ASPEN TECH POLICY HUB

POLICY

How the FDA Can Make Medical Devices Easier to Secure

DANIEL BARDENSTEIN

EXECUTIVE SUMMARY

Software vulnerabilities in "smart" medical devices pose a serious threat to hospitals and patients alike. Not only are many medical devices vulnerable to potential cyber attacks, but many are designed in such a way that makes it difficult for healthcare organizations to secure them without risking patient safety. As the primary regulator for medical devices, the Food and Drug Administration (FDA) can help protect healthcare organizations and patients by ensuring that medical device manufacturers make their devices easier to secure.

Specifically, the FDA should require manufacturers to build a Device Query Interface (DQI) into their medical devices that allows device owners to easily secure their devices without impacting patients using those devices. To enact this proposal, the FDA should add a DQI requirement to its existing premarket cybersecurity guidance, leveraging the draft language and sample architecture included in this brief.

With DQI-enabled medical devices, device owners – especially cybersecurity teams at healthcare facilities – can leverage established cybersecurity methodologies, such as active scanning, to efficiently retrieve real-time data about their medical devices without risking device malfunction. With this data, including each device's security and vulnerabilities, healthcare facilities will be better equipped to prevent cyber attacks and to make risk-informed cybersecurity decisions. This solution, used successfully in other industries, would significantly reduce the risk of cyber attacks on healthcare organizations, saving the healthcare industry billions of dollars and saving patients' lives.[1]

PROBLEM

As "smart" medical devices become increasingly common in our hospitals and homes, the lack of cybersecurity of these digitally connected devices poses a greater and greater risk to patients and healthcare facilities. Current estimates suggest that the average US hospital has over 20,000 connected medical devices, averaging 10–15 devices per patient bed.[2] At the same time, studies suggest that nearly half of these medical devices are vulnerable to a potential cyberattack.[3] Malicious cyber actors can hack into these insecure devices — from Wi-Fi–connected X-ray machines in emergency rooms to Bluetooth-enabled pacemakers in our bodies — and potentially steal sensitive patient data, shut down a hospital, or disable a life-saving device.

It is critically important for security teams across all industries to rapidly identify vulnerabilities in the devices that they're responsible for, such as laptops, servers, websites, and smart devices. Once they confirm that a device is vulnerable and determine the potential impact of that weakness on patient health, they can make data-driven decisions on how best to secure the device or to reduce the risk. However, security teams in healthcare facilities lack this critical visibility into their medical devices because they aren't able to leverage a cybersecurity best practice: active scanning.

Active scanning is a best practice in cybersecurity that allows security teams to identify devices on their network and potential vulnerabilities in those devices using automated tools (see Figure 1). During active scanning, a scanning tool first sends a large number of requests to a device to get information about that device. Next, the device then sends back a response to every request it receives. This data may include what software is running on the device or how it's configured. The returned data is then analyzed for potential weaknesses or checked against a list of known vulnerabilities, such as the Common Vulnerabilities and Exposures (CVE) database. Finally, stakeholders, including the security team or medical professionals, use this information to decide on the best way to protect an insecure medical device, making sure that the solution won't risk patient safety.

While other approaches exist, cybersecurity experts prefer active scanning because it is cheaper and more accurate than the alternatives, and can also detect more devices on a network and more detailed

