COSMOS
Navigate the Compliance Universe

Compliance Today - April 2024

Erika M. Riethmiller (erika.riethmiller@uchealth.org, linkedin.com/in/erika-riethmiller-33652656/) is the Chief Privacy Officer at UCHealth in Aurora, CO.

Recently published federal healthcare and public health sector-specific voluntary cybersecurity performance goals

by Erika M. Riethmiller

On December 6, 2023, the U.S. Department of Health and Human Services (HHS) released a*Healthcare Sector Cybersecurity* strategy paper.[1] This paper outlines HHS's goal to establish voluntary cybersecurity performance goals (CPGs) in alignment with the healthcare industry input, to enhance cybersecurity within the healthcare and public health (HPH) sectors. Since 2003, the federal government's Cybersecurity and Infrastructure Security Agency (CISA) Healthcare and Public Health Sector has been recognized by the federal government as one of 16 critical infrastructure sectors identified as being so vital to the U.S. that their incapacitation or destruction would have a debilitating effect on national security and public health or safety. This paper was largely in response to the White House's March 2023 publication of its *National Cybersecurity Strategy* which outlined the administration's priorities regarding cyber resiliency in the U.S. by stating "Cybersecurity is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defense."[2]

The paper also built upon a July 2021 White House "National Security Memorandum Improving Cybersecurity for Critical Infrastructure Control Systems."[3] This memorandum outlined a series of actions that needed to be taken by the federal government to develop general (e.g., non-sector-specific) CPGs that would be consistent across all critical infrastructure sectors. CISA, in coordination with the National Institute of Standards and Technology (NIST), was tasked with developing these non-sector-specific CPGs. NIST is a nonregulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

On January 24—49 days after issuance of the strategy paper—HHS published the HPH CPGs along with a new "gateway website" designed to assist healthcare organizations in prioritizing implementation of the CPGs and easily access pertinent resources that could be used by organizations when implementing both the essential and enhanced CPGs.[4]

Why did HHS publish HPH CPGs so quickly?

First, the need was great. The HPH critical infrastructure sector has witnessed unparalleled increases in cyberattacks over the past decade. HHS's Office for Civil Rights (OCR) website—as described in the strategy paper—offers one glimpse into the explosion of cyberattacks against OCR-regulated healthcare entities, evidencing that from 2018 to 2022, there was a 278% increase in large breaches (breaches impacting over 500 individuals) reported to OCR that were the result of a ransomware cyberattack.[5]

Secondly, work to develop cyber-resilient resources for the healthcare sector, together with industry stakeholders, has been in place since 2015 when the Cybersecurity Information Sharing Act of 2015 (CSA)—a law designed to "improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats"—was passed into law.[6] This law made it easier for organizations to share personal information with the government in cases of cybersecurity threats, created a system for federal agencies to receive threat information from private organizations, and required that a task force be established to develop a document that "brought forth cybersecurity awareness and provided best practices for mitigating the most pertinent cyber issues within the healthcare sector."[7] CSA also established the 405(d) Program, which, later in 2017, resulted in the establishment of the 405(d) Task Group, a collaborative team of federal government and healthcare industry subject matter experts who have been hard at work since 2017 creating resources for healthcare organizations to enhance awareness of cyber risk and defend against cyberattacks.

To understand the impetus behind the HPH CPGs, it's important to look historically at recent federal cyber regulations and the federal government's players in the cybersecurity field.

- **CISA** – It works to protect the nation from cyber and physical threats and increase the cyber resilience of the nation's critical infrastructure.
- **HHS** – The federally designated Sector Risk Management Agency for the HPHs regarding cybersecurity. (Pursuant to the Homeland Security Act of 2002, as amended, and Presidential Policy Directive 21.)
- **Health Sector Coordinating Council (HSCC)** – A coalition of private-sector critical healthcare infrastructure entities organized to partner with and advise the federal government on identifying and mitigating strategic threats and vulnerabilities facing the sector's ability to provide services and assets to the public.
- **HSCC's Cybersecurity Working Group** – A group of more than 400 industry and government organizations collaborating to develop strategies to combat emerging and ongoing cybersecurity challenges to the health sector.

So, what exactly are CPGs?

Compliance experts may think first about OIG's "compliance program guidance," or CPGs. OIG issued these CPGs in the late 1990s (and updated them in 2023), which are also voluntary and provide structure to various entities to use when designing compliance programs to meet federal requirements.[8] HHS's cybersecurity-related CPGs are different. They are intended to provide healthcare industry stakeholders (e.g., hospitals, safety net providers, healthcare delivery organizations, and industry vendors) with a set of prioritized cybersecurity practices that can be adopted and implemented to lessen cyber risks these organizations are currently facing. There are two categories of the HPH CPGS—"essential" and "enhanced" with essential goals targeting minimum standards and practices for cybersecurity performance and enhanced levels designed to encourage adopting more advanced practices to address cyber risks. All HPH CPGs are intended to address the overall risk to the nation of insufficient cybersecurity practices and controls by healthcare sector participants to "improve cyber resiliency and protect patient safety."[9]

The HPH CPGs are based heavily on two resources: NIST's Cybersecurity Framework (CSF) and the CISA 405(d) resources, including the *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)* publications specific to small and medium/large organizations.[10] These critical federal government resources and tools are referenced heavily in each of the specific HPH CPGs.

