Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare | TLP:WHITE | Alert ID : e7a16ecc | Sep 14, 2023, 08:36 AM

This week, *Hacking Healthcare*™ breaks down what Health-ISAC members can expect from a revision to a National Institute of Standards and Technology (NIST) guidance document on HIPAA Security Rule implementation. Then, we provide a brief update on when to expect the upcoming Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) rule and what kind of feedback is being asked for.

Welcome back to *Hacking Healthcare*™.

Health-ISAC Hobby Exercise 2023

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 wishing 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

Update: NIST Guidance on HIPAA Security Rule Implementation

For roughly the past two years, the National Institute of Standards and Technology (NIST) has been working in collaboration with the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) to create a revised cybersecurity resource guide for the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.[i] Since we last raised this issue, NIST has received over 250 unique comments on what stakeholders would like to see in the revised document. While the final version of *Special Publication (SP) 800-66 Revision 2* (SP 800-66) is not expected until later this year, NIST has provided an update on what can be expected.[ii]

As NIST themselves describes it, SP 800-66 "provides practical guidance and resources that can be used by regulated entities of all sizes to safeguard ePHI," and it "aims to help organizations improve their overall cybersecurity posture, while also complying with the Security Rule."[iii] While HIPAA has not

changed drastically over the years, the previous revision of SP 800-66 was published roughly 15-years ago in 2008.[iv]

Going into the revision process, NIST was particularly interested in hearing from stakeholders regarding what could be done to improve the documents organization, formatting, sections, and descriptions to make it more useful. Based on the comments they received, here is what we can expect when the final draft is published.

More Specific Resources for Small, Regulated Entities
NIST expressed their desire to "collaborate with other public and private sector entities to help create these resources, which may include tools, use cases, or more specific guidance."[v] However, these resources are likely to be separate from SP 800-66. NIST expects to provide further information on what this effort may look like "in the coming months."[vi]

General Clarifications
The primary example provided was clarifying the difference between "risk analysis" as a term defined within the HIPAA Security Rule and "risk assessment" as a "process by which a regulated entity can determine the level of risk to ePHI."[vii] NIST also plans to clarify references to and recommended usage of the HHS Security Risk Assessment (SRA) Tool.

Updated Security Rule Standards Mapping
SP 800-66 Revision 1 included a useful appendix that mapped the "Security Rule standards and implementation specifications to NIST publications relevant to each Security Rule standard, and to applicable security controls detailed in NIST SP 800-53."[viii] The new revision will replace this appendix with their online Cybersecurity and Privacy Reference Tool (CPRT), which will help facilitate mapping to a broader set of NIST publications, including the Cybersecurity Framework (CSF) Subcategories. This change will also allow the mappings to be updated more frequently.

HIPAA Security Rule Resources Reorganization
NIST will also move their resources section from an appendix to being hosted online. As with the mapping, NIST believes this move will help ensure that the HIPAA Security Rule Resources will continue to be updated. These resources have also been reorganized from "foundational to more complex" to make it easier for less mature organizations to know where to start.

Action & Analysis
Included with Health-ISAC Membership

CIRCIA Update

At the recent Billington CyberSecurity Summit, Cybersecurity and Infrastructure Security Agency (CISA) officials revealed a rough estimate for when they plan on publishing their Notice of Proposed Rulemaking (NPRM) for their Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) rule, as well was what they hope to get from industry stakeholders in terms of feedback. Given the impact this rule will have on the healthcare sector, we thought a brief update was in order.

For those struggling to keep up with the various new and proposed incident reporting rules and regulations, CIRCIA was passed by Congress and signed into law in March of 2022. It requires CISA "to develop and implement regulations requiring covered entities to report to CISA covered cyber incidents and ransom payments."[xi] While Congress laid down some required inclusions and guardrails for what the incident reporting would look like, such as requiring covered entities to report covered incidents within 72 hours, the details of who would be covered, what incidents would be covered, and the nature and content of the reports was broadly left up to the CISA rulemaking.
We may not need to wait too much longer before getting a much better sense of what the reporting rule will look like. CISA Director Jen Easterly is quoted as saying CISA is "finishing" the NPRM and that it "should be out later this year or early next year."[xii], [xiii]

Furthermore, CISA's Senior Advisor for Technology and Innovation, Lauren Boas Hayes, was quoted as emphasizing that while stakeholders have previously weighed in on how CISA should approach "covered entities" and "covered incidents," CISA expects to ask for additional feedback on these aspects when the NPRM is released.

Action & Analysis
Included with Health-ISAC Membership

Congress
Tuesday, September 12th
Senate – Judiciary Committee - An oversight hearing to examine A.I., focusing on legislating on artificial intelligence.

Senate – Commerce, Science, and Transportation Committee - Hearings to examine the need for transparency in Artificial Intelligence.

Wednesday, September 13th
No relevant meetings

Thursday, September 14th
No relevant meetings

International Hearings/Meetings
No relevant meetings

[i] https://csrc.nist.gov/news/2023/update-on-the-revision-of-nist-sp-800-66
[ii] https://csrc.nist.gov/pubs/sp/800/66/r2/ipd
[iii] https://www.nist.gov/blogs/cybersecurity-insights/nists-planned-updates-implementing-hipaa-security-rule-cybersecurity
[iv] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-66r1.pdf
[v] https://www.nist.gov/blogs/cybersecurity-insights/nists-planned-updates-implementing-hipaa-security-rule-cybersecurity

[vi] https://www.nist.gov/blogs/cybersecurity-insights/nists-planned-updates-implementing-hipaa-security-rule-cybersecurity
[vii] https://www.nist.gov/blogs/cybersecurity-insights/nists-planned-updates-implementing-hipaa-security-rule-cybersecurity
[viii] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-66r1.pdf
[ix] https://healthsectorcouncil.org/wp-content/uploads/2022/10/HSCC-CWG-Comments-of-NIST-SP800-66r2.pdf
[x] https://www.nist.gov/blogs/cybersecurity-insights/nists-planned-updates-implementing-hipaa-security-rule-cybersecurity
[xi] https://www.cisa.gov/sites/default/files/publications/CIRCIA_07.21.2022_Factsheet_FINAL_508%20c.pdf
[xii] https://www.meritalk.com/articles/easterly-partnerships-critical-as-cisa-nears-finish-line-on-circia/
[xiii] https://federalnewsnetwork.com/cybersecurity/2023/09/circia-cmmc-inch-closer-with-rulemaking-marathons-nearing-crucial-stage/

Report Source(s)

Health-ISAC

Reference | References

CISA
Federal News Network
Health-ISAC
NIST-CSF
Health Industry Cybersecurity Practices
meritalk
NIST-CSF
NIST-CSF
NIST-CSF

Tags

Incident Reporting, CIRCIA, Hobby Exercise, Hacking Healthcare, NIST, NIST Guide, HIPAA

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.