Report on Medicare Compliance Volume 27, Number 24. July 02, 2018
Inertia Is a Risk With Myriad Security Resources; Overlap May Help

By Nina Youngstrom

It's somewhat of a contradiction: Hospitals often fall short on security risk assessments, but there's an overabundance of resources on how to conduct them. It's perhaps causing analysis paralysis, even though they are required to perform risk assessments under the HIPAA security regulation, a security expert says.

"In health care, the main thing you must do is adhere to HIPAA, but most of us who have been doing this for a while recognize it's a bit long in the tooth," says Barry Mathis, a principal in PYA. While people who work on preventing breaches and cyberattacks rely on other sources for guidance, there are now so many, including the Health Information Trust Alliance (HITRUST), which created a common security framework (CFS); the National Health Information Sharing and Analysis Center (NH-ISAC); the National Institute of Standards and Technology (NIST SP 800-30); the SANS Institute's Top 20; American Institute of Certified Public Accountants' System and Organization Controls (SOC) for cybersecurity; and The Healthcare Cybersecurity Communications Integration Center . It's possible to get overwhelmed, Mathis says.

Brief Description of Some Major Security Frameworks

More than enough resources are out there to help hospitals with cybersecurity, says Barry Mathis, a principal in PYA. Here's a summary of some. Contact Sully Baker at sbaker@pyapc.com *and Mathis at* bmathis@pyapc.com*.*

Title	Owner/Licensor	Framework	Purpose	Details

Title	Owner/Licensor	Framework	Purpose	Details
HIPAA	US Code of Federal Regulations §164.308, §164.310, §164.312	Compliance guideline with three safeguards: Physical, Technical, Administrative. Each safeguard includes multiple criteria, some being required, while others are only addressable (must have valid business reason not to implement control).	Designed for a large range of covered entities and business associates. Include the requirements, processes and procedures, and Protected Health Information (PHI) documentation requirements. Designed to require less resources and time to implement, while maintaining a satisfactory measure of safety.	

Title	Owner/Licensor	Framework	Purpose	Details
HITRUST	HITRUST Alliance	A single all-encompassing audit based off of **Regulatory** (state, federal, domain specific) requirements; **Organization** (geographic factors, amount of covered lives); **System** (data stores, external connections, number of users/transactions).	Scales according to the type, size and complexity of organization and systems. There are **14** control categories, **45** control objectives and **149** control specifications. At least 64 control specifications must be in place to become certified. Includes HIPAA rule, with COBIT, NIST and several other IT security compliance guidelines.	A prescriptive audit including 14 control categories: Information Security Management, Access Control, Human Resources Security, Risk Management, Security Policy, Organization of Information Security, Compliance, Asset Management, Physical and Environmental Security, Communications and Operations Management, Information Systems Acq. Dev. & Maintenance, Information Security Incident Management, Business Continuity Management and Privacy Practices.

Title	Owner/Licensor	Framework	Purpose	Details
NIST	US Department of Commerce	Framework has three parts: Core (activities, outcomes, references and approaches to cyber security); Profile (two-tier approach to explaining the objectives and outcomes "as is," with a target profile of objectives and outcomes "to be"; Tiers (Clarifies an organization's view on cyber security risk and the sophistication of management)	Made publically available to the private sector in April 2018. Based off of a variety of other standards (COBIT, CCSS CSC, etc.) which assist in the understanding and management to reduce cyber security risks. Assesses businesses to utilize cost-effectiveness for maximizing IT security expenditures.	

Title	Owner/Licensor	Framework	Purpose	Details
American Institute of Certified Public Accountants (AICPA) SOC CS	AICPA	Performed by a CPA. Two aspects of the exam: Description of the Cyber Security Risk Management (CSRM) program; Effectiveness of security controls to achieve objectives.	Has been referred to as the GAAP of cyber security. Based on other frameworks (NIST, ISO 27001). Output of the exam are provided with three key components: Description of the CSRM; Management's Assertion; Practitioner's Report.	1. Description of CSRM: Description designed to provide about how entity defines its information assets, how they manage threats and P&P's implemented and operated to protect that info. A 'description criteria' is used to prepare and evaluate the CSRM program. 2. Management's Assertion: This addresses a) description is in-line with the description criteria, b) the controls that achieved objectives were set forth in 'control criteria,' created by AICPA like the 'description criteria.' 3. Practitioner's Report: An opinion-based report to determine a) the description is presented in line with the description criteria and b) controls within the entity's CSRM were effective to achieve the objectives based on the control criteria.
SANS Top 20	SANS Institute	Over the years, SANS Tops 20 has evolved into the list of critical security controls recommended by the Council on Cyber Security (CCS).	Provides a list of key actions an organization should take to block or mitigate cyber security risks. Every release of lists provides an updated version that alters or adds the previous controls.	

"There are almost too many sheriffs in town," he says. "It's confusing." Inertia could set in because of the information deluge with so many "frameworks." That would be self-defeating, however, Mathis says. "You can throw a rock and hit any of these and it would be better than doing nothing," he says. "Get off the couch and do something."

Hospitals want to know which resources they should use to help prevent a breach and, if a breach occurs, how they can show the government they did their best to prevent or manage it. They will have a better idea of which framework to use if they complete a security risk assessment, he says. It's also useful to let go of the idea of risk assessments as a one-and-done obligation. "It's no longer about the assessment or the audit. It's about a program—managing it end to end, knowing you may pull different pieces" from various frameworks. That will serve organizations well if a breach is investigated by the HHS Office for Civil Rights. "They want to see how the sausage is made," Mathis explains.

All the frameworks are very good, Mathis says. Which you use depends on what surfaces in the risk analysis. "You don't want to ignore HHS or commercialized frameworks," he says. "You can crosswalk them, depending on what kind of complexity your organization has." For example, a critical access hospital may take HIPAA's security standards and crosswalk them with the SANS Top 20. "That may be enough, but you won't know until you complete your risk assessment." Mathis thinks the SANS Top 20 covers a lot of ground. "It matches everything HIPAA has except breach notification," he says.

Or your security risk assessment may meet all the standards for HIPAA, but you might want to make additional moves to comply with the NIST version of CFS and SANS. "When you put all three together, there are not a lot of steps. They're all the same, but restated in different vernacular," Mathis says.

For example, audit controls are addressed by SANS CSC 6, HITRUST 06.i, HIPAA and NIST SP 800-53 AU-1, he says. CSC 6 is the maintenance, monitoring, and analysis of audit logs. HITRUST 06.i pertains to Information Systems Audit Controls. HIPAA (45 C.F.R. Sec. 164.312(b)) requires organizations to implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. NIST SP 800-53 AU-1 suggests that an organization develop, document, and disseminate to workforce members an audit and accountability policy on the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, as well as procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. "All of these frameworks are addressing audit controls," Mathis says. "You could be compliant in this area for all four frameworks by completing minimal steps during one assessment."

Contact Mathis at bmathis@pyapc.com.