HHS's intent with the voluntary HPH CPGs is to use them to inform the department's "potential future regulatory action." Importantly for healthcare entities subject to HIPAA compliance, the strategy lays out HHS's plans to:

- Have all hospitals meeting HPH CPGs "in the coming years."[11]
- Require OCR to update the HIPAA Security Rule to include new cybersecurity requirements.
- Enforce new cybersecurity requirements through the "imposition of financial consequences for hospitals."[12]
- Work with Congress to increase resources for HHS to investigate potential HIPAA violations, conduct proactive audits of covered entities and business associates (BAs), and increase civil monetary penalties for HIPAA violations.

So, while voluntary, HPH CPGs already appear to have more strength and potential enforcement consequences behind them than other voluntary federal guidelines.

How does this affect healthcare providers, BAs, and related entities?

There are already many good reasons for organizations to become more aware of cyber risk and enhance their cybersecurity posture. Risks to organizations for not doing so include reputational, compliance and regulatory, operational, financial, and information technology risks. Additionally, the benefits to organizations of being cyber secure are numerous and include protection from network downtime, the ability to withstand extortion attempts, not having to pay ransoms to have company data returned or released, financial stability, company resilience, and organizational reputation. Being cyber-resilient is becoming a market differentiator. The anticipated publication of HPH CPGs is one more good reason to get started now on improving your cybersecurity risk posture.

As previously mentioned, the federal government has been working diligently for years to ensure that organizations of all types and sizes have the resources they need to enhance their cybersecurity posture. It is not hard to imagine that, at some point, there simply won't be any more excuses for organizations that choose not to take advantage of these resources—including the new HPH CPGs—to adequately protect their organizations and information systems from the foreseeable, common, and constant threat of cyberattacks against the HPH.

What can you do now that the new HPH CPGs are published?

Use the new HPH CPGs as a guide to update and enhance your organization's information security program to harden your electronic information systems and protect the information within them against harm from cyberattacks. For healthcare organizations, this is especially critical given the opportunity for, and the risk that, these cyberattacks will impact patient care. In a recent Ponemon Institute study, 21% of survey respondents reported that cyberattacks were linked to a rise in mortality rate in their organizations.[13]

Check out the previously published cross-sector (e.g., non-sector-specific) cybersecurity CPGs.[14] These CPGs are also designed to reduce the frequency and severity of cyberattacks across all the nation's critical infrastructure organizations. Similar to the HPH CPGs, they are aligned to the NIST CSF functions and provide cybersecurity practices with "known risk-reduction value" to entities who adopt and implement them. Examples from both groups of CPGs include information security basics such as asset inventory, revoking credentials for departing employees, organizational cybersecurity leadership, phishing-resistant, multi-factor authentication, incident reporting, planning, and preparedness.

Don't forget about another great opportunity HHS offers to HIPAA-regulated entities—recognized security practices (RSPs). Organizations that are able to adequately document and demonstrate to OCR that RSPs have been in place enterprise-wide for at least the past 12 months may be entitled to decreased lengths and severity of audits, and reduced enforcement penalties and fines for HIPAA violations.[15] The RSPs and HPH CPGs rely heavily on the same two resources: NIST's CSF and the 405(d) Task Group publications and resources. Check out the introductory video by HHS that explains what these RSPs entail, how to demonstrate compliance with the HITECH Amendments regarding RSPs, and how a strong compliance program—in alignment with HIPAA's Security Rule—can help organizations defend against cyberattacks.[16] While these RSPs are voluntary, e.g., OCR cannot penalize an organization for *not* implementing them, they can be a forceful tool in an organization's toolbox when it finds itself subject to an enforcement action by OCR for violating HIPAA's Security Rule.

Use HPH CPGs to assess third-party vendors' cybersecurity posture to ensure that they have rigorous cyber compliance programs and effective controls in place to mitigate harm from cyber enemies. Another resource from the HSCC Cyber Working Group, the *Supply Chain Risk Management Guide,* provides healthcare organizations with actionable guidance and practical tools to manage cybersecurity risks based on their dependencies within the health system supply chain.[17] Larger organizations are encouraged to use the guide to leverage their standing and influence within the healthcare industry's supply chain by recommending incorporating the guidance and tools into their suppliers—and their suppliers' suppliers—information security programs.

