HEALTHCARE SECTOR CYBERSECURITY

Introduction to the Strategy of the U.S. Department of Health and Human Services

HEALTHCARE SECTOR CYBERSECURITY

Introduction to the Strategy of the U.S. Department of Health and Human Services

Introduction

The healthcare sector is particularly vulnerable to cybersecurity risks and the stakes for patient care and safety are particularly high. Healthcare facilities are attractive targets for cyber criminals in light of their size, technological dependence, sensitive data, and unique vulnerability to disruptions. And cyber incidents in healthcare are on the rise. For instance, HHS tracks large data breaches through its Office for Civil Rights (OCR), whose data shows a 93% increase in large breaches reported from 2018 to 2022 (369 to 712), with a 278% increase in large breaches reported to OCR involving ransomware from 2018 to 2022.

Cyber incidents affecting hospitals and health systems have led to extended care disruptions caused by multi-week outages; patient diversion to other facilities; and strain on acute care provisioning and capacity, causing cancelled medical appointments, non-rendered services, and delayed medical procedures (particularly elective procedures). More importantly, they put patients' safety at risk and impact local and surrounding communities that depend on the availability of the local emergency department, radiology unit, or cancer center for life-saving care.

President Biden has made clear that all Americans deserve the full benefits and potential of our digital future. In the National Cybersecurity Strategy[1], released March 1, 2023, President Biden laid out the U.S. Government's approach to improving the nation's cyber defense and securing our digital infrastructure. The plan included establishing cybersecurity regulations to secure critical infrastructure, using Federal incentives to build security, and holding the stewards of data accountable. As America's healthcare system continues to undergo a digital transformation, it is critical that Government and industry work together to fulfill the President's vision to secure our healthcare system and protect patients from cyber threats. This paper provides an overview of HHS' proposed framework to help the healthcare sector address these cybersecurity threats and protect patients.

Current HHS Cybersecurity Activities within Existing Authorities

Pursuant to the Homeland Security Act of 2002, as amended, and Presidential Policy Directive 21, HHS serves as the Sector Risk Management Agency (SRMA) for the Healthcare and Public Health Sector. In that role, HHS performs the following activities, among others:

- Sharing cyber threat information and intelligence with the sector to mitigate risk from prominent and emerging threats

[1] National-Cybersecurity-Strategy-2023.pdf (whitehouse.gov)

- Providing the sector with technical assistance, guidance, and resources to comply with data security and privacy laws
- Issuing cybersecurity guidance and threat alerts for medical devices
- Publishing healthcare-specific cybersecurity best practices, resources, and guidance

Building off the National Cybersecurity Strategy, HHS partnered with industry to conduct the 2023 Hospital Cyber Resiliency Landscape Analysis[2] to ascertain the current state of hospitals' cybersecurity performance and needs, and to identify additional authorities and resources necessary to address those needs. As a first step coming out of the April 2023 Landscape Analysis publication, HHS took immediate action to fully execute its cybersecurity mission within existing authorities and resources. For example:

1) HHS updated its voluntary healthcare-specific cybersecurity guidance, *Health Industry Cybersecurity Practices*[3], to reflect the current landscape of cybersecurity threats hospitals face.
2) HHS released free healthcare-specific cybersecurity trainings[4] to help small and medium-sized healthcare facilities train their staff on basic cybersecurity practices.
3) The Food and Drug Administration issued guidance[5] for medical device manufacturers outlining pre-market cybersecurity recommendations and requirements for all new medical devices.
4) The HHS Office for Civil Rights issued new telehealth guidance[6] for healthcare providers and patients to help educate patients on telehealth and the privacy and security of protected health information.

HHS is maximizing its sector support within existing authorities and resources. For more information on HHS's sector-facing cybersecurity activities, please see the attached infographic below.

Path Forward on Cybersecurity Improvements

HHS will take the following concurrent steps to build on the aforementioned actions and advance cyber resiliency in the healthcare sector:

1) Establish voluntary cybersecurity performance goals for the healthcare sector
2) Provide resources to incentivize and implement these cybersecurity practices
3) Implement an HHS-wide strategy to support greater enforcement and accountability
4) Expand and mature the one-stop shop within HHS for healthcare sector cybersecurity

1. Establish voluntary cybersecurity goals for the healthcare sector

[2] 405d-hospital-resiliency-analysis.pdf (hhs.gov)
[3] HICP-Main-508.pdf (hhs.gov)
[4] 405(d) :: Knowledge on Demand (hhs.gov)
[5] Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions (fda.gov)
[6] HHS Office for Civil Rights Issues Resources for Health Care Providers and Patients to Help Educate Patients about Telehealth and the Privacy and Security of Protected Health Information | HHS.gov

Currently, healthcare organizations have access to numerous cybersecurity standards and guidance that apply to the sector, which can create confusion regarding which cybersecurity practices to prioritize. HHS, with input from industry, will establish and publish voluntary sector-specific cybersecurity performance goals, setting a clear direction for industry and helping to inform potential future regulatory action from the Department.

The Healthcare and Public Health Sector-specific Cybersecurity Performance Goals (HPH CPGs) will help healthcare institutions prioritize implementation of high-impact cybersecurity practices. HPH CPGs will include both "essential" goals to outline minimum foundational practices for cybersecurity performance and "enhanced" goals to encourage adoption of more advanced practices.

