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.

Encryption at rest

An infamous example of an addressable label is the access control standard and encryption implementation specification. Under the rule, access to ePHI must be controlled (the standard) through encryption and decryption protocols (the implementation specification).[8] This implementation specification is an addressable one. A reader could not be faulted for concluding that the federal government is here *recommending* that devices containing ePHI should be encrypted.

However, as many compliance professionals know, this is not how the standard has been enforced by regulatory authorities. Over the last decade, when the Office for Civil Rights (OCR) and the U.S. Department of Health & Human Services investigate a reported breach, an unencrypted device containing ePHI is considered a serious violation. The newsroom at the OCR website is littered with reports of health systems, hospitals, and physician groups that took the encryption provision as optional and were punished with heavy fines,[9] strict corrective action plans,[10] and enforcement settlements because an unsecured device was lost by the HIPAA-covered entity.

For compliance professionals reviewing remote work plans and arrangements, it is imperative that every device that leaves the facility and stores ePHI be encrypted. From a practical standpoint, that means electronic medical records and other systems containing ePHI should only be accessible by a company-maintained device or available through a portal that prevents downloading (more on this later). It goes without saying that devices that leave the facility or campus are much more likely to be lost or stolen. Information technology (IT) should be queried to ensure that all laptops, mobile phones, flash drives, and external hard drives contain password-protected, industry-level encryption and that ePHI systems are not accessible from noncompany assets. Audit several company devices in your possession or available to you to check whether they do in fact have secure hard drives.

Because of the enforcement history around this implementation specification, it is not advisable to treat this addressable provision as optional or scalable, even though the rule calls for the flexibility-of-approach matrix. That being said, the rule does technically allow for documentation and alternatives in the event that an addressable provision is not “reasonable and appropriate.”[11] If it is not possible for your organization to deploy encryption to all devices that are being sent to employees’ homes—given the need for haste in, say, a public health crisis, this may very well be the case—those reasons should be thoroughly documented, as well as alternative measures. Post-crisis mediation should be baked into the plan and the documentation.

Encryption in flight

The previous addressable measure applies to data at rest. But data moving between devices or systems are also vulnerable. The transmission security standard of the rule requires that technical security measures that protect data sent or received within and over electronic communications network be implemented.[12] Like the access control standard, this standard includes an implementation specification for encryption that is addressable. Unlike the access control standard, it does not have the history of enforcement that makes it a de facto requirement.

The typical way that covered entities secure networks and transmission for remote workers is through secure portals or virtual private networks (VPNs). They enable an employee to use any Wi-Fi (public or private) to connect to a network containing sensitive information through a secured connection. However, secure portals and VPNs can be expensive, the number of licenses limited, and they might require preinstallation by an IT specialist or remote access to a company device. They are also unreliable in the sense that they depend on the employee enabling them in order for them to be active.

If these measures are not reasonable and appropriate given the public health crisis, training and direction to remote employees can provide some transmission security. Without a VPN or secure portal, employees should never access patient information over a public network, like in a coffee shop. This would include emails and documents that might contain ePHI, as well as any electronic medical record systems. But in this time of social distancing, many workers will likely be on their home Wi-Fi anyway. Home Wi-Fi networks and routers can be reasonably secured and encrypted with some simple steps.

Home networks are less likely to be the subject of a local attack quite simply because the attacker has to be within range of the network to take advantage of many vulnerabilities. But the reality of apartment complexes or shared living spaces means that many strangers could have access to an employee's home network without employee's realizing it. Luckily, many common vulnerabilities can be patched by the remote employee. Below is a sample communication that contains these security steps:

> Dear remote staff:
>
> Help us secure patient information by making sure your home internet network is safe from intrusion. By following the steps below, you will greatly improve the security of your internet connection while you work from home. These steps will also make your own personal and family use of your internet connection more secure:
>
> - Confirm encryption is enabled on your home Wi-Fi network.
> - Look under your Wi-Fi properties through your computer's connection. Under "Security type," look to see if "WPA" or "WPA2" is listed.
> - If there is nothing, or some other protocol is enabled, check if it can be enabled through your router. If not, reach out to IT.
> - Change the default router login information (username and password).
> - Turn on the router's built-in firewall, if available.
> - Change the default Wi-Fi login information (username and password).
>
> Information about how to change these settings can typically be found on the back or bottom of your Wi-Fi device or router. You can also check the user manual. A webpage link and default admin login information that you can use to take the security measures above will be provided. If you cannot locate these, your internet service provider may also be able to help. For more information about how to implement these critical security measures, please contact your manager or the IT department.

