MITRE Center for Data-Driven Policy

CYBERSECURITY AND PATIENT SAFETY IN THE HEALTHCARE SETTING

By Meredith Benedict, Penny Chase, and Margie Zuk

The healthcare sector faces a complex set of challenges in its information technology and operational environment, with threats that can impact patient care, business operations, medical devices, facilities, protected health information, and public confidence.[1] Healthcare delivery organizations (HDOs) remain a prime target for cyber attacks. Home and mobile health data collection and exchange increase attack surfaces; a number of steps need to be taken to enable these innovations to scale safely and engender user confidence.

Implementing cyber hygiene practices is a shared responsibility across the federal government and private sector. The technologies that are bringing new innovations to healthcare are rapidly evolving and attackers are becoming more sophisticated. The process for creating cyber hygiene practices needs to be streamlined and agile to adapt to different clinical environments and varying levels of expertise, resources, and computational capabilities. These practices must also be designed to not inadvertently interfere with patient safety.

As a nonprofit operator of federally funded research and development centers focused on both advancing cybersecurity innovation and modernizing healthcare, MITRE brings a unique perspective to this space. MITRE's interdisciplinary approach, informed by our work across federal agencies, helps healthcare stakeholders identify and capture best practices for incorporating cybersecurity into the healthcare setting, fortify their institutions against cyber attacks, and support the development of new cybersecurity policies to address emerging threats.

Initially derived in response to Senator Mark Warner's white paper *Cybersecurity is Patient Safety: Policy Options in the Health Care Sector*, this paper summarizes insights and recommendations for policymakers on ways to improve cybersecurity across the health sector. MITRE subject matter and technical experts who contributed to this report are working across government and in partnership with providers to help address the threats facing HDOs and inform planning for future defensive capabilities.

MITRE Observations and Recommendations to Improve Cybersecurity in the Healthcare Setting

IMPROVING OUR NATIONAL CYBERSECURITY RISK POSTURE IN THE HEALTHCARE SECTOR

Build on the mature security practices developed by government HDOs (e.g., the Defense Health Agency's [DHA] secure baselines and Department of Veterans Affairs' [VA] patch management process) and the health cybersecurity framework developed by the Healthcare and Public Health Sector Coordinating Council (HSCC) and the Department of Health and Human Services (HHS) to create more tailored guidance for health sector stakeholders.

1. Include HDOs operated by the federal government (e.g., VA and DHA, which make up a large share of the healthcare market) in the Health Care Cybersecurity Ecosystem figure developed by Senator Warner,[2] alongside federal agencies providing regulation and oversight.
2. Consider healthcare industry members' interest in a more tailored guidance in the National Institute of Standards and Technology (NIST) Cybersecurity Framework targeting HDOs and medical device manufacturers.
3. As NIST develops version 2.0 of the Cybersecurity Framework, consider developing a healthcare-specific NIST Cybersecurity Framework 2.0 profile collaboratively through an industry association or organization using a NIST-provided template. In March 2023, the HSCC and HHS published the Health Care and Public Health Cybersecurity Framework Implementation Guide. This guide could be leveraged in creating a profile.

MODERNIZING REGULATORY FRAMEWORKS, INCLUDING HIPAA SECURITY[3] AND PRIVACY[4] RULES, TO INCREASE CYBERSECURITY PROTECTIONS

The healthcare ecosystem now extends beyond healthcare providers and their business relationships. The federal government should increase assurance that patients have awareness and agency over data security, risk, and sharing, with the ability to seek redress for the unauthorized use of data.

4. Incorporate in each of the HIPAA Rules that non-covered entities cannot use the term "HIPAA compliant," and reference Federal Trade Commission (FTC) consumer protections against deceptive or misleading claims and marketing.
5. Capture additional data protection specifications for Health Information Technology in the HIPAA Security Rule from the Office of the National Coordinator (ONC) (e.g., data segmentation, data tagging) and require updates to the regulations as specifications change and are adopted.
6. Update HIPAA Rules to clarify that certain healthcare data collected by wearables, health Internet of Things (IoT) devices, and healthcare apps that may currently be deemed "health adjacent data" are protected health information and therefore subject to the HIPAA Rules.
7. Ensure a cohesive, integrated, and adaptable regulatory framework incorporating HIPAA, ONC regulations, FTC rules, and the rules and agreement on Human Subjects Research. This framework and these rules should be amended to:

a. Recognize the patient as an interested party in data transactions when those transactions involve a patient's personal health data.

