ASPEN TECH POLICY HUB

PROJECT

DANIEL BARDENSTEIN

To learn more about this project, please visit aspentechpolicyhub.org.

THE ASPEN INSTITUTE

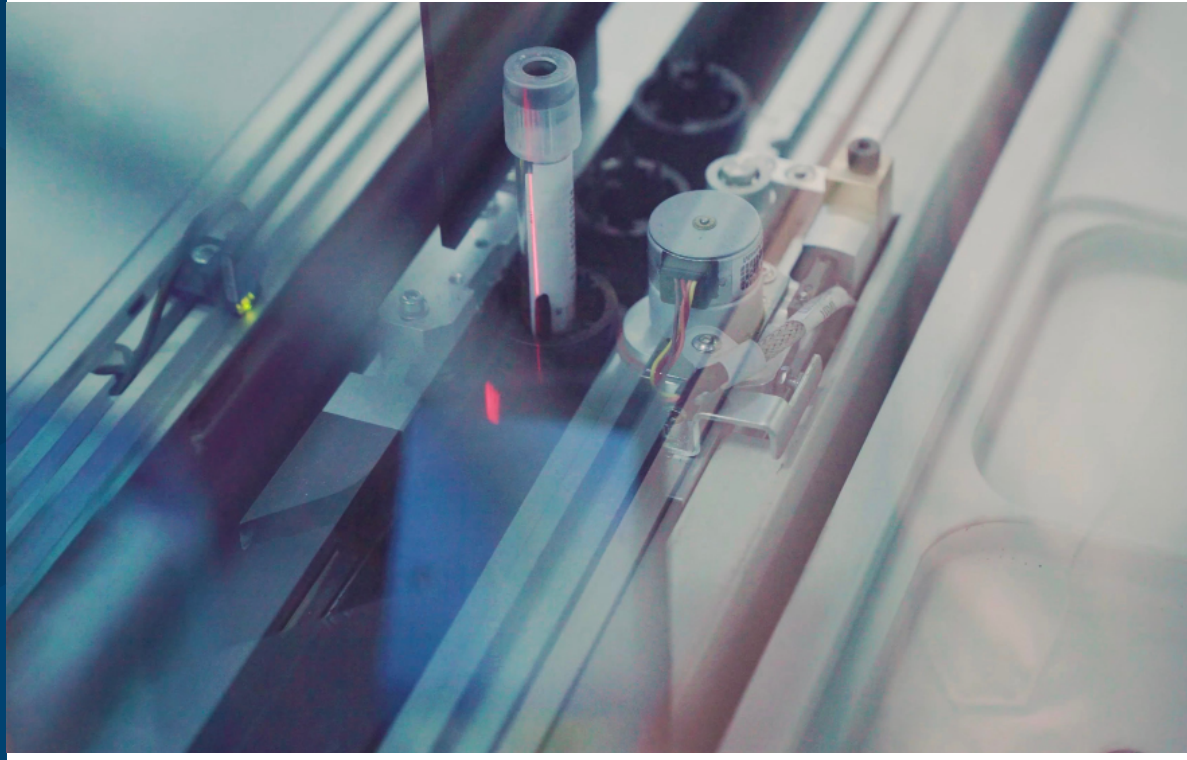

Photo by Testalize Me via Unsplash

"Smart" but Insecure: Improving Medical Device Cybersecurity

Expediting the disclosure and discovery of vulnerabilities in connected medical devices.

EXECUTIVE SUMMARY

As "smart" medical devices continue to proliferate across the healthcare sector, healthcare organizations have been increasingly targeted by ransomware and other debilitating cyber attacks. These devices are often vulnerable to attacks, potentially allowing malicious hackers to steal patient data, modify medical exam results, or disrupt life-supporting machines. As the regulator for medical devices, the Food and Drug Administration (FDA) should act now to ensure that manufacturers minimize the risk that software vulnerabilities in their devices pose to patient safety and healthcare facilities. This project proposes that the FDA:

- Establish a clear list of specific cybersecurity minimum requirements for medical devices to receive FDA approval; and
- Direct manufacturers to build a specific feature – a Device Query Interface – into their medical devices to make them easier to secure for device owners.

THE PROBLEM

Vulnerable medical devices pose a grave risk to patient safety and privacy. Despite existing cybersecurity guidance from the FDA, critical gaps remain in how medical device manufacturers address the risks posed from their devices. Specifically, device manufacturers aren't doing everything possible to rapidly disclose to users newly discovered vulnerabilities in their devices, nor do they make it easy for customers to determine if they're impacted by a vulnerability.

> *Device manufacturers aren't doing everything possible to rapidly disclose to users newly discovered vulnerabilities in their devices.*

THE SOLUTION

To facilitate manufacturers' disclosure of new vulnerabilities and allow healthcare facilities to make more risk-informed decisions about medical devices, the FDA should:

- **Create a "cyber baseline" of minimum cybersecurity requirements for every medical device to receive FDA approval.** This will make medical devices harder to hack, reduce costs for manufacturers, and protect patients and hospitals from potential harms caused by cyber attacks.
- **Add guidance for manufacturers to make it easier to retrieve important security information from their devices without impacting device operations.** This will make it significantly easier and less risky for security teams in healthcare facilities to track their devices, determine how vulnerable their devices are, and make risk-informed decisions about securing those devices.

For more information about this proposal, please see: (1) a policy brief detailing the proposed cybersecurity baseline requirements; (2) a policy brief explaining the proposed Device Query Interface (DQI) requirement; and (3) a sample FAQ document for manufacturers and healthcare organizations on the DQI proposal.

ASPEN TECH POLICY HUB

PROJECT

ABOUT THE HUB

The Aspen Tech Policy Hub is a Bay Area policy incubator, training a new generation of tech policy entrepreneurs. We take tech experts, teach them the policy process, and support them in creating outside-the-box solutions to society's problems.

The Aspen Institute
2300 N St. NW, Suite 700
Washington, DC 20037
202 736 5800

THE ASPEN INSTITUTE