December 5, 2022

MITRE Corp. and FDA Release Updated Guidance on Medical Device Cybersecurity Incidents

Medical device cybersecurity has been top of mind at the Food and Drug Administration (FDA) in recent years. In April, the FDA proposed an update to its current guidance on cybersecurity for medical devices and recently released its Cybersecurity Modernization Action Plan. Following these moves, the FDA and MITRE Corp. released an updated version of their "Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook." The playbook provides healthcare organizations with actionable strategies and resources for responding to cyber incidents while ensuring medical device security. First published in 2018, the playbook outlines how hospitals and other healthcare delivery organizations can develop a cybersecurity preparedness and response framework. It intends to supplement existing emergency management and/or incident response capabilities at healthcare organizations with regional preparedness and response recommendations for medical device cybersecurity incidents. Its focus is on response to an incident stemming from a compromised medical device and not day-to-day risk management. While the entire document is worth reviewing, we identified a few key recommendations from the document that hospitals and others may wish to consider further in the context of their own cybersecurity incident response planning processes.

- Know your regional partners: Develop mutual aid agreements with regional partners for medical device cybersecurity or supplements as part of broader incident response mutual aid agreements—to include loaner devices, diverting patients to a facility with operational devices, and incident response assistance.
- Bake cybersecurity incident response into the procurement process: During the procurement process, consider securing a commitment by the manufacturer to participate in your facility's cybersecurity exercises to build the facility-manufacturer relationship, define the roles and responsibilities of each party, and better understand the coordination efforts needed during a device incident. Consider building the cost for mitigating device vulnerabilities into the device purchase and/or maintenance fees (e.g., ensuring that spare or extra devices will be available during an incident).
- Know your devices: Maintain a centrally managed, baseline set of information about all medical devices (e.g., operational status, location, network information).
- Incident response plan: During your next review of your organization's incident response plan, consider whether your plan includes a risk-based process for bringing medical devices back online or workarounds/contingencies for extended downtimes (e.g., days, weeks, months).

Day Pitney's healthcare and cybersecurity attorneys have dozens of years of combined experience advising hospitals and other healthcare providers on incident response planning, mitigation, response, and recovery. Please let us know if you would like to discuss this new guidance and our thoughts on how hospitals and others can best use it to protect their organization and
patients.

Would you like to receive our *Day Pitney C.H.A.T. Newsletter?* Sign up here.

Authors

William J. Roberts

Partner

Hartford, CT | (860) 275-0184

wroberts@daypitney.com