HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

Avoid Most Common HIPAA Violations With Best Practices, Education

HIPAA breaches can happen even to the best prepared healthcare organizations, but knowing the most common failings can improve your chances of staying in the good graces of the Office for Civil Rights (OCR).

Organizations sometimes have a false sense of preparedness because they put policies in place and think that is enough, says **Lucie F. Huger**, JD, an officer, attorney, and member of the healthcare practice group at Greensfelder, Hemker & Gale in St. Louis. "I see a lot of technical compliance, but one thing I see organizations overlooking on a routine basis is the human element involved," Huger says. "Through those mistakes, even with the best policies in place, you can still be violating HIPAA. People get curious and click on links in phishing emails, which can be very dangerous to an organization. Or, I see it when people work too quickly and provide information about a patient to the wrong person."

Data management and restricted access can address some of the inevitable human failings that lead to HIPAA breaches, says **Jorge Rey**, CISA, CISM, risk advisory services principal at Kaufman Rossin in Boca Raton, FL, which provides business consulting and compliance services. If employees have limited or no access to protected health information (PHI), they cannot release it even accidentally, he explains. "We've seen a lot of healthcare institutions trying to limit the access that everyone has," he says. "They are becoming better at understanding where that data resides to prevent that unauthorized access. Laptops were a big issue for a couple years because data was not encrypted and data were being lost, but we've seen in the past couple of years that is becoming less common."

When training staff and physicians on HIPAA compliance, healthcare organizations should tailor the content to explain what HIPAA compliance looks like in the day-to-day work environment for that organization, says **Melissa Soliz**, JD, an attorney with Coppersmith Brockelman in Phoenix. Leaders should provide practical guidance on how to protect the privacy and security of health information, she says. "HIPAA trainers and educators often forget to cover some of the most basic HIPAA compliance measures that are most effective in protecting the privacy and security of health information," Soliz says.

She cites these examples of important points often overlooked:

- Reminding workforce members to not take any health information outside the organization unless it is necessary to do so and permitted by the organization's policies and procedures;
- Prohibiting workforce members from accessing health information systems through devices such as cellphones or tablets or storing health information on such devices that do not meet HIPAA standards or are not approved for use by the organization;
- Prohibiting workforce members from posting details about or pictures of patients in the workforce members' social media posts;
- Reminding workforce members that paper records containing health information cannot be disposed of in open garbage or recycling bins;
- Instructing workforce members on how to avoid cyberattacks, such as phishing emails;
- Informing workforce members of who to contact if they want to ask HIPAA-related questions, who to contact if they suspect there has been an unauthorized use or disclosure of health information, and where the organization's HIPAA policies and procedures are located.

It is important that the organization maintains robust privacy and security policies and procedures, Soliz says. Further, the organization should implement those policies and procedures through regular training, auditing, and enforcement. The most common mistakes employees make is individual carelessness, such as leaving paper patient records in an unlocked car, clicking on phishing links in emails, or inadvertently disclosing patient health information in a social media post about their

workday, Soliz says. "Educational efforts often focus on abstract privacy and security concepts without providing workforce members with sufficient context to understand how they can be HIPAA compliant within their work environment," Soliz says. "Providing workforce members with concrete examples of what HIPAA compliance and noncompliance looks like will enable organizations to avoid the most common errors."

Soliz cites a recent example in which a small dental practice paid OCR $10,000 as part of a corrective action plan arising out of the practice's response to a patient's social media review, in which the practice disclosed the patient's last name and details of the patient's health condition. *(Read more about this case at: http://bit.ly/2pPYg30.)* "OCR imposed a $2.15 million civil monetary penalty on a health system that lost paper records on over 1,400 patients, allowed a reporter to share a photograph of an operating room containing patient health information on social media, and had an employee who had been inappropriately accessing and selling patient records since 2011," Soliz says of another case. *(Read more about this case online at: http://bit.ly/2Pii0qI.)*

