COSMOS
Navigate the Compliance Universe

Compliance Today - July 2024

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

HIPAA compliance: It is time for a remodel

By Dawn Morgenstern, CHPC, CCSFP

The foundation

The HIPAA Privacy and Security rules have been in place since 2003 and 2005, respectively. These rules set the foundation and basic structure of our HIPAA programs. For perspective, in 2003, the top movie was *Finding Nemo*, and the latest technology was a Nokia cell phone that could store up to 50 messages and 50 contacts.

The U.S. Department of Health and Human Services Office for Civil Rights (OCR) implemented the Phase 1 Audits (the 2011–2012 Audit Pilot Program) and Phase 2 Audits (the 2016–2017 desktop audits) in accordance with the Health Information Technology for Economic and Clinical Health Act to conduct periodic audits to ensure that covered entities (CEs) and business associates (BAs) subject to the requirements comply with them.

However, not much changed until the January 2013 Omnibus Rule. This finalized the Breach Notification Rule, which expanded individual rights and reasonable disclosures. It also made BAs directly liable for compliance with the Security Rule and certain requirements of the Privacy Rule. We updated our programs and added them to the existing structure.

The building blocks

Today, we face more advanced technology, interoperability, and storage capabilities. To supplement the technology-agnostic requirements of the Security Rule, we have seen continuous improvements by the National Institute of Standards and Technology (NIST), the Healthcare & Public Health Sector Coordinating Council and 405(d) Task Group, and the Office of the National Coordinator for Health Information Technology. Furthermore, we saw the enactment of Public Law 116-321, effective January 5, 2021, "To amend the Health Information Technology for Economic and Clinical Health Act to require the Secretary of Health and Human Services to consider certain recognized security practices of covered entities and business associates when making certain determinations, and for other purposes."[1]

Yet, CEs and BAs continue to struggle with implementing the HIPAA rules, and the threat landscape continues to advance as bad actors find new and different ways to exploit vulnerabilities. In the most recent *Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance* for calendar year 2022, OCR noted they had not initiated any audits in 2022 due to a lack of financial resources.[2] OCR described that "audits are reviews of covered entities and business associates that are initiated not because of any particular event or incident indicating possible noncompliance on the part of the covered entity or business associate, but rather based on the application of a set of objective selection criteria."

Furthermore, OCR noted that there had been significant increases in complaints filed and large breaches reported. OCR identified the need for regulated entities to improve compliance with the HIPAA rules—particularly the Security Rule standards.

The remodel

With this in mind, we should step back and assess our current programs and determine where we need to remodel to bring the programs up to date with the current landscape and standards. Start with what we know and make a plan:

- The audit protocols provide valuable insight into what OCR expects a CE or BA to do. OCR will collect information from "39 online survey questions that will be sent to 207 covered entities and business associates that participated in the 2016–2017 OCR HIPAA Audits."[3] This sets the stage for improving the audit protocols aligned with current trends.
- "NIST Special Publication (SP) 800-66 [R2], aims educate readers about the security standards included in the HIPAA Security Rule and assist regulated entities in their implementation of the Security Rule."[4] The key activities and sample questions for each standard aid a CE or BA in understanding what makes up the interior finishes of our program.
- The 405(d) Health Industry Cybersecurity Practices (HICP) describe controls needed to protect the organization and, most importantly, patient safety. The 405(d) HICP focuses on five current threats: social engineering, ransomware attacks, loss/theft of equipment/data, insider, accidental, or malicious data loss, and attacks against network-connected medical devices.[5]
- The NIST Cybersecurity Framework 2.0 should be "used to address cybersecurity risks alongside other risks of the enterprise, including those that are financial, privacy, supply chain, reputational, technological, and physical in nature."[6]