Health Sector Coordinating Council
Cybersecurity Working Group

Health Industry Cybersecurity -

Recommendations for Government Policy and Programs

MARCH 2025

Contents

Introduction

Cyber threats to the healthcare sector are a well-documented reality of modern healthcare delivery. Ransomware attacks against members of the ecosystem including hospitals, insurance providers, third-party service providers, and other healthcare delivery organizations (HDOs) routinely deny access to patient care, 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.

The increasing complexity of today's connected healthcare ecosystem presents potentially massive systemic cyber risks: unanticipated and poorly understood interdependencies; unknown inherited security weaknesses; overreliance on vendor solutions; systems that fail to account adequately for human factors related to cybersecurity controls; and 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 business and delivery of healthcare are evolving through the adoption of digital consumer wellness and fitness technologies, remote care models, and accelerating consolidation of health systems, third-party vendors, and new disruptive healthcare business models. As a result of these drivers, healthcare frequently occurs outside of hospitals and clinician offices, which requires transmission of telehealth, remote care, and home health data across uncontrolled home and public networks and cloud services. Further, valuable data derived from personal lifestyle devices such as fitness trackers, smart watches can now augment clinical data and decisions.

Thus, ensuring that an individual health provider, IT, payer, pharmaceutical or medical technology capability is "cybersecure" alone is no longer sufficient; modern care delivery and its supporting infrastructure require that all disparate pieces of the evolving healthcare ecosystem be considered and appropriately secured.

This imperative can be addressed through negotiated cybersecurity regulation, 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 offers considerations for how government policy and programs can 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" – objectives and outcomes - than on the "how" – specific requirements and processes, these recommendations are meant to stimulate creative

discussion between government and industry about initiatives that can measurably improve cybersecurity management across the health sector.

About the Health Sector Coordinating Council

The Healthcare and Public Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG) is an industry-led advisory council of healthcare entities partnering with government in alignment with national critical infrastructure protection policy to identify and mitigate systemic cyber threats and vulnerabilities facing the sector's ability to deliver its services and assets to the public. The CWG membership involves more than 470 healthcare providers, pharmaceutical and medical technology companies, payers, health IT entities, public health and government agencies collaborating to develop free healthcare cybersecurity practices and policy recommendations, and motivate sector-wide responsibility and investment in the imperative that ***cyber is patient safety***.

Cybersecurity Wellness Themes and the Five-Year Strategic Plan: Principles for Advancement

To organize our prescriptions for cyber health in the sector, the HSCC coalesces around high-level *Themes for Cyber Wellness* and our *Health Industry Cybersecurity Strategic Plan (HICSP)*. Together, these guiding foundations help categorize interrelated approaches to our cybersecurity challenges. They establish the principles by which we propose and negotiate policy, investment, and assistance programs. And they present a framework for identifying and holding accountable our shared responsibilities for voluntary cybersecurity management that evolves with the threat, and mandatory requirements that set uniform baselines for regulatory compliance.