Conclusion

As information technology and security teams work to adopt HPH CPGs, compliance and privacy experts can assist them and their organizations in becoming more cyber-resilient by incorporating the CPGs into their compliance and privacy programs as well. Hold a staff meeting on cyber awareness and discuss how the bad guys can trick staff into clicking on links; post educational cyber materials in break rooms where they will be seen by all, such as the 405(d) "How are the Phish Biting Today" poster,[18] promote HSCC's video "Cybersecurity for the Clinician" which offers free continuing medical education/continuing education unit credits to providers,[19] demonstrate how critical being cyber-resilient is to your patients' safety by promoting that staff views the 405d video on "Cyber Safety is Patient Safety."[20]

Cybersecurity is a shared responsibility. Our safety, prosperity, and livelihoods depend on all of us doing our part to harden and defend our organizations from cyberattacks to ensure the safety of our patients and their information. Especially in the HPH, where connectivity of information systems is commonplace and immensely important to caring for the health of our citizens, the cyber exploitation of even one organization's data is a risk to us all.

Takeaways

- The U.S. Department of Health and Human Services (HHS) published a set of healthcare-specific cybersecurity performance goals (CPGs) designed to assist healthcare organizations that adopt and implement them in becoming more cyber-resilient.
- The CPGs are based largely on two existing federal government resources: the National Institute of Standards and Technology's Cybersecurity Framework and HHS's 405(d) publication, *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*.
- While voluntary, HHS states that their plan is to have all hospitals meet the CPGs in the coming years.
- These CPGs will be used by HHS to "inform future regulatory action" against healthcare entities.

- Don't delay improving your cybersecurity posture, as "cyber safety is patient safety!"

1 U.S. Department of Health and Human Services, *Healthcare Sector Cybersecurity*, December 2023, https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf.
2 The White House, *National Cybersecurity Strategy*, March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
3 The White House, "National Security Memorandum Improving Cybersecurity for Critical Infrastructure Control Systems," July 28, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/.
4 U.S. Department of Health and Human Services, "HHS Releases New Voluntary Performance Goals to Enhance Cybersecurity Across the Health Sector and Gateway for Cybersecurity Resources," news release, January 24, 2024, https://aspr.hhs.gov/newsroom/Pages/HHS-Releases-CPGs-and-Gateway-Website-Jan2024.aspx.
5 U.S. Department of Health and Human Services, *Healthcare Sector Cybersecurity.*
6 Cybersecurity Information Sharing Act of 2015, 114th Congress (2015-2016), S. Rept. 114-32.
7 HHS 405(d), "About Us," accessed January 29, 2024, https://405d.hhs.gov/about.
8 U.S. Department of Health and Human Services, Office of Inspector General, " Compliance Guidance," accessed January 29, 2024, https://oig.hhs.gov/compliance/compliance-guidance/.
9 U.S. Department of Health and Human Services, *Healthcare Sector Cybersecurity.*
10 HHS 405(d), "How Can We Help You," Cornerstone Publications, accessed January 29, 2024, https://405d.hhs.gov/information.
11 U.S. Department of Health and Human Services, *Healthcare Sector Cybersecurity*; HHS 405(d), "How Can We Help You."
12 U.S. Department of Health and Human Services, *Healthcare Sector Cybersecurity*, 4.
13 Ponemon Institute, *Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care*, 2023,https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf.
14 Cybersecurity & Infrastructure Security Agency, *Cross-Sector Cybersecurity Performance Goals*, March 2023 Update, https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf.
15 RSPs are broken into three categories to include: cybersecurity practices and controls that align to the NIST Cybersecurity Framework (CSF), cybersecurity practices and subpractices from the *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients* (HICP technical volumes), as well as other statutory or regulatory-recognized programs and processes that address cybersecurity.
16 Nick Heesters, "OCR Recognized Security Practices Video Presentation," U.S. Department of Health and Human Services, Office for Civil Rights, YouTube video, 30:38, October 31, 2022, https://www.youtube.com/watch?v=e2wG7jUiRjE.
17 Health Sector Coordinating Council, Cybersecurity Working Group, *Supply Chain Risk Management Guide v2.0*, October 2023, https://healthsectorcouncil.org/wp-content/uploads/2023/10/HIC-SCRiM_2023-2.pdf.
18 405(d), "How are the Phish Biting Today?" poster, accessed January 29, 2024, https://405d.hhs.gov/Documents/405d-five-threats-email-phishing-poster.pdf,
19 Healthcare Cybersecurity, "Cyber Safety Is Patient Safety," Cybersecurity for the Clinician, Healthcare and Public Health Sector Coordinating Council, YouTube video, 6:14, April 4, 2023, https://www.youtube.com/watch?v=rS0gT6bIiYw.
20 405(d), "Cyber Safety is Patient Safety," home page, accessed January 29, 2024, https://405d.hhs.gov/.