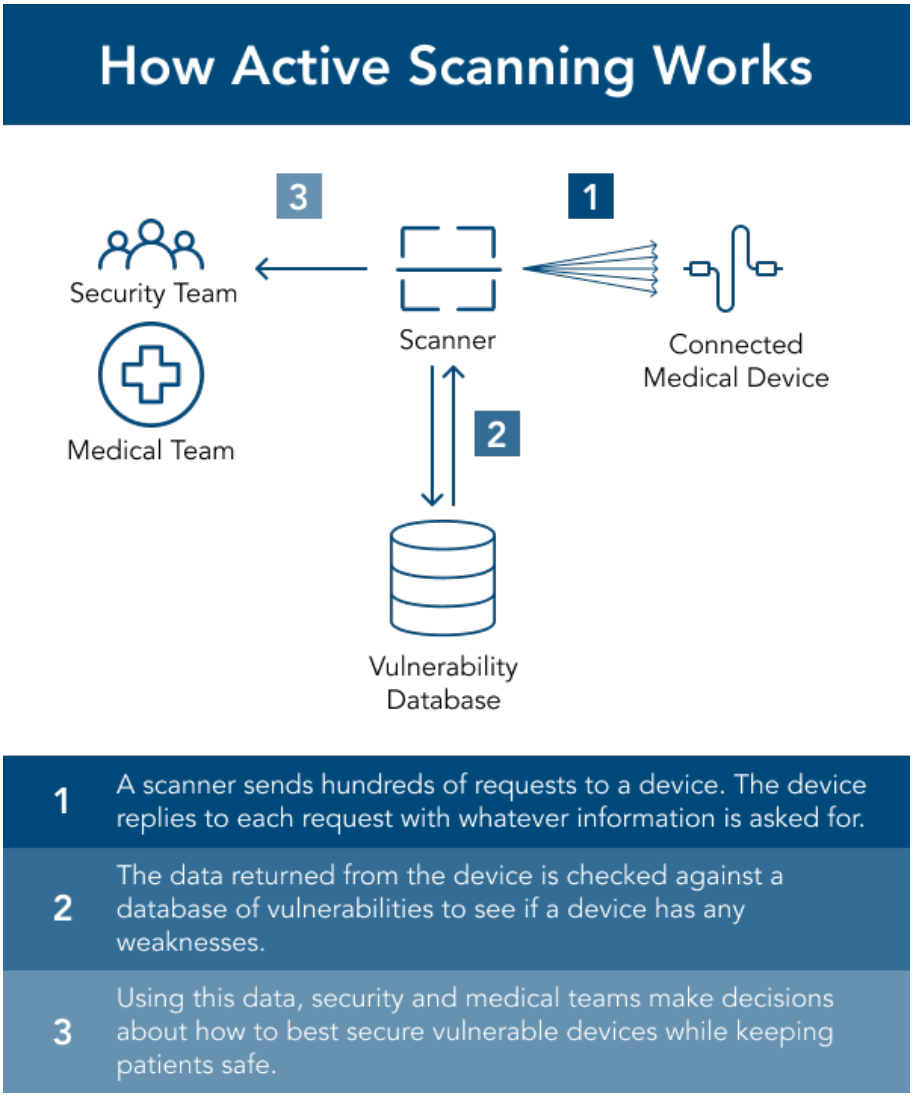

Figure 1

information on those devices.[4]

However, connected device companies don't build their medical devices to withstand the hundreds or thousands of requests that active scanning requires, which can overwhelm devices and cause them to malfunction. In a similar way to how old or small computers freeze up when trying to run large or complex programs (such as a video game or a photo editor), many medical devices are easily overloaded by the effort of responding to all of the requests from the active scan. Companies build devices this way because it's more expensive to make devices more resilient, such as by adding more processing power or memory.

Since malfunctioning medical devices can negatively impact patient safety, healthcare security teams aren't able to run active scans on

their devices. In addition, device manufacturers have discouraged or contractually forbidden healthcare organizations from running active scans on their medical devices because the manufacturer can become liable if one of their devices malfunctions and causes harm to a patient. As a result, healthcare organizations lack visibility into and awareness of the security of their devices, and they lack critical data to make informed decisions on how best to secure their devices to protect patients.

Ultimately, this leaves healthcare facilities and patients exposed to the risk of medical devices being hacked by cyber attackers, which can have devastating effects — from shutting down an entire hospital network to causing delays in care indirectly, which could lead to patient deaths.[5]

RECOMMENDATIONS

The FDA should require manufacturers to implement a Device Query Interface (DQI), which would give device owners and security teams a safe way to retrieve important security information about a medical device without disrupting its operation. Specifically, the FDA should add a DQI requirement into their premarket cybersecurity guidance, which manufacturers must follow in order for their devices to receive FDA approval. Appendix A provides draft language for the DQI requirement.

