Booz | Allen | Hamilton®

# Securing Connected Medical Devices

OCTOBER 2019

# THE CHALLENGE IN SECURING CONNECTED MEDICAL DEVICES

The rise of ***connected medical devices***—which are devices that connect or integrate with other systems (e.g., other devices, tools, networks, and services)—represent significant innovations in patient care. These innovations face new and diverse threats not previously in existence. As soon as a medical device is connected in some way—either wirelessly or wired, using a persistent connection or one that is transient, either one-directional or bi-directional—the medical device becomes much easier to disrupt and the potential disruption much more severe. Whereas unconnected smart devices contain vulnerabilities that have created sensational news headlines, local proximity (e.g., physical contact or within 2–3 feet) is required for these vulnerabilities to be exploited. The need for (near) physical access to exploit vulnerable devices has made it difficult for sophisticated adversaries to achieve widespread effects.

**Physical proximity is not required to compromise a connected medical device.** To an attacker, connected medical devices are just computers on the network and they are vulnerable to the same types of cyberattacks that threaten every digital device. In July 2019, the Department of Homeland Security (DHS) released an advisory relating to a set of vulnerabilities known as URGENT/11, which were present in nearly 200 million devices worldwide[1] running VxWorks software.[2] It was shocking news—the vulnerabilities disclosed and the potential for exploitation had been present since 2006. Three months later (in October 2019), the Food and Drug Administration (FDA) released its own warning that some medical devices were affected by the URGENT/11 vulnerabilities, and that, **"These vulnerabilities may allow anyone to remotely take control of the medical device** and change its function, cause denial of service, or cause information

*The medical device ecosystem is at a critical moment where strong leadership across industry, government, and the public is needed as we prepare for a secure connected future.*

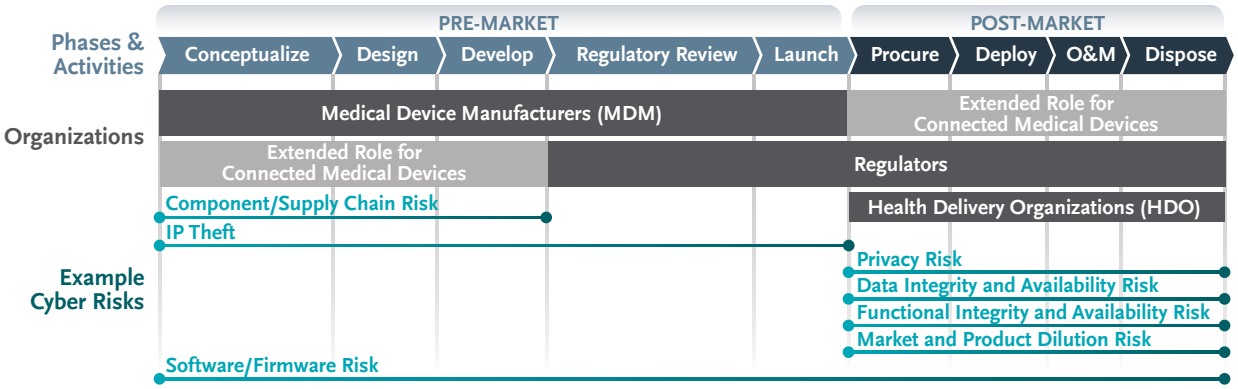


Figure 1: The Lifecycle of a Connected Medical Device and the Potential Threats at Each Phase

leaks or logical flaws, which may prevent device function."[3]

**The connected health ecosystem faces unique threats and risks.** The medical device lifecycle (Figure 1) is the sequence of activities needed to move a medical device from an idea (i.e., conceptualization) to end of life (i.e., disposal)—potentially years or decades later. This lifecycle has proven successful in addressing the paramount concerns of efficacy and safety when bringing unconnected medical products to market. Connected medical devices bring new challenges.

1. Connected medical devices extend the roles of some organizations. To properly assess efficacy and safety of connected medical devices, regulators are extending their activities further into the pre-market phase (e.g., to define or validate that security requirements are met).[4] Medical Device Manufacturers (MDM) are increasingly becoming information technology (IT) partners, who have a new and direct role in the post-market phase (e.g., to sustain the systems that connected medical devices rely on to operate). Health Delivery Organizations (HDO) face new roles too, as they learn to mitigate risks within connected health devices that rely on third party, off-premise technology to work properly.
2. Connected medical device vulnerabilities never "expire." As the URGENT/11 crisis demonstrated, sometimes even "secure" systems have latent vulnerabilities that go from "undisclosed" to "easily exploited" in a matter of days. Because physical access is not required, threat actors have the opportunity to spend years working to exploit undisclosed vulnerabilities that escaped into the wild.
3. A threat-centric mindset is needed to secure the connected health ecosystem. It is possible for sophisticated attackers to surreptitiously change diagnosis or treatment data without detection.[5] Defining policies and assessing compliance are not sufficient to prevent this type of compromise. Even the most compliant organizations still fall victim to sophisticated threats, with 77% of successful attacks using pre-existing vulnerabilities.[6] Potential threats and exploits (e.g., using MITRE ATT&CK7) must be continually assessed throughout the lifecycle.
4. Connected medical devices face diverse risks, with no "one size fits all" solution. Patients and healthcare professionals must be able to rely on the confidentiality, integrity, and availability of connected medical devices (and their data). But there are many potential risks that have the potential to erode this trust—from supply chain issues (pre-market) to privacy concerns (post-market). No single "security" approach is sufficient; many complementary solutions are needed.

