ASPEN TECH POLICY HUB

POLICY

Requiring a Cybersecurity Baseline for Medical Device Approval

DANIEL BARDENSTEIN

EXECUTIVE SUMMARY

While connected medical devices have tremendous benefits for practitioners and patients, many of these rapidly proliferating devices lack basic cybersecurity protections, putting both patients and healthcare facilities at risk of being hacked. To ensure that manufacturers better secure their devices, this brief proposes that the Food and Drug Administration (FDA) require that all medical devices include a minimum set of specific cybersecurity protections in order to receive FDA approval. Doing so will reduce the risk of cyber attacks to healthcare organizations and patients alike.

Hacked medical devices are a grave security risk. Insecure medical devices can lead to devastating cyber breaches in hospitals, leaked patient records, or even direct harm to the patient.

The FDA's current approach to cybersecurity standards is to provide "nonbinding recommendations" to device manufacturers.[1] As a result, many device manufacturers still do not implement basic protections sufficiently, if at all, nor comply with FDA recommendations.

These proposed "cybersecurity baseline" requirements would establish a clear list of minimum cyber protections that medical devices must contain in order to receive FDA approval. The requirements would include certain existing FDA recommendations, such as ensuring that all manufacturer-created passwords are unique, complex, and random, as well as other best practice protections, such as protections against brute-force attacks.

To implement this proposal, the FDA should, in the order below:

1. Assemble a group of experts across the healthcare cybersecurity space, especially security practitioners employed by manufacturers and healthcare providers, to review relevant regulations and frameworks and propose an initial list of baseline protections;
2. Create a new regulation stating that all medical devices must include the baseline protections in order to receive FDA approval; and
3. Add the cyber baseline into the FDA's premarket cybersecurity guidance.

This proposal – supported by both manufacturers and healthcare security personnel – will immediately and effectively incentivize manufacturers to better secure their medical devices. Ultimately, this will protect the health, safety, and privacy of all Americans, secure the US healthcare system from cyber attacks, and maintain the FDA's position as a global leader in medical device cybersecurity.

PROBLEM

As cyber attacks increasingly target the US healthcare sector, the proliferation of connected medical devices poses a critical risk to patients and healthcare organizations alike. A recent study suggests that the average US hospital has 20,000 connected medical devices, translating to 10–15 devices per hospital bed.[2] However, a vast majority – more than 80% – of these medical devices lack basic cybersecurity protections against or are susceptible to cyber attacks that could put patients and healthcare facilities at serious risk.

Cybersecurity researchers have demonstrated the potential impact of a nefarious hacker accessing an insecure medical device. Ethical hackers have achieved complete remote control on a smart pacemaker; have hacked into X-ray machines to add fake tumors to the results; and have hacked into a smart insulin pump to change the dosage.[3]

Cyber attackers have also exploited insecurities, such as weak passwords, in medical devices to hack into hospital networks, where they can steal data and disrupt operations. In 2021 alone, cyber breaches exposed

over 40 million medical records of US citizens, causing hospitals to pay hefty fines and compromising patient confidentiality.[4] Hacked medical devices in hospitals can also lead to ransomware attacks, which cost US hospitals $21 billion collectively in 2020 alone.[5] Ransomware attacks have shut down nearly half of US hospitals at one time or another, which has delayed care for patients and may have been responsible for patient deaths.[6]

As the primary regulator for medical devices, the FDA has encouraged device manufacturers to make their devices more secure, and has pushed back on extremely insecure devices. According to one FDA employee interviewed by the author, the FDA has previously denied approval for at least one medical device due to poor cybersecurity.

However, rather than explicitly requiring specific cyber protections, the FDA currently provides "nonbinding recommendations" to manufacturers.[7] Each manufacturer must interpret what security protections are needed to get FDA approval and how to implement those protections. This has several concerning effects. First, cyber protections across medical devices aren't consistent. In other industries like automotives, consumers can trust that all cars, regardless of manufacturer, have the same basic security features, whereas medical device manufacturers lack a clear standard for cybersecurity protections and implement different protections in different ways. In addition, many manufacturers neglect to implement best practice cyber protections or don't implement them properly.

While there is little, if any, quantitative data on the cybersecurity of medical devices in the market, dozens of healthcare security experts interviewed by the author, including hospital cybersecurity staff and consultants who are hired to test hospital networks and devices, regularly encounter medical devices that lack basic cybersecurity protections.

