Health Industry Cybersecurity
Recommendations for Government Policy and Programs

April 2023

Introduction

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

In addition, the healthcare sector itself is evolving through the adoption of digital consumer wellness and fitness technologies, as well as the shift towards remote care models, accelerating consolidation of health systems and new disruptive healthcare business models, which were greatly accelerated by the COVID-19 pandemic and financial pressures. As a result of these drivers, healthcare now frequently occurs outside of hospitals and clinician offices. Telehealth, remote care, and home health are all driving the integration of healthcare technologies with,

for example, patients' home networks, and require transmission of data across uncontrolled networks (home, public) and cloud services. Further, valuable data that can be derived from personal lifestyle devices (e.g., fitness trackers, smart watches) can now augment clinical data and decisions. Ensuring that a hospital or clinician's office is "cybersecure" alone is no longer sufficient; modern care delivery requires that all disparate pieces of the evolving healthcare ecosystem be considered, and appropriately secured as well.

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

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

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

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

About the Health Sector Coordinating Council

The Healthcare and Public Health Sector Coordinating Council (HSCC) is a coalition of private-sector critical healthcare infrastructure entities organized under the National Infrastructure Protection Plan to partner with and advise the government in the identification and mitigation of strategic threats and vulnerabilities facing the sector's ability to deliver services and assets to the public. The HSCC Cybersecurity Working Group (CWG) is a standing working group of the HSCC, composed of more than 400 industry and government organizations working together to develop strategies and best practices to address emerging and ongoing cybersecurity challenges to the health sector.

Healthcare Cybersecurity Policy and Program Proposals for Government Consideration

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

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

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

Preparedness Support and Information Sharing

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

- Consider applying the review and approval procedures of the HHS 405(d) program to additional joint publications by HHS and the HSCC Cybersecurity Working Group. As the 405(d) Program has a successful track record of partnership with HSCC, this model should continue with consideration of options for how it may be enhanced with continued industry-driven leadership.
- Boost funding for HHS Health Sector Cyber Coordination Center (HC3) to be a primary knowledge sharing and analysis resource within HHS to support healthcare cybersecurity in coordination with CISA. Congress should make HC3 an appropriated line item.
- Remove potential regulatory or legal barriers (eg., antitrust, Stark law, etc) to the formation of a health provider consortium that would develop and promote uniform minimum cybersecurity program requirements for any entity that sells hardware, software or services to a health system. This could be modeled on, for example, a FEDRAMP-type govt conduit to 3rd party cyber risk management requirements using a version of the HSCC Model Contract - https://healthsectorcouncil.org/model-contract-language-for-medtech-cybersecurity-mc2.
- Assign an office within HHS, (similar to a "Bureau of Census" for healthcare cybersecurity) in partnership with industry, to develop a program to measure cybersecurity performance in the health provider sector.
- For legislative consideration: In the reauthorization Pandemic and All Hazards Preparedness Act (PAHPA):
    - Designate high impact cyber and ransomware attacks, which result in the disruption and delay of health care delivery at one or more critical access, safety net and rural emergency hospitals, as "all hazards" incidents to activate FEMA and other government response support services;
    - Fund and provide support for the appropriate federal agencies to help hospitals and health systems enhance their emergency preparedness, response, resiliency and recovery capabilities related to cyberattacks (one of the recommendations included in the landmark report to Congress issued by the

2017 Health Care Industry Cybersecurity Task Force established under the Cybersecurity Act of 2015); and

- Fund the appropriate federal agencies to provide emergency response for high impact cyberattacks targeting hospitals and health systems and provide human, technical and financial support to the victim organizations to minimize harm to public health and safety.