Training should be aligned with the organization's policies and procedures and it must be practical, says **Erin S. Whaley**, JD, partner with Troutman Sanders in Richmond, VA. Too often, organizations provide generic HIPAA training, she says. "The generic trainings are, at best, not based on the organization's policies and procedures and, at worst, inconsistent with the organization's policies and procedures. Customizing generic trainings will help ensure consistency and alignment with the organization's policies and procedures," she says. "Another pitfall is training on concepts instead of practical application of those concepts. By offering real-life examples and horror stories, organizations can help their staff and physicians recognize and avoid risky or noncompliant behavior."

One of the most frequent system-level oversights is failure to perform a complete annual risk assessment, Whaley says. Considering the number of cloud-based solutions, some organizations believe they can rely on their vendors to perform these assessments. However, these organizations are obligated to conduct a thorough assessment for all their systems, she explains. "These assessments may be informed by information from vendors but should not be delegated to the vendors," Whaley says.

In terms of individuals, the most prevalent mistakes usually are simple human error, such as losing a laptop, sending an email to the wrong person, or discarding PHI in the wrong bin, Whaley says. "There is still a surprising amount of paper PHI in practices. Paper PHI must be properly disposed of to ensure destruction," Whaley says. "Organizations should have a secure bin for discarded paper PHI, but the organization may only have a few of these secured bins throughout the facility. For efficiency, individuals sometimes keep a shred box at their desks so that they don't have to walk to the secure bin each time they need to discard a document, even though this may not be consistent with the organization's policies and procedures."

The individual may empty this "shred box" only occasionally when it is full, Whaley explains. If the cleaning crew inadvertently throws this box away in the trash or recycling instead of the secure bin, this could be a breach. Investigating and reporting this type of incident is difficult and completely avoidable, Whaley adds. When providing HIPAA education, it is important to ensure the workforce appreciates that management has bought in relative to compliance, says **Brad Rostolsky**, JD, an associate with Reed Smith in Philadelphia. Training should not be viewed as "something you just need to do," he says. "Beyond that, it's important to do more than provide a HIPAA 101 training," he advises. "Training should spend some time focusing on the actual policies and procedures of the business."

From a system perspective, one of the more common challenges is logistics, Rostolsky says. The bigger the entity, the more challenging it is to communicate information throughout that entity in a timely and efficient manner, he says. "It's important to ensure that a process is in place for the workforce to understand who in the privacy office needs to know what information and when they need to know it," he says. "A basic example of this would be to prospectively designate a particular individual to receive subpoenas, or even just requests for PHI, so that the requests are processed appropriately."

Individuals, on the other hand, often violate HIPAA merely because they do not fully appreciate that one person's action, or failure to adhere to what may seem like an annoying rule, can significantly affect a large business, Rostolsky says.

"To this end, part of training should include examples of where big dollar enforcement actions were triggered by the noncompliant actions of a single individual," he suggests.

Training also should be provided in different forms, says **Michele P. Madison**, JD, partner with Morris Manning & Martin in Atlanta. For example, there should be training at orientation, staff meeting reminders about HIPAA safeguards, and education about ransomware attacks. Healthcare organizations also can conduct phishing exercises to test employee response, sharing the results on an annual basis during the staff member's performance review, Madison suggests.

"One common mistake is providing an initial education forum at orientation and requiring annual review of an

online training program that fails to address the specific job functions or roles of the individual," she says. "The lack of specific and continuous training may not adequately prepare the staff member for his or her job and lead to a mistake that causes a breach."

