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.