RECOMMENDATION

The FDA should establish a clear list of minimum cyber protections that medical devices must possess in order to receive FDA approval. An initial proposed list of these baseline recommendations can be found in the Cybersecurity Baseline Standards document here. This baseline includes requirements drawn from existing FDA recommendations,

such as ensuring that all manufacturer-created passwords are unique, complex, and random, as well as other best practice protections, such as protections against brute-force attacks, where attackers repeatedly try different usernames and passwords to access a device.

To accomplish this, the FDA should gather a group of cybersecurity and medical device experts to identify an initial list of required cyber protections, using the above Cybersecurity Baseline as an initial starting point. After this list is developed, the FDA should write a new regulation that requires all medical devices to meet a specific set of cybersecurity protections, and then publish an initial list of protections in its "Pre-Market Cybersecurity Guidance," which identifies all requirements for new products to receive FDA approval. See Appendix A for how the FDA would use the group of experts to produce the first list of cyber protections.

The list of minimum cyber protections should include established best practices that broadly apply to all medical devices, including strong passwords, data encryption, and multifactor authentication. While some of these protections already exist as "nonbinding recommendations" in current FDA guidance, the group of experts should consider other protections outlined in similar standards, such as prevention against brute-force attacks.

This list of minimum protections is not meant to be an exhaustive list of every necessary cybersecurity protection that should be applied to medical devices. There are hundreds (if not thousands) of types of medical devices (depending on the definition used), each of which can be used in various clinical contexts, such emergency rooms (ERs) or diagnostic clinics. This list would represent a baseline, which the FDA can build on incrementally to account for the variety of device types and clinical contexts. See Appendix B for a list of relevant standards and regulations, and a list of cybersecurity protections they share in common that serves as a starting point.

This approach addresses two of the core causes of manufacturers neglecting to build in security protections in their devices. First, a clear list of requirements will remove ambiguity for manufacturers deciding which minimum cybersecurity protections are needed in their devices. Second, tying these requirements to FDA approval adds

an enforcement mechanism. FDA approval is a critical certification that manufacturers need to sell their medical devices publicly (and therefore make money), so manufacturers face a strong financial incentive to cooperate.

This policy proposal promises significant benefits for the FDA, manufacturers, healthcare organizations, and patients alike:

1. Protecting Patient Safety and Saving Lives

First and most importantly, patients will be more protected from the consequences of having their medical devices hacked. As discussed above, cyber attackers can steal and leak sensitive data, alter test results, or disable life-saving devices. More secure medical devices also means that hospitals will be more secure from cyber attacks, decreasing the likelihood of shutdowns that delay care to – and potentially harm – patients.

2. Increased Trust in Medical Devices

In the same way people trust that they won't get sick from the eggs or meat they buy or the medicines they take (which are subject to FDA regulation), ensuring a common baseline of cybersecurity protections will help people better trust the medical devices they use or purchase, regardless of the manufacturer. This will lift the responsibility off of patients and healthcare providers to assess the security of a device before purchasing, saving them time and money.

3. Preventing Breaches and Cyber Attacks in Hospitals

More secure medical devices means fewer hackable targets for cyber attackers, reducing the risk of hospitals and other healthcare facilities falling victim to breaches or ransomware attacks. Fewer successful cyber attacks means that healthcare facilities will avoid the significant financial and personnel costs of responding to and recovering from an incident, as well as avoiding potential fines for exposing sensitive medical records.

4. Efficiency and Cost Savings for Manufacturers

Every one of the many cybersecurity personnel employed at device manufacturers interviewed by the author supported the idea of a clear list of cybersecurity requirements for FDA approval. According

to those interviewed, manufacturers spend a considerable amount of time debating which cyber protections to implement in a new device. This constant debate pits business development teams, who want to get devices to market as quickly as possible, against product security teams, who want to make sure they pass the FDA's cybersecurity review. If the FDA denies approval for a device, manufacturers face on average a year-long delay getting the product to market, which is incredibly costly.[8] By establishing a clear list of requirements, the FDA could help manufacturers avoid this ambiguity and more easily budget and plan for these protections early in the product design process. This approach will especially help clarify requirements for medical device startups (or other small or less mature companies), who don't always have the awareness, personnel, or incentives to implement FDA cyber guidance.

5. Global Leadership and Alignment with the Current Administration

Raising the bar of cybersecurity is not only a top priority of the current Administration and its "Build Back Better" philosophy; the current administration has published cybersecurity requirements for all federal agencies and the gas/pipeline sector, among others.[9,10] In addition, the FDA stands to be the first global government medical regulator to publish a required cybersecurity baseline, sustaining the FDA's stature as a leader in global medical device cybersecurity.