The medical device ecosystem is at a critical moment where strong leadership across industry, government, and the public is needed as we prepare for a secure connected future. To successfully combat cybersecurity threats, every stakeholder will need to take action in a manner different than today—with the agility to adapt their actions over time as the threats they face evolve.

# ADDRESSING THE CHALLENGE

In Spring 2019, the eHealth Initiative (eHI) convened a roundtable of healthcare executives for a multi-disciplinary discussion on the challenges and potential solutions for securing medical devices. The key takeaways of that discussion were:

- ***The status quo is not sufficient.*** Securing the connected health ecosystem is a present challenge that has the potential to disrupt the entire industry if not dealt with quickly.
- ***Everyone plays a role.*** Potential solutions require many coordinated and diverse activities, working in concert to properly address all threats and risks.
- ***Important work is already underway.*** The industry has already created significant resources (e.g., the Joint Security Plan) as a starting point. There is much more to do, but many of the important issues are currently being discussed.
- ***Keep an eye to the future.*** The solutions required to "fix" today's vulnerable devices are not the same as those required to "prevent" future devices from being vulnerable. The future needs to be designed while still addressing today's needs.
- ***More engagement is needed.*** Health Sector Coordinating Council (HSCC) and Health Information Sharing and Analysis Center (H-ISAC) events are a great way to engage stakeholders in productive dialogues that can benefit everyone.

# RESOURCES

The following resources are available to assist stakeholders in advancing their cyber-readiness:

- The Healthcare and Public Health Sector Coordinating Council
  - Medical Device and Health IT Joint Security Plan
  - *Healthcare and Public Health Sector-Specific Plan*
  - *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*
- U.S. Food and Drug Administration
  - FDA Fact Sheet
  - FDA Cybersecurity
- U.S. Department of Homeland Security
  - Memorandum of Understanding 225-19-002
  - Cybersecurity and Infrastructure Security Agency
  - National Cybersecurity and Communications Integration Center
  - United States Computer Emergency Readiness Team
  - Industrial Control Systems Cyber Emergency Readiness Team
- U.S. Department of Health and Human Services Cyber Security Guidance Materials
  - Ransomware Information
- National Institute of Standards and Technology Cybersecurity Framework
- *Careful Connections: Building Security in the Internet of Things*, published by the Federal Trade Commission
- The National Network of Fusion Centers
- The Joint Commission's emergency management resources

# END NOTES

[1] https://www.wired.com/story/vxworks-vulnerabilities-urgent11/

[2] https://www.us-cert.gov/ics/advisories/icsa-19-211-01

[3] https://www.fda.gov/medical-devices/safety-communications/urgent11-cybersecurity-vulnerabilities-widely-used-third-party-software-component-may-introduce

[4] https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices-0

[5] https://www.washingtonpost.com/technology/2019/04/03/hospital-viruses-fake-cancerous-nodes-ct-scans-created-by-malware-trick-radiologists/

[6] http://www.pharmexec.com/lessons-pharma-merck-cyber-attack

[7] https://attack.mitre.org/


MEDICAL REPORT
02-08-38 MALE
: 02 :43 080
:586 :89 403
:253 :684 :01
:99 :RP_809

**About Booz Allen**

For more than 100 years, business, government, and military leaders have turned to Booz Allen Hamilton to solve their most complex problems. They trust us to bring together the right minds: those who devote themselves to the challenge at hand, who speak with relentless candor, and who act with courage and character. They expect original solutions where there are no roadmaps. They rely on us because they know that—together—we will find the answers and change the world. To learn more, visit BoozAllen.com.

**About eHI**

eHealth Initiative and Foundation (eHI) is a Washington, DC based, independent, non-profit organization whose mission is to serve as the industry leader convening executives from multi-stakeholder groups to identify best practices to transform healthcare through use of technology and innovation. Working with its membership, eHI conducts, research, education and advocacy activities to support the transformation of healthcare which addresses stakeholder needs, particularly those of patients.