Another common mistake is failing to provide continuous security awareness training, she says. Such training is a requirement of HIPAA, Madison notes, and technology is constantly changing. Therefore, the organization's security safeguards should be reviewed on a regular basis. Staff should be trained on the new and upgraded security safeguards as well as the vulnerabilities and risks associated with electronically accessing, storing, or transmitting PHI, she says. "[OCR] fines and penalties have focused upon organizations failing to implement a comprehensive security risk analysis. Failing to fully evaluate all mobile devices and the different access points to the organization's information technology infrastructure is a significant risk to the organization," Madison explains. "In addition, when the technology infrastructure changes, even to troubleshoot an issue, the risk assessment should be performed to identify any safeguards that need to be implemented as part of the change to the system."

Social media continues to pose a significant risk for HIPAA violations, says **Susan Tellem**, RN, BSN, APR, a partner with Tellem Grody Public Relations in Los Angeles, which assists providers with their responses to HIPAA violations. Instagram and Facebook create an easy medium for people to violate HIPAA, Tellem says. But beyond those channels, there are many ways healthcare employee can inadvertently disclose PHI and never even realize it, she adds.

"Faxing of some PHI is allowed, but a fax can wind up easily in the wrong hands," she says. "What if a healthcare professional is taking a break and decides to share a photo of what she is eating with an open patient file in the background? Photo sharing among doctors and patients is becoming more common and may be shared by accident." ■

Enforcement Action Follows Predictable Path, Starts With a Letter

A healthcare organization's involvement with OCR may begin with a simple letter acknowledging a complaint and providing guidance documentation related to it, notes **Elizabeth Litten**, JD, partner and HIPAA privacy and security officer with Fox Rothschild in Princeton, NJ. "Sometimes, [OCR] will send a complaint warning letter, knowing that it may be a one-off, but they want to make the covered entity aware and ensure it is complying with HIPAA," Litten explains. "Sometimes, they'll ask the covered entity to respond in some way, but, frequently, if they think it just involves one incident or individual, they will say they consider it closed but will be concerned if the problem persists."

For a more serious concern, OCR will assign a case number and ask for substantial information, such as policies and staff education records. Typically, OCR gives a 30-day deadline, but often will grant an extension if requested. "They may ask for documentation on what occurred, your policies and procedures, how you addressed the incident. They'll ask for very specific information, even financial information, to get a sense of who your business associates are," she says. "They may ask for specific names and titles of individuals involved."

The letter usually says that if an organization does not respond, that will be considered a violation of HIPAA. The course of OCR's response will be determined largely by the nature of the complaint, says **Emily Quan**, JD, an attorney with Weinberg Wheeler Hudgins Gunn & Dial in Atlanta. Impermissible use and disclosure is the most common type of complaint.

"With that complaint, typically, the covered entity will be asked for some information to review the complaint," Quan says. "[OCR is] looking at when this potential violation occurred, whether the entity is covered by the privacy rule, whether the complaint was filed within the usual six months, and whether the incident actually violates the privacy rule." The outcome can be tough to predict. OCR could determine there was no violation, or the agency could rule there was a violation, and levy various civil penalties. Quan says this is why it is vital to conduct a comprehensive risk analysis early. "This is a process that tends to snowball, particularly if this involves a massive health system or institution. There can be a number of offshoots from the investigation, with each one of them requiring time and resources to investigate."

There are countless HIPAA violations every year that are never detected or reported, says **Eric D. Fader**, JD, an attorney with Rivkin Radler in New York City. A media report may trigger an investigation, as with a recent case in which OCR fined a health system more than $2 million after reporters shared a photograph of an operating room screen that included a patient's medical information *(See previous article in this issue for more information.)*

"Sometimes, the OCR will begin an investigation after receipt of a complaint from a patient or other party," Fader says.

"However, I think most often, the filing of a covered entity's or business associate's own breach report with OCR will trigger the investigation."

OCR uses wide latitude when determining potential penalties. Generally, a breach or other HIPAA violation in and of itself will not result in an expensive fine. If the breach affects few people and was identified and corrected promptly, an investigation is less likely. Still, OCR has made a point of publicizing some tiny breaches, just to show that "size isn't everything," Fader cautions.

