HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

OCR Concerned About HIPAA Contingency Plans

Developing a good HIPAA contingency plan is critical to ensuring a facility can access data during a disaster or cyberattack, and it also is required for HIPAA compliance. Creating that plan may require more assessment and planning than one might imagine, and it's the kind of thing that can be lacking in an otherwise good HIPAA program.

The HHS Office for Civil Rights (OCR) recently urged healthcare organizations to develop contingency plans for crises that could compromise protected health information (PHI) covered under HIPAA.

"Contingency plans are critical to protecting the availability, integrity, and security of data during unexpected adverse events. Contingency plans should consider not only how to respond to disasters such as fires and floods, but also how to respond to cyberattacks," OCR said. "Cyberattacks using malicious software such as ransomware may render an organization's data unreadable or unusable. In the event data is compromised due to a cyberattack, restoring the data from backups may be the only option to recover the data and restore normal business operations."

The OCR reminder, along with multiple sources for guidance in developing contingency plans, is available at: https://bit.ly/2uF0ap4.

A contingency plan is required under 45 CFR Section 164.308(a)(7), which established HIPAA. Covered entities must establish and appropriately implement policies and procedures for responding to an emergency or other occurrence that damages systems containing electronic protected health information, notes **Lucie F. Huger**, JD, an officer, attorney, and member of the healthcare practice group at Greensfelder, Hemker & Gale in St. Louis.

An emergency or other occurrence includes an unforeseen event, such as a natural disaster or a cyberattack, she says. Huger explains the necessary elements of a HIPAA-compliant contingency plan should include:

1. Data backup: Figure out how to create and maintain retrievable, exact copies of protected electronic health information;
2. Disaster recovery: Create procedures to restore any data that are lost;
3. Emergency mode operation: Produce procedures to enable the continuation of critical business processes to protect the security of protected electronic health data while operating in an emergency mode.

Other items to address in a contingency plan include procedures for periodic testing and revision of contingency plans, and assessing the relative criticality of specific applications and data in support of other contingency plan components.

"You need to first start with performing a risk analysis to identify your organization's risks and vulnerabilities. In developing a risk analysis, the organization should identify the potential threats to their data, identify the associated risk to the data, and note preventive controls," she says. "The [OCR] has provided guidance to entities suggesting that entities prioritize their critical systems and critical information to help them to focus on developing a contingency plan."

Different organizations face different risks because they maintain varying systems and implement contrasting controls, Huger notes. What may be a risk for a hospital system may not be the same for a small physician's office, she says.

"An effective contingency plan can be a game changer in the event of a ransomware attack because if an entity can use its backup data to get its operations back up and running, it minimizes the impact of the attack," she explains.

The clear identification of plan objectives is critical to the success of any contingency plan, along with ensuring those objectives include measurable and purposeful processes designed to achieve those goals, says **Ryan Buckner**, JD, principal with Schellman & Company, an independent security, privacy, and standards compliance assessor.

"Simple and clear objectives tend to be more effective at enhancing compliance and controls over time vs. designing a plan that does everything on day one. Many organizations fall victim to overly complicating their contingency plans," he says. "While it is important to ensure your organization achieves meaningful and desirable outcomes, oftentimes, organizations simply get in their own way by primarily focusing directly on process or IT solutions without first addressing the key questions regarding the plan's objectives."

Often, this requires a level of discipline and planning from those who are used to accomplishing tasks quickly, Buckner says.

"Focus on a risk-based set of contingency plan objectives, establish the measurable processes designed to meet those objectives, test the plan against those objectives, and improve the plan based on those results over time," he advises.

The requirement for contingency plans is broad, notes **Elizabeth Davidson**, PhD, professor of information technology management at the Shidler College of Business at the University of Hawaii at Manoa. All HIPAA-covered entities, such as hospitals, physician practices, health insurers, and home health services providers, as well as their business associates such as cloud-based electronic health record (EHR) vendors, must maintain a contingency plan for protecting, recovering, and restoring protected health data in the event of a business disruption.

A contingency plan begins with a risk assessment that identifies all information systems that handle protected health data, including computers, laptops, mobile devices, software, and databases, she says.

"This survey must be comprehensive, because not all PHI are contained in one EHR," she says. "Many health services providers big and small still have vital PHI in paper records, specialized computerized systems, or even Excel spreadsheets."

The risk assessment classifies the sources, probability, and implications of adverse events, such as hardware malfunctions or natural disasters. This allows the organization to prioritize and focus its plan based on the probability and cost of an adverse event.

"For instance, brief power outages may happen several times a year, but the impact on PHI is generally not high. Conversely, a once-in-a-100-year weather catastrophe has low probability of occurring, but could lead to wide-scale loss of protected health data," Davidson says. "In Hurricane Katrina in 2005, many medical facilities and physician offices in New Orleans were flooded, and patient health records were destroyed and permanently lost."

Based on the risk assessment, the contingency plan includes a data backup procedure for all electronic PHI, a disaster recovery guide specifying how lost or damaged PHI and associated information systems will be restored, and an emergency mode operation policy detailing how the organization will function during an emergency while also protecting PHI, Davidson explains.