The Device Query Interface (DQI)

As an analogy, if someone was trying to find information about guests staying at a hotel, active scanning would entail knocking on the door of every single room. A DQI acts as the concierge in the lobby, a single point of contact who can provide a wide breadth of information about occupancy rate or where a certain guest is staying.

An Analogy: A Hotel Congierge
Active Scanning is like trying to identify every guest in a hotel by knocking on each door and seeing if anyone is inside.
The Device Query Interface (DQI) is like a hotel concierge, whom you can simply ask "How many guests are staying in the hotel tonight?" or "In what room is Jane Doe?"

A DQI is a feature built into each medical device that would act as the "digital concierge" for each device. A cybersecurity professional responsible for securing a device could send specific questions (or, in more technical parlance, queries) to the device via its DQI and would get back the relevant information. In technical terms, the DQI would collect real-time data about the device's health, security settings, and configuration, and provide that data to authorized users.

In contrast to active scans, which can overwhelm medical devices with hundreds or thousands of requests, security teams only need to send a single request to a medical device's DQI to obtain this important data.

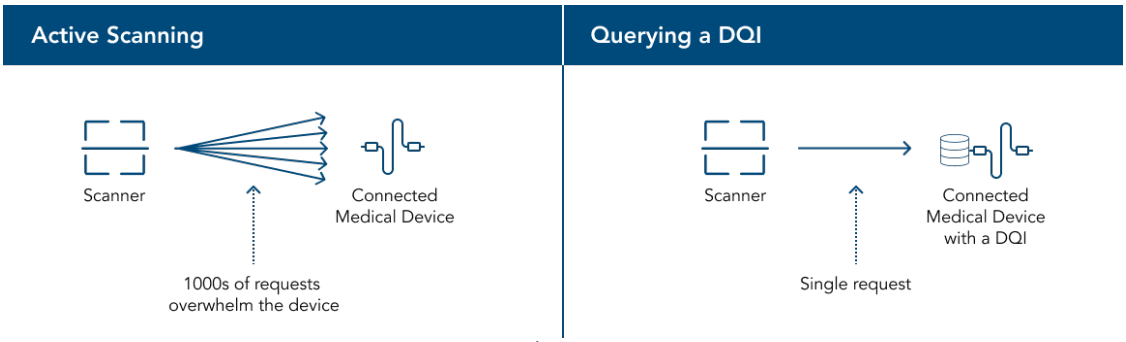

Figure 2

Since it takes less digital effort (e.g., processing power and memory) to respond to a single request, a medical device with a DQI is much less likely to malfunction.

Existing Precedent and Value

DQI-like mechanisms are used successfully in other connected-device markets. For example, connected devices in the industrial controls systems (ICS) market, which broadly includes devices that control industrial processes from power generation to assembly-line manufacturing, allow "selective probing, which functions similarly to DQI systems."[6] As with medical devices, ICS devices perform critical functions that can't be interrupted, like controlling the flow of electricity and water to a local city. As a result, this constraint prevents security teams from running active scans against ICS devices as well. With selective probing, which is built into devices from many top manufacturers including Langner, Rockwell, Siemens, and Honeywell, security teams can make targeted requests to their devices

without causing device malfunction.[7] This way, security teams in the ICS space can get the data they need to secure their devices without risking disrupting their operations.

DQI Queries

Active scan data is invaluable in helping security teams identify functional issues or security vulnerabilities in medical devices that cyber attackers could hack into. This information helps stakeholders make weighty or cost-intensive decisions, such as choosing whether to replace, disable, or upgrade a problematic device.

