ALSTON & BIRD

Health Care/Privacy, Cyber & Data Strategy ADVISORY

FEBRUARY 5, 2024

HHS Issues Cybersecurity Performance Goals Specific to the Health Care and Public Health Sector

by Angela Burnette, Kate Hanniford, and Elinor Hiller

On January 24, 2024, HHS published voluntary Cybersecurity Performance Goals (CPGs) for the health care and public health (HPH) sector to "help healthcare organizations prioritize implementation of high-impact cybersecurity practices." According to HHS, health care organizations can use these CPGs to prioritize(1) strengthening cyber preparedness; (2) improving cyber resiliency; and (3) protecting patient health information and safety. HHS added that these CPGs were "informed by common industry cybersecurity frameworks, guidelines, best practices, and strategies (e.g., Healthcare Industry Cybersecurity Practices, National Institute of Standards and Technology (NIST) Cybersecurity Framework, … and the National Cybersecurity Strategy)."

What do health care organizations need to know now about these new HHS CPGs?

Are These Newly Announced CPGs Really Voluntary?

According to HHS, currently yes – these CPGs are "goals" that are "voluntary." The CPGs are a follow-up to a December 6, 2023 HHS press release that previewed that HHS would be "publishing new voluntary health care-specific cybersecurity performance goals" as one of four HHS pillars to help health care organizations strengthen their cyber resiliency. On the same day, HHS released the concept paper Healthcare Sector Cybersecurity.

Although these CPGs are divided into "Essential" and "Enhanced," both types of goals are a "voluntary subset of cybersecurity practices." According to HHS, the Essential CPGs present a floor of minimum safeguards for "common vulnerabilities," while the Enhanced CPGs help health care organizations "mature their cybersecurity capabilities" and adopt "more advanced practices."

Separate and apart from the CPGs, keep in mind that covered entities and business associates will still have their independent obligations to comply with the HIPAA Security Rule.

What Does HHS List as Essential CPGs?

The following CPGs are Essential:

- Mitigate Known Vulnerabilities
- Email Security
- Multifactor Authentication
- Basic Cybersecurity Training
- Strong Encryption
- Revoke Credentials
- Basic Incident Planning and Preparedness
- Unique Credentials
- Separating User and Privileged Accounts
- Vendor/Supplier Cybersecurity Requirements

What Does HHS List as the Enhanced CPGs?

The following CPGs are Enhanced:

- Asset Inventory
- Third Party Vulnerability Disclosure
- Third Party Incident Reporting
- Cybersecurity Testing
- Cybersecurity Mitigation
- Detect and Respond to Relevant Threats
- Network Segmentation
- Centralized Log Collection
- Centralized Incident Planning and Preparedness
- Configuration Management

If These Essential and Enhanced CPGs Are Voluntary, Is the HIPAA Security Rule Being Paused?

No. HHS specifically confirmed that it "will continue to investigate potential HIPAA violations." Additionally, HHS, through the Office for Civil Rights, reorganized early last year to create a new Enforcement Division, positioning enforcement as a priority likely to remain at the forefront in 2024.

Will HHS Be Amending the HIPAA Security Rule? If So, When?

Probably yes. According to the HHS press release and concept paper, HHS plans to "begin an update" to the HIPAA Security Rule in the spring of 2024 "to include new cybersecurity requirements" that will "be informed by" the recently announced voluntary CPGs. Based on an Office of Management and Budget regulatory agenda published in the fall of 2023, proposed amendments to the HIPAA Security Rule are initially slated for September 2024, but that timeframe might change.

According to HHS, they also plan to "work with Congress to increase civil monetary penalties for HIPAA violations and increase resources for HHS to investigate potential HIPAA violations, conduct proactive audits, and scale outreach and technical assistance for low-resourced organizations to improve HIPAA compliance." (Keep in mind that civil monetary penalties for HIPAA violations are already subject to annual cost-of-living adjustments.)

It is unclear whether future proposed amendments by HHS to the HIPAA Security Rule will incorporate comment and input from covered entities and business associates – and also still align with the HIPAA Security Rule's current flexibility recognized in 45 CFR 164.306. The HIPAA Security Rule's implementation specifications are currently stated as either "required" or "addressable." The HIPAA Security Rule currently permits covered entities and business associates to consider certain factors (such as size, complexity and capabilities, technical infrastructure, hardware and software security

capabilities, costs, and probability/criticality of potential risks to electronic protected health information) to determine what is reasonable and appropriate for their own IT environment. At least two of the Essential CPGs appear to retain some flexibility. The Multifactor Authentication CPG mentions "where safe and technically capable," and the desired outcome for the Vendor/Supplier Cybersecurity Requirements CPG mentions "appropriate measures." Stay tuned for proposed rules from HHS addressing the HIPAA Security Rule.

Will CMS Also Propose New Cybersecurity Requirements?

