during a time, when exactly the opposite is needed.

Given the complex challenges of not only preparing for but responding to cybersecurity incidents, we emphasize again that overall supportive efforts will encourage stakeholders to improve their cyber readiness. Companies need to be bolstered to better respond to threats.

We recognize the challenges in developing legislation on this important topic and stand ready to assist in any way we can. Please contact Katie Mahoney at [REDACTED] or [REDACTED] if you have any questions or would like additional information.

Sincerely,



Maria Ghazal
President & CEO



April 16, 2024

The Honorable Brett Guthrie
Chairman
Subcommittee on Health
Committee on Energy and Commerce
U.S. House of Representatives
2123 Rayburn House Office Building
Washington, DC 20215

The Honorable Anna Eshoo
Ranking Member
Subcommittee on Health
Committee on Energy and Commerce
U.S. House of Representatives
2123 Rayburn House Office Building
Washington, DC 20215

Re: MGMA Statement for the Record — House Committee on Energy and Commerce Hearing, “Examining Health Sector Cybersecurity in the wake of the Change Healthcare Attack”

Dear Chairman Guthrie and Ranking Member Eshoo:

The Medical Group Management Association (MGMA) thanks you for holding this important hearing examining health sector cybersecurity in the wake of the Change Healthcare attack. MGMA members were significantly impacted by the cyberattack and continue to deal with the fallout. We appreciate the Committee reviewing how this caused so much disruption to our nation’s health system and examining policies to help mitigate future cyberattacks.

With a membership of more than 60,000 medical practice administrators, executives, and leaders, MGMA represents more than 15,000 group medical practices ranging from small private medical practices to large national health systems, representing more than 350,000 physicians. MGMA’s diverse membership uniquely situates us to offer the following policy recommendations.

On Feb. 21, Change Healthcare experienced a cyberattack that critically impacted the U.S. healthcare system, causing unprecedented outages. Change Healthcare touches one in three patient records and processes 15 billion healthcare transactions annually.¹ With one corporate entity providing so many services to such a wide swath of the nation’s healthcare ecosystem, the disruptions caused by the malicious cyberattack resulted in substantial harm.

Impact of the Change Healthcare cyberattack on medical groups

Given the breadth of services Change Healthcare offers, MGMA members felt myriad negative consequences following the cyberattack, including: severe billing and cash flow disruptions, inability to submit claims, limited or no electronic remittance advice (ERA) from health plans, electronic prescriptions could not be transmitted, lack of connectivity to data infrastructure, health information technology disruptions, and much more. Physician practices diligently instituted workarounds for various

¹ Department of Health and Human Services, [Letter to Health Care Leaders on Cyberattack on Change Healthcare](#), March 10, 2024.

processes to remain operational, which required significant labor costs and time to institute, diverting critical resources from patient care.

The lack of cash flow that resulted from the Change Healthcare attack led to medical groups having to make difficult financial decisions as it was early in the year and practices already had limited working capital on hand due to tax considerations. Smaller practices were particularly affected given their tight margins and had to utilize lines of credit with high interest rates just to keep their doors open. Practices have had to make drastic payroll decisions in the wake of the attack; one MGMA member's statement to CNN sums up the gravity of the situation: "We are hemorrhaging money, this will probably be the last week we can keep everybody on full time without having to do something."²

While some of Change Healthcare's systems have come back online, effects of the attack still remain — there's an extensive backlog of claims being processed, some groups are still not receiving ERAs impacting their ability to reconcile claims, many payers are have not reconnected to Change Healthcare's systems, and practices are still utilizing resource-intensive workarounds. Further, we still do not know the full extent of the cyberattack as both Change Healthcare and law enforcement authorities are investigating a potential data breach. In totality, the Change Healthcare cyberattack continues to ripple throughout this nation's health system.

Federal response and policy considerations to support physician practices

As the scope of the cyberattack became apparent, MGMA wrote to the Department of Health and Human Services (HHS) on Feb. 28 expressing the severity of its impact to medical groups and advocating for the agency to use all tools at its disposal to mitigate the damage.³ Thankfully, HHS instituted numerous flexibilities in response and offered accelerated and advanced payments to hospitals and providers to help mitigate the consequences from the cyberattack. We appreciate the Department heeding our call and swiftly acting to assist practices.

