COSMOS
Navigate the Compliance Universe

Compliance Today - December 2023

Dawn Morgenstern (dawn.morgenstern@clearwatersecurity.com, linkedin.com/in/dawn-morgenstern/) is Chief Privacy Officer, Senior Director of Consulting Services, at Clearwater in Nashville, TN.

Leveraging 405(d) HICP: A recap and overview of 2023 updates

by Dawn Morgenstern

If the U.S. Department of Health and Human Services' (HHS) 405(d) *Health Industry Cybersecurity Practices* (HICP) guidelines have been on your organization's radar or already implemented in your organization, you likely know that updates were recently released for 2023 reflecting changes in healthcare risks and vulnerabilities and how organizations should respond to the changing threat landscape.[1]

405(d) HICP is a voluntary set of federally recognized standards, and according to Pub. L. No, 116–321—which was signed into law in 2021—HHS must recognize the adoption of cybersecurity best practices—like 405(d) HICP during an investigation.[2] If an organization can demonstrate that they have had 405(d) HICP in place for no less than 12 months prior to the point of an investigation, it may result in the mitigation of fines and early, favorable regulatory treatment.

To be clear, Pub. L. No. 116–321 doesn't provide regulatory relief regarding HIPAA compliance but offers much-needed alignment and guidance between National Institute of Standards and Technology/Cybersecurity Framework and 405(d) HICP. In the event of an HHS Office for Civil Rights (OCR) investigation, OCR will ask which framework you've adopted and expect that you can demonstrate when the implementation and use of these best practices.

Why we need 405(d) HICP

When HIPAA became law in 1996, healthcare didn't know a lot about cybersecurity—processes and frameworks were still being developed, and they've continued to evolve over the last 20-plus years.

As a result, HIPAA guidelines didn't account for an organization's capabilities, resources, or threats—creating ambiguity that can make it difficult for healthcare organizations to understand what safeguards and controls they need to put in place to be HIPAA compliant and to protect patient data adequately. 405(d) HICP helps clarify some of that ambiguity by identifying cybersecurity best practices through a lens that recognizes small, medium, and large organizations.

This is particularly critical as healthcare's threat landscape evolves and grows increasingly complex. Cyberattackers target healthcare organizations with ransomware more than any other industry, and a healthcare breach now costs, on average, almost $11 million. What's more is the connection between a successful ransomware attack and increased mortality rate and length of stay.[3] In other words, cybersecurity is patient safety.

Pub. L. No. 116–321 and 405(d) HICP offers some alignment between the government and the private sector

regarding best practices to protect this part of the critical infrastructure—aligning organizations of all sizes toward a common goal: to develop guidelines and practices that can best be used against cybersecurity threats.

Who should implement 405(d) HICP?

The short answer is that 405(d) HICP was designed for all healthcare-covered entities and business associates (BAs). 405(d)'s *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients* (2023 Edition) is a free publication that examines cybersecurity threats and vulnerabilities that affect the healthcare industry.[4] The related technical volumes go on to outline 10 cybersecurity practices to mitigate them:

- *Technical Volume 1* is for small entities and can stand-alone.[5]
- *Technical Volume* 2 is for medium and large healthcare entities:[6]
    - Medium-size entities must follow medium cybersecurity practices.
    - Large entities must follow medium and large cybersecurity practices.

While 405(d) HICP has a strong healthcare focus, the guidelines are also for other organizations, like practice management organizations, managed services, small device manufacturers, health plans, pharmaceutical organizations, and others. All covered entities and BAs can utilize it as part of their ongoing cybersecurity lifecycles.