OCR usually has much less patience and understanding when the covered entity or business associate has not adopted required HIPAA policies and procedures, has not properly trained and retrained its employees (no less often than once per year), failed to conduct required periodic enterprise-wide risk assessments, or failed to investigate and report a breach timely.

The absence of a business associate agreement between a covered entity and its business associate or between the business associate and its subcontractor can compound the potential penalty. "Breaches happen," Fader says. "An entity that has taken HIPAA seriously and that investigates and takes corrective action promptly, and that doesn't attempt to deceive OCR or minimize the severity of its actions, has a good chance of getting off lightly."

Enforcement is not limited solely to the imposition of monetary fines, notes **Matthew R. Fisher**, JD, partner with Mirick O'Connell in Worcester, MA. Enforcement can include investigations, audits, requirements for corrective actions, and private lawsuits, although litigation will not fall directly under HIPAA.

It is difficult to find any pattern for when a fine will be imposed. If there is a particularly egregious violation or the organization can pay a substantial fine, then infractions may be more likely to result in a monetary penalty. "Additionally, OCR is increasingly focused on denial of access problems, which suggests more fines could be coming on that front," Fisher suggests.

An investigation may not necessarily make headlines, but it does affect an organization and take time and resources. For enforcement, OCR's primary options are monetary penalties and/or corrective actions. "Monetary penalties are imposed in few instances, but there does not seem to be any rhyme or reason as to when a penalty will be imposed. Corrective actions often consist of technical advice to help organizations better comply with HIPAA requirements," Fisher says. "Corrective actions will result quite frequently when an interaction occurs between an organization and OCR because some issue of noncompliance will likely arise. A corrective action is often collaborative and not punitive, as OCR wants to see good practices put into place."

Enforcement will follow a standard course of investigation, audit, discussion, determination of baseline issues, and then outcome. The first few stages will consist of document requests and a written or verbal back and forth. Often, the goal is to establish that efforts are in place for an organization trying its best. "Even with the best of efforts, mistakes or issues can arise. The good faith effort at demonstrating compliance will be a big factor in influencing the outcome of an investigation or potential issue," Fisher says. "If an organization is ignoring or deliberately not implementing a policy or procedure required by HIPAA, then issues will arise."

In an ordinary course, the timeframe for resolution of an issue will be a few months. OCR usually will send a document request within one month of a large breach report or an individual complaint filing. From there, an organization will have about two weeks to submit a response. Some time later, OCR will reveal the resolution to the organization. "That is the ordinary course. However, recent monetary penalties seem to take years from the underlying incident," Fisher observes. "There is no indication as to why so much time passes, though it could be that there is a lot of back and forth going on in the background."

The biggest impact on a potential outcome is transparency and taking good faith steps to comply with HIPAA. OCR recognizes that no organization can be perfect all the time. Still, so long as honest efforts are taken, OCR will be willing to work collaboratively.

Sometimes, the OCR investigation reveals relatively minor violations that can be corrected without significant penalties, says **Kimberly J. Gold**, JD, partner with Reed Smith in New York City. OCR may only seek corrective action in these instances. They may seek changes to an organization's HIPAA policies, procedures, and training. In more serious cases, OCR will pursue penalties in addition to corrective action. Criminal charges are seen less frequently. The course of enforcement typically is determined by how egregious a HIPAA violation is in the mind of OCR. "A data breach involving hundreds of thousands of individuals and underlying HIPAA violations, like the failure to conduct a security risk assessment, could trigger significant penalties," Gold warns. "Even the failure to execute business associate agreements has led to penalties. Less serious violations that can be quickly remedied are often easier to resolve without financial penalty."

In addition to cooperating, maintaining strong records (including documentation of policies, procedures, training, and risk assessments) will go a long way with OCR. "Should OCR investigate a large data breach and find no evidence of a risk assessment having been performed, or of any commitment to a HIPAA compliance program, enforcement will be more likely," she cautions. ■