The cyberattack on Change Healthcare made it evident that there are significant vulnerabilities in our healthcare system, which must be addressed — especially as the threat of such attacks only continues to rise. **Moving forward, health plans, clearinghouses, and other third-party vendors must have safeguards and contingency plans in place to better protect physician practices from such significant cash flow and administrative impacts resulting from a cyber incident.**

The Committee should examine whether further authorities and flexibilities should be granted to federal agencies responding to future attacks to support physician practices. Specifically, the Committee should ensure that the statute governing advanced payments to Part B providers allows for a quick response time from HHS to a future attack, and that repayment terms are not onerous, adding another stressor during a time of acute uncertainty. Additionally, the Committee should review whether other policies should be introduced such as waiving timely filing requirements for health plans, reducing prior authorization burden, and relaxing other requirements as it may be impossible to fulfill them with such widespread outages. This would be a significant step to allow practices to function with a semblance of efficiency during a cyberattack of this size.

² Sean Lyngaas, CNN, "[‘We’re hemorrhaging money’: US health clinics try to stay open after unprecedented attack](#)," March 9, 2024.

³ MGMA, [Letter to CMS on Change Healthcare Cybersecurity Attack](#), Feb. 28, 2024.

Physician practices must continue to work to ensure they have adopted ironclad cybersecurity policies and procedures to best protect the data of their patients and their ability to provide high-quality care. When contemplating the fallout, we urge against establishing penalties, or conditioning relief funds, for medical groups in response to cyberattacks perpetuated against other healthcare actors. There are a multitude of security and data privacy regulations governing medical groups; introducing barriers to future relief would work against supporting medical groups' ability to operate in the face of considerable interruption.

It is important to note that physician practices have access to widely different levels of cybersecurity resources depending on their size. The President's budget acknowledged the need to bolster cybersecurity resources within the healthcare sector, allocating \$800 million to assist "high-need, low-resourced" hospitals to help implement cybersecurity practices.⁴ The budget also proposed \$500 million for an incentive program for advanced cybersecurity practices for hospitals. **Ensuring that all physician practices are afforded resources similar to those proposed for hospitals is critical.** We support practices incorporating voluntary cybersecurity goals, like those recently published by HHS, to bolster their defenses against future attacks.

These are sophisticated criminal cyberattacks often sponsored by nation states that are not only impacting healthcare but many other industries in addition to federal, state, and local governments. **Exacerbating a terrible situation by adding further penalties to medical groups beyond what is already in place would be overly punitive for practices not responsible for the attack and operating in full compliance.** Resources should be devoted to law enforcement agencies to bolster their actions to combat these cyberattacks and prevent them before they begin. Our nation's law enforcement agencies have the expertise and training to stop these criminals — we should ensure they have every resource necessary at their disposal.

Conclusion

MGMA looks forward to working with the Committee to reinforce the resiliency of the cybersecurity defenses for this nation's health system. It is critical to ensure physician practices can continue providing high-quality patient care in the face of substantial disruptions. If you have any questions, please contact James Haynes, Associate Director of Government Affairs, at [REDACTED] or [REDACTED].

Sincerely,

/s/

Anders Gilberg
Senior Vice President, Government Affairs

⁴ Department of Health and Human Services, [Fiscal Year 2025 Budget in Brief](#), pg. 80, March 11, 2024.

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com.

<https://www.wsj.com/business/earnings/unitedhealth-swings-to-1q-loss-on-cyberattack-related-costs-4d0a2497>

BUSINESS | EARNINGS

UnitedHealth Stock Jumps After Earnings Beat Expectations, Despite Cyberattack

Company expects the attack to hit its full-year earnings

By [Anna Wilde Mathews](#) [Follow](#) and [Sabela Ojea](#) [Follow](#)

Updated April 16, 2024 11:26 am ET



The cyberattack struck UnitedHealth's Change Healthcare business. PHOTO: PATRICK SISON/ASSOCIATED PRESS

Investors are breathing a sigh of relief about UnitedHealth Group's **UNH 6.29%** ▲ earnings.

The healthcare giant's first-quarter adjusted earnings topped Wall Street's estimates, despite a cyberattack that will weigh on the healthcare and insurance company's full-year results.