CONCLUSION

By establishing a clear, easy-to-understand list of cybersecurity requirements, the FDA stands to dramatically increase the cybersecurity and trustworthiness of medical devices, protect hospitals, and save patients. The FDA would send a clear message to the healthcare industry that cybersecurity is a critical consideration in medical devices and make it easier for manufacturers to know how to secure their devices. Adopting this proposal would protect future patients and healthcare facilities for generations to come, as medical devices continue to become ubiquitous across the healthcare field. Ultimately, the FDA would be fulfilling its mission to "[protect] the public health by ensuring the safety, efficacy, and security" of medical devices and other food and drug-related products.[11]

Appendix A: Creating an Initial List of Required Cyber Protections

1. **Goal and Scope**

   The goal of this initiative is to identify a minimum set of cybersecurity protections applicable to all medical devices. This baseline is not meant to be exhaustive, or to address the variety of types of medical devices or clinical contexts in which they are used; these factors can be addressed in future iterations of the minimum cybersecurity protections after the baseline is published.

2. **Gather Experts**

   First, the FDA would recruit a diverse group of experts experienced in cybersecurity (particularly the security of "internet-of-things" devices), medical devices, FDA approval processes, and healthcare delivery to volunteer time for this effort. The group should also include experts across government (including the FDA), device manufacturers, and healthcare organizations.

3. **Timing**

   The group should have six months to identify the cybersecurity baseline for FDA approval. This provides ample time to review existing frameworks and review final recommendations, but ensures that the impact of this effort isn't too delayed.

4. **Approach**

   The group should review existing frameworks and global regulations for medical device or internet of things (IoT) security, as medical devices are a type of IoT device. Relevant frameworks and regulations include: National Institute for Standards and Technology (NIST) Foundational Cybersecurity Activities for IoT Device Manufacturers, IoT Security Foundation's IoT Security Compliance Framework, the ETSI EN 303645 standard, and the United Kingdom's IoT Code of Practice. See Appendix B for a comparison of some of these frameworks. After identifying common protections across frameworks, the group should refine the list for practices that are most relevant for medical devices.

Appendix B: Common Cybersecurity Protections Across Relevant Frameworks

Medical devices are a subset of smart devices or "internet of things" (IoT) devices. While there aren't any medical device–specific cybersecurity frameworks yet, there are several well established IoT security frameworks that can be used to identify a cybersecurity baseline for medical devices.

The standards included are:

- Internet of Things Security Foundation's Security Assurance Framework (IoTSF SAF)[12]
- ETSI EN 303645 version 2 (ETSI)[13]
- United Kingdom's Code of Practice (UK CoP)[14]
- IoXT Alliance's Base Profile (IoXT)[15]

A green square indicates that the relevant standard requires and/or strongly recommends this practice.

Cybersecurity Feature	IoTSF	ETSI	UK CoP	IoXT
Access Controls				
Any default passwords must be sufficiently strong and unique, and randomly generated.	■	■	■	■
Passwords cannot be null, blank, or obvious (e.g., the same as the username, or including the name of the manufacturer or device).	■			■
If a device lacks a strong, unique default password, the device must force owners to create a new password during initial setup.	■	■	■	■
Multifactor authentication should be enabled if and when possible.	■	■		■
All credentials across the device and its relevant components must be sufficiently secured.	■	■	■	
Mechanisms should exist to limit the effectiveness of brute-force attacks, such as disabling an account after several failed login attempts.	■	■		
Only authenticated and authorized users should be able to configure the device.	■	■		

Reporting Vulnerabilities				
The device manufacturer must have a Coordinated Vulnerability Disclosure Program (CVDP) in place. The CVDP should be publicized and easily discoverable, such as appearing on the manufacturer's website.				
The CVDP must accept submissions from external researchers and other parties. There must be an easily discoverable method for vulnerability/defect submissions, such as a website/web portal or an email address.				
The scope of the CVDP must include the device and other relevant components.				
Responsible disclosure of defects to impacted parties that must take action/timely manner; Secure notification/disclosure process				
Supportability and Updates				
The manufacturer must have a published patch/update policy for the device.				
All software components in the device should be securely updateable (e.g., encrypting updates and transferring them over encrypted channels).				
The device should prevent the abuse of the patch/update function, including preventing version rollbacks.				
After initial setup, the device should automatically check periodically for updates.				
The device should verify the authenticity and integrity of software updates, which should be cryptographically signed.				
Manufacturers must inform device owners when a device update is required and provide information on the risks mitigated by the new updates.				
The manufacturer must publish a policy for when the device reaches its "end of life," when the manufacturer will no longer support it. This policy includes how far in advance the manufacturer will notify device owners, and any potential loss of functionality that results.				
The manufacturer must publish a minimum support period and/or an expiration date for software and/or security updates.				

