SHARING SINCE 2010 Health-ISAC™
Collaborating for Resilience in Healthcare

Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare ○ TLP:WHITE Alert ID : 36d37c9f Oct 06, 2023, 08:43 AM

This week, *Hacking Healthcare*^{TM} starts by examining the newly issued Food and Drug Administration (FDA) final guidance related to the cybersecurity of medical devices. The new document updates nearly 10-year-old guidance and comes just prior to more stringent enforcement of the medical device submission requirements.

Welcome back to *Hacking Healthcare.*^{TM}

Health-ISAC European Summit

The Health-ISAC would like to remind members that there is still time to register for the upcoming 2023 European Summit. The event will be held in Dubrovnik, Croatia, from October 17 to October 19. For those interested in learning about responsible artificial intelligence or getting an update on NIS2, please consider registering before the deadline on October 12.

Link: https://web.cvent.com/event/3e5fb53c-28a0-4d5d-ad1b-7b82eb63d4ce/summary

The Health-ISAC Hobby Exercise 2023

The Health-ISAC is pleased to announce the fourth iteration of our Hobby Exercise Americas on October 25th in Washington DC. The Hobby Exercise is an annual Healthcare and Public Health (HPH) event designed to engage the healthcare sector and strategic partners on significant security and resilience challenges. The overarching objective is to inform and provide opportunities for continuous organizational improvement while increasing healthcare sector resiliency.
Members who wish to know more or express an interest in participating should visit the following registration link: https://portal.h-isac.org/s/community-event?id=a1Y7V00000VJ560UAD

FDA Issues Updated Medical Device Cybersecurity Guidance

On September 26, the FDA released its final guidance for medical device cybersecurity. Entitled, *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions,*[i] the 57-page document updates and replaces the existing guidance, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, from 2014. Let's examine the reasons for the new guidance, what content to expect, and what Health-ISAC members may wish to consider doing in response to it.

Background

The FDA's rationale for the updated guidance included specifically citing the increase of medical devices and electronic exchange of medical device-related health information as well as more frequent and severe cyber threats to the healthcare sector, all of which could lead to patient harm if not adequately addressed.[ii]

It also takes into account new medical device manufacturer obligations that stem from the passage of section 3305 of the Consolidated Appropriations Act, 2023.[iii] Section 3305 laid out cybersecurity related requirements for a variety of applications and submissions related to Subchapter A of Chapter V of the Federal Food, Drug, and Cosmetic Act (FD&C Act). While the new FDA guidance is not specific to Section 3305, "the recommendations in [the new guidance] intended to help manufacturers meet [those] obligations."[iv] Coincidently, or not, this new updated guidance was published in the days ahead of the FDA's expected ramping up of enforcement of the new rules found in Section 3305, which technically went into effect many months ago.[v]

The updated guidance is meant to compliment other existing medical device cybersecurity guidance, including:

- Post-market Cybersecurity Guidance[vi]
- Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software[vii]
- Content of Premarket Submissions for Device Software Functions[viii]

Content

In addition to highlighting general principles, the updated guidance reflects the new realities outlined above by especially emphasizing "the importance of ensuring that devices are designed securely and are designed to be capable of mitigating emerging cybersecurity risks throughout the total product lifecycle (TPLC)."[ix] This TPLC approach is particularly illustrated through the recommendations related to secure design and the use of a Secure Product Development Framework (SPDF), which the guidance describes as "a set of processes that reduce the number and severity of vulnerabilities in products throughout the device lifecycle."[x]

The section on implementing an SPDF is the largest of the document and includes details of its relation to security risk management, security architecture, and cybersecurity testing. The FDA does not advocate for any specific framework, noting instead that organizations should exercise flexibility to apply what makes sense for their particular circumstances. However, the guidance does provide the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF), "the medical device-specific framework that can be found in the Medical Device and Health IT Joint Security Plan (JSP) and IEC 81001-5-1," as examples that may align with necessary regulations.[xi]

Action & Analysis

Available with Health-ISAC Membership

Congress

Tuesday, October 3

No relevant meetings

Wednesday, October 4

No relevant meetings

Thursday, October 5

No relevant meetings

International Hearings/Meetings

No relevant meetings

About the Author

Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has 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, 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.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISAC's annual Hobby Exercise and provides legal and regulatory updates for the Health-ISAC's monthly Threat Briefing.

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

Tim can be reached at tmcgiff@venable.com.

[i] *Medical Devices: Quality System Considerations and Content of Premarket Submissions*: https://www.fda.gov/media/119933/download

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

[iii] https://www.congress.gov/bill/117th-congress/house-bill/2617

[iv] https://www.federalregister.gov/documents/2023/09/27/2023-20955/cybersecurity-in-medical-devices-quality-system-considerations-and-content-of-premarket-submissions

[v] https://cyberscoop.com/fda-cybersecurity-medical-devices/

[vi] https://www.fda.gov/media/95862/download

[vii] https://www.fda.gov/media/72154/download

[viii] https://www.fda.gov/media/153781/download

[ix] https://www.federalregister.gov/documents/2023/09/27/2023-20955/cybersecurity-in-medical-devices-quality-system-considerations-and-content-of-premarket-submissions
[x] https://www.fda.gov/media/119933/download
[xi] https://www.fda.gov/media/119933/download
[xii] https://www.fda.gov/media/119933/download
[xiii] https://www.fda.gov/medical-devices/workshops-conferences-medical-devices/webinar-final-guidance-cybersecurity-medical-devices-quality-system-considerations-and-content#:~:text=On%20September%2025%2C%202023%2C%20the,and%20Content%20of%20Premarket%20Submissions

Report Source(s)

Health-ISAC

Reference | References

FDA
FDA
cvent
federalregister
FDA
congress
Health-ISAC
Health-ISAC
Cyberscoop
FDA
FDA

Tags

Regulation, Hobby Exercise, Hacking Healthcare, Medical Devices, FDA

For Questions and/or Comments:

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

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

Hacking Healthcare�:

Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has 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, 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.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISAC�s annual Hobby Exercise and provides legal and regulatory updates for the Health-ISAC�s monthly Threat Briefing.

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

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.