Compliance Today - May 2019

Federally Qualified Health Center: Improve cybersecurity with a hiccup!

by Rich Curtiss, CISSP, ITIL

Rich Curtiss (rich.curtiss@coalfire.com) is a Principal, Healthcare Risk Assurance Services, at Coalfire in Alpharetta, GA.

Last December, the Department of Health and Human Services (HHS) released the publication "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients" (HICP).[1] Lightheartedly, the HICP is referred to as the "hiccup" (the federal government is fond of converting abbreviations and acronyms into pronounceable names). The HICP is designed to help healthcare organizations of all sizes identify threats and potential mitigation strategies and provide healthcare-specific cybersecurity best practices. So, what relevance does this have for a Federally Qualified Health Center (FQHC)? HHS describes the significance of this publication and effort as follows:

> The industry-led effort was in response to a mandate set forth by the Cybersecurity Act of 2015 Section 405(d), to develop practical cybersecurity guidelines to cost-effectively reduce cybersecurity risks for the healthcare industry. The publication marks the culmination of a two-year effort that brought together over 150 cybersecurity and healthcare experts from industry and the government under the Healthcare and Public Health (HPH) Sector Critical Infrastructure Security and Resilience Public-Private Partnership. It was the result of a true public-private partnership to better secure the nation's health systems.[2]

How HICP can support HIPAA security

An FQHC is a community-based healthcare provider that receives funds from the Health Resources Services Administration (HRSA) Health Center Program to provide primary care services in underserved areas. An FQHC must meet a stringent set of requirements, including providing care on a sliding-fee scale based on ability to pay, and operate under a governing board that includes patients.

An FQHC is considered a covered entity (CE) according to the Health Insurance Portability and Accountability Act (HIPAA) and, therefore, must meet all the same compliance requirements as a commercial for-profit or nonprofit CE. To that end, an FQHC must be fully compliant with the HIPAA Privacy, Breach Notification, and Security Rules as defined in the Code of Federal Regulation (CFR).[3]

Most FQHC organizations operate on thin budgets and have to make difficult decisions regarding annual operating expenses and capital expenditures. One of the programs competing for budget is HIPAA. The HICP is intentionally segmented for small, medium, and large organizations to accommodate a "reasonable and appropriate" implementation of a security program. This ensures HIPAA security budgets and resources are suitably scoped.

HICP is a compendium of four publications. The primary document explores five current threats and presents ten practices to mitigate the identified threats. Technical Volume 1 discusses the ten cybersecurity practices accompanied by sub-practices for small healthcare organizations.[4] Technical Volume 2 discusses the ten cybersecurity practices accompanied by sub-practices for medium and large healthcare organizations.[5] The resources and templates portions include a variety of cybersecurity resources and templates for end-user reference.

It is clear that the vast majority of FQHCs are aligned with Technical Volume 1: Cybersecurity Practices for Small Organizations. This document is similar in construct to the other technical volumes but differentiates the small organization as follows:

> Small health care organizations tend to have limited resources for managing their cybersecurity practices, but they are no less subject to cyberattacks. Indeed, the five threats identified in the Main Document can be very disruptive to small organizations. For example, if a small provider practice loses a laptop with unencrypted personal health information (PHI), a publicized breach could result. Such a breach could have consequences for both the provider's patients and the practice's reputation. (emphasis added)

This differentiation is important for the FQHC, because the methods to address the ten cybersecurity practices and five threat scenarios may differ significantly for a small, resource-constrained healthcare provider. The practices and threats are listed in the tables below.

Cybersecurity Practice	
Email Protection Systems	Configuration, education, and phishing simulation
Endpoint Protection Systems	Basic endpoint protection
Access Management	Basic access management
Data Protection and Loss Prevention	Policy, procedures, and education
Asset Management	Inventory, procurement, and decommissioning
Network Management	Segmentation, physical security, guest access, and intrusion prevention
Vulnerability Management	Vulnerability management
Incident Response	Incident response and ISAC/ISAO participation
Medical Device Security	Medical device security
Cybersecurity Policies	Policies

Table 1: Cybersecurity Practices and Sub-Practices for Small Organizations

Cybersecurity Practice Threat Scenarios	
Email phishing attack	Malware delivery or credential attacks. Both attacks further compromise the organization.
Ransomware attack	Assets locked and held for monetary ransom (extortion). May result in the permanent loss of patient records.
Loss or theft of equipment or data	Breach of sensitive information. May lead to patient identity theft.
Accidental or intentional data loss	Removal of data from the organization (intentionally or unintentionally). May lead to a breach of sensitive information.
Attacks against connected medical devices that may affect patient safety	Undermined threats to patient safety, treatment, and well-being.

Table 2: Five Prevailing Cybersecurity Threats to HealthCare Organizations

This document is only available to members. Please log in or become a member.

Become a Member Login