Device Security				
The device's software must leverage a secure boot mechanism based on a hardware root of trust, which is enabled by default.	■	■	■	■
The device must alert device owners if there is a potential malfunction or security issue.	■	■	■	
All cryptography must leverage current best practice algorithms and methodologies.	■	■	■	■
All data (at rest and in transit) and communications must be encrypted.	■	■	■	■
All nonessential or unused ports and services must be disabled.	■	■	■	■
The manufacturer must provide guidance to device owners on how to effectively secure and configure the device.	■	■	■	
The device must generate logs and telemetry for relevant device activities, processes, or issues.		■	■	
Other Components				
Any other digital components of the medical device related to device operation must be appropriately secured. This includes cloud applications, web applications, web servers, and mobile applications.	■			
Manufacturers must provide a Software Bill of Materials (SBOM) to the FDA and to device owners.	■			
The device should be resilient to power and network outages, and minimize risk to patient safety and network security (e.g., "fail-safe" and "fail-secure").	■	■	■	

Appendix C: A Proposed Cybersecurity Baseline

CYBERSECURITY BASELINE FOR MEDICAL DEVICES

Summary

The below requirements should apply to all medical devices in order to receive Food and Drug Administration (FDA) approval. This list is not exhaustive, and certain other cybersecurity controls may be appropriate to specific medical devices. By establishing a clear baseline of cybersecurity requirements for medical devices, the FDA can signal to device manufacturers what features must be present in their devices in order to receive FDA approval.

Some of these requirements also apply to "post-market" guidance, or requirements that still apply after a device is already approved and on the market. For these post-market requirements, the FDA should periodically verify that device manufacturers are compliant.

Guiding Principles

Security by Default

Whenever possible, security mechanisms should be enabled by default in medical devices unless there is a valid reason to require users to enable them manually.

Secure the Broad Scope

All security requirements and principles for medical devices should extend to any other technology required for the device's function, such as cloud applications, web servers, websites, or mobile applications.

Version 1.0

1. **Devices must have secure passwords and authentication:**

   - Devices must not have universal default passwords.
   - Any default device passwords must be sufficiently strong (as dictated by the latest or relevant best practices), unique, and randomly generated.

- Devices should not allow weak or obvious passwords, such as null or blank passwords or, a password that is obvious (such as the same as the username, the name of the manufacturer or device, etc.).
- Devices can be managed and configured only by authenticated and authorized users. In order to configure the device, a user must be forced to authenticate and must have the proper permissions.
- Devices, where possible, should have multifactor authentication enabled by default.

2. **Devices must secure sensitive data and communications:**

- All credentials on the device must be stored securely.
- All sensitive data must be encrypted at rest and in transit.
- All communications must be encrypted.
- Devices must use only the sufficiently strong and proven mechanisms for encryption (e.g., encryption algorithms).

3. **Manufacturers must keep software updated:**

- The manufacturer must have a published patch/update policy, including a method for notifying customers of new updates and how to access those updates.
- The manufacturer must publish an expected end-of-life date for the device and/or a minimum support period, during which the manufacturer will provide regular feature and security updates.
- After initial setup, the device should automatically check for new updates. If a new update is available, the device should notify the device owner.

4. **Manufacturers must minimize the attack surface:**

- All ports, services, or interfaces (physical or virtual) that are nonessential (i.e., not required for the device to function) must be disabled.
- The manufacturer must provide a list of necessary or expected network communications required for device function. This should include relevant details such as source/destination ports and remote hostnames, to enable device owners to allow necessary traffic and block unnecessary traffic to and from a device.

5. **All software must be validated:**

- Devices must leverage a secure boot mechanism based on a hardware root of trust.
- All software updates must be validated for integrity (e.g., all software must be cryptographically signed).

6. **Devices must prevent common attacks:**

- The device should prevent unauthorized attempts to rollback a device to a previous version of software or firmware, and should notify device owners of any such attempts.
- The device must possess some mechanism to prevent brute-force attacks, such as by disabling an account after a certain number of failed login attempts.