Top five security threats for healthcare

The 405(d) HICP 2023 edition was updated to reflect the changes in the healthcare threat landscape and is a good indicator of what healthcare organizations of all sizes and structures are coming up against. 405(d) outlines the following top five healthcare cybersecurity threats for 2023:

1. **Social engineering (new in the 2023 edition)**: This top threat was previously email phishing but was expanded to encompass similar threats in addition to email phishing, like smishing, whaling, business email compromise, and more. Social engineering refers to an attempt to trick someone into giving out personal information or infecting a device by clicking on a link that gives hackers access to various sources of data.
2. **Ransomware**: This is an attack that gives hackers control of data or a computer system they hold hostage until a ransom is paid.
3. **Loss or theft of equipment or data**: Everyday devices such as laptops, smartphones, and USB/thumb drives are lost or stolen and could end up in attackers' hands.
4. **Insider, accidental, or intentional data loss**: These threats exist within every organization where employees, contractors, or other users access your organization's technology infrastructure, network, or databases.
5. **Attacks against network-connected medical devices**: Connected medical devices represent a growing attack vector many organizations have yet to adequately address in their risk management strategies. One study found that 53% of hospital-connected medical devices and other Internet of Things devices have a known critical vulnerability.[7]

Practices and subpractices

Section 405(d) includes practices and subpractices healthcare organizations can apply based on organization size. When you see how the volumes impact small, medium, and large organizations, notice the top threats outlined in various controls to mitigate the threats. The practices are high-level, while the subpractices offer more detail. These practices and subpractices can help guide your actions and investments in your healthcare cybersecurity program.

The practices are designed to help strengthen cybersecurity capabilities by:

- Enabling organizations to evaluate and benchmark cybersecurity capabilities effectively and reliably.
- Sharing knowledge, common practices, and appropriate references across organizations to improve cybersecurity competencies.
- Enabling organizations to prioritize actions and investments—knowing what to ask—to improve cybersecurity.

Each volume of subpractices builds off the previous area. For example, small healthcare organizations have three related subpractices: email system configuration, education, and phishing simulation. For email system configuration, a small healthcare organization should consider controls to enhance email security, such as avoiding free or "consumer" email systems and ensuring you have basic spam/antivirus installed, active, and automatically updated.

For a medium-sized healthcare organization, the subpractices go into more detail, including basic email protection controls, multifactor authentication for remote email, email encryption, and workforce education.

Large organizations can build on that further by developing email protection systems that use advanced and next-generation tooling, digital signatures, and analytics-driven education. It's recommended that your organization use its risk analysis processes to help identify and prioritize the rollout of these controls.

2023 updates to HICP's recommended practices and subpractices

405(d) HICP recommends 10 best practices your organization can use to mitigate common threats and align them with organization size. These recommendations are not intended to be a list of controls all organizations must implement. Instead, it's a series of recommended practices for risk mitigation techniques.

The 405(d) practices are described in Vol. 1 for small organizations and Vol. 2 for medium and large organizations. Each practice also has subpractices and controls. Medium-sized organizations should start with subpractices for medium-sized organizations. Large organizations should review subpractices for both medium-sized and large organizations.

The HICP 2023 edition includes updates to two of the practices and three new subpractices:

- *Practice #9: Network Connected Medical Device Security*: This section has been fully updated with new subpractices to account for the growing use of connected medical devices.
- *Practice #10: Cybersecurity Oversight and Governance*: This was previously referred to as Cybersecurity Policies but was updated to account for the oversight and governance structures that organizations should have in place as part of their cybersecurity programs.
    - Cybersecurity Insurance is new under Practice #10. With the prevalence of cyberattacks on healthcare organizations, cybersecurity insurance has become an important component of your overall cyber risk management strategy. The HICP guidelines offer information on what your

insurance policies should cover.

    - Cybersecurity Risk Assessment and Management is new under Practice #10. The new HICP edition now includes guidance on performing risk assessments and offers free federal tools you can use to perform them on your own.

- Attack Simulation is new under Practice #7. The guidelines stress the importance of simulating attacks to test your controls and safeguards and outline what to include in your simulations.

While these are the major changes reflected in the 2023 update, other minor changes and updates were made throughout the HICP guidelines, so it's a good idea to read the entire 2023 edition if you are thinking about or have already implemented the 405(d) practices.

The 405(d) HICP 2023 edition also highlights two recommended practices every covered entity and BA should consider as part of their overall cybersecurity strategy:

1. **Zero trust**: Building a zero-trust architecture encompassing multilayer protections strengthens your security posture. This means validating all device and user identities—both internal and external—before granting access to network resources. You can use this approach to mitigate vulnerabilities that network trends create—including bring your own device, cloud-based services, and remote workers. Your organization can enable a zero-trust strategy at all network levels to ensure a strong security posture. Implementing an access and identity management solution and leveraging a least-privilege access process together are good starting points for a zero-trust model.