Its shares rose over 6% to above \$474, shortly after the market open. As of Monday's close, the stock was down 15% this year.

In a call with Wall Street analysts, the company aimed to soothe investors' worries about rising medical costs, saying they weren't coming in higher than expected and its Medicare business remains on track.

UnitedHealth **UNH 6.29%** ▲ also stuck with its full-year adjusted earnings guidance.

Shares of UnitedHealth's competitors, including Humana and Elevance, also showed some early morning increases. The company is often seen as a bellwether in the sector.

The cyberattack struck the company's Change Healthcare business, and UnitedHealth is working on restoring services. It expects the attack to hit its full-year earnings by between \$1.15 and \$1.35 a share. It also anticipates direct-response costs of 85 cents to 95 cents a share for the year.

UnitedHealth Chief Executive Andrew Witty said healthcare costs had risen sharply last year, and he attributed the increase largely to an aftereffect of the Covid-19 pandemic. The company said that so far in 2024, healthcare cost patterns are not continuing to spike higher, and they are matching its projections. "Everything looks pretty much as expected," Witty said.

The insurance unit's medical-loss ratio, the share of premiums spent on medical care, was 84.3% in the first quarter. Without the impact of the Change incident, the result was only slightly above a FactSet consensus analyst projection of 83.8%. Due to the Change hack, UnitedHealth suspended many practices that constrain medical-services use, such as requiring authorization for certain types of care.

UnitedHealth said it has restored most Change functionality and is working to retain and win back customers to its offerings. "We're going to bring it back much stronger than it was before," Witty said.

The company updated its 2024 net earnings outlook to \$17.60 to \$18.20 a share to reflect the sale of its Brazil operations and the expected costs of the cyberattack.

For the first quarter, UnitedHealth posted a net loss of \$1.22 billion, or \$1.53 a share, compared with a profit of \$5.77 billion, or \$5.95 a share, for the same

period a year earlier, with results pulled down by a charge related to the sale of the Brazil operation as well as the cyberattack impact.

Stripping out one-time items, UnitedHealth's earnings per share came in at \$6.91. Analysts surveyed by FactSet had forecast adjusted earnings per share of \$6.61.

Revenue climbed 8.6% to \$99.80 billion, beating analysts' expectations of \$99.23 billion, according to FactSet.

Write to Anna Wilde Mathews at Anna.Mathews@wsj.com and Sabela Ojea at sabela.ojea@wsj.com

Videos



STATEMENT
of the
American Medical Association

U.S. House of Representatives
Committee on Energy and Commerce
Subcommittee on Health
“Examining Health Sector Cybersecurity in the Wake of the
Change Healthcare Attack”

April 16, 2024
Division of Legislative Counsel
202-789-7426

Statement for the Record
of the
American Medical Association
to the
Committee on Energy & Commerce
Subcommittee on Health

Re: Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack

April 16, 2024

The American Medical Association (AMA) appreciates the opportunity to submit the following Statement for the Record to the U.S. House of Representatives Committee on Energy and Commerce, Subcommittee on Health, as part of the hearing entitled, “Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack.” The AMA commends the Subcommittee for focusing attention on and exploring solutions to the massive cyberattack on Change Healthcare and the resulting outage that is impacting patients, physicians, hospitals, pharmacies, labs, and countless additional health care professionals, providers, and entities across the country. The AMA has been particularly concerned about the impact of the outage on small and independent physician practices that live financially on the margins and do not have the resources to weather a storm such as this. As such, much of this statement focuses on issues and actions needed to protect the sustainability and solvency of those critical but vulnerable practices.

Although the hackers are ultimately to blame for this breach, the AMA has been disappointed by the response of many of the most resourced players in the health care system to meet the moment thus far, especially in their failure to support physician practices serving small, rural, or underserved communities. We hope that Congressional interest in the actions, or inactions as it may be, of these players will serve to ignite a sense of corporate citizenship in time to help the many physicians in crisis.

