COSMOS
Navigate the Compliance Universe

Compliance Today - January 2023

Kelly McLendon (kmclendon@complianceprosolutions.com, https://www.linkedin.com/in/kelly-mclendon-rhia-chps-1855686/) is Senior Vice President Compliance and Regulatory Affairs at CompliancePro Solutions, a wholly owned subsidiary of Genzeon LLC, Exton, PA.

Christopher Lyons (bnl41200@yahoo.com, https://www.linkedin.com/in/cmlyons/), CISSP, HCISPP, Director of Cybersecurity at CompliancePro Solutions, a wholly owned subsidiary of Genzeon LLC, Exton, PA.

Reduce OCR enforcement: Get recognized cybersecurity practices in place

By Kelly McLendon, RHIA, CHPS, and Christopher Lyons, CISSP, HCISPP

Cybersecurity has continued to evolve across all public and private sectors that rely on digital personal information. This would typically be patient information in American healthcare under the U.S. Department of Health & Human Services (HHS) purview. HHS has taken a leadership role in coordinating efforts to align industry cybersecurity practices, which will strengthen defenses against ever-increasing (external and internal) cyberattacks. A new amendment to Health Information Technology for Economic and Clinical Health (HITECH) Act provides regulatory enforcement incentives to entities that use (for at least 12 consecutive months) recognized security practices, to be subsequently discussed.[1] These incentives target covered entities and business associates subject to the HIPAA Security Rule. HHS recommends adopting recognized cybersecurity practices that can reduce liability under regulations already in effect—particularly the HIPAA Security Rule—but stop short of being safe harbors or providing formal regulatory relief.

As ransomware and other forms of malware and cyberattacks have increased, there have been several initiatives from the US government and the private sector to combat these trends. Rules have been issued, education content released, reminders circulated, and notices of enforcement for failure to adequately institute protective safeguards ramped up.

Federal agencies such as the Office for Civil Rights (OCR) and the Federal Trade Commission, among many others, have increasingly offered content such as educational materials while at the same time pressing enforcement actions meant to show that the regulators are serious about compliance with their rules. These actions use regulatory enforcement as incentives to tighten IT security to better arm these businesses to fight what has become, in essence, cyberwarfare between many bad actors, including those that are state-sponsored or protected and the vast numbers of healthcare providers, payers, exchanges, and networks. Added to those issues is the problem of insiders within the systems with protected or sensitive information who are malicious in intent.

405(d) and health industry cybersecurity practices (HICP) provide useful tools for cybersecurity programs

Across the world, bad actors (external and internal) are regularly identifying new and unique methods to probe for vulnerabilities in networks and applications to identify weak spots or flaws to access confidential data, trade secrets, or conduct other nefarious activities. Their efforts yield a constant barrage against entire systems and networks, looking for weaknesses they may exploit. The methods used are continuously adapting to meet new security controls implemented by businesses.

While the methods evolve, many of the exploits have stayed the same—either with some changes or sometimes without the need to change. Methods such as social engineering are not new; however, they are still exploitable as many companies still need to employ the systems or methods identified to eliminate these older methods. Ransomware and phishing are two of the most common forms of attack today. Efforts such as the HICP-recommended cybersecurity practices can help to expand and standardize what practices and controls should be considered by any organization for cyberdefense.

According to the HHS "Fact Sheet: Cybersecurity Act of 2015, Section 405(d)," "in 2017 HHS convened the 405(d) Task Group leveraging the Healthcare and Public Health (HPH) Sector Critical Infrastructure Security and Resilience Public-Private Partnership. The Task Group is comprised of a diverse set of over 150 members representing many areas and roles, including cybersecurity, privacy, healthcare practitioners, Health IT organizations, and other subject matter experts."[2]

The 405(d) Task Force executed its mission by examining existing US cybersecurity safeguards, protections, controls, and practices, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). However, in a somewhat simplified form and with an added dimension, they tailored the controls and practices into three versions based on organizational size (small, medium, or large), providing a sample definition of each. This new framework will greatly help companies of all sizes apply industry-accepted practices using a well-established CSF such as the NIST CSF within their environment, regardless of size or complexity.

The 405(d) Task Group agreed on developing HICP components: a main document, two technical volumes based on organizational size, and a robust appendix of resources and templates:[3]

- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)
- Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations
- Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations
- Resources and Templates
- Cybersecurity Practices Assessments Toolkit (Appendix E-1)

With these published tools, including end-user training content, a physician's practice can clearly see which cybersecurity controls and practices should or could be used for their small-sized business and use coordinated content to train its workforce. The same is true for a middle-sized network of offices or clinics as well as larger entities such as hospitals. Other entities, such as payers and business associate vendors, can also choose size based on their own interpretation of the intent of the practices.