2. **Defense in depth**: A holistic cybersecurity approach, such as defense-in-depth, can slow attacks and minimize damage. Defense-in-depth layers have multiple security safeguards rather than relying on a single layer. If one layer is inadequate, another layer will hopefully prevent a full breach. This is a best practice strategy you can implement in different ways (for different entity sizes) due to relevance across your entire infrastructure; the 405(d) HICP guide recommends that you include identity and access user controls, perimeter security, network security, patch management, intrusion prevention, and endpoint solutions. These are covered in more detail under their relevant practices in technical Vols. 1 and 2.

Demonstrating adequate protections

To leverage the full advantage of a 405(d) program in your organization, you'll need to have a process for documenting that the HICP guidelines have been implemented and for how long. This is because in the event of an OCR investigation, according to Pub. L. No. 116–321, an organization must demonstrate that they have had recognized cybersecurity best practices in place for no less than 12 months before the point of an incident or investigation. Here are some recommended forms of documentation suggested by HHS:

- A copy of policies and procedures on practice implementation
- Completed project plans or similar documentation showing implementation date(s)
- Documentation of sufficient detail explaining how your organization implemented these practices (including implementation of specific elements or subpractices and scope of implementation throughout your organization)
- Name of individual(s) responsible for implementation
- Training materials provided to your workforce and training dates

- Other documentation for OCR consideration
    - OCR will consider all documentation that adequately demonstrates that the recognized security practices have been in place for at least the previous 12 months

405(d) is not a replacement for risk analysis

405(d) is not a replacement for ensuring the appropriate HIPAA policies and procedures are in place for your organization; rather, for 405(d) success, your risk management strategies should be comprehensive in scope.

All organizations associated with developing the 405(d) program recommend beginning with a risk analysis, the results of which can help you identify and prioritize the rollout of your 405(d) HICP controls.

Takeaways

- 405(d) Health Industry Cybersecurity Practices offer healthcare organizations more specificity around cybersecurity best practices by the organization's size.
- Best practices can be found in technical volumes, and as such, they build on each other.
- 405(d) expanded the email phishing security threat to social engineering in the 2023 edition, accounting for additional tactics used by cyberattackers.
- Zero-trust and defense-in-depth are two strategies every covered entity and business associate should utilize regardless of size.
- The practice and subpractices have been updated to reflect the changing threat landscape and best practices for mitigating risk.

1 U.S. Department of Health and Human Services, "What's New in the HICP 2023 Edition," accessed October 10, 2023, https://405d.hhs.gov/Documents/405d-hicp-highlight.pdf.
2 An act to amend the Health Information Technology for Economic and Clinical Health Act to consider certain recognized security practices of covered entities and business associates when making certain determinations, and for other purposes, Pub. L. No. 116–321, 13412, 134 Stat. 5072 (2021) (codified as 42 U.S.C. § 17931), https://www.govinfo.gov/app/details/PLAW-116publ321.
3 IBM, *Cost of a Data Breach Report 2023*, accessed October 20, 2023, https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700077724064012&p5=e&gclid=CjwKCAjwp8OpBhAFEiwAG7NaEiYtyiG
4 Healthcare & Public Health Sector Coordinating Council, *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*, 2023 Edition, accessed September 25, 2023, https://405d.hhs.gov/Documents/HICP-Main-508.pdf.
5 Healthcare & Public Health Sector Coordinating Council, *Technical Volume 1: Cybersecurity Practices for Small Healthcare Organizations*, 2023 Edition, accessed September 25, 2023, https://405d.hhs.gov/Documents/tech-vol1-508.pdf.
6 Healthcare & Public Health Sector Coordinating Council, *Technical Volume 2: Cybersecurity Practices for Medium and Large Healthcare Organizations*, 2023 Edition, accessed September 25, 2023, https://405d.hhs.gov/Documents/tech-vol2-508.pdf.
7 Healthcare & Public Health Sector Coordinating Council, *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*, 2023 Edition, 29.