HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

HIPAA Compliance a Concern as Working from Home Becomes Norm

Working from home is the new normal and will be for many healthcare employees for a while, so adjustments are necessary to maintain compliance with HIPAA. Protected health information must be managed properly whether the employee is in the healthcare facility or at home.

Most healthcare providers should have crafted compliance programs for remote employees before the advent of the COVID-19 pandemic. Certainly, the pandemic has pushed the urgency of such plans to the forefront, says **Richard J. Tarpey**, PhD, assistant professor in the Jones College of Business at Middle Tennessee State University.

"In my prior practitioner healthcare career and leader of Sarbanes-Oxley and HIPAA compliance programs in the past, I can say that compliance is not flexible based on the location of the workforce. It is absolutely reasonable to expect the same level of security for remote workers as is in place for employees on company property," he says. "There are several examples in the last few years of healthcare providers being held financially accountable due to the loss of PHI [protected health information] data by remote employees."

The first step is for companies to completely understand which employees have remote access, Tarpey says. Existing remote access should be reviewed and reaffirmed to those employees with valid business justification. Companies should require, and employees should be willing to sign or reaffirm, confidentiality and HIPAA compliance documents. "It is a good idea to refresh the employee obligations in the employees' minds at this time," Tarpey says.

Compliance documents should highlight policies prohibiting using company-issued devices for non-company-related work, as well as preventing non-employees from using company-issued devices or using any personal devices that connect to company networks. Also underscore the importance of properly storing PHI-sensitive printed documents, and logging off all systems after finishing work.

Policies should clearly state the consequences of violation, Tarpey says. It also is a good idea to provide refresher information for employees on printing documents at home that contain PHI information. If reasonable, companies can consider providing HIPAA-compliant shredders for employees' use at home. Alternatively, companies can create structured processes for employees to drop off printed documents no longer needed at the company location via social distancing-safe processes.

On the technology side, companies should require remote employees to use a VPN to access company infrastructure when working remotely. Also, ensure the encryption of home wireless router traffic with secure (not default) passwords. Companies can best control access by issuing remote employees who access PHI a company-owned device that is encrypted and password-protected.

"The best [tactics] are to have strong remote work and data access policies, signed HIPAA compliance documentation for each remote access worker, and robust device management policies for any device connecting to the company network," Tarpey says. "While risk mitigation of a PHI data breach can never eliminate the risk with remote employees, the key determining accountability factor in the eyes of [Health and Human Services] is how well the company has managed system access, data access, system-connected devices, encryption, and employee policies."

The COVID-19 pandemic has prompted healthcare providers to ramp up work-from-home programs for non-clinical staff, often for the first time, and certainly at a scale not seen before, says **Rich Temple**, vice president and chief information officer at Deborah Heart and Lung Center in Browns Mills, NJ. "I think all providers need to operate from the premise that the level of cybersecurity protection

provided in a work-from-home environment can be no less than what it would be in an on-site working environment," Temple says. "The consequences of data breaches and security lapses, if anything, are greater in a work-from-home environment, since the control of who is seeing what is reduced when working in a household environment. The negative consequences of breaches are still the same, regardless of where the breach originated."

With a VPN, users go through the same, secure tunnel that allows IT teams to know exactly what volume of users are on what systems at different times. IT teams can allow "one-stop shopping" reporting on security red-flags, such as multiple failed log-in attempts or unusual access patterns (e.g., logging into systems at unusual days or times for particular users), Temple notes. The single point of entry also facilitates appropriate access to only the systems an individual needs to perform his or her job.

Another highly desirable protection to put in place, if at all possible, is two-factor authentication (2FA), Temple says. Instituting 2FA largely mitigates the risk of someone using a shared or otherwise purloined password to gain access to a system to which they are not entitled.

"The virtual desktop infrastructure [VDI] environment we have rolled out here at Deborah Heart and Lung allows us to greatly reduce our exposure to any malware issues that may reside on a user's home computer. [It] also minimizes the potential for data loss, [losing] electronic protected health information [ePHI], or [misplacing] other proprietary data assets," Temple says. "When a user logs into our environment, they are presented with a containerized, segregated virtual desktop ... our environment does not allow any sharing of programs or data between the home computer and the user's isolated VDI session."

The worst-case scenario is anything installed on the virtual desktop is destroyed when the virtual desktop logs itself off after a prescribed period and will not cross over and pose a risk to other users' virtual desktops, Temple explains.