Likely yes. According to the HHS concept paper, "CMS will propose new cybersecurity requirements for hospitals through Medicare and Medicaid." Per HHS, the future proposed cybersecurity standards "would be incorporated into existing programs, including Medicare and Medicaid." New CMS requirements could come in the form of Medicare or Medicaid conditions of participation for hospitals or as part of the Medicare Promoting Interoperability Program. CMS has used these mechanisms to support broader HHS programs. For example, CMS recently proposed "disincentives" for health care providers found by the HHS Office of Inspector General to have committed information blocking.

It is unclear whether future proposed enforceable cybersecurity requirements from CMS will go through a rulemaking process and comment period and also incorporate the HIPAA Security Rule's current flexibility.

Will There Be Any Financial Assistance or Other Incentives for the CPGs?

Possibly yes. According to HHS, its "ongoing work to enhance cybersecurity for health care and public health sectors" will include working "with Congress to obtain new authority and funding to administer financial support and incentives for domestic hospitals to implement high-impact cybersecurity practices."

In its concept paper, HHS mentioned two types of potential incentives. First, HHS envisioned "an upfront investments program to help **high-need healthcare providers, such as low-resourced hospitals**, cover the upfront costs" to implement Essential CPGs. Second, HHS envisioned "an incentives program to encourage **all hospitals** to invest in advanced cybersecurity practices" to implement Enhanced CPGs. Stay tuned for future HHS announcements and details.

Are These CPGs Relevant to 405(d)?

Although not formally stated, it would make sense that HHS would consider implementation of at least some CPGs as a recognized security practice. Under Section 13412 of the HITECH Act, HHS must take into consideration when a covered entity or business associate can adequately demonstrate that certain "recognized security practices" were "in place" for the past 12 months when determining a potential fine, audit results, or other remedies for potential HIPAA Security Rule violations. The 405d Program is focused on "providing organizations across the nation with useful and impactful Healthcare and Public Health (HPH) focused resources, products, and tools that help educate, raise awareness, and provide vetted cybersecurity best practices which drive behavioral change and strengthen the sector's cybersecurity posture against cyber threats."

Here, the stated purpose of the HHS CPGs is to "help healthcare organizations prioritize implementation of high-impact cybersecurity practices." The HHS CPGs were "adapted" from the Cybersecurity and Infrastructure Security Agency's March 2023 CPGs and "informed by" the National Cybersecurity Strategy. The HHS CPGs also contain two appendices, which crosswalk "Desired Outcomes" to the NIST Cybersecurity Framework (V1.1) and NIST 800-53 Rev 5 controls.

The HHS CPGs also contain a linked training course. When clicked, the "Launch Tour" button takes the reader directly to HHS's 405d website. Those HHS CPG training materials emphasize that the CPGs are mapped to "HICP, NIST, and the CISA CPGs." The end of the HHS CPG training course provides links to additional resources (dated January 29, 2024) that include a link to the HHS 405d Program.

As a reminder, HHS continues to release a substantial amount of material about 405d, including via https://405d.hhs.gov (see the tabs titled "News and Events" and "Resource Library") and through OCR press releases. For example, see 405(d): Cornerstone Publications for various Health Industry Cybersecurity Practices resources, including: (1) Managing Threats and Protecting Patients (2023 edition plus Technical Volumes 1 and 2); (2) 5 Cybersecurity Threats; (3) 10 Mitigating Practices; and (4) Hospital Resiliency Landscape Analysis.

Are the HHS CPGs Already Mapped to Specific Threat Scenarios or Attack Vectors?

Yes. The HHS CPGs are mapped to specific "threats," as well as to NIST 800-53. See Appendix 1 for Essential CPGs and Appendix 2 for Enhanced CPGs. Additionally, a "Deploying the CPGs" section maps the HHS CPGs to common attack vectors.

What Are the Four HHS Cybersecurity Resiliency Pillars That Health Care Organizations Should Keep an Eye Out For?

The four pillars of HHS's ongoing work are:

1. Publish voluntary CPGs (which HHS notes are in addition to HHS/FDA efforts to improve medical device cybersecurity).
2. Incentivize and implement cybersecurity practices.
3. Implement an HHS-wide strategy to enhance enforcement and accountability (will propose enforceable cybersecurity standards).
4. Expand and mature a cybersecurity "one-stop shop" within HHS (including improved coordination between HHS and the federal government and improved partnership with the industry).

Conclusion

There is much activity in 2024 in the cybersecurity space for health care organizations, and we expect that to continue. If you have any questions about the HHS CPGs or the 405d Program, or if we can assist with cybersecurity readiness or incident response, please let us know.

You can subscribe to future Health Care and/or Privacy, Cyber & Data Strategy advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions, or would like additional information, please contact one of the attorneys with our Health Care Team or one of the attorneys with our Privacy, Cyber & Data Strategy Team.