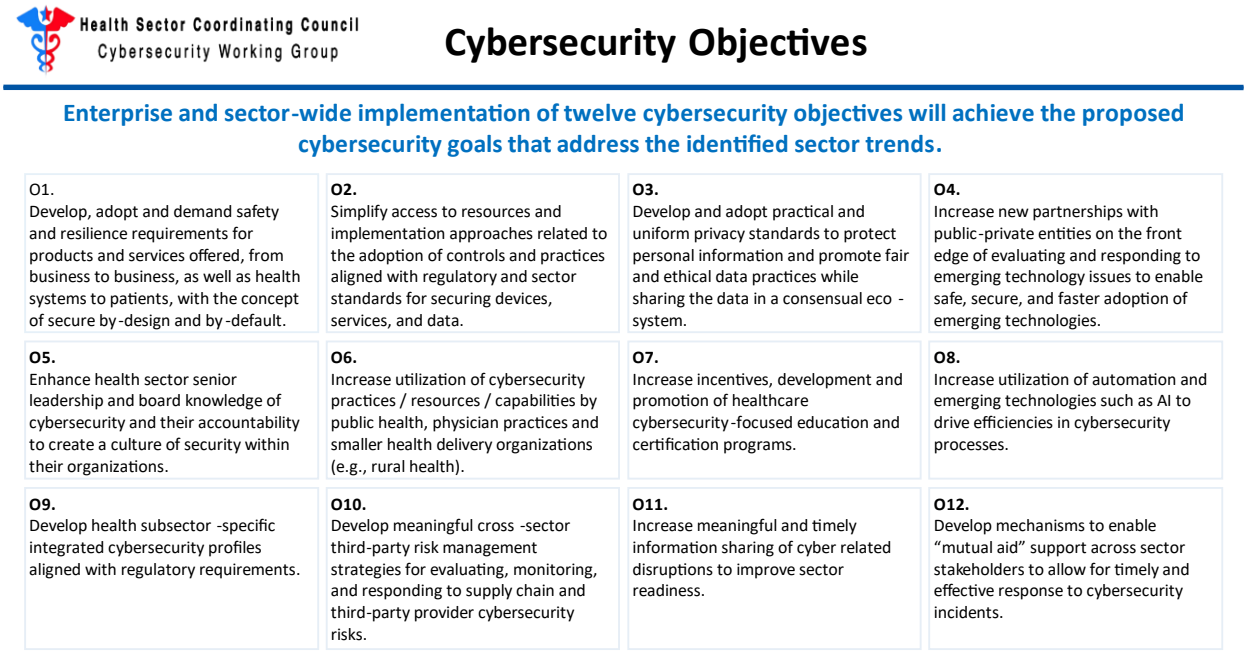
The *Cyber Wellness Themes* are: *Access* - the notion that resources and understanding about managing our cyber environment should be accessible, simple, and implementable with a culture of security; *Community* – imagining a "911 Cyber Civil Defense" of mutual aid, collaborative preparedness and incident response on the principle that the adversary must beat all of us to beat one of us; *Innovation* – that we continue to develop and adopt new technologies in healthcare and security, while we innovate how we manage our healthcare cybersecurity environment, constantly learning, adapting, and evolving to meet the ever-changing threat landscape; and *Workforce* – filling the workforce gap in cybersecurity for healthcare by building a pipeline of next generation cyber leaders while innovating in workforce training about the fundamentals of cyber hygiene.

The 2024-29 HICSP matches healthcare industry trends and related cybersecurity challenges with 12 Implementing Objectives (see Figure 1 below) that individual organizations, health system subsectors, the industry as a whole, and the government must address collaboratively to achieve a higher, more persistent and reflexive state of healthcare cybersecurity. End-state success of the Strategic Plan will demonstrate better sector-wide cyber wellness – a diagnosis upgrade from critical to stable condition – with the following outcomes:

- 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.
- A Cyber Safety Net of financial, policy and technical assistance supports 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.

Figure 1



Healthcare Cybersecurity Policy and Program Proposals for Government Consideration

The following policy and programmatic recommendations are offered for HHS, CISA, Congress and other Federal agencies to support healthcare cybersecurity. The recommendations are grouped into the following topical categories, linked here to their location in the document: 1) Preparedness and Information Sharing; 2) Financial Support and Incentives; 3) Incident Response and Recovery; 4) Workforce; and 5) Regulatory Reform.

Most of these functional-area recommendations align with the HSCC's "Cyber Wellness" themes of *Access, Community, Innovation and Workforce* and many of the twelve implementing Objectives captained in the sector's five-year Cybersecurity Strategic Plan.

The second section of this paper provides a brief overview of foundational policy documents that frame healthcare cybersecurity management and compliance in the context of the critical infrastructure public-private partnership.

1. Preparedness and Information Sharing

*The following Preparedness and Information Sharing recommendations operationalize the HSCC cyber wellness themes of **Access**, **Community** and **Innovation**, and address numerous Health Industry Cybersecurity Strategic Plan Objectives.*

1.1 HHS should join with the HSCC and healthcare stakeholders in a national communications and outreach campaign to the health provider community and its supporting infrastructure about the imperative of cyber security as a patient safety issue. This begins with a federated communications strategy featuring the many healthcare-specific cybersecurity practices offered by industry and government that help users to 1) monitor threats; 2) manage risks; 3) secure medtech; 4) respond and recover; and 5) measure effectiveness.