I. Impact of Change Healthcare outage on physician practices

Although Change Healthcare was not a well-known entity until recently, it is a health care giant. Even *before* UnitedHealth Group’s (UHG’s) subsidiary Optum purchased Change Healthcare in 2022, the company facilitated over 15 billion health care transactions and approximately \$1.5 trillion in adjudicated claims—more than one-third of all U.S. health care expenditures annually.¹

For many physicians, hospitals, and health insurance companies, Change Healthcare serves as a clearinghouse through which eligibility inquiries are received and responded to, claims are submitted and processed, and remittance is sent back to the physician or health care provider. For

¹ Change Healthcare Annual Report (Form 10-K) for year ended Dec. 31, 2020, available at https://ir.changehealthcare.com/node/7326/html#tx904010_8.

some payers, Change Healthcare even handles the claims payment. Change Healthcare’s importance as the “middleman” transmitting health care claims from physicians and hospitals to insurance companies in the United States cannot be overestimated. But that does not even come close to covering the extent of Change Healthcare’s reach in the health care system. Change Healthcare also plays a role in communicating prescriptions to pharmacies and determining pharmacy, insurance, and patient costs. It facilitates exchanges between physicians, hospitals, and labs—including the ordering of labs and the sending of results. Change Healthcare supports the exchange of information related to prior authorizations (PAs) and other utilization management requirements. And it has products and services that reach into practice management systems and electronic medical record (EMR) systems for dozens of other practice management, clinical, and revenue cycle purposes. And so, when Change Healthcare turned off its systems on February 21 upon news of the cyberattack, the US health care system more or less came to a screeching halt.

Nearly two months later, for most physicians, functionalities dependent upon Change Healthcare systems are still not up and running, at least not completely, and practices continue to try and function without all the Change Healthcare services on which they depended.

Last week, the AMA released informal [survey findings](#)² showing the ongoing, devastating impact of the Change Healthcare outage on physician practices. The survey was conducted from March 26 through April 3 and involved a convenience sample of more than 1,400 respondents.

Claims and process disruptions

Despite assurances from UHG that a large percentage of claims are being submitted and processed, the recent AMA survey data found that practices continue to face disruptions in their ability to submit claims and receive payment on those claims. Thirty-six percent of those who responded reported suspended claim payments, 32 percent are still unable to submit claims, and 22 percent are unable to verify eligibility for benefits.

Additionally, the AMA has heard from physician practices who are unable to obtain electronic remittance advice from health plans, even when they receive payment. In fact, 39 percent of the AMA survey respondents are having trouble obtaining electronic remittance advice. As a result, practices have no ability to reconcile payments with claims and are not able to collect patient cost-sharing (51 percent of survey respondents have lost revenue due to the inability to collect patient co-pays and cost-sharing).

The AMA also received significant feedback related to disruptions in electronic lab ordering. For example, a four-physician maternal-fetal medicine practice serving 45 percent of high-risk pregnancies in New Mexico has been unable to electronically communicate lab orders and results for nearly two months because its electronic clinical system is connected to Change Healthcare. Predictably, the AMA survey shows that practices of 10 or fewer physicians appear to be particularly hard hit.

² <https://www.ama-assn.org/system/files/change-healthcare-survey-results.pdf>.

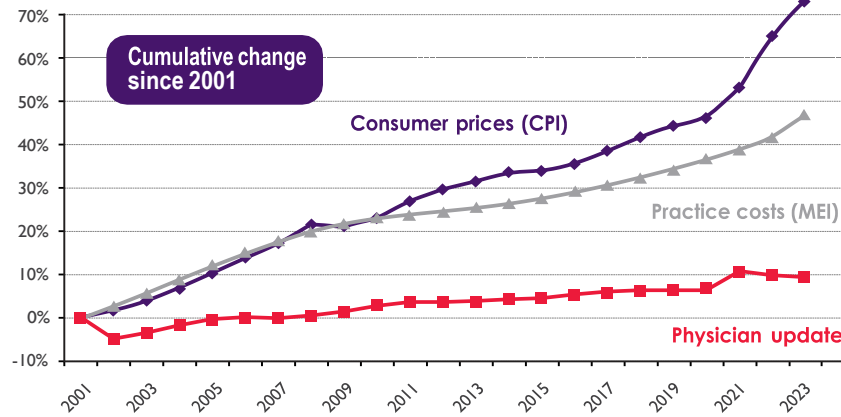
Employment of workarounds and new clearinghouses