7. **Devices must facilitate customers/owners to effectively manage and secure them:**

- Manufacturers must provide guidance to device owners on how to effectively secure the device, and how to check and ensure the device's secure configuration.
- Devices must generate logs, alerts, and/or other telemetry that captures device activity or potential malfunctions, security issues, or health issues.
- The device must allow owners to perform standard security best practices for managing and security a device, such as installing antivirus or other security software, scanning the device for asset inventory and vulnerability discovery, remotely querying the device, and more. Device owners should be able to conduct these activities without risking device malfunction.
- Device owners must provide the device's cybersecurity build of materials (CBOM) and/or software build of materials (SBOM), which contains a list of all software, firmware, and hardware on the device, the versions of each, and the individuals or organizations who developed or currently own each component.

8. **Devices should be resilient:**

- The device should be resilient to temporary power and network outages, such that patients using the devices aren't adversely impacted.
- If the device fails due to outages or other reasons, it should fail into a safe (fail-safe) and secure (fail-secure) state, meaning that patients using the device shouldn't be adversely impacted, nor should the device become less (cyber)secure.

9. **Manufacturers should provide a (post-market) coordinated vulnerability disclosure:**

   Manufacturers must establish coordinated vulnerability disclosure programs (CVDPs), the scope of which covers the device and relevant components. The CVDPs must be easily discoverable by third-party researchers, such as by having a public website. The CVDP must also allow researchers to easily submit potential vulnerabilities or issues, such as via a web portal or to a dedicated email address. Manufacturers must reply and investigate vulnerabilities in a timely manner. If a vulnerability in a medical device is discovered that requires notifying customers, the manufacturer must have an established process and mechanism to securely notify its customers of the vulnerability and potential mitigations.

Endnotes

1 *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff*, US Food and Drug Administration, October 18, 2018, https://www.fda.gov/media/119933/download.

2 Heather Landi, "82% of Healthcare Organizations Have Experienced an IoT-Focused Cyberattack, Survey Finds," Fierce Healthcare, Aug 29, 2019, https://www.fiercehealthcare.com/tech/82-healthcare-organizations-have-experienced-iot-focused-cyber-attack-survey-finds.

3 Lily Hay Newman, "A New Pacemaker Hack Puts Malware Directly on the Device," *Wired Magazine*, August 9, 2018, https://www.wired.com/story/pacemaker-hack-malware-black-hat/; Shoshanna Solomon, "Israeli researchers show medical scans vulnerable to fake tumors," *Times of Israel*, April 4, 2019, https://www.timesofisrael.com/israeli-researchers-show-medical-scans-vulnerable-to-fake-tumors/; Lily Hay Newman, "These Hackers Made an App That Kills to Prove a Point," *Wired Magazine*, July 16, 2019, https://www.wired.com/story/medtronic-insulin-pump-hack-app/.

4 Kat Jercich, "The Biggest Healthcare Data Breaches of 2021," *Healthcare IT News*, November 16, 2021, https://www.healthcareitnews.com/news/biggest-healthcare-data-breaches-2021/.

5 Stacey Wiener, "The Growing Threat of Ransomware Attacks on Hospitals," Association of American Medical Colleges, July 21, 2020, https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals.

6 Phil Muncaster, "Half of US Hospitals Shut Down Networks Due to Ransomware," *Infosecurity Magazine*, August 16, 2021, https://www.infosecurity-magazine.com/news/half-us-hospitals-shut-networks/; Melanie Evans, Robert McMillan, and Kevin Poulsen, "A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death," *Wall Street Journal,* September 30, 2021, https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116.

7 See Premarket Submissions, *supra* note 1.

8 "Why Product Recalls Cost Medical Device Manufacturers $5,000,000 a Day," Trievr Recall Management, accessed October 20, 2021, https://trievrrecallmanagement.com/why-product-recalls-cost-medical-device-manufacturers-5000000-a-day/.

9 Executive Order 14028 of May 12, 2021, "Executive Order on Improving the Nation's Cybersecurity," https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

10 "DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators," Department of Homeland Security, July 10, 2021, https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators.

11 "What We Do," The Food and Drug Administration, accessed Nov 17, 2021, https://www.fda.gov/about-fda/what-we-do#mission.

12 Security Assurance Framework," Internet of Things Security Foundation, accessed November 17, 2021, https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/IoTSF-IoT-Security-Assurance-Framework-Release-3.0-Nov-2021-1.pdf.

13 "ETSI EN 303 645 V2.1.0," ETSI, published April 2020, https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf.

14 Code of Practice for Consumer IoT Security," United Kingdom Department of Digital, Culture, and Media Support, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf.

15 "ioXt 2021 Base Profile Version 2.0," ioXT Alliance, https://static1.squarespace.com/static/5c6dbac1f8135a29c7fbb621/t/6078677c7d7b84799f1eaa5b/1618503553847/ioXt_Base_Profile.pdf.