HACKING HEALTHCARE™

Health-ISAC Weekly Blog -- Hacking Healthcare™

○○○ TLP:WHITE

Jan 04, 2024

Happy New Year H-ISAC members!

To kick off 2024, *Hacking Healthcare*™ begins by providing a breakdown of what we know and might expect from an upcoming proposed rule to modify the HIPAA Security Rule. We assess what kinds of expectations members should have about the timing of such a revision and what members might want to do in the meantime. Next, we examine a Government Accountability Office (GAO) report on medical device cybersecurity. Specifically, we take a look at what kinds of hurdles the GAO found for private sector members looking for government support.

Welcome back to *Hacking Healthcare*™.

HHS Signals Intention to Propose Modifications to HIPAA Security Rule

A notice posted to the website of the Office of Information and Regulatory Affairs (OIRA) within the Office of Management and Budget (OMB) suggests that the Department of Health and Human Services (HHS) intends to propose modifications to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule in fall of 2024.[i] Let's explore what we know so far.

The importance of the HIPAA Security Rule cannot be overstated for its role in standardizing security requirements for electronic protected health information (ePHI) at the U.S. federal level. However, HIPAA and the Security Rule have increasingly come under scrutiny for not being regularly updated to meet modern cybersecurity and privacy challenges. The OIRA notice itself cites public, media, and U.S. congressional interest in some form of HIPAA related modernization.[ii], [iii] In response to this feedback, HHS' acknowledgement of the "recent dramatic increase in cyber-attacks on the health care sector," newer and more complex cyber threats, and the evolution of healthcare IT, HHS appears ready to issue proposed modifications of the Security Rule tentatively set for around September of this year.

According to the notice, HHS had considered the possibility of addressing identified issues through new guidance, but they have determined that "this would be insufficient to prevent and address cybersecurity threats and vulnerabilities facing the U.S. health care system," and that "Revisions to the existing HIPAA Security Rule will help ensure the cybersecurity of individuals' ePHI."[iv]

Action & Analysis
*Included with Health-ISAC Membership*

GAO Report Flags Private Sector Hurdles to Accessing Government Support Related to Medical Devices

In late December 2022, the *Consolidated Appropriations Act, 2023* was passed into law. This Act included language directing the Government Accountability Office (GAO) to review cybersecurity in medical devices, including assessing the challenges that "relevant non-federal entities are facing challenges in accessing federal support on medical device cybersecurity."[vi] Some of its findings are worth briefly examining.

Context

For context, the GAO is an independent agency meant to provide unbiased information and assessments and to "help improve the performance and ensure the accountability of the federal government."[vii] Their tasking in the *Consolidated Appropriations Act, 2023* aligned with the Food and Drug Administration (FDA) being granted additional authorities to oversee medical device cybersecurity. For this report they engaged with relevant federal agencies and 25 relevant non-federal entities, which included several Health Delivery Organizations (HDOs), Medical Device Manufacturers (MDMs), and several healthcare associations and working groups.

Content

The 46-page report focuses on examining four areas:

- To what extent are relevant non-federal entities facing challenges in accessing federal support on medical device cybersecurity?
- To what extent have federal agencies addressed the challenges identified above?
- To what extent are key government agencies coordinating on medical device cybersecurity?
- To what extent do limitations exist in agencies' authority over medical device cybersecurity?

Some of the findings and recommendations include:

- The GAO recommending that the FDA and the Cybersecurity and Infrastructure Security Agency (CISA) update their mutual coordination agreement to support the cybersecurity of medical devices – to which both agencies concurred.
- The finding that the FDA does not yet know if they would "benefit from [having] additional authorities over the cybersecurity of medical devices," and that it would take some time to determine the adequacy of their recently increased authorities.[viii]

However, there were some other issues identified by the GAO report that are worth analyzing in more detail below. Specifically, a sizeable portion of the non-federal entities engaged by the GAO highlighted issues around the challenges they had being made aware of and accessing federal support for medical device cybersecurity.

Action & Analysis
Included with Health-ISAC Membership

Additionally, if you do not feel you have adequate access or contact with federal subject matter experts at CISA or within HHS, the Health-ISAC would like to remind you that we are happy to facilitate introductions or advocate on behalf of members. Please do not hesitate to reach out to membership@h-isac.org.

Congress
Tuesday, January 2
No relevant hearings

Wednesday, January 3

No relevant meetings

Thursday, January 4
No relevant meetings

[i] https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202310&RIN=0945-AA22
[ii] https://www.warner.senate.gov/public/_cache/files/f/5/f5020e27-d20f-49d1-b8f0-bac298f5da0b/0320658680B8F1D29C9A94895044DA31.cips-report.pdf
[iii] https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202310&RIN=0945-AA22
[iv] https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202310&RIN=0945-AA22
[v] https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202310&RIN=0945-AA22
[vi] https://www.gao.gov/assets/d24106683high.pdf
[vii] https://www.gao.gov/about
[viii] https://www.gao.gov/assets/d24106683.pdf
[ix] https://www.gao.gov/assets/d24106683.pdf
[x] https://www.gao.gov/assets/d24106683.pdf

Reference(s)	reginfo, senate, gao, gao, gao
Report Source(s)	Health-ISAC

Alert ID 73552176

View Alert

Tags Public-Private, Security Rule, Regulatory, Hacking Healthcare, HIPAA

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

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.

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**