2. Provide resources to incentivize and implement these cybersecurity practices

HHS will work with Congress to obtain new authority and funding to both administer financial support for domestic hospital investments in cybersecurity and, in the long term, enforce new cybersecurity requirements through the imposition of financial consequences for hospitals. HHS envisions the establishment of two programs:

- An **upfront investments program**, to help high-need healthcare providers, such as low-resourced hospitals, cover the upfront costs associated with implementing "essential" HPH CPGs, and
- An **incentives program** to encourage all hospitals to invest in advanced cybersecurity practices to implement "enhanced" HPH CPGs.

3. Implement an HHS-wide strategy to support greater enforcement and accountability

Funding and voluntary goals alone will not drive the cyber-related behavioral change needed across the healthcare sector. Given the increased risk profile of hospitals, HHS aspires to have all hospitals meeting sector-specific CPGs in the coming years. With additional authorities and resources, HHS will propose incorporation of HPH CPGs into existing regulations and programs that will inform the creation of new enforceable cybersecurity standards.

HHS is working towards and expects to seek comment on these proposed actions based on the HPH CPGs:

- CMS will propose new cybersecurity requirements for hospitals through Medicare and Medicaid.
- The HHS Office for Civil Rights will begin an update to the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, in spring of 2024, to include new cybersecurity requirements.

HHS will also continue to work with Congress to increase civil monetary penalties for HIPAA violations and increase resources for HHS to investigate potential HIPAA violations, conduct pro-active audits, and scale outreach and technical assistance for low-resourced organizations to improve HIPAA compliance. In the interim, HHS will continue to investigate potential HIPAA violations.

4. Expand and mature the one-stop shop within HHS for healthcare sector cybersecurity

HHS will mature its "one-stop shop" cybersecurity support function for the healthcare sector within the Administration of Strategic Preparedness and Response (ASPR) to more effectively enable industry to access the support and services the Federal Government has to offer. A one-stop shop will enhance coordination within HHS and the Federal Government, deepen government's partnership with industry, increase HHS's incident response capabilities, and promote greater uptake of government services and resources such as technical assistance, vulnerability scanning, and more. ASPR has the response expertise and capabilities appropriate for helping the sector navigate and access the array of cybersecurity supports available from HHS and across the Federal Government.

Next Steps

Taken together, HHS believes these goals, supports, and accountability measures can comprehensively and systematically advance the healthcare sector along the spectrum of cyber resiliency to better meet the growing threat of cyber incidents, especially for high-risk targets like hospitals. Acting on these priorities will protect the health and privacy of all Americans and enable safe access to health care.

HHS #Cyber Team

HHS works as a team to help the Healthcare and Public Health (HPH) sector prepare for and respond to cyber threats. Cyber Safety is Patient Safety!

The Advanced Research Projects Agency for Health (ARPA-H) launched the Digital Health Security (DIGIHEALS) project to ensure patients continue to receive care in the wake of a medical facility cyberattack.

The Health Sector Cybersecurity Coordination Center (HC3) enriches and analyzes cyber security threat information to develop objective mitigations for and in collaboration with the health and public health sector. HC3 achieves this through directed engagements, action based alerts, and public threat briefings.

The HHS 405(d) Program is a collaborative effort between the Health Sector Coordinating Council and the federal government to align healthcare industry security approaches by providing useful HPH-focused resources to help educate, raise awareness, and drive behavioral change.

The Office of the National Coordinator for Health Information Technology (ONC) in the HHS Office of the Secretary, is a resource to the entire health system to support the adoption of health information technology and the promotion of nationwide, standards-based health information exchange to improve healthcare, including information privacy and security.

The Office of National Security (ONS) conducts all-source intelligence analysis to inform HHS policy and drive operational planning activities. ONS executes its mission, through departmental and Intelligence Community coordination, by providing timely and relevant threat intelligence to HHS senior leaders and staff involved in executing the HPH SRMA mission.

ASPR

The Administration for Strategic Preparedness and Response's (ASPR) coordinates all HHS cybersecurity support and leads external collaboration in its role as the Sector Risk Management Agency (SRMA) on behalf of HHS for the Healthcare and Public Health (HPH) sector.

The Centers for Medicare & Medicaid Services (CMS) protects and controls the confidentiality, integrity, and availability of CMS information and information systems. CMS also works to promote cybersecurity and safe care in response to cyber threats across its programs, including Medicare, Medicaid, the Children's Health Insurance Program, and the Health Insurance Marketplaces.

The Office for Civil Rights (OCR) administers and enforces the HIPAA Privacy, Security, and Breach Notification Rules through investigations, rulemaking, guidance, and outreach. The HIPAA Rules establish rights for individuals to their protected health information (PHI), requirements for HIPAA regulated entities on uses and disclosures of PHI, and privacy and security protections of PHI. OCR supports improved cybersecurity through cybersecurity investigations resolved with technical assistance, corrective action plans, or civil money penalties and by publishing cybersecurity resources for regulated entities and consumers through guidance, bulletins, newsletters, videos, and applications.

The Food and Drug Administration (FDA) informs patients, healthcare providers and facility staff, and manufacturers about cybersecurity vulnerabilities for connected medical devices and requires that medical devices meet specific cybersecurity guidelines.

CWG

The HHS SRMA Cybersecurity Working Group (CWG) is the primary mechanism used to coordinate HHS's execution of its statutory responsibility as the HPH SRMA. The CWG is the body that coordinates and collaborates across the HHS cyber community to identify cyber threats to the HPH sector, coordinates across HHS divisions to prepare for and mitigate potential or identified cyber incidents, shares information, and coordinates policy recommendations and messaging to strengthen and build resiliency within the HPH sector against cyber threats.