A DQI would be preprogrammed to answer certain types of queries that provide similar data to what an active scan traditionally returns. For example, a user would be able to query a device's DQI for the device's digital identifiers, health status, software and firmware names and versions, and current configuration. Appendix B provides an initial list of queries and data that a DQI would support. See Appendix C for examples of data that the DQI should provide.

Benefits

This proposal would be immensely beneficial for healthcare organizations, device manufacturers, and patients.

Healthcare organizations will gain more visibility into their medical devices and make more data-driven decisions. As the Chief Information Security Officer of a large hospital system described to the author, "Without this data, hospitals are totally blind."[8] DQI-enabled medical devices will give healthcare organizations more visibility into their medical devices, helping them identify the devices most susceptible to being hacked. With this visibility and other DQI-provided information, healthcare decision makers can more accurately and confidently weigh financial costs, risk to patients, and other factors to make data-driven decisions about securing their devices.

Healthcare organizations will reduce their chances of being hacked. Some estimates suggest that the average medical device possesses six exploitable vulnerabilities, making them attractive targets for cyber attacks.[9] When a new software vulnerability is discovered, there is essentially a race between cyber attackers and cyber defenders (in this case, healthcare security teams): attackers try to find and hack into vulnerable devices, while defenders must protect their devices before

attackers compromise them. A DQI allows defenders to use automation to rapidly search for vulnerable devices so they can find insecure devices before hackers do. Ultimately, this will prevent successful cyber attacks, which can harm patients and incur significant costs for healthcare facilities.

Patient privacy and safety will be more protected. When healthcare organizations are better able to secure their medical devices, they reduce the risk of cyber attacks. As a result, patients will be less likely to have their healthcare records accessed or to face delays in care caused by cyber attacks. In 2020 alone, cyber attacks led to the illegal access or leakage of over 29 million healthcare records in the United States.[10] In the past few years, we have also seen the first claims of patient deaths caused (indirectly) by cyber attacks shutting down hospitals and delaying care. Succinctly put, fewer cyber attacks means saving lives and protecting patients' confidentiality.[11]

Healthcare facilities will avoid significant costs. Every insecure medical device is a potential entry point for an attacker to launch a devastating hack. If healthcare security teams can better secure their devices with a DQI, they can reduce the chances of getting hacked and save their organizations millions of dollars in the future. Responding to and recovering from cyber attacks is incredibly expensive. Breached hospitals now pay upwards of $9 million on average if patient records are accessed or stolen during a cyber attack.[12] Ransomware attacks — which are increasingly common and have caused shutdowns in nearly half of US hospitals — cost the healthcare sector $21 billion in 2020 alone, costing individual victims, such as the University of Vermont Medical Center, as much as $50 million from a single attack.[13]

Manufacturers retain flexibility and decision making. The proposed DQI mechanism is a high-level feature that can be implemented in many different ways (see Appendix B for implementation options and considerations). This gives manufacturers the flexibility and autonomy to decide how best to implement a DQI for their specific devices, allowing them to meet the requirement effectively and with minimal burden.

Manufacturers also stand to protect their brand and reduce expensive recalls by enabling their customers to better secure their devices with a DQI mechanism. Suppose a manufacturer's device gets hacked and

ends up harming a patient. The manufacturer is then required to inform the FDA, which may lead to public disclosure and potentially a recall, which can cost manufacturers up to $600 million.[14]

CONCLUSION

Connected medical devices are an important evolution in patient health but also introduce the risk of cyber attacks, which can jeopardize healthcare facilities and patients. Currently, medical device manufacturers have designed their devices in a way that makes it difficult for healthcare security teams to adequately protect them. By requiring device manufacturers to implement a Device Query Interface in their devices, the FDA can immediately and effectively help the entire healthcare sector to defend itself from cyber attacks. This will save lives and protect patients,while saving healthcare organizations millions – if not billions – of dollars by reducing the chance of a successful cyber attack. By getting manufacturers to do everything they can to minimize the risks posed by software vulnerabilities and vulnerable medical devices, the FDA can set a standard for the global healthcare industry to ensure that technology in healthcare continues to do more good than harm.