i. Offer the patient additional awareness and agency over securing, sharing, and removing data from services and databases.

ii. Provide a means for patients to file claims against entities that violate these rules.

b. Clearly set out cybersecurity expectations to protect patient data in this framework and incorporate into these rules as applicable.

i. The rules (especially the FTC consumer protection rules) should include provisions requiring the education of patients about the different levels of cyber protective services that the entities using their data employ.

c. The FTC Health Breach Notification rule is currently reactive in the event of a breach. Third-party, non-HIPAA-covered entities should be encouraged to take proactive measures to better protect individuals' data.

i. This could look like specific cybersecurity and other data protection requirements for entities holding sensitive data.

ii. Consider whether corrective action plans could be required for companies that do not demonstrate offering the required level of protection.

d. The FTC should explore the benefits of secure smart contracts and similar technologies for use when companies seek to engage with individuals regarding data exchange, usage, or storage.

DEVELOPING THE HEALTHCARE CYBERSECURITY WORKFORCE

Cybersecurity skills should be developed from within the healthcare arena and not viewed as the purview of a separate workforce.

8. The Hospital Incident Command System is an often-used healthcare-oriented emergency management methodology that could serve as both model and potential integration point for cybersecurity workforce development training.

9. The designated lead HDO should work with, or deputize, personnel from NIST's National Initiative for Cybersecurity Education (NICE) to administer a workforce development program. A team that includes experienced healthcare cybersecurity experts, workforce development experts, and professionals with clinical operations, healthcare technology management, and health IT expertise should develop its curriculum.

a. MITRE produced a comprehensive Medical Device Cybersecurity Training model for VA healthcare technology management professionals that provides tiered learning capabilities tied to the NICE Framework and, where available, existing training materials that could be readily expanded beyond medical devices to encompass broader healthcare IT cybersecurity.

IMPROVING HDO CYBERSECURITY CAPABILITIES

The process for creating cyber hygiene practices needs to be streamlined and agile, and to recognize that one size does not fit all. Medical devices have different clinical functions and computational capabilities, so the trade-offs between security and patient safety will vary. HDOs have different clinical environments and varying levels of expertise and resources to implement cyber hygiene practices, so their practices may also differ.

10. Including minimum cyber hygiene in Medicare Conditions of Participation (CoP) would have a major impact on adoption but must accommodate an ability to quickly evolve practices as the technology and threat environments evolve, and to define different sets of practices appropriate for different HDO environments.

    a. An alternative, or addition, to establishing cyber hygiene requirements in the CoP would be assigning the Accrediting Organizations (e.g., The Joint Commission and DNV) with the responsibility to set more detailed requirements than those established in the CoPs, as well as to create additional certification programs beyond accreditation for Medicare.

11. Require medical device manufacturers to update their products throughout the life cycle and consider requiring additional steps to ensure that medical device security patches are provided in a timely fashion to ensure the software that runs it can be reasonably protected against current cybersecurity threats. Transparency, with reasonable lead times, about end of life is important so HDOs can plan for replacement.

12. Accelerated paths to creating and managing Software Bill of Materials (SBOMs) throughout the device life cycle should be pursued in ways that are efficient, streamlined, and maximally useful for software users while not unduly burdensome for software producers. We note that:

    a. The Food and Drug Administration's (FDA) work on SBOMs with industry has positioned the health IT industry, as a group, to be more ready than others to bring SBOMs into the requirements for products. However, the challenges of managing SBOMs are not trivial, and the FDA needs to adopt a solution-based approach rather than a technology-based approach to the life-cycle management of SBOMs. MITRE research supports an approach that combines multiple, evolving technologies in a meeting place solution, to achieve maximum value while mitigating unexpected burdens for industry.

    b. While the ability of industry to include SBOMs in new products will be cleaner and easier to implement, SBOMs have potential value for all software products. Including some form of retroactive requirement for SBOMs can bring significant value to cyber supply chain risk management; the government needs to make this process as streamlined as possible for industry.

