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

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 medtech 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.

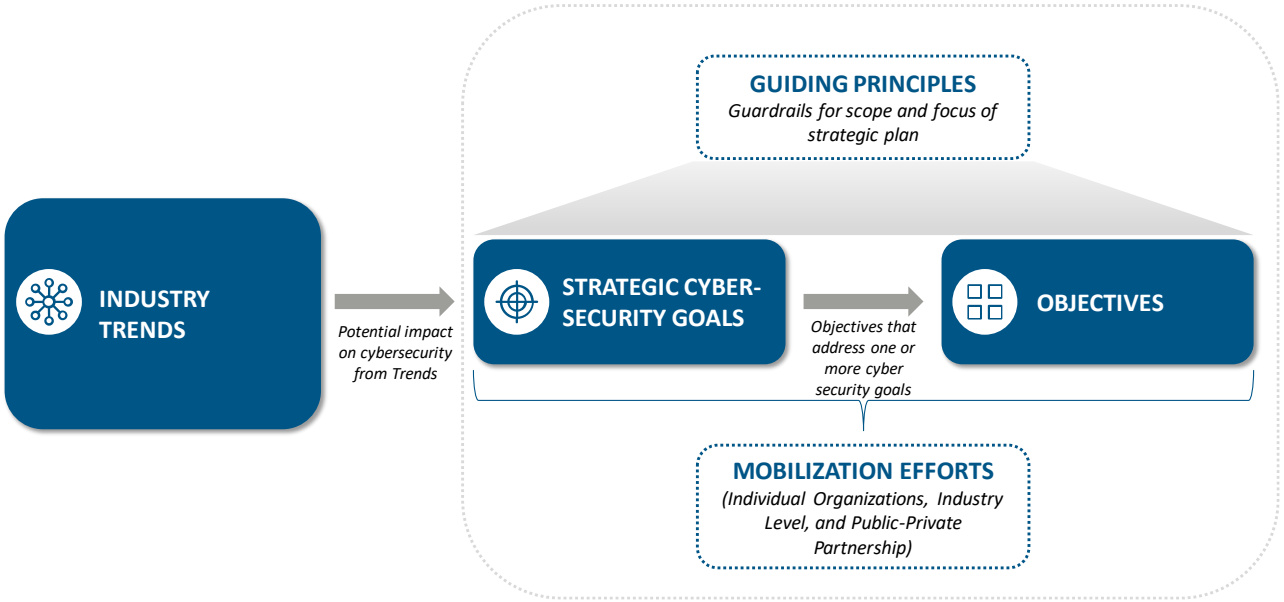
B. About the Health Sector Coordinating Council

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**

Development of the Health Industry Cybersecurity Strategic Plan



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** 1 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 Error! Reference source not found.**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	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:
		• Ongoing chronic care
		• Hospital at home care
		• Consumer-Driven
		  ○ Wellness care (consumer drives the need / desire of care)
		  ○ Direct to consumer lab tests, and
		  ○ Software as a medical device at home
		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.
		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.

T2	Adoption of emerging and disruptive	There is an increase in pace of innovation and accelerated adoption of emerging technologies to deliver wellness and care differently, drive

ID	Key Industry Trends (Current & Future)	Description
	technologies will accelerate	operational efficiencies, gain deeper insights, and reduce costs. Specific categories of trends include: **Data Analytics (Data Driven Insights / Decision Support):** 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. **Accelerated Adoption of Artificial Intelligence:** 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: • 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 **Adoption of Emerging Technologies:** 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. **Novel Digital Biomarkers of Health and Disease:** 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

ID	Key Industry Trends (Current & Future)	Description
		high risk groups, and provide individualized risk and mitigation strategies in an on-going, continuous model. In the same way that consumers 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. **Digital Transformation:** 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 cloudfying" 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. 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." 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.
T3	The business of healthcare will continue to change and adapt	The health sector is experiencing rapid change in business models, driven by: • 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. 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.

ID	Key Industry Trends (Current & Future)	Description
T4	Acute Financial Distress will not abate	Costs to care delivery continue to increase at an unsustainable level. While all subsectors are feeling cost pressures, healthcare delivery organizations are facing: • 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. These factors in turn drive: o Increased mergers, acquisitions, & divestitures (MA&D) and consolidation activities; o Focus on cost reduction; o Closures / reduced options for health services, especially in rural areas; and o Increase in out-of-data / out-of-support vulnerable technologies. Similarly, other healthcare sub-sectors like medical device and pharmaceutical manufacturers respond to increasing operational costs and regulatory pressures by shifting some operations offshore.
T5	Workforce recruitment and talent management will face competitive pressures from supply and demand pressures	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. 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. 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.

ID	Key Industry Trends (Current & Future)	Description
T6	Governments will be challenged to develop coordinated and coherent policies for a rapidly evolving and complex health system	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 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** Context on Goals for additional context and clarification on the intent and scope of each cybersecurity goal. See **Appendix D** Goals to Objectives Mapping for mapping of Goals to Cybersecurity Objectives (O) that is covered later in this document in Section **VI**. The following **Table** 3maps 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 • **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	✓	✓	✓	✓	✓	✓	

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
G2	Cybersecurity and privacy practices and responsibilities are understandable to healthcare technology consumers and practitioners	✓	✓			✓	✓	
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	✓	✓				✓	

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
G5	Emerging technology is rapidly and routinely assessed for cybersecurity risk, and protected to ensure its safe, secure, and timely use	✓	✓	✓	✓			
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**								