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

Appendix A: Draft Sample Language

This appendix contains draft language that the FDA would add to its current premarket cybersecurity guidance under section B, "Detect, Respond, Recover: Design Expectations:", subsection 1, "Design the Device to Detect Cybersecurity Events in a Timely Fashion," in a new line (h):[15]

> (h) The design should provide an interface by which an authenticated user can remotely query for real-time information about the identity, health, security, and configuration of the device while minimizing risk of disrupting device operations. This query mechanism should be developed to allow regular use, as would be generally performed to follow cybersecurity best practices, by a device owner without risk of resetting or interrupting device operations.
>
> This information should be sufficient to allow a device owner to identify the device, understand the device's current settings and configurations, and provide the names and versions of any software and firmware running on the device to identify potential vulnerabilities.
>
> Manufacturers must establish and maintain procedures for utilizing this mechanism, and provide accessible and updated documentation to device owners.

Appendix B: DQI Sample Implementations and Considerations

The DQI is a product feature that can be implemented in various ways based on the nature of each medical device, such as the technologies it uses and the clinical contexts in which it is used (e.g., an implanted device versus a device that sits in one's home).

Basic components

At its core, a DQI consists of the following components:

1. *A certain interface or endpoint that can receive (authenticated) requests*. The main functionality of a DQI is receiving and responding to requests. There are many different ways to implement this functionality, depending on the specific device and its technologies. See the "Protocols" section below for examples.
2. *A method to aggregate real-time data about itself.* To increase response time and efficiency, a device could even periodically prepare and store frequently requested data, making it instantly available when requested.
3. *Returning data to the user.* The device must be able to return formatted responses to the user or system that made the request.

Protocols

Manufacturers can select from established methods of communication protocols based on each device's specific requirements. Below is a list of some commonly used "internet-of-things" (IoT) communication protocols and some environments where they can be used:

- HTTP/HTTPS
- Message Queueing Telemetry Transport (MQTT)
- Constrained Application Protocol (CoAp)
- Windows Management Instrumentation (WMI)
- Simple Network Management Protocol (SNMP)

- Link Layer Discovery Protocol (LLDP)
- WebSocket

Security Considerations

One potential risk of DQIs is that making it easier for security teams to get information about a medical device also makes it easier for potential cyber attackers to do the same. It is common practice for cyber adversaries to perform "reconnaissance," — i.e., researching and collecting data on a potential victim network or device — in order to find a weakness to exploit.

To ensure that only authorized people (and not attackers) can use the DQI to get this information, manufacturers should follow the FDA's existing guidance on secure design when implementing the DQI. For example, manufacturers should ensure that the DQI responds only to authenticated requests — that is, from users who have verified their identities (such as by entering a username and password). In addition, manufacturers should encrypt all communications to and from the DQI so that cyber attackers can't intercept or snoop on the data. Moreover, following existing FDA cyber guidance, manufacturers should provide guidance to their customers on other ways to limit unauthorized access to the DQI, such as by implementing IP- or hardware-based allow-listing.[16]

Manufacturers should also minimize the potential abuse of the DQI mechanism to overwhelm the device with traffic asking for security information. For example, manufacturers can use common approaches like rate limiting, where the device limits the number of requests (per minute, hour, day, etc.) to the DQI to ensure that the device isn't overwhelmed by queries.

Appendix C: DQI Sample Data

In order to be most useful, the DQI should provide data to a device owner or a security team to help them make risk-informed decisions about securing a device. Examples of important data include a device's identity, health status, security configuration, and potential vulnerabilities. To ensure that all manufacturers provide a consistent set of data that's useful, the FDA should include a minimum or suggested set of data fields for the DQI.

Below is a proposed set of data that manufacturers should ensure are available via their DQI implementations. The FDA can solicit additional feedback via public comment on proposed guidance.