- HHS and CISA should coordinate with major cyber insurance carriers and their state regulatory agencies to encourage the reference of HICP into cyber insurance policy requirements, similar to the incentive codified in P.L. 116-321. This can include participation in the Health-ISAC or other information sharing and analysis organizations as one element of good practice that would improve premiums and coverage. Such a coordination process could build on the past DHS initiative of the Cyber Incident Data and Analysis Working Group (CIDAWG).
- Presently, cyber liability carriers have varying and inconsistent cybersecurity control requirements for determining premiums and coverage. Consistency in expectations for insurance will scale for providers' investments in risk management programs.
- Protect health delivery organizations from class action lawsuits if they can demonstrate that they implement NIST CSF, HICP, or other recognized cybersecurity practices. This could incentivize more robust adoption and implementation of security controls.
- Continue development, outreach and provision of innovative CISA support programs, such as the Cyber Hygiene (CyHy) program, the Joint Cyber Defense Collaborative and table-top cyber exercises, that can be tailored, in close consultation with HHS, to healthcare entities.
- With respect to ongoing threat monitoring and analysis, timely and actionable government sharing of cyber threat and incident information is frequently inadequate for private sector needs. When developing threat and remediation advisories for the health sector, CISA, HHS and law enforcement should, as a matter of protocol under MOU, consult with designated industry sector leaders through Health-ISAC and HSCC with credible – and as appropriate, global - threat intelligence and analysis that can be

compared and reconciled with government intelligence ahead of release of any advisories. This would ensure that both industry and government leaders are generally aligned before publication to the broader community about the accuracy of the intelligence, its relevance to and impact on the sector, and appropriate remediation procedures.

- Tailor a classified information sharing program involving health sector-designated liaison representatives, CISA, HC3, and law enforcement agencies, so that the liaison representatives can provide consideration and feedback to federal threat analysts on what is most relevant and actionable to the Sector.
- Consider incentives, support and protections for health systems working with government in various forms of proactive operational collaboration against threats and attacks, impending or in-process.

Financial Support and Incentives

- CMS reimbursement incentives: If an institution demonstrates implementation of HICP, the NIST CSF, or other recognized security practices as incentivized in P.L. 116-321 as mitigation for HIPAA-enforcement liability following a data breach, CMS similarly can offer additional reimbursement under a concept of "meaningful protection." This could include additional CMS reimbursement to HDO's participating in the Health-ISAC or other ISAO's, implementation of active legacy medical technology cyber security management and replacement programs, and cybersecurity being included among performance goals overseen by hospital boards. Such incentive programs could be phased-in, measuring progress over time, alignment with HICP or other recognized security practices, and tying incentives to the cost/difficulty/scale of particular control frameworks and other cybersecurity investments in the clinical environment.
- HHS should establish needs-based grant, subsidy and incentive programs to help under-resourced health systems wanting to improve situational awareness by participating in the Health-ISAC or other information and sharing and analysis organizations.

- CISA and HHS should encourage state insurance regulatory agencies to work with insurance companies to tie reduced premiums and/or improved coverage for cyber insurance to participation in the Health-ISAC and other information sharing and analysis organizations as one element of an appropriate cybersecurity risk management program.
- HHS should provide funding support and/or technical assistance for critical access, safety net and rural emergency hospitals to remediate urgent vulnerabilities or mitigate threats. Many organizations struggle to take advantage of information made available via various channels including agencies, information sharing organizations, product vendors, etc. Local and regional FBI and CISA offices can enhance health sector outreach and communications channels to under-resourced health systems.
- Add specified cybersecurity tools and services as an allowable expense under the FCC Health Connect Fund subsidy of the Universal Service Administrative Company (USAC). This would leverage the purchasing power of under-resourced systems to supplement the current and more narrow WAN/Core Network investment expense.
- HHS should compile a reference of federal subsidies and grants across the government that fund cybersecurity services, tools, and education for health providers.

Incident Response and Recovery

- When responding to an incident, timely and actionable government sharing of cyber threat and incident information is frequently inadequate for private sector needs. When developing threat and remediation advisories for the health sector, CISA, HHS and law enforcement should, as a matter of protocol under MOU, consult with designated industry sector leaders through Health-ISAC and HSCC with credible – and as appropriate, global - threat intelligence and analysis that can be compared and reconciled with government intelligence ahead of release of any advisories. This would ensure that both industry and government leaders are generally aligned before publication to the broader community about the accuracy of the intelligence, its relevance to and impact on the sector, and appropriate remediation procedures.