Practices are working tirelessly to establish workarounds for the Change Healthcare outage. For example, 31 percent of physicians who responded to our recent survey are using manual and electronic workarounds to simply get paid on claims and to be able to submit claims to payers. As part of these efforts, physician practices are being forced to enter into new and potentially costly arrangements with alternative clearinghouses. Nearly 48 percent of physicians who responded have engaged alternative clearinghouses to conduct electronic transactions, and comments such as “[it is costing] \$10,000 just for the set-up of a ‘back-up’ clearinghouse” were common responses. Unfortunately, we have also received comments that indicate some clearinghouses may be taking advantage of this crisis by increasing costs and extending minimum lengths of contracts, placing further pressure on practice finances.

Physician practice impact

Decreased revenue, along with increased demands on staff, are forcing physician practices to make some difficult financial decisions in response to this system outage. According to the recent AMA survey, 44 percent of respondents were unable to purchase supplies, 31 percent were unable to make payroll, and 85 percent have had to commit additional staff time and resources to complete revenue cycle tasks. For those 80 percent of respondents who have lost revenue from unpaid claims and for claims they still cannot submit, a band-aid solution has been to use personal funds to cover practice expenses (55 percent of respondents) or take out loans to buy supplies, pay their staff, handle overhead costs, and pay their vendors. But the potential long-term impact of this outage is the permanent loss of many small and independent practices that simply will not be able to keep their doors open. The AMA has heard from physicians stating that this crisis “...may bankrupt our practice of 50 years in this rural community...” and “I am now going to get acquired by a hospital system because I just can’t bear the financial responsibility.” The repercussions of this crisis will be felt by communities long after Change Healthcare is back up and running.

The situation with Change Healthcare underscores the fragility of physician practices and the need for Medicare payment reform. According to data from the Medicare Trustees, Medicare physician pay has increased just 9 percent over the last twenty-three years, or 0.4 percent per year on average. Note that the 9 percent includes the temporary 2.93 percent update that expires at the end of this year. In comparison, the cost of running a medical practice increased 54 percent between 2001 and 2024, or 1.9 percent per year. Inflation in the cost of running a medical practice, including increases in physician office rent, employee wages, and professional liability insurance premiums, is measured by the MEI. As a result, Medicare physician pay doesn’t go nearly as far as it used to. As shown in the chart below, when adjusted for inflation in practice costs, Medicare physician pay declined 29 percent from 2001 to 2024, or by 1.5 percent per year on average. Physician practices cannot continue to absorb increasing costs or weather crises such as the Change Healthcare outage while their payment rates dwindle.



Sources: Federal Register, Medicare Trustees' Reports, Bureau of Labor Statistics, Congressional Budget Office.

Concerns for patients

Even against that backdrop of remarkable challenges, only 15 percent of practices who responded to the recent survey have reduced office hours. But physicians are worried about their patients' access to care from being unable to verify and accept patient insurance prior to visits. We stress that the inability to confirm insurance benefits and patient financial responsibility is particularly problematic at this time of year, as many patients have not yet met their out-of-pocket deductible. Physicians also report difficulties in managing prescriptions and completing PAs, processing assistance program discounts, and ordering labs or receiving results. Physician stories such as "...I have one patient that was unable to get her biological for two months as she was unable to afford the cash cost and her disease flared significantly..." are not uncommon.

II. Immediate action needed to support physician practices impacted by outage

Immediate action is needed to assist physicians and their practices in maintaining solvency and keeping their doors open for patients. Assistance should come in the form of advance payments, administrative relief, and a targeted focus on restoring practices' electronic systems.

Financial assistance/advance payments

The AMA has been advocating for immediate and targeted financial relief for physician practices from all payers in the form of advance payments based on claims history. For many physician practices devastated by the Change Healthcare outage, such payments can serve as a lifeline.