13. MITRE interviewed HDOs while developing the MITRE Ransomware Resource Center. We learned that HDOs desire a single point of entry for cybersecurity information and reporting and they are more willing to share information now than in the past. HDOs want a streamlined way to share information about cyber incidents, vulnerabilities (especially in medical devices), patching and mitigations for those vulnerabilities, and best practices for responding to and recovering from cyber incidents. In addition, they want not only to share this information, but also to analyze the data to understand trends, better understand risk, and prioritize their cyber activities.

    a. When considering models for information sharing it is important that smaller and less-resourced HDOs can participate, both financially (even a few thousand dollars may be too costly for a small HDOs) and technically (the information needs to be actionable, not just for organizations with full-fledged Security Operations Centers).

b. In addition to considering Information Sharing and Analysis Centers as an information sharing model, the health sector should look at approaches from other sectors. For example, the aviation sector shares near-miss information and technical studies to improve aviation safety in the MITRE-operated Aviation Safety Information Analysis and Sharing (ASIAS) Program. ASIAS has drawn together a wide variety of safety data and information sources across government and industry, including voluntarily provided safety data. The program has matured to the point that it now incorporates voluntarily provided safety data from operators that represent 99 percent of U.S. air carrier operations in the National Airspace System. ASIAS continues to pioneer advanced analytical capabilities to provide safety teams with enhanced insight into these operations.

EMERGENCY PREPAREDNESS AND RESPONSE

Cybersecurity incidents need to be included in emergency response and preparedness planning as a hazard due to widespread impacts and potential for long-term disruption.

14. HDOs should be required to train all staff members within their system to use alternate or legacy systems in the event of catastrophic failure to connected systems. These procedures need to be documented in the HDO's emergency preparedness and response plans and regularly exercised. The unique challenges posed by cyber attacks compared with other hazards are extended downtimes (weeks or months) and widespread disruptions across the HDO and potentially the region.

    a. In addition, HDOs should develop regional relationships with peers and emergency management organizations (e.g., HHS Administration for Strategic Preparedness and Response, Healthcare Coalitions and Regional Disaster Health Response Systems, Cybersecurity and Infrastructure Security Agency (CISA), and Federal Emergency Management Agency regional representatives) that can provide aid in preparing for, responding to, and recovering from an incident, as discussed in the Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook.

15. Assets such as medicines, vaccines, devices, and other medical supplies needed for an effective response to a cyber incident should be considered for inclusion in the Strategic National Stockpile (SNS) to ensure continuity of clinical care in affected regions. Consideration of recommendations from health cyber experts in healthcare delivery will optimize the U.S. Government investments in the SNS. Conducting regional pilots is one of several strategies to answer some of these planning questions and define the most appropriate models.

16. Consider regulation that would include, at a minimum, monitoring market function and opportunistic behavior by insurers offering policies for cyber insurance that functions to provide organizations such as HDOs coverage for cyber attacks and related risks.

CYBERSECURITY IN THE HEALTHCARE AT HOME SETTING

Individual and provider-driven healthcare at home and mobile health models are expected to increase due to individuals' desire to receive more of their care at home and efforts to provide more equitable access to care in rural and other underserved areas, among other reasons. These new modalities and networks for home and mobile health data collection and exchange also increase attack surfaces, raising patient safety and individual privacy and security considerations.

17. Elevate the visibility of the attack surface vulnerabilities in models of care established in the home setting by HDOs and ensure that questions regarding the home environment are examined without creating undue burden on the end users.

    a. Create a stepped workforce training program targeting the home healthcare provider workforce and consider how training for these workers can enable them to earn more as they develop increased capabilities.

    b. Classify different types of devices (e.g., a device that is directly communicating to an HDO with no data-at-rest, a device with data-at-rest that then moves to an HDO, a device with data-at-rest that moves to a manufacturer's cloud) and define who has control of, and liability regarding, which elements. In general, we agree with the recommendations in the National Cybersecurity Strategy[5] regarding these issues.

    c. Expand efforts to educate and train individuals using the devices; we also agree with the National Cybersecurity Strategy regarding the need for IoT security labels that inform individuals of risks and rights.

    d. Engage small and startup businesses and consumer health and wellness companies in the work of the HSCC Cybersecurity Working Group.

    e. Incentivize appropriate mitigations and configurations, such as the adoption of common standards and mandating that Internet Service Providers and software companies have responsibilities, rather than placing the entire burden on HDOs, medical device manufacturers, or home users.

    f. Prioritize federal investment in research and other activities that yield insights into the opportunities and risks related to artificial intelligence (AI) as that technology evolves, and devise policy mechanisms to flexibly address vulnerabilities created by AI, such as those that may impact patient and consumer safety and outcomes and/or be exploited by cyber criminals.