Another issue is the "paper" component of individuals' job duties, Temple says. In an office, paper containing PHI can be stored in a desk at a cubicle. With good "HIPAA hygiene," one can protect this information from unauthorized eyes. However, with employees working from home, provider organizations lose those structural safeguards. It becomes much harder to ensure family members or others do not see PHI lying on a coffee table.

Printing PHI should be sharply restricted, if not prohibited altogether, for employees working at home, says **Janet Hunt**, senior director of IT user support at Apria Healthcare, a provider of home respiratory services and medical equipment based in Lake Forest, CA. Apria employees have worked remotely to an extensive degree long before COVID-19. Hunt says restrictions on printing PHI are a necessary part of HIPAA compliance.

"It's impossible to know where that PHI goes once it's printed on paper. We can't have it sitting around someone's home for just anyone to come by and see," she says. "With some reasonable precautions, I think employees can be just as HIPAA-compliant working from home as they are in the workplace."

The printing issue is an example of how employees can be tripped up by the peculiarities of working at home, says **Elizabeth Litten**, JD, partner and HIPAA privacy and security officer with Fox Rothschild in Princeton, NJ. "I know of a physician who was staying at her parents' house and had to submit a lab report. She did it from her own laptop just as a quick way to transmit it. Unbeknownst to her, it also printed to the printer in her old bedroom," Litten says. "She didn't realize that for a long time. That PHI was sitting there for her parents and anyone else who happened to be there to see it. There are more opportunities for inadvertent breaches when you're working from home, even if you're trying to do it properly, because someone can just walk by and see what's on your screen or overhear what you're talking about."

Implementing good tools for remote access and ensuring verification of the user are the keys to HIPAA compliance at home, says **Matthew R. Fisher**, JD, partner with Mirick O'Connell in Worcester, MA.

"To some degree, the HIPAA considerations when having a workforce operating from their homes as opposed to the office do not introduce new concepts. The basics of ensuring that workstations and network access remain secure should be paramount," he says. "On the whole, the policies should focus on maintaining the integrity of the system and keeping data as secure as possible. For example, allowing remote access to the entire system with no more than a username and password would not be advisable. Instead, some form of multifactor authentication or other mechanisms for vetting a request for access should be implemented."

On top of system-based tools, sending reminders to individuals working remotely of how to secure work areas and data can be beneficial, he says. Reminders can take the form of teachable moments or short pieces on how to apply office-based procedures to a home environment.

IT staff will play a large role in ensuring HIPAA compliance for

remote employees, says **Timothy E. Monaghan**, JD, partner with Shutts & Bowen in West Palm Beach, FL. He says the question should be: Are our communications with employees working from home protected to the same degree as communications between our employees when working from our facilities and offices?

If the issue is communication between the healthcare entity and persons not on its payroll (such as outside counsel or consultants), the security issue is not new to COVID-19. Perhaps COVID-19 is causing the entity to review security issues in general, Monaghan offers. If this is the case, the pandemic may be uncovering issues that have been present for some time. If so, the entity would be justified in asking outside parties with whom it conducts business to demonstrate compliance with privacy and security regulations.

Another solution is to ensure sensitive information is not shared with outside parties who may not need it for their work.

"If I anticipate receiving PHI from a client, I make sure that I have a HIPAA-compliant Business Associate Agreement in place before I receive the PHI. I work with our IT folks to arrange for secure transmission and storage," Monaghan says. "Most of the time, however, I can do my work without personally identifying information. I simply advise the client to exclude that information from any communications with me."

As always, organizations should be careful to ensure PHI is shared on a "need to know" basis. This is true whether the person receiving it is working in the office or at home, Monaghan says.

"A number of HIPAA requirements have been waived. I believe this is in general recognition of the fact that we are in extraordinary times. It is more important now to keep healthcare organizations running as smoothly as possible and to simply make sure we save lives," Monaghan says. "It probably is not reasonable to expect the same level of security at home right now, but ... we should make sure that our pre-COVID practices were in order and that exceptions to full compliance are reasonable under the circumstances. In other words, we can't assume that all transgressions will be forgiven because we are in this crisis."

Covered entities should ensure HIPAA compliance the same way they did pre-pandemic: by analyzing the risks and adopting safeguards that minimize those risks, says **Jeffrey Drummond**, JD, an attorney with Jackson Walker in Dallas. There were many healthcare providers and other health industry businesses that already worked remotely or allowed employees to telecommute while maintaining HIPAA compliance.