The AMA is grateful to the Centers for Medicare & Medicaid Services (CMS) for quickly standing up the Change Healthcare/Optum Payment Disruption (CHOPD) Accelerated Payments to Part A Providers and Advance Payments to Part B Suppliers in March. The AMA also welcomed the March 15 Center for Medicaid & CHIP Services (CMCS) Informational Bulletin (CIB) providing enforcement discretion to allow Medicaid programs to elect a State Plan Amendment (SPA) option for implementation of interim payments to Medicaid fee-for-service providers. It is important to note the particular vulnerability of many physicians who care for Medicaid patients and may not have access to other forms of advance payment while serving

marginalized communities. The AMA continues to urge state Medicaid directors to take advantage of this SPA option, especially given that less than one percent of respondents to the AMA's recent survey answered that they have received advance payments from state Medicaid plans.

Additionally, UHG should be recognized for the significant resources it has put behind its advance payment program. While initially many physicians who applied saw inconsequential amounts being offered and walked away from the program, it is our understanding that UHG's loan program now provides funding not just based on estimates of unpaid UHG claims since the outage, but all insurer claims, to assist struggling practices and hospitals. The AMA is aware of many practices that have been able to keep their doors open to patients because of this assistance.

Disappointingly, we have seen very few other health insurers establish any advance payment or loan programs to help their contracted physicians. According to the recent AMA survey data, only 4.5 percent of respondents have received assistance from commercial health plans other than UHG. To the AMA, that is appalling. During the suspension of claim submission and payment, health plans have retained premium dollars and, in fact, collected interest on those patient, employer, and government payments for up to two months. For companies that make billions of dollars in profit each year and purport to be partners with physicians in patient care to feel no sense of obligation to support our health care system when it is in crisis is unconscionable and a crisis in and of itself. **The AMA asks Congress to urge these commercial payers to provide advance payments to physician practices impacted by the Change Healthcare service outage**, and especially to small, independent practices.

Suspend all PA, quality reporting, and similar administrative requirements

The Change Healthcare outage has impacted the ability of practices to exchange information needed for payer's administrative requirements such as PA and quality reporting. For example, the outage has obstructed both the electronic exchange of PA information between physicians and many health plans and pharmacy benefit managers (PBMs), as well as access to the clinical guidelines used by many payers, making completion of these requirements difficult, if not impossible. Moreover, the outage's impact on pharmacies', labs', and imaging centers' communications has significantly complicated utilization management processes.

Additionally, the Change Healthcare outage has required an "all-hands-on-deck" approach to keep physician practices running and patients being seen. We already know that physicians and their staff spend an average of two working days each week on PAs alone,³ even as these processes threaten patients' access to care.⁴ Always, but especially now, physician and staff time could be much better spent on addressing outage issues and reducing the toll that service disruptions are having on the provision of care, rather than dealing with PA hassles.

For these reasons, we ask that **Congress ensure that all health plans temporarily suspend their utilization management programs and other unnecessary administrative requirements on physician practices.**

Importantly, CMS has extended the 2023 Merit-based Incentive Payment System (MIPS) data submission deadline and is now reopening the 2023 (MIPS) Extreme and Uncontrollable

³ <https://www.ama-assn.org/system/files/prior-authorization-survey.pdf>.

⁴ <https://www.nytimes.com/2024/03/14/opinion/health-insurance-prior-authorization.html>.

Circumstances (EUC) Exception Application to provide relief to clinicians impacted by this cybersecurity incident. The AMA recognizes the relief this will provide to practices and urges other payers to follow with similar administrative relief in their quality reporting programs.

Focus on restoring function for independent physician practices

Certainly, the best solution for many physician practices is to have their Change Healthcare products restored and functioning again. Media reports suggest that for many large systems and hospitals, functionality is returning. However, given member feedback, the AMA fears that small physician practices outside of large systems are not a priority for service restoration. While understanding the reasoning behind prioritizing reconnection of systems that move large claim volumes, the AMA stresses that it is the smaller practices that may not have received advance payments or have the ability to take out loans or dip into personal savings that are now teetering on insolvency. In fact, survey respondents have reported tens of thousands of dollars in unexpected costs to reestablish a portion of their business operations, and even some reporting more than \$100,000. As such, **the AMA asks health plans and policymakers to help ensure that small and independent physician practices are not the last in line when it comes to restoring functionality.**

III. Protections needed for physician practices after outage is resolved

In addition to the immediate relief needed for physician practices, it is imperative that policymakers and health plans establish flexibilities for practices in the months and even years to come following this crisis. Without plans in place to alleviate the burdens and chaos that are bound to ensue as Change Healthcare comes back online and processes resume, the stability of physician practices will remain threatened. Below are examples of a few actions that will help physician practices. The AMA recognizes many more solutions are needed in addition to these as physicians struggle to recover from the financial and administrative turmoil resulting from this cyberattack.