About MITRE

MITRE is a not-for-profit company that works in the public interest to tackle difficult problems that challenge the safety, stability, security, and well-being of our nation. We operate multiple federally funded research and development centers (FFRDCs) with over 10,000 technical and subject matter experts working to solve problems for a safer world. For over 50 years, MITRE has been at the forefront of the nation's cybersecurity, and since 2014, MITRE has operated the National Cybersecurity FFRDC, which also supports NIST's National Cybersecurity Center of Excellence. MITRE is also a trusted advisor to policymakers, providing formal and informal support to the Office of the National Cybersecurity Director and the Federal Chief Information Security Officer.

Furthermore, the healthcare sector has relied extensively on MITRE's cybersecurity capabilities and expertise. MITRE operates the only Health FFRDC dedicated to modernizing healthcare, and works on behalf of sponsors across the Department of Health and Human Services. Through multidisciplinary teams, this Center serves all federal agencies with health and human services missions: the Centers for Medicare & Medicaid Services, Centers for Disease Control and Prevention, Food and Drug Administration, National Institutes of Health, Health Resources and Services Administration, Administration for Children and Families, and more. MITRE capabilities include conducting landscape analyses of cybersecurity ecosystems in the healthcare setting, as well as authoring articles, developing playbooks, and publishing reports to help healthcare practitioners and stakeholders identify and capture best practices for incorporating cybersecurity into the healthcare setting and fortify their institutions against threats. MITRE also serves in an advisory capacity on the HSCC Cybersecurity Working Group supporting the development of best practice documents for health providers, medical device security, supply chain cybersecurity, cyber workforce development, and more.

Meredith Benedict is a Principal in MITRE Labs' Health Innovation Center. In collaboration with MITRE Engenuity, she works to leverage MITRE's diverse capabilities in digital health, policy, and systems engineering to the challenge of maximizing healthspan and accelerating human-centered, integrated, and safe AgeTech solution innovations. Previous MITRE roles include serving as co-project lead for the independent Coronavirus Commission for Safety and Quality in Nursing Homes and as project or task lead of various projects to advance program and policy innovations for MITRE's FFRDC sponsors in health and veterans affairs.

Penny Chase is a Senior Principal Scientist and IT and Cybersecurity Integrator in the Data and Human Centered Solutions Innovation Center in MITRE Labs. She has spent 37 years leading MITRE and government-sponsored projects in medical device and healthcare cybersecurity; malware and threat information sharing; malware analysis and reverse engineering; machine learning; and human language technology.

Margie Zuk is a Senior Principal Cybersecurity Security Engineer at MITRE, with over 40 years of cybersecurity experience. She is currently the Cyber Engagement Lead for Healthcare in the Cyber Solutions Innovation Center, where she leads MITRE's support to the FDA CDRH on Medical Device Cyber Security and supports health cyber initiatives across HHS. Margie also serves as an advisor to the Healthcare and Public Health Sector Coordinating Council (HSCC) Cybersecurity Working Group.

With special thanks for contributions from:

Beverly Ortega Babers, Domestic Policy Lead, MITRE's Center for Data-Driven Policy

Katie Enos, Senior Principal, Government Relations
Robert D. Lieberthal, PhD, Principal, Health Economics
Kathy Mikk, Principal, Health Policy Analysis
Sue Wang, Principal Cybersecurity Engineer

[1] https://healthcyber.mitre.org/wp-content/uploads/2021/11/77409909WP_-Health-Delivery-Organizations-and-Ransomware_Final-11-23.pdf
[2] Figure 1, Page 7 0320658680B8F1D29C9A94895044DA31.cips-report.pdf (senate.gov)
[3] Health Insurance Portability and Accountability Act Security https://www.hhs.gov/hipaa/for-professionals/security/index.html
[4] Summary of the HIPAA Privacy Rule | HHS.gov
[5] National-Cybersecurity-Strategy-2023.pdf (whitehouse.gov)

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™