1.2 Joint security guidance published by HHS and HSCC tend to have more credibility, reach and adoption than publications released independently by either. Procedures for developing joint publications should be formalized and structured similar to how the HHS 405(d) program and HSCC produced the flagship cybersecurity guide "Health Industry Cybersecurity Practices (HICP)– Managing Threats and Protecting Patients" and the "Hospital Resiliency Cyber Landscape Analysis".

1.3 Strengthen the 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.

1.4 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.

1.5 Generally 50% of healthcare breaches and ransomware attacks on healthcare are due to breaches against third party technology and service providers; we should accordingly explore national-security based regulatory mechanisms to hold technology, software and service providers supporting critical health infrastructure to higher levels of accountability for enhanced product and enterprise cybersecurity requirements, similar to FDA pre-market and post-market cybersecurity requirements on medical device manufacturers subject to safety and quality standards, using a cleared entities list approach similar to FEDRAMP.

1.6 Designate high impact cyber and ransomware attacks, which result in widespread disruption and delay of health care delivery at critical access, safety net and rural emergency hospitals, as "all hazards" incidents to activate appropriate Federal government response support for state, regional and local emergency response services.

1.7 HHS should encourage health sector organizations to join and actively participate in Health-Information Sharing and Analysis Center (Health-ISAC) as part of a robust resilience strategy. The U.S. Department of Treasury set the precedent in 2014 in issuing a statement recommending that all financial institutions "... participate in the [Financial Services] ISAC as part of their process to identify, respond to, and mitigate cybersecurity threats and vulnerabilities....Rapidly evolving cybersecurity risks reinforce the need for all to have methods for obtaining, monitoring, sharing, and responding to threat and vulnerability information (*source*)." HHS should adopt a similar recommendation with appropriate financial support and incentives

particularly for resource-constrained health providers described below so that healthcare and public health organizations can benefit from the rapid sharing of cybersecurity risks and mitigating controls.

1.8 Cyber insurance carriers have varying and inconsistent cybersecurity control requirements for determining premiums and coverage of insured healthcare entities. For cyber risk reduction and risk transfer efficiencies to scale across the sector, consistency in expectations is needed for assessing providers' investments in risk management programs. Accordingly, 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 signed into law as P.L. 116-321 on January 5, 2021. This law recognized breached entities' implementation of HICP, the NIST Cybersecurity Framework and other recognized security practices as mitigating factors that HHS must consider when pursuing a HIPAA data breach enforcement action. Reference practices could also include participation in the Health-ISAC or other information sharing and analysis organizations (ISAO's) as an element of good cybersecurity practice that would improve premiums and coverage.

1.9 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.

1.10 Continue development, outreach and provision of innovative CISA support programs, such as the Cyber Hygiene (CyHy) program and cyber exercises, that can be tailored in close consultation with HHS to healthcare entities.

1.11 Government sharing of cyber threat and incident intelligence frequently does not meet private sector needs because it is not timely, relevant or actionable. 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 an advisory release. This would ensure that both industry and government leaders are generally aligned – rather than sending inconsistent messages - before publication to the broader community about the accuracy of the intelligence, its relevance to and impact on the sector, and appropriate remediation procedures.

1.12 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.

1.13 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. This may require reauthorization of the protections contained in the Cybersecurity Information Sharing Act of 2015 (CISA), sunsetting in 2025, which aims to improve cybersecurity by encouraging information sharing between private sector entities and government agencies about cyber threats, allowing them to collaborate more effectively in identifying and mitigating cyberattacks, while also providing legal protections for companies sharing this information.

2. Financial Support and Incentives

*The following Financial Support and Incentives recommendations operationalize the HSCC cyber wellness themes of **Access** and **Community,** and address numerous Health Industry Cybersecurity Strategic Plan Objectives.*

2.1 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, aligning 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.

