FDA Collaborates with MITRE to update Medical Device Cybersecurity Playbook

Related Professionals

Hamilton B. Barber
803.253.8236
HBarber@nexsenpruet.com

Practices

Health Law

Industries

Health Care

Article
12.06.2022

On November 14, 2022, under contract with the United States Food and Drug Administration (FDA), the MITRE Corporation (MITRE), an organization that administers the National Cybersecurity Center of Excellence, a federally funded research and development center dedicated to cybersecurity, published an update to the *Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook* (the "Playbook"). MITRE also published a *Quick Start Companion Guide* to the Playbook, which is shorter than the Playbook and consists of tables that align with the structure of the Playbook. MITRE, under contract with the FDA, had prepared and published the first version of the Playbook in October 2018, which followed the 2017 *WannaCry* ransomware attack (the first known ransomware attack to affect networked medical devices). Since the publication of the first version of the Playbook, the healthcare and public health sector has experienced an increasing number of cyber incidents. For instance, from mid-2020 through 2021, 82% of healthcare systems reported a cyberattack, 34% of which reportedly involved ransomware. Moreover, 133 healthcare entities in the United States appeared on a ransomware extortion blog in 2021.

The Playbook is a resource designed primarily for healthcare delivery organizations (HDOs), such as hospitals and large physician practices, and can be incorporated into an HDOs' existing medical device cybersecurity response plan or serve as a starting point for HDOs that have no response plan. The Playbook outlines a framework to assist HDOs, their staff involved in medical device cybersecurity incident preparedness and response, and other stakeholders, such as device manufacturers and other entities that support HDOs' response efforts, prepare for and respond to medical device-related cybersecurity incidents helping ensure effectiveness of medical devices and patient care and safety. The framework outlined in the Playbook is designed to provide baseline medical device cybersecurity information for emergency preparedness and response; define roles and responsibilities for internal and external responders; describe a standardized approach to response efforts that yields an appropriate and unified regional response; enhance coordination among medical device cybersecurity stakeholders; identify resources HDOs may leverage as a part of preparedness and response activities; and inform decision making.

According to the Playbook, regional outreach and collaboration can strengthen HDO preparedness for and response to medical device-related cybersecurity incidents. Regional collaboration to strengthen *preparedness* may come in the form of, but is not limited to, sharing medical device best practices, conducting joint exercises, and sharing cybersecurity alerts. Regional collaboration to strengthen *incident response* may come in the form of, but is not limited to, requests for technical assistance and notification to regional partners of aberrant device behavior or discovered vulnerabilities. Some examples of regional partners include state and local health and law enforcement agencies, local Federal Bureau of Investigation (FBI) InfraGard chapters, Cybersecurity and Infrastructure Security Agency (CISA) regional offices, regional hospital trade associations, and regional Health Information Exchange(s) (HIE).

The Playbook's high-level structure for the process by which HDOs prepare for and respond to medical device cybersecurity incidents, namely attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with medical devices, is informed by the incident response lifecycle outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 Revision 2, *Computer Security Incident Handling Guide*. The phases of the incident response lifecycle are as follows:

- Preparation: "establishing an incident response capability so that the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks, and applications are sufficiently secure."
- Detection and Analysis: "determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem."
- Containment, Eradication, and Recovery:
  - *containment* prevents an incident from overwhelming resources or increasing damage;
  - *eradication* remediates affected hosts; and
  - *recovery* "restore[s] systems to normal operation, confirm[s] that the systems are functioning normally, and (if applicable) remediate[s] vulnerabilities to prevent similar incidents."
- Post-Incident Activity: "improving security measures and the incident handling process … by reviewing what occurred, what was done to intervene, and how well intervention worked."

According to the Playbook, during the Preparation phase, HDOs assess their cybersecurity posture and develop incident handling processes and procedures, which may include, among other things, incorporating cybersecurity principles in medical device procurement processes, such as articulating via written agreement responsibility and accountability as between the medical device manufacturer and HDOs; inventorying medical device assets; analyzing hazard vulnerabilities; conducting training; and creating draft communication templates for different incident response messaging needs. During the Detection and Analysis phase, HDOs establish that an incident has occurred; categorize and prioritize the incident to determine the appropriate level of response; informally and formally report and notify individuals in accordance with legal obligations; analyze the incident; and document all the activities undertaken as part of incident response. During the Containment, Eradication, and Recovery phase, many HDOs implement a "contain, clean, and deny" strategy to halt the incident, repair the damage, and restore services and a "monitor and record" strategy when cybercriminal activity is suspected. During the Post-Activity phase, HDOs identify what went well and what did not go well during the incident response process, which is information that can be leveraged to improve existing plans and aid regional partners.

Although cybersecurity threats and vulnerabilities cannot be eliminated, the Playbook is a resource that can assist HDOs and other stakeholders in reducing their cybersecurity risks. In addition to (or as part of) their incident management and response teams, HDOs should involve experienced cybersecurity legal counsel throughout the incident response lifecycle to ensure their organization's legal obligations are being considered and met, as appropriate.