May 17, 2022

TLP White

This week, Hacking Healthcare begins with a look at the growing regulatory and legislative efforts to address medical device cybersecurity. We will break down what the various guidance and regulations ask for or would require, what their chances are going forward, and what might be coming next. Then, we provide a preview of what to expect from the European Union's (EU) update to its Network Information Security Directive (NIS). The updated directive appears poised to add tens of thousands of new entities to its scope and introduces controversial aspects like cyber incident reporting. Welcome back to *Hacking Healthcare*.

1. **Growing Efforts to Address Medical Device Cybersecurity**

   Medical device cybersecurity has received plenty of attention recently. In the past two months the Food and Drug Administration (FDA) has released draft guidance on the issue, and two bills have been introduced in Congress that would amend portions of the Federal Food, Drug, and Cosmetic Act (FD&C Act) to address various aspects related to device security in line with what the FDA had previously requested. Taken together, these efforts provide a sense of what many medical device manufacturers should be expecting.

   <u>FDA Cybersecurity in Medical Devices</u>

   In early April, the FDA issued a draft guidance document on an update to medical device cybersecurity within the context of what it described as a quickly evolving cyber threat landscape that increasingly carries the risk of clinical impact.[1] The 49-page *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions — Draft Guidance for Industry and Food and Drug Administration Staff* invited public comments on what will eventually replace aging guidance once it is made final. The guidance hinted at the need for an iterative approach to device cybersecurity and the need for a focus on "mitigations throughout the total product lifecycle (TPLC)" of devices.[2]

   Among the various topics the new guidance addresses are general principles like designing for security, transparency, and submission documentation, and specific topics like using a Secure Product Development Framework (SPDF) to manage cybersecurity risks.

H.R. 7667 - Food and Drug Amendments of 2022

The Food and Drug Amendments of 2022 Act is a broad bill that encompasses revisions and extensions to "the user-fee programs for prescription drugs, medical devices, generic drugs, and biosimilar biological products, and for other purposes."[3] However, it would also amend the FD&C Act through the addition of Section 524C. *Ensuring Cybersecurity of Devices*.

This amendment seeks to ensure cybersecurity throughout the lifecycle of a "cyber device" by introducing cybersecurity requirements that would demonstrate a "reasonable assurance of safety and effectiveness."[4] While the bill allows for the Secretary of the Department of Health and Human Services (HHS) to determine the full extent of the requirements, at a minimum, manufacturers would need to:[5]

- Have a plan to appropriately monitor, identify, and address in a reasonable time post-market cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and procedures

- Design, develop, and maintain processes and procedures to ensure the device and related systems are cybersecure, and shall make available updates and patches to the cyber device and related systems throughout the lifecycle of the cyber device to address on a reasonably justified regular cycle, known unacceptable vulnerabilities; and as soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks

- Provide in the labeling of the cyber device a software bill of materials, including commercial, open-source, and off-the-shelf software components.

- Comply with such other requirements as the Secretary may require to demonstrate reasonable assurance of the safety and effectiveness of the device for purposes of cybersecurity, which the Secretary may require by an order published in the Federal Register

Notably, while the definition of cyber device is very broad, the Secretary of HHS would be given the authority to "identify devices or types of devices that are exempt from meeting the cybersecurity requirements."[6]

S. 3983 & H.R. 7084 PATCH Act

The PATCH Act seeks to amend the FD&C Act to include a section on device cybersecurity similarly to H.R. 7667. In fact, its wording is nearly identical, and it covers the exact same provisions regarding the requirements that device manufacturers would have to follow. This includes ensuring cybersecurity throughout a device's lifecycle, introducing baseline cybersecurity requirements, and allowing for the Secretary of HHS to make exemptions. However, it is a much more targeted bill that only seeks to address device cybersecurity rather than broad revisions to the FD&C Act.

