Why the HIPAA Security Rule Needs a Refresh

Outdated technical terms and some vague definitions and procedures must be amended to address a threat-heavy landscape.

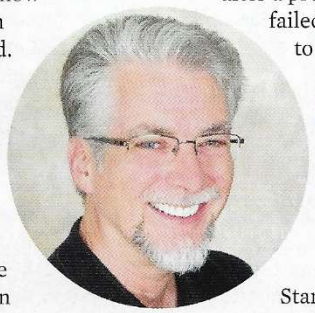
When the HIPAA Security Rule was first proposed in 1998, internet speeds would have been considered lethargic by today's standards — and medical records were in paper format.

A lot has changed in the decades since, except for the Security Rule.

Finalized in 2003, the rule establishes national standards for administrative, physical and technical safeguards that ensure the confidentiality and safety of electronic protected health information.

But I'm surprised to find that many people who talk about HIPAA compliance have never read the rule. Otherwise, they would know that a number of modern concerns go unaddressed.

Key words such as cyberattack, email, ransomware, phishing, smartphones, texting and virtual assistant do not appear. Other terms are vague or have dual meaning, raising the odds of misinterpretation or accidental noncompliance.



OUT WITH THE OLD

As healthcare cyberthreats grow in number and severity, it's time to update the HIPAA Security Rule to recognize modern technology and best practices.

Several implementation specifications are outdated and should be removed from the rule. For example, requiring login monitoring made sense in the 1990s when systems ran on mainframes, but it makes no sense in a client-server environment.

Another is mandating integrity controls under the rule's standard for transmission security. In the era of modems and phone line transmission, data errors could occur. Today's transmission protocols are reliable; most are sent using some form of encryption.

Although encryption is an "addressable" implementation specification in the current rule, it needs to be a requirement, with exceptions properly managed via compensating controls.

MORE CLARITY NEEDED

Additionally, the rule must address modern-day tools and security issues, such as requiring user account lockout after a predetermined number of failed login attempts. According to the National Institute of Standards and Technology, this is the top security control to prevent hacking.

> "I'm surprised to find that many people who talk about HIPAA compliance have never read the rule."

The HIPAA Security Rule is also missing some key definitions that should be added or clarified. These include:

- **Risk analysis:** Many interpreted this to mean an assessment of compliance. (Adding to the confusion, NIST uses "risk assessment" interchangeably with risk analysis.) The definition should recommend a frequency for conducting analyses on all applications and systems storing PHI.
- **Policies:** For most, this word means a document that defines management's expectations. To IT folks, "policies" can refer to technical settings or controls. Active Directory or enforced workstation settings are policies.
- **Incidents:** Back in 1998, having your network "pinged" was a reportable incident. Today, we're constantly pinged. The industry needs realistic benchmarks of when ransomware or phishing are reportable breaches.
- **Executive accountability:** By approving budgets, executives can determine how much money will be allocated to information security, and they should be held accountable for the results.

FOCUS AND VIGILANCE

Compliance, as leaders know, is attained through the implementation of robust procedures and plans. But I'm not aware of any hacker who has been thwarted by a set of compliance documents.

This is why a focus must be placed on technical controls to prevent or detect hacking and malicious code, rather than administrative policies that divert resources from real security. ■

TOM WALSH is a nationally recognized speaker and a co-author of four books on healthcare information security. He has nearly 30 years of industry experience.

Hiring an ethical hacker can help detect vulnerabilities in your organization. Learn about penetration testing at **healthtechmagazine.net/PenTesting**.