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
G8	Foundational resources and capabilities are available to support cybersecurity needs across all healthcare stakeholders regardless of size, location, and financial standing	✓	✓		✓	✓	✓	
	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	☑ Health Delivery ☑ Health Insurer ☑ Service Provider ☑ Health Software / Device Manufacturer ☐ Industry Group ☑ Government	G2, G4, G5, G6	• 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
				gauge their capabilities in various aspects, including backup procedures, ransomware preparedness, incident response capabilities, business continuity, IT disaster recovery, and testing protocols
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	■ Health Delivery ■ Health Insurer ■ Service Provider ■ Health Software / Device Manufacturer ■ Industry Group ■ Government	G1, G3, G4, G5, G6, G7, G8, G9	• 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	☐ Health Delivery ☐ Health Insurer ☐ Service Provider ☐ Health Software / Device Manufacturer ■ Industry Group ■ Government	G2, G3, G4, G10	• 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	■ Health Delivery ■ Health Insurer ■ Service Provider ■ Health Software / Device Manufacturer ■ Industry Group ■ Government	G2, G4, G5, G6, G7, G9	• 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
				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
O5	Enhance health sector senior leadership and board knowledge of cybersecurity and their accountability to create a culture of security within their organizations	☑ Health Delivery ☑ Health Insurer ☑ Service Provider ☑ Health Software / Device Manufacturer ☐ Industry Group ☐ Government	G7, G8, G10	• 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)	■ Health Delivery ☐ Health Insurer ☐ Service Provider ☐ Health Software / Device Manufacturer ■ Industry Group ■ Government	G8, G9	• 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	■ Health Delivery ■ Health Insurer ■ Service Provider ■ Health Software / Device Manufacturer ■ Industry Group ■ Government	G2, G8, G10	• 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
				mutual assistance for incident response • Government initiatives that will positively incentivize or subsidize cybersecurity training for physician practices and smaller health delivery organizations that support underprivileged communities • Peer-peer sharing of cybersecurity practices and other materials • 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 • Marketing programs by broad and subsector-based industry groups promote 405(d) HICP, and relevant HSCC leading practices publications • Ability to use billing code for time spent on education by health providers • Addition of cyber course for medical oriented degrees • Health insurance payers and cyber insurance industry drive requirements for cyber proficiency • 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	☐ Health Delivery ☐ Health Insurer ☐ Service Provider ☐ Health Software / Device Manufacturer ■ Industry Group ■ Government	G5, G6, G8	• 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	■ Health Delivery ■ Health Insurer ■ Service Provider ■ Health Software / Device Manufacturer ■ Industry Group ■ Government	G2, G3, G4, G8, G9	• 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	■ Health Delivery ■ Health Insurer ■ Service Provider ■ Health Software / Device Manufacturer ■ Industry Group ■ Government	G1, G2, G4, G7, G9	• 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	☑ Health Delivery ☑ Health Insurer ☑ Service Provider ☑ Health Software / Device Manufacturer ☑ Industry Group ☑ Government	G8, G9	• 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	☐ Health Delivery ☐ Health Insurer ☐ Service Provider ☐ Health Software / Device Manufacturer ☑ Industry Group ☑ Government	G8, G9	• 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
				• 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)	• 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	• 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	• 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** Call to Action: Public-Private Partnership Mobilization (I) 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**

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

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
G1 - Healthcare and wellness delivery services are user-friendly, accessible, safe, secure, and compliant	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: • 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
G2 - Cybersecurity and privacy practices and responsibilities are understandable to healthcare technology consumers and practitioners	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.
G3 - Cybersecurity requirements are readily available, harmonized, understandable, and feasible for implementation across all relevant health and public health sub-sectors	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).

Cybersecurity Goals	Context / Clarifications
G4 - Health, commercially sensitive research, and intellectual property data are reliable and accurate, protected, and private while supporting interoperability requirements	The intent of this objective is to accomplish the following: • 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.
G5 - Emerging technology is rapidly and routinely assessed for cybersecurity risk, and protected to ensure its safe, secure, and timely use	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.
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.	The intent of this objective is to establish requirements and accountability of product developers for "secure by-design" products.
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)	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.
G8 - Foundational resources and capabilities are available to support cybersecurity needs across all healthcare stakeholders regardless of size, location, and financial standing	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.

Cybersecurity Goals	Context / Clarifications
G9 - The health and public health sector has established and implemented response and resilience strategies to enable uninterrupted access to healthcare technology and services	The intent of this objective is to look at resilience holistically for sustaining critical business and patient care operations and its safety. This includes: • 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
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	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.

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 (P³) Initiative Examples
I8	Develop and share a concise educational resource on essential security measures with key stakeholders.
I9	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	• **O2.** Simplify access to resources and implementation approaches related to the adoption of controls and practices aligned with regulatory and sec-tor 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	• **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

Ref ID	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	• **O2.** Simplify access to resources and implementation approaches related to the adoption of controls and practices aligned with regulatory and sec-tor 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	• **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 sec-tor 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

Ref ID	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	• **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 sec-tor 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	• **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 sec-tor 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

Ref ID	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	• **O2.** Simplify access to resources and implementation approaches related to the adoption of controls and practices aligned with regulatory and sec-tor 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	• **O2.** Simplify access to resources and implementation approaches related to the adoption of controls and practices aligned with regulatory and sec-tor 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

Ref ID	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	• **O2.** Simplify access to resources and implementation approaches related to the adoption of controls and practices aligned with regulatory and sec-tor 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	• **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