2.2 Unregulated third-party technology and service providers represent both a major threat vector and costly third-party risk management demands. Health providers should not bear sole burden for policing their vendors; such third parties must be held to an enforceable higher cybersecurity standard when they support critical healthcare infrastructure where lives are at risk.

2.3 Workforce augmentation for needed cybersecurity skills should be funded at the federal level through ongoing commitment of CISA technical support programs, and at the federal and state levels for subsidizing the use of contracted managed security providers, academic institutions' deployment of student engineers and cybersecurity majors in programs such as the Consortium of Cybersecurity Clinics (https://cybersecurityclinics.org/); state national guard assistance for cybersecurity incident response, and other programs.

2.4 Maintain and expand of the U.S. Department of Agriculture's Rural Loan Program, which supports rural entities such health providers with various forms of cybersecurity support:

- Funding equipment and infrastructure
- Securing rural development's portfolio through managing risk to healthcare facilities
- Potential technical assistance provider
- Conduit to rural community leaders and health care providers to share information and resources

2.5 As one-time grant support payments generally cannot be used for hiring, grant programs should be tailored to the specific needs the Resource-Constrained health providers and should be ongoing as part of the payment structure.

2.6 CISA and HHS should encourage state insurance regulatory agencies to work with insurance companies to devise incentive programs that 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.

2.7 HHS should explore mechanisms to fund or incentivize qualified managed security service providers (MSSPs) to assist 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.

State, regional, local support services can partner with FBI and CISA offerings to enhance health sector security.

2.8 HHS should establish needs-based subsidy and incentive programs to help resource-constrained health systems wanting to improve situational awareness by participating in the Health-ISAC or other information and sharing and analysis organizations.

2.9 Add specified cybersecurity tools; services and surge workforce capacity as allowable expenses 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.

2.10 HHS should compile a reference of federal subsidies and grants across the government that fund cybersecurity services, tools, and education for health providers.

3. Incident Response and Recovery

The following Incident Response and Recovery recommendations operationalize the HSCC cyber wellness themes of ***Community*** and ***Innovation,*** *and address numerous Health Industry Cybersecurity Strategic Plan Objectives.*

3.1 [*repeated from above*] Government sharing of cyber threat and incident intelligence frequently does not meet private sector needs because it is not timely, relevant or actionable. 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 an advisory release. This would ensure that both industry and government leaders are generally aligned – rather than sending inconsistent messages - before publication to the broader community about the accuracy of the intelligence, its relevance to and impact on the sector, and appropriate remediation procedures.

3.2 Government information and incident response interfaces with industry should clearly articulate and rapidly-deliver actionable intelligence when implementing its cyber incident reporting collection and analysis authorities.

3.3 Because health systems are burdened with multiple differing report forms and overlapping agency requirements for the same incident, incident reporting timeframes and methodologies should be standardized across government regulatory entities.

3.4 Cyber-attack victim reporting requirements should be waived while an incident response is underway in the early stages of discovery and operational triage.

3.5 Provide federal-sponsored incident response support for organizations that are experiencing security incidents and in need of assistance getting through and recovering from the breach.

3.6 Expand innovative law enforcement disruption initiatives against both foreign and domestic threat groups to reduce ecosystem risk creating the most harm to hospitals.

3.7 As incentives for voluntary reporting and information sharing with the government, 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.

3.8 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.

3.9 Partner government and industry research support toward technical and operational efficiencies for effective incident response and continuity to ensure rapid return to health delivery operations following a severe cyber attack.

4. Workforce

*The following Workforce recommendations operationalize the HSCC cyber wellness themes of **Access** and **Workforce**, and address numerous Health Industry Cybersecurity Strategic Plan Objectives. A number of recommendations supplement those made in the forthcoming HSCC Report and Recommendations on Cybersecurity for U.S. Resource-Constrained Health Providers.*

4.1 HHS should 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® 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.

4.2 Fund federal, and supplement state-subsidized - "civilian cyber health corps" programs. 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 corps such as the U.S. Public Health Service Commissioned Corps - https://www.hhs.gov/surgeongeneral/corps/index.html. Also suggest establishing career pathways that do not require a full 4 years of college (i.e. certificate programs and associates).