Data	Category	Description or Sample Data
Device Identifier	Identification	Unique alphanumeric string
IP address	Identification	Device IP Address
MAC Address	Identification	Device MAC Address
Device Manufacturer	Identification	Name of the device manufacturer
Device Model and Version	Identification	Model or product name of the device, and the primary product version number
Device software and firmware version	Asset and Vulnerability Management	
Device CBOM/SBOM and Versions	Asset and Vulnerability Management	
Date of last update/patch	Asset and Vulnerability Management	The date and time of the last update or patch to this device
Date of last reset	Asset and Vulnerability Management	The date and time of the last time the device was reset or turned on
Open ports	Asset and Vulnerability Management	
Health status and alerts	Health Information	Recent device resets, or if certain functions aren't working
Device configuration	Configuration Management	Current device configuration, such as relevant or important fields that control the functioning of the device

Endnotes

1 Hannah Mitchell, "Ransomware Attacks Cost Healthcare Orgs $20.8B in 2020," *Beckers Hospital Review*, July 28th, 2021, https://www.beckershospitalreview.com/cybersecurity/ransomware-attacks-cost-healthcare-orgs-20-8b-in-2020.html.

2 Forescout Research Labs, "Connected Medical Device Security: A Deep Dive into Healthcare Networks," *Forescout Research Labs*, accessed October 8, 2021, https://www.forescout.com/resources/connected-medical-device-security-a-deep-dive-into-healthcare-networks/.

3 *Id.*

4 "Understanding OT/ICS Asset Discovery: Passive Scanning vs. Selective Probing," *Langner, Inc.*, accessed November 21, 2021, https://www.langner.com/2018/08/understanding-ot-ics-asset-discovery-passive-scanning-vs-selective-probing.

5 "UHS Hospitals Hit By Ryuk Ransomware, Forced to Shut Down," Security Magazine, accessed October 20, 2020, https://www.securitymagazine.com/articles/93482-uhs-hospitals-hit-by-ryuk-ransomware-forced-to-shut-down-systems; 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.

6 See Langner, *supra* note 4.

7 *Id.*

8 Chief Information Security Officer of confidential hospital system, Zoom interview with author, October, 27, 2021.

9 Greg Slabodkin, "Medical Device Security Continues to be Casualty of Hospital-Medtech Divide," *MedTechDive*, accessed November 13, 2021, https://www.medtechdive.com/news/cybersecurity-medical-devices-hospital-divide-fda/609252/.

10 "2020 Healthcare Data Breach Report: 25% Increase in Breaches in 2020," *HIPAA Journal*, January 19, 2021, https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/.

11 Mike Milliard, "Hospital Ransomware Attack Led to Infant's Death, Lawsuit Alleges," *Healthcare IT News*, October 1, 2021, https://www.healthcareitnews.com/news/hospital-ransomware-attack-led-infants-death-lawsuit-alleges; William Ralston, "The Untold Story of a Cyberattack, a Hospital and a Dying Woman," *Wired Magazine*, November 11, 2020, https://www.wired.co.uk/article/ransomware-hospital-death-germany.

12 "The Average Cost of a Healthcare Data Breach is Now $9.42 Million," *HIPAA Journal*, Jul 29, 2021, https://www.hipaajournal.com/average-cost-of-a-healthcare-data-breach-9-42-million-2021/.

13 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/; Jackie Drees, "'We Just Got Caught Up in a Broader Attack': UVM Medical Center Details $50M Ransomware Strike," *Beckers Hospital Review*, July 23, 2021, https://www.beckershospitalreview.com/cybersecurity/we-just-got-caught-up-in-a-broader-attack-uvm-medical-center- details-50m-ransomware-strike.html.

14 Trievr Recall Management, "Why Product Recalls Cost Medical Device Manufacturers $5,000,000 a Day," acessed October 22, 2021, https://trievrrecallmanagement.com/why-product-recalls-cost-medical-device-manufacturers-5000000-a-day/.

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

16 *Id.*