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

effects of a cyber attack, such that the request can be processed quickly across the interagency to provide timely assistance to the victim organization. This would be modeled after a similar RTA negotiated between the financial sector and the government.

Workforce

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

Regulatory Reform

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

- Enhance CMS Fraud protection programs to reduce the value and thus demand of stolen ePHI and other data, and thus attempts at cyber expoitation.

######

Policy Foundation and Current Developments

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

- **Omnibus Appropriations Act Section 3305,** p. 1374 (December 2022): requires medical device manufacturers to ensure that their devices meet select minimum cybersecurity requirements, supported by device manufacturers and health delivery organizations;
- **National Cybersecurity Strategy, The White House** (March 2023): with an emphasis on protection of and minimum controls for critical infrastructure industries
- Policy options paper **"Cybersecurity is Patient Safety"** released by Senator Mark Warner (D-VA) (November 2022)
- **Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)** (March 2022): Require (p. 127) critical infrastructure owners and operators to report to the Cybersecurity and Infrastructure Security Agency within 72 hours of a substantial cyberattack or within 24 hours of a ransomware payment. Rulemaking process will take up to 3.5 years.
- **S. 3904 Healthcare Cybersecurity Act of 2022** (March 2022): - proposes closer collaboration between the Department of Health and Human Services and the Cybersecurity and Infrastructure Security Agency, with the goal of strengthening cybersecurity in the health and public health sectors.
- **Securities and Exchange Commission proposed rules** (March 2022) aimed at bolstering the cybersecurity-related disclosures of regulated public companies that would require covered public companies to, among other things:
    - Report material cybersecurity incidents on Form 8-K within four business days of a materiality determination.
    - Routinely update investors on such incidents in quarterly and annual reports.

- Analyze whether individually immaterial cybersecurity incidents are material in the aggregate and report those in quarterly and annual reports.
- Make periodic disclosures regarding the company's cyber-related risk management policies and procedures.
- Periodically disclose cyber-related governance information, including the board's oversight and management's implementation of cyber-related risk management policies and procedures.
- Make periodic disclosures regarding board-level expertise in cybersecurity.

- **Federal Trade Commission** policy statement (September 2021) directing health apps and connected device companies to comply with the Health Breach Notification Rule. Under the Rule's requirements, vendors of personal health records ("PHR") and PHR-related entities must notify U.S. consumers and the FTC, and, in some cases, the media, if there has been a breach of unsecured identifiable health information or face civil penalties for violations. The Rule also covers service providers to these entities.
- Class action lawsuits (June 2021) against Scripps Health in State and Fed Courts re ransomware effect on violation of California Confidentiality of Medical Information Act, Federal Trade Commission unfair trade practice regulations and the HIPAA privacy and security rules.
- Government Accountability Office report (June 2021) on the need for enhanced HHS Industry Partnership responsibilities.
- HHS OIG Report on Lack of CMS Cybersecurity Oversight of Networked Medical Devices in Hospitals (June 2021).
- Executive 14028 Order on Improving the Nation's Cybersecurity (May 2021): Section 4 encompasses medical technology security by specifying procurement requirements for Software Bills of Materials and agency guidance on purchasing systems with software defined as "critical software" for purposes of ensuring appropriate security before purchasing or deploying.
- P.L. 116-321 (HR 7898) HITECH Act Amendment (January 2021) requires OCR to consider mitigating fines and audit during a data breach enforcement if it determines

that a breached entity has implemented recognized cybersecurity practices, such as NIST CSF and 405(d) Health Industry Cybersecurity Practices over the previous year.

- **FY '21 NDAA Section 9002** (p. 3383), January 1, 2021– which codified Sector-Specific Agencies (SSAs), previously defined in Presidential Policy Directive 21 (PPD-21), as Sector Risk Management Agencies (SRMAs), and defined how DHS and SRMAs should work with each other to protect critical infrastructure.
- **Cybersecurity Act of 2015** (pp. 104-108): §405c directed HHS to establish the Health Care Industry Cybersecurity Task Force and §405d directed HHS to convene an industry partnership program that eventually joined the HSCC Cybersecurity Working Group and produced the Health Industry Cybersecurity Practices.

##