4.3 Augment workforce development programs such as in the HITECH Act, which funded health IT workforce training programs: the University-Based Training Program and Community College Consortia Program. In total the two programs trained 21,437 students from all 50 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands at 91 academic institutions. See: https://www.healthit.gov/data/quickstats/hitech-workforce-development-programs.

4.4 HHS should explore mechanisms to fund or incentivize qualified managed security service providers (MSSPs) as workforce augmentation to assist critical access, safety net and rural emergency hospitals to remediate urgent vulnerabilities or mitigate threats. Many organizations struggle to operationalize information provided by government agencies, information sharing organizations, product vendors, etc. State, regional, local support services can partner with FBI and CISA offerings to enhance health sector security.

4.5 HHS should establish needs-based subsidy and incentive programs to help resource-constrained health systems wanting to improve situational awareness by participating in the Health-ISAC or other information and sharing and analysis organizations (ISAOs).

4.6 Add specified cybersecurity tools, services and surge workforce capacity as allowable expenses 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.

4.7 HHS should compile a reference of federal subsidies and grants across the government that fund cybersecurity services, tools, and education for health providers.

4.8 Map 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.

5. Regulatory Reform

5.1 As the primary cross-sector healthcare advisory council focused exclusively on critical infrastructure cybersecurity, the HSCC is prepared to engage with government leadership in a phased series of policy consultations and workshops to negotiate a modernized, coherent, practical, scalable and *effective* framework that combines both mandatory and flexible voluntary practices for healthcare technology, enterprise and health provider cybersecurity. A successful model for this type of public-private engagement is the development of the NIST Cybersecurity Framework initially published in 2014 after 1 year of work, a process convened and guided by NIST with content generated by the industry owners and operators of critical infrastructure – those most knowledgeable and responsible for securing it.

5.2 The December 2024 HHS notice of proposed rulemaking updating the HIPAA Security Rule did not demonstrate sufficient insight to the complexities of achieving effective cybersecurity protections for the health sector, nor acknowledge the considerable work the sector and government partners have accomplished in good faith and urgency over the past 6 years to build a collective cyber defense. The HIPAA Security Rule update process should be reset with the collaborative process described above.

5.3 As recommended in the 2017 Health Care Industry Cybersecurity Task Force report, HHS should work across the regulatory Operating Divisions (ASPR, OCR, ONC, CMS, FDA) and other cyber- and data-regulating government entities involving cybersecurity and privacy (FTC, SEC, etc) to cross-map and harmonize regulatory requirements on health systems that duplicate or conflict. A holistic, coherent cybersecurity 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.

5.4 Enhance CMS fraud protection programs to reduce the value and thus demand of stolen ePHI and other data, and thus attempts at cyber exploitation.

5.5 Harmonize current sector specific regulations to possible future regulations on Consumer Data Privacy and Security as well as Artificial Intelligence to further create a holistic, coherent strategy with clear aligned requirements and regulatory authority.

Policy Foundation and Current Developments

The following partial list of legislative, regulatory or executive actions 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.

1. **National Security Memorandum 22 on Critical Infrastructure Security and Resilience** (April 2024); focuses on government organization around working with owners and operators to secure the nation's critical infrastructure industries
2. **Executive Order 13800 – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure** (May 2017); in alignment with HSCC partnership and workforce recommendations, states U.S. policy to "support the cybersecurity risk management efforts of the owners and operators of the Nation's critical infrastructure", resulting in reports on support for critical infrastructure at greatest risk and on supporting the growth and sustainment of the nation's cybersecurity workforce.
3. **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;
4. **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 underway and set to conclude in 2026.
5. **Securities and Exchange Commission rule** (December 2023) 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.
6. **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.
7. **Government Accountability Office report** (June 2021) on the need for enhanced HHS Industry Partnership responsibilities.

8. **HHS OIG Report** on Lack of CMS Cybersecurity Oversight of Networked Medical Devices in Hospitals (June 2021).
9. **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.
10. **P.L. 116-321 (HR 7898) HITECH Act Amendment** (January 5, 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.
11. **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.
12. **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.

##