Prohibit retroactive denials based on eligibility or lack of utilization management approval

In addition to the previously mentioned utilization management challenges the Change Healthcare outage has brought, it has also prevented electronic insurance eligibility verification. Standard operating procedures for most physician practices include submitting batch electronic eligibility requests every evening to confirm insurance coverage, benefits, and co-pay amounts for patients with appointments scheduled for the next business day. Without this capability, physicians continue to care for their patients, but they could later be liable if a patient's coverage has lapsed. As such, **the AMA is urging policymakers to ensure that all health plans waive any claim denials based on lack of patient insurance eligibility or utilization management approval for practices impacted by the outage.**

Waive timely filing deadlines for claims and appeals

Many health plans enforce deadlines for timely filing of claims based on the date of service. However, given the extensive challenges with claim submission resulting from the Change Healthcare outage, many physician practices are not currently able to meet those deadlines and will continue to have delays in claim submission. Enforcement of these timelines could result in

nonpayment to practices, further exacerbating the financial impact of this crisis. We note that some practices are already reporting denials due to late claim submission resulting from the service disruption. **Therefore, the AMA is urging policymakers to ensure that all health plans are required to waive timely claim filing requirements. Similarly, any time limitations on the filing of appeals should be waived as well.**

Loan repayments

Many physician practices have accepted advance payments and loans through UHG, Medicare, and Medicaid that are helping maintain their financial viability. However, there is growing concern about the repayment expectations and the impact that premature or aggressive recoupment would have on practices.

The AMA is advocating for flexibility and leniencies in repayment requirements to ensure that the rug is not pulled out from under financially vulnerable practices just as they are beginning to reestablish their footing. It will be important for the sponsors of advance payments to ensure that claim submission and payment processes are functioning for all a practice's payers, rather than just the sponsor's plan, before requiring repayment. Additionally, it will be critical that sponsors clearly communicate with practices about how recoupments will be processed and specifically identify amounts withheld for loan repayments on remittance advice to differentiate them from other payer recoupment processes.

Communication on scope of the breach

Physician practices are frequently the first and primary contact for patients to the health care system. Therefore, it is imperative that the scope of the breach and the impact on patients' data are fully communicated to physician practices. The urgency of this issue has been heightened in recent days by credible reports that a second cybercriminal organization possesses the data from the Change Healthcare breach and is threatening to publish this information unless UHG meets ransom demands. The AMA therefore urges Congress to demand that UHG disclose the amount and types of patient and health care provider data that have been compromised, the associated harms to privacy, and how UHG will respond and address individuals' identification theft. We expect, at the very least, that UHG should provide guaranteed identification protection for no less than two years for all individuals whose identity has been compromised.

IV. Long-term considerations for the health care system

While immediate and near-term relief and flexibilities for physicians and patients are paramount, the AMA urges Congress to begin considering long-term policy changes and protections needed to both deter future cyberattacks and protect physician practices if—and realistically, when—they happen again.

The AMA anticipates that Congress will investigate the causes of this breach, whether existing cybersecurity laws are strong enough, and whether such laws were being followed. The AMA hopes that Congress will also look at where response requirements can be strengthened and whether it makes sense to incorporate flexibilities for federal and state governments to respond to health care cyberattacks, similar to those flexibilities provided for public health emergencies.

Additionally, we strongly urge Congress to consider why consolidation in the health insurance market is permitted to the extent that a single company can have indisputable dominance over the entire health care system so that that when they are attacked, the entire system goes down.

Finally, the AMA urges Congress to reevaluate the environment that has led so many physician practices to be in the position of financial vulnerability. Ensuring physician practices have resources to weather a crisis like the Change Healthcare outage and continue serving their patients has to start with ensuring physicians' financial security.

Thank you for the opportunity to submit this statement. We look forward to working with the Subcommittee to address the immediate and long-term needs of physician practices in light of the Change Health cyberattack and outage.