Codify
BY AAPC

Health Information Compliance Alert

Mythbusters: Dispel These 5 Common HIPAA Security Myths

Tip: Analyze your risks or pay the price.

As more and more data security incidents occur, it's clear that HIPAA Security Rule woes are on the rise. And while many covered entities (CEs) find it easy to keep their organizations in line with Privacy Rule protocols, they fail to implement and follow up on the guard rails that protect against Security Rule violations.

Reasoning: If you utilize any kind of health IT to access and disclose patients' electronic protected health information (ePHI), then you must abide by HIPAA Security Rule standards. This often requires that you vigilantly investigate problems, sometimes daily, and keep your compliance in check with audits and analysis - as well as keep on top of the compliance of your IT vendors and business associates (BAs).

As you wade through the HIPAA Security Rule minutiae, don't let these popular myths - identified by the **Office of the National Coordinator for Health Information Technology** (ONC) - bog you down.

1. Small Providers Don't Get Risk Analyses' Reprieves

Myth: I'm a small, rural provider, and only large organizations are required to perform a comprehensive risk analysis.

Reality: All providers who qualify as CEs under HIPAA must perform a risk analysis. "Many physicians don't understand that this is the first element in HIPAA security," says attorney **Abby Pendleton**, of **The Health Law Partners, PC**, in Farmington Hills, Michigan. "This type of risk analysis is the starting point to find potential vulnerabilities and then put into place the appropriate safeguards. It is the stepping stone to implement HIPAA, but not enough practitioners do it."

Incentives: In addition, providers who rely on EHR incentive payments under the **Centers for Medicare & Medicaid Services** (CMS) Promoting Interoperability (PI) programs must conduct one. "In 2019, the Security Risk Analysis measure will remain a requirement of the Medicare Promoting Interoperability Program as it is imperative in ensuring the safe delivery of patient health data," reminds CMS.

Tip: You may want to back up your risk analysis with documentation that includes your plans for addressing risks and fixing issues. Why? It's the first thing the **HHS Office for Civil Rights** (OCR) will ask for if you have a HIPAA data breach. Plus, the PI Security Assessment is the most audited Merit-Based Incentive Payment Systems (MIPS) measure, warns **Cherie Kelly-Aduli**, CEO of **QPP Consulting Group** in Mandeville, Louisiana and a **MedAxiom** consultant, in a MedAxiom blog post.

2. Use of CEHRT Does Not Translate to Compliance

Myth: As long as I'm using some kind of Certified EHR Technology (CEHRT), my practice remains compliant.

Reality: "Even with a certified EHR, you must perform a full security risk analysis," reminds the ONC. "Security requirements address all electronic protected health information you maintain, not just what is in your EHR."

Advice: It's not only important that you do a risk analysis, but it's also critical that you update your EHR if you want to keep those federal incentives coming. In a nutshell, MIPS eligible clinicians (ECs) as well as Medicare-eligible hospitals, dual-eligible hospitals, and critical access hospitals (CAHs) are required to use 2015 Edition CEHRT in 2019 attestations and PI submissions.

3. It's Not Your Vendors Responsibility to Keep You Compliant

Myth: My EHR vendor is in charge of my HIPAA security compliance.

Reality: Unfortunately, you cannot buy HIPAA compliance. If a third-party vendor says its encryption product is "HIPAA compliant," that company is simply telling you that the product fulfills the HIPAA encryption guidelines for stored data and data over networks.

Just because an encryption product meets HIPAA's data encryption guidelines does not mean that you're ultimately complying with the HIPAA Security Rule simply by using the product. In terms of encryption, the Security Rule standard states that you must "implement a mechanism to encrypt and decrypt electronic protected health information."

What to do: This standard is "addressable," meaning that you must carefully analyze your organization's operations to determine what type of encryption product is "reasonable and appropriate" for your business. You must base your analysis on a variety of factors related to your organization, such as:

- Your organization's size, complexity and capabilities;
- Your organization's technical infrastructure, hardware and software security capabilities;
- The costs of encryption measures; and
- The probability and criticality of potential risks to ePHI.

4. Don't Drop the HIPAA Compliance Ball

Myth: We managed our security risks last year after our analysis; we're good now.

Reality: Whether you get your Security Rule facts from the federal mandates or your IT staff, you should know that HIPAA security is ongoing with daily monitoring, weekly check-ins, monthly audits, and yearly assessments.

"The risk analysis process should be ongoing," explains OCR guidance. "In order for an entity to update and document its security measures 'as needed,' which the Rule requires, it should conduct continuous risk analysis to identify when updates are needed."

Remember: How often you assess the security of ePHI in your organization depends on the size and scope of your firm, taking into account past breaches, incident response, and how quickly threats are realized and managed. "A truly integrated risk analysis and management process is performed as new technologies and business operations are planned, thus reducing the effort required to address risks identified after implementation," OCR maintains.

5. HIPAA Security Rule Compliance Is Worth Every Penny

Myth: Why should I put money aside for HIPAA security? As a small provider, my chances of a data breach are non-existent.

Reality: "For the ninth year in a row, healthcare organizations had the highest costs associated with data breaches at $6.45 million - over 60 percent more than the global average of all industries," cautions **IBM** and the **Ponemon Institute** in its 2019 Cost of a Data Breach Report.

Oftentimes, small businesses are the hardest hit because they don't allocate funds to manage their data security risks upfront, and the price to recover from incidents can be crippling, suggests the report. That's why it's important for organizations, big and small, to invest in security planning and use the information they get from assessing their risks to protect patients' ePHI as well as their bottom lines.

"Healthcare has traditionally been less sophisticated when it comes to information security ... [but] now is the time to get serious about protecting systems, because lives and institutions are at stake," notes HIPAA expert **Jim Sheldon-Dean**, founder and director of compliance services at **Lewis Creek Systems LLC** in Charlotte, Vermont.

Resource: Review the OCR's guidance on the HIPAA Security Rule at www.hhs.gov/hipaa/for-professionals/security/index.html?language=es.

Codify
BY AAPC