Of course, one email notice to employees is not enough to achieve any type of compliance. Your standard compliance best practices should be deployed here to ensure employees are following the rules. For example, managers over remote workers should be recruited to help train staff and confirm they are implementing these measures. Compliance or IT staff can assist in spot-auditing employee networks to see if they are in fact encrypted. Many privacy departments do privacy walk-throughs to check whether clinical areas are secure and operating within privacy policies. Deploy a similar protocol for remote workers: virtual privacy walk-throughs. Finally, a work-from-home agreement that lays out these and other security requirements and expectations should be created and signed by all employees.

These practices should be started even if VPNs or secure portals are available. A VPN is only useful when it is actually being used, so take steps to retrain and remind staff about their availability, as well as other security features and rules.

This is an addressable provision, so the compliance department should thoroughly document the reasons and efforts of this approach. Be prepared to justify why you could not implement a company-sponsored transmission encryption protocol or technology if necessary. Cost of implementation, speed during a crisis, temporary nature of remote work, and alternative measures should all be documented. This documentation should be available if a breach occurs or if a regulatory agency investigates.

Workstation use and security

The final set of security standards we will look at applies to workstations that can access ePHI. The workstation standards under the Security Rule—“Workstation Use” and “Workstation Security”—are below:

> Standard: Workstation use. Implement policies and procedures that specify...the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.[13]
>
> Standard: Workstation security. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.[14]

Because these are standards and, unlike the first two standards considered here, do not have implementation specifications, compliance professionals should apply the flexibility-of-approach matrix discussed at the beginning of the article to comply with them. Using that framework can help implement a compliant approach that is tailored to your organization.

As a practical matter, this standard presents challenges for remote workers. The physical impediments that exist in hospitals, medical offices, and office buildings (e.g., locked doors, employee-only areas and entrances, nursing station walls) cannot be easily implemented or required in a home and would not be very effective against an employee’s family in any case. An enterprising toddler can make short work of any physical barriers, and limited space available to employees at home may not facilitate separable workspaces.

Often, covered entities or business associates respond to these standards by placing strict requirements on employees working from home, like mandating that they operate only behind locked doors in separate rooms from any family members. Though this policy would certainly meet the standards, it is not always possible for employees to do so depending on their living situation (e.g., in small apartments or in a time when many children are at home and need some level of supervision). In an age where a lot more employees are working from home than before, covered entities and business associates need to be more cognizant of these realities.

Note that the workstation standards only require that workstations be *specified* by the entity and the physical safeguards be implemented. The details are left to the entity. Keep in mind also that an *unrealistic* mandate quickly becomes an *ignored* policy, which itself becomes a compliance risk. It is prudent in these situations to come up with manageable expectations, for two main reasons: (1) to avoid causing undue anxiety during an already anxious time, and (2) to refrain from imposing unnecessary obligations that the OCR might hold against the organization when determining whether it is following its own privacy policies. The more appropriate approach is to examine the standard and apply a framework for both determining the best ways to implement that standard and document why it was the best way forward for your organization.

Home workstations

Under the flexibility matrix discussed at the beginning of the article, covered entities and business associates must evaluate four factors:

1. Size and complexity of their organization,
2. Their technical security capabilities,
3. The costs, and
4. The probability of risk to ePHI.

As we saw above, the workstation standards require (1) policies and procedures specifying the physical environments used to access ePHI and (2) that physical safeguards be implemented to prevent unauthorized access to that ePHI.

While applying the flexibility matrix to work-from-home practices, several important observations can be made. First, the probability of risk to ePHI, from a physical intrusion standpoint, is low. Hospitals are high-traffic areas, where hundreds of different people a day might have access to workstations with little to no supervision. Physical barriers are necessary to protect privacy and security. But homes have far less foot traffic; the same half a dozen people have regular access to a home, and any stranger is going to be recognized as out of place. We can conclude that the fourth factor in the flexibility approach is low.

This observation can be combined with the second factor, which allows that where technical security measures protect the data, redundant physical measures are not always necessary. Again, for public businesses, multiple layers of security are necessary. But when devices are password protected and encrypted, the risk of ePHI loss is far lower when working remotely. Bearing these two factors in mind, compliance professionals can make more targeted recommendations when considering the workstation standards for their organization.

