August 8, 2022

TLP White

This week, Hacking Healthcare begins by examining a new draft publication from the National Institute of Science and Technology (NIST) that is meant to help organizations comply with the HIPAA Security Rule. We briefly break down the new document's contents and explain how Health-ISAC members can contribute to improving the draft. Then we briefly highlight the work of a new U.S. government council that is attempting to tackle the problem of an increasing amount of unaligned cybersecurity incident-reporting regimes that threaten to place a heavy burden on cyber attack victims.

Welcome back to *Hacking Healthcare*.

1. **NIST Publishes HIPAA Cybersecurity Guide**

   Failure to comply with the various parts of HIPAA can land covered entities in regulatory hot water, but navigating and implementing all the requirements needed to be considered compliant aren't always clear and easy. Helpfully, the National Institute of Science and Technology (NIST) has issued a revised draft publication designed to help organizations protect patient health information and comply with the HIPAA Security Rule.[1]

   Published on July 21st, *Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide* is a 152-page document that "aims to help educate readers about the security standards included in the *Health Insurance Portability and Accountability Act* (HIPAA) Security Rule."[2] Within it, organizations can find:[3]

   - An overview of the HIPAA Security Rule;
   - Risk assessment guidance for regulated entities on assessing and managing risks to electronic protected health information (ePHI);
   - Risk management guidance;
   - Typical activities that a regulated entity might consider implementing as part of an information security program; and

- Additional resources that regulated entities may find useful in implementing the Security Rule.

The new draft publication has also been helpfully designed to make use of other NIST products like the NIST *Cybersecurity Framework* (CSF) and NIST *Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations* (SP 800-53). In fact, NIST has "mapped all the elements of the HIPAA Security Rule to the Cybersecurity Framework subcategories and to controls in NIST SP 800-53's latest version."[4]

The new NIST draft publication is freely available on the NIST website.

NOTE: The Healthcare Sector Coordinating Council will be submitting comments to NIST. If you are interested in contributing your thoughts, please contact Greg Garcia at https://healthsectorcouncil.org/contact/.

Action & Analysis
Membership required

2. DHS Cyber Incident Reporting Council Starts Up

On July 22, the first-ever meeting of the Cyber Incident Reporting Council (CIRC) took place. CIRC, which was authorized by Congress as part of the *Cyber Incident Reporting for Critical Infrastructure Act*, is "a new Council composed of federal agencies with a Congressional mandate to coordinate, deconflict, and harmonize existing and future federal cyber incident reporting requirements."[5]

CIRC's representatives, which include individuals from the Department of Homeland Security (DHS), the Securities and Exchange Commission (SEC), Federal Bureau of Investigation (FBI), Office of the National Cyber Director (ONCD), and HHS, are intent on "meaningfully [improving] cybersecurity, [and reducing the] burden on industry by advancing common standards for incident reporting."[6]

They are tasked with reporting to Congress in 180 days from the first meeting with recommendations on how the federal government can achieve harmonization across different cyber incident-reporting regimes.

Action & Analysis
Membership required

3. **Hacktivists Target Organization Over Anti-abortion Stance**

   Hacktivism is not new, but it has generally been reported on in relation to international politics. China and Russia are routinely cited as examples of countries that benefit from individuals carrying out activities aligned with state goals, with or without a certain level of prodding or tacit approval from the government.

   According to a report from CyberScoop, "Pro-choice hacktivists leaked more than 74 gigabytes of data connected to evangelical organizations," due to the organizations' support for the recent U.S. Supreme Court decision that overturned *Roe v. Wade*.[7] If that motive is substantiated, it further highlights the growing cyber risk from political and ideological activists related to social issues.

   The data was published freely online with the goal of highlighting what the hacktivists called "a worrying trend of far-right and anti-abortion activists aligning themselves with the evangelical Christian movement [and] hiding their funding sources behind laws that allow church ministries to keep their donations secret."[8] They described their attack as an act of "radical transparency."[9]

   Action & Analysis
   Membership required

Congress

Tuesday, August 9th:
- No relevant hearings

Wednesday, August 10th:
- No relevant hearings

Thursday, August 11th:
- No relevant hearings

International Hearings/Meetings

- No relevant meetings

EU –

- No relevant meetings

Conferences, Webinars, and Summits

August 8, 2022

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, 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.nist.gov/news-events/news/2022/07/nist-updates-guidance-health-care-cybersecurity

[2] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.ipd.pdf

[3] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.ipd.pdf

[4] https://www.nist.gov/news-events/news/2022/07/nist-updates-guidance-health-care-cybersecurity

[5] https://www.dhs.gov/news/2022/07/25/readout-inaugural-cyber-incident-reporting-council-meeting

[6] https://www.dhs.gov/news/2022/07/25/readout-inaugural-cyber-incident-reporting-council-meeting

[7] https://www.cyberscoop.com/evangelical-wmtek-liberty-counsel-hack-donors-operation-jane/

[8] https://www.cyberscoop.com/evangelical-wmtek-liberty-counsel-hack-donors-operation-jane/

[9] https://www.cyberscoop.com/evangelical-wmtek-liberty-counsel-hack-donors-operation-jane/