COSMOS
Navigate the Compliance Universe

Compliance Today - November 2020
HIPAA at home: Remote workers and the Security Rule

By Nick Weil, JD, LLM, CHPC, CHC

Nick Weil (nick.weil@ankura.com) is Director, Data Privacy and Compliance, at Ankura Consulting, living in Omaha, NE.

- linkedin.com/in/nick-weil-0a004649/

As the COVID-19 pandemic continues throughout the country and the world, most employers have elected (or been directed) to send nonessential personnel home to work remotely. With the high uncertainty about when a vaccine will be available and how effective it will be,[1] it is safe to say remote work will be a short- to medium-term reality at least. It may also be a long-term reality; public health necessity could accelerate a preexisting trend toward telecommuting across all industries and all sectors. For months and years to come, compliance professionals should be prepared to answer questions and develop protocols for complying with the Health Insurance Portability and Accountability Act (HIPAA)[2] at home.

For HIPAA-covered entities, much of the workforce is clinical and patient-facing, and so remote work from home is not available in any circumstance. But many health systems have sent nonessential staff to home offices—from personnel managers to case managers, compliance officers to coders. For business associates not directly serving patients or providing an essential service, many staff are now remote. Despite some HIPAA waivers being issued due to the pandemic, both covered entities and business associates are still expected to comply with the Security Rule. With many homes now hosting spouses and children during work hours, it is a good time to review some of the HIPAA requirements for a secure workspace.

This article will focus on the HIPAA Security Rule's provisions for the protection of electronic protected health information (ePHI) and consider how they should be reviewed and implemented in light of shelter-in-place and remote situations. We will also look briefly at the HIPAA Privacy Rule and consider some practical takeaways for privacy officers and compliance professionals.

The Security Rule

Of the three rules promulgated in the wake of HIPAA (Privacy, Security, and Breach Notification), the Security Rule is perhaps the one most often overlooked by compliance professionals. For one thing, it is the most technical—though, as we will see, the rule tries to avoid being too technical in order to prevent rigid technical requirements that are not scalable to different types of healthcare entities or elastic enough for the ever-accelerating pace of technical progress. It is for these reasons that it is also the least clear of the three rules; one of its first headings is titled "Flexibility of Approach,"[3] which is a good summary for the whole rule itself. The rule reads:

> In deciding which security measures to use, a covered entity or business associate must take into account the following factors:
>
> i. The size, complexity, and capabilities of the covered entity or business

associate.

ii. The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.

iii. The costs of security measures.

iv. The probability and criticality of potential risks to electronic protected health information.[4]

We will come back to this framework further in the article. For now, suffice it to say that this flexibility matrix built into the Security Rule offers both an opportunity and a challenge for compliance professionals trying to determine how and to what extent remote healthcare workers should be using and securing ePHI at home. It is an opportunity because baked into the rule is the language of recommendation rather than requirement. But this presents a challenge, too, because unclear requirements make for unclear compliance. How do you know you are in compliance with the Security Rule if the rules are not black and white? We will spend our time in this article addressing that question.

Addressable vs. required

One of the most unique parts of the Security Rule is the "addressable" or "required" labels that can be found throughout.[5] The rule as a whole is a series of standards, each structured in parts based on whether it is an administrative, technical, or physical safeguard for ePHI. Under most of these standards are "implementation specifications." Each implementation specification is labeled addressable or required.[6]

Those implementation specifications marked required are self-explanatory, but the addressable provisions require more unpacking. They should *not* be read as merely optional or recommended. Fundamentally, they are, but if an entity chooses not to follow an addressable implementation specification, analysis and documentation must accompany that decision. For every addressable implementation specification in the Security Rule, covered entities and business associates should:

i. Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and

ii. As applicable to the covered entity or business associate -

   a. Implement the implementation specification if reasonable and appropriate; or

   b. If implementing the implementation specification is not reasonable and appropriate -

1. Document why it would not be reasonable and appropriate to implement the implementation specification; and

2. Implement an equivalent alternative measure if reasonable and appropriate.[7]

According to the rule, (1) assessment, (2) documentation, and (3) alternatives are needed if any addressable provision is set aside. But as this article will show, that is sometimes easier said than done.