One option is to update or create the aforementioned work-from-home agreement; including a section describing the physical environment is a good place to start. The security provisions recommended in earlier sections of this article could also be included, such as encrypting all ePHI devices, restricting access to noncompany devices, employee directives on encrypting and securing of home networks, and the prohibition of using public Wi-Fi networks to access ePHI, unless some other security technology is in place. Under a "home workstation" section, the organization should describe what it requires of remote employees. For example, laptop or computer screens should be faced away from any nonemployee when in use, and when not in use, devices must remain locked and passwords not shared. Live discussions involving protected health information, whether with patients or other staff, must occur in a setting as private as possible, behind a closed door or another room of the house. Combine this with technical measures that automatically lock devices after a few minutes of inactivity, and these practices can be sufficient to meet the workstation standards, ensure security of ePHI use in the home, and relieve employees from unnecessary burdens while working remotely.

Incidental disclosures in the home

Let’s conclude with a brief note on the incidental use and disclosure provision in the HIPAA Privacy Rule and how it can be applied to remote workers accessing ePHI. The incidental disclosure rule is a slippery principle,[15] but the OCR has published a helpful guide to it that provides a good summary of the standard.[16]

The best example of an incidental disclosure occurs in every waiting room of a doctor’s office. Certain information cannot help but be overheard when a patient is checking in for an appointment. The rule acknowledges these realities and permits these disclosures when certain safeguards are in place. For example, treatment should be reserved for patient rooms, and staff should keep voices down where possible to prevent additional privacy disclosures.

As waiting rooms empty to prevent the spread of the coronavirus, email, phone, and the home office have become the virtual waiting rooms of the healthcare system. A spouse who inadvertently sees a laptop screen when they bring coffee to their partner as they process hospital bills from the kitchen table is an incidental disclosure. A toddler crawling on their mother’s lap while she exchanges emails with her nursing staff from the couch is an incidental disclosure. A physician conducting a televisit with a patient being overheard faintly through home walls by the family watching TV is an incidental disclosure.

The HIPAA Security and Privacy rules have built-in flexibilities for just these situations. Assuming there is a necessary, legitimate, and permissible use or disclosure of ePHI at work, and the reasonable safeguards discussed in this article and in the rule have been applied, every risk of breach does not need to be eliminated for a covered entity or business associate to create work-from-home standards. It is as important as ever that privacy and security of patient information be maintained as a pandemic ravages the healthcare system. But just as crucial are reasonable work-from-home measures that give healthcare workers, insurance payers, and business associates the tools and the access they need to continue to help patients during these trying times.

Takeaways

- Work-from-home orders and trends heighten the need for HIPAA security.
- The Security Rule offers both opportunities and challenges in its flexibility-of-approach model.
- Devices and networks should be encrypted and secured when allowing work from home.
- Staff can be empowered to take simple steps to secure their own home and Wi-Fi networks.
- Reasonable policies, training, and auditing can mitigate the security risk and allow for telecommuting.

[1] Katie Thomas and Jesse Drucker, “When Will You Be Able to Get a Coronavirus Vaccine?” *The New York Times*, September 17, 2020, https://nyti.ms/3mxMCCQ.
[2] Health Insurance Portability and Accountability Act Pub. L. 104-191, 110 Stat. 1936 (1996).
[3] 45 C.F.R. § 164.306(b) .
[4] 45 C.F.R. § 164.306(b)(2) .
[5] Office for Civil Rights, “What is the difference between addressable and required implementation specifications in the Security Rule?” U.S. Department of Health & Human Services, last reviewed July 26, 2013, https://bit.ly/3hYi3U0.
[6] 45 C.F.R. § 164 app. A , subpart C.
[7] 45 C.F.R. § 164.306(d)(3) .
[8] 45 C.F.R. § 164.312(a)(2)(iv) .
[9] U.S. Department of Health & Human Services, “Failure to Encrypt Mobile Devices Leads to $3 Million HIPAA

Settlement," news release, November 5, 2019, https://bit.ly/32YRrfu.

[10] U.S. Department of Health & Human Services, "Ambulance Company Pays $65,000 to Settle Allegations of Longstanding HIPAA Noncompliance," news release, December 30, 2019, https://bit.ly/3jLZAul.

[11] 45 C.F.R. § 164.306(d)(3)(ii)(B) .

[12] 45 C.F.R. §164.312(e)(2)(ii) .

[13] 45 C.F.R. § 164.310(b) .

[14] 45 C.F.R. § 164.310 .

[15] 45 C.F.R. § 164.502(a)(1)(iii) .

[16] Office for Civil Rights, "Incidental Uses and Disclosures," U.S. Department of Health & Human Services, last reviewed July 26, 2013, https://bit.ly/35iXVZx.