"The plan should specify procedures to periodically assess and update the contingency plan and to test the plan occasionally," she says. "An untested, out-of-date contingency plan is like driving around with a flat spare tire in the trunk. It won't help if you have a tire blowout on the highway."

Contingency planning begins with understanding PHI management regulations and the organization's objectives and priorities, she says. Fortunately, risk assessment and contingency planning steps are well-understood processes, which most large organizations can undertake with their own IT and clinical staff.

Small-to-medium-sized organizations may need to contract with consultants who are experts in data security and contingency planning to work with the managers and clinical staff.

"Finally, the plan should include training and education of all staff members, who will carry out the plan should the need arise," Davidson says. "If you don't know how to change that flat tire, having a spare in the trunk won't be of much help when a tire blows."

The complexity and scope of a contingency plan will reflect the complexity and size of the organization, Davidson says. The plan for a multi-location healthcare services network will necessitate orders of magnitude more complex than for a small physician practice. However, a well-developed plan is just as important for a small organization, she notes.

"Imagine a solo physician practice that has all its patient medical records in an EHR on a computer server in the back office. Now, imagine that the server is stolen or lost in a fire or flood," she says. "Without a plan in place, this small practice would be out of business and also legally liable for having lost the medical records. A contingency plan would ensure the PHI data were backed up off-site, specify how to restore data, and instruct staff how to deal with patients until the EHR and data are restored."

Many organizations find it hard to justify spending resources to prepare for adverse events that may never happen, Davidson says. However, not creating an adequate plan means hoping that risks won't happen and that if they do, things won't be all that bad.

"The reality is that failure to plan for disruptions that can impact PHI

puts patients' safety and well-being at risk. The organization may face fines for lack of compliance and be held financially liable to patients whose PHI are lost," she says. "If the loss is severe, the organization may lose patients whose trust in the organization's ability to keep their PHI data safe is lost."

Typically, developing a contingency plan will require forming a committee of stakeholders, says **Alaap B. Shah**, JD, an attorney with Epstein Becker & Green in Washington, DC. That committee should include, but is not limited to, individuals with responsibilities related to compliance, information technology, facilities management, finance and administration, human resources, and communications.

"This committee will need to work together to define recovery requirements relative to key business functions; document the impact of an extended loss to operations and key business functions; and evaluate options for disaster prevention, impact minimization, and orderly recovery," he says. "It ultimately will develop a written contingency plan that is understandable, easy to use, and easy to maintain, with clearly defined triggers and response roles and responsibilities."

Shah also emphasizes that a contingency plan should not sit on a shelf and collect dust, but rather should be tested and improved over time.

The recent message from OCR shows that contingency plans are on the table when the office looks at any organization's HIPAA compliance, notes **Nick Merkin**, CEO of Compliagent, a company in Los Angeles that advises healthcare companies on compliance and data security issues. OCR hasn't created any new requirements, but it is making known its concerns that covered entities may be giving short shrift to this one.

Merkin also notes that contingency plans should cover a wide range of potential ways PHI access could be compromised, from the catastrophic natural disaster to more mundane problems.

"It could be something high-tech and dramatic like a ransomware attack, or it could be something as simple as a leaky roof that damages your servers, and your servers go down," he says. "The OCR was specific about that, reiterating that you need a disaster recovery plan that will tell you how to restore or access that data no matter what the cause of the problem."

The goal is to ensure that you can continue to provide quality care even when PHI is compromised in some way, he says.

"One of the problems I see is that a lot of organizations are still newly adopting things like EHRs and making the transition from a paper record. There is sort of a slow realization that protecting that data is important and how you protect it may be different from how you protected data when it was stored in a file cabinet in your storage room," he says. "A lot of organizations make the mistake of just downloading something off the web or depending on an employee who used to work in an organization sort of like yours. What you end up with are templates and not policies and procedures tailored to your organization, which can make a big difference in a breach or an emergency." ■

Legal Case Shows Risk of Improper Patient Info Disclosure

An ongoing legal case illustrates the risk healthcare providers face when they do not properly safeguard patient data and make it available to third parties without consent, even when complying with a subpoena.

A recent legal ruling allows patients in Connecticut to sue any healthcare entity for damages related to a HIPAA violation, and the same theory would hold in many other states.

The Connecticut Supreme Court recently ruled that patients in the state can sue doctors and other healthcare providers for the disclosure of their confidential medical records without the patient's consent. The ruling involved a client represented by **Bruce Elstein**, JD, an attorney with the law firm of Goldman Gruder & Woods, who explains that *Byrne v. Avery Center for Obstetrics & Gynecology* has been in litigation for 12 years.

Elstein's client, Emily Byrne, received prenatal care at the OB/GYN practice in Westport, CT. In 2004, she specifically told the practice not to release her records to her former partner, Andro Mendoza. The following year, she moved to Vermont.

"She had broken off that relationship with the father of the child and informed the office to provide to him no information," Elstein says.

Mendoza filed paternity actions against Byrne in Connecticut in May 2005 and sent the OB/GYN practice a subpoena requesting all of Byrne's medical records. The practice mailed the records to the New Haven Regional Children's Probate Court,