For comparison, the PATCH Act's requirements language is provided below:

- Have a plan to appropriately monitor, identify, and address in a reasonable time postmarket cybersecurity vulnerabilities and exploits
- Have a plan and procedures for a Coordinated Vulnerability Disclosure to be part of submissions to the Food and Drug Administration
- Collect and maintain such other information as the Secretary may (by order published in the Federal Register or by other process) require to demonstrate a reasonable assurance of the safety and effectiveness of the cyber device
- Design, develop, and maintain processes and procedures to make available updates and patches to the cyber device and related systems throughout the lifecycle of the cyber device to address, on a reasonably justified regular cycle, known unacceptable vulnerabilities; and as soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks
- The manufacturer shall furnish to the Secretary a software bill of materials, including commercial, open-sourced, and off-the-shelf software components that will be provided to users

Action & Analysis

Included with H-ISAC Membership

2. Network Information Security Directive 2

Those organizations operating within the EU should be aware that the update to the NIS Directive is heading toward completion and that finalized language is not far off. While we don't know the exact language, an overview of some of the more important issues was provided by EU Parliamentary Rapporteur Bart Groothuis.[7]

For those who are unfamiliar with NIS, here is a short background. The original NIS Directive was adopted in 2016 as "the first piece of EU-wide cybersecurity legislation."[8] It was meant to improve cybersecurity across the EU, and every EU member was supposed to adopt national-level legislation that was in line with the text. NIS outlined aspects like cross-border collaboration, national capabilities, and what national supervision of critical sectors like healthcare should look like. It also detailed specifics related to security requirements, incident notification, processing of personal data, and penalties.[9]

The update to this Directive is NIS2, which the EU believes will provide "for a high common level of cybersecurity across the Union, to further improve the resilience and incident response capacities of both the public and private sector and the EU as a whole."[10] Once the text of NIS2 is finalized, it will fully replace the original NIS Directive.

Listed below are some of the more notable changes:[11, 12]

- The revised Directive aims to remove divergences in cybersecurity requirements and in implementation of cybersecurity measures in different member states
- The directive will formally establish the European Cyber Crises Liaison Organisation Network, EU-CyCLONe, which will support the coordinated management of large-scale cybersecurity incidents
- No longer will EU member states determine which entities meet the criteria to qualify as operators of essential services — a size-cap rule will ensure that all medium and large entities in a covered sector will be covered
- NIS2 will introduce a "light touch" cyber incident-reporting notification requirement with a 24-hour deadline. Within 72 hours, organizations must report whatever information they have available
- EU member states will be given 21 months to "transpose" the final text

Action & Analysis
Included with H-ISAC Membership

Congress-

Tuesday, May 17th:

- No relevant hearings

Wednesday, May 18th:

- Senate – Committee on Health, Education, Labor, and Pensions: Hearings to examine cybersecurity in the health and education sectors.

Thursday, May 19th:

- No relevant hearings

International Hearings/Meetings-

- No relevant meetings

EU –

- No relevant meetings

Conferences, Webinars, and Summits

https://h-isac.org/events/

Contact us: follow @HealthISAC, and email at contact@h-isac.org

About the Author
Hacking Healthcare is written by John Banghart, who served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, and as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

---

[1] https://www.fda.gov/media/119933/download

[2] https://www.fda.gov/media/119933/download

[3] https://www.congress.gov/bill/117th-congress/house-bill/7667

[4] https://www.congress.gov/bill/117th-congress/house-bill/7667

[5] https://www.congress.gov/bill/117th-congress/house-bill/7667

[6] https://www.congress.gov/bill/117th-congress/house-bill/7667

[7] https://www.euractiv.com/section/digital/podcast/nis2-all-you-need-to-know/

[8] https://www.enisa.europa.eu/topics/nis-directive

[9] https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[10] https://www.consilium.europa.eu/en/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/

[11] https://www.euractiv.com/section/digital/podcast/nis2-all-you-need-to-know/

[12] https://www.consilium.europa.eu/en/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/