While each business will face its own peculiar issues, some risks expected in a work-from-home situation include data transmission security, data storage security, and person/entity/device authentication, Drummond notes. However, there are readily available safeguards for each new risk.

"It's always a good idea to limit employee access to information needed for the job. Given the potential increased risk of working from home, covered entities and business associates should readdress employee access and limit wherever possible," he says. "However, a healthcare provider should not impose any data access limitations that will impact the quality of care."

HIPAA always requires taking reasonable steps to ensure the security of protected health information. Changes in work environment do not change the expected level of security, Drummond says. What is reasonable in an emergency situation may be unreasonable in a time of calm and normalcy.

"The question in current COVID-affected times is what level of security may be reasonably obtained, given the current situation? A VPN is not as secure as a closed-access system. In that respect, working from home is going to have a lower level of security," Drummond says. "However, during a time of government-mandated work-from-home orders, that 'lower' level of security might be just as reasonable — HIPAA-compliant — as the higher level during non-pandemic times."

New approaches leveraging machine learning-based data governance enable institutions to continually monitor their data, receive notifications when a compliance risk emerges, and automate its remediation, according to **Alok Tayi**, vice president of life sciences at Egnyte, a company in Mountain View, CA, that provides data security services

"Among our customers, the key risks that have emerged involve training, data exposure, and moving data between applications. To enable learning, we have seen many companies implement distributed training tools and screen sharing to share best practices," he says. "Two [tactics] to tackle data exposure are to centralize data in what is called a 'single source of truth' and apply machine learning to see when sensitive data is exposed. Native integrations between your data repository and applications facilitate a single area of control."

Considering the dynamic effect of COVID-19, transmitting data to employees working at home may be the wrong framework, Tayi says. Instead, it may be appropriate to maintain

a central, unified database to which access is provisioned. This approach facilitates a strong security envelope around the data, but affords seamless access if permitted.

"It is possible for data to be as secure in a work-from-home model as in an office-driven one. Doing so requires the proper technologies be implemented to ensure safe and secure access," Tayi says. "Approaches like machine learning-based data governance, centralized repository models, and single sign-on enable personnel and patients to have comfort and confidence around the security of their data."

Many HIPAA threats come down to inappropriate access to patient data outside the intended context. This fundamental risk to PHI data is no different in a remote work environment than in a physical office, says **Paul Trulove**, chief product officer with SailPoint, a company based in Austin, TX, that provides data security services.

"Healthcare employees should be following the same IT security best practices as they would in the office to minimize the risk of a potential data breach," he says. "Healthcare organizations can enhance their ability to protect PHI in a remote working environment by focusing on two key areas. First, ensure workers accessing PHI are connecting to a secure network when they access internal systems that have patient data. Second, make sure they are not transmitting PHI to personal devices or personal email accounts."

Employees should use corporate-owned devices and apps sanctioned only by IT, Trulove says. "Identity management is still a critical business essential as healthcare organizations continue to operate out of the home by following the same identity governance standards. To do this, they need to continually review who has access to what, and deprovision that access if it is no longer appropriate or when someone no longer works at the organization," he says. "This is critical now more than ever as people continue to be remote." ■

7 Steps to Better HIPAA Compliance at Home

Ensuring HIPAA compliance with employees working from home will require a systematic approach. **Robert K. Neiman**, JD, principal with Much Shelist in Chicago, offers seven steps for better compliance:

• Hold a Zoom call for all employees reminding them of the company's HIPPA policy and their obligations. Ensure the policy states employees working remotely and accessing protected health information (PHI) use company-owned, encrypted, password-protected, and VPN-equipped devices. Prohibit employees from using personal devices to store or access PHI. Direct all employees accessing PHI remotely to e-sign their understanding and agreement.

• Allow employees to access only the PHI they need to handle their job. Limit access accordingly.

• Prohibit any use of the company-owned device by any third party, including friends and family.

• Make sure employees' passwords for their company device and wireless router are sufficient. They should be long and complicated enough, using a combination of letters, numbers, and symbols, to minimize the risk of hacking.

• Limit PHI printing. If any employee must print any documents containing PHI, then require he or she shred printed documents before disposing them.

• Require employees working remotely to disconnect from the company system when their work is finished for the day.

• Prohibit employees from leaving their company device in their personal vehicles at any time to avoid the risk of device theft via a break-in. ■