Health Information Compliance Alert

Case Study: Safeguard Patients' ePHI With Better Access Controls

Tip: Don't skimp on emergency access plans.

Virtual work has allowed many covered entities (CEs) to stay afloat during the pandemic. Though immensely helpful in the long run for the industry, this spike in remote work has coincided with a decline in security protocols and an increase in data breaches.

With ransomware attacks and major hacking incidents dominating the headlines, you may be thinking that internal threats aren't that big of a deal anymore. But, two recently published reports from top data security firms coupled with fresh guidance from the HHS Office for Civil Rights (OCR) suggests that managing insider threats from employees is just as critical as your external safeguards.

Definition: Malicious and unintentional threats from internal actors go hand-in-hand. While most staff, business associate (BA), and vendor data security incidents are accidental, they still cause an unintentional threat to your business. However, these same actors can also wreak havoc as malicious threats, corroding, corrupting, or hacking your system from the inside out.

Common unintentional data incidents triggered by staff, BAs, and vendors include:

Accidental disclosure: For example, accidental disclosures happen when an employee posts something about a patient on social media without written consent or sends an email to the wrong person with patients' protected health information (PHI) in it.

Social engineering: Hackers utilize this popular technique, most often through phishing schemes in email. For example, an employee clicks on an attachment and unleashes chaos on your system from the malware in the attachment.

Physical issues: When physical records are not properly disposed of, trouble often ensues. OCR offers explicit directions for the proper disposal of PHI to ensure it doesn't get into nefarious hands.

Mobile devices: Unencrypted lost or stolen mobile devices with ePHI on them remain a thorny problem for the healthcare industry and perennially lead to large-scale breaches.

Check Out 2 New Cybersecurity Studies

Human error remains the top reason that the healthcare industry continues to be besieged with cyberattacks, says Verizon in its "Data Breach Investigations Report, 2021." Despite a shift from more internal breaches to external over the past few years, inside threats still accounted for 39 percent of healthcare breaches last year, the Verizon report shows.

Trends show that lack of security know-how, training, and slipshod access controls are the primary culprits leading to data security incidents, indicates Verizon's study.

Additional research shows why the healthcare industry needs to have tighter controls on ePHI. COVID-19 made infiltration easier for hackers, but healthcare workers also have more access to sensitive files than staff in other industries, which accounts for that health data being "overexposed," according to the Varonis study, "2021 Data Risk Report: Healthcare, Pharmaceutical, & Biotech."

"Nearly 20 percent of files are open to every employee in healthcare organizations (on average),” cautions Varonis. And, "31,000 sensitive files (HIPAA + financial + proprietary research) are open to everyone.” It shouldn't be a surprise that the Varonis study considers the staggering opportunity for PHI/ePHI loss as an "existential risk” in the healthcare industry, especially with "1 in 10 sensitive files open to every employee,” the report says.

Manage Staff Access to Files, OCR Says

As cybersecurity woes continue to plague the healthcare industry, OCR reminds CEs that protecting ePHI with stellar access controls and management are HIPAA Security Rule requirements. "Information access management is an administrative safeguard for ePHI and access control is a technical safeguard for ePHI,” the agency says in the summer 2021 Cybersecurity Newsletter.

The two requirements are different, but both are necessary to adequately protect ePHI and work best when implemented in tandem.

Information access management refers to the system CEs and BAs create in determining who will have access to ePHI. Other items that fall under this Security Rule administrative requirement include:

- Creating access policies, procedures, and an implementation plan.
- Outlining who will be responsible for authorizing access and enforcing the protocols.
- Documenting, reviewing, and revising the information access management plan.

"These policies typically govern the parameters for which individuals in particular workforce roles may be granted access to particular systems, applications, and data,” OCR expounds. "Those parameters would reflect what information access is necessary for a workforce member to do their job.” Additionally, HIPAA compliance teams must remember to write up protocols that always take the minimum necessary standard into account to secure ePHI.

Access controls are exactly what the title implies. They are technical tools that assist CEs and BAs with governing access to ePHI and health IT. Examples of this Security Rule technical safeguard include firewalls, network access control, logging, and monitoring of systems.

OCR breaks down the access controls requirement into these four implementation specifications, according to the Cybersecurity Newsletter:

1. Unique user identification: This requirement refers to all IT users having a unique username to log into the system. OCR advises against sharing user IDs as this increases the chance of compromising your systems and decreases workers' accountability for their actions.

2. Emergency access procedure: This crucial protection puts a contingency plan in place for access controls during emergencies such as natural disasters or power outages. OCR uses the example of healthcare workers using telehealth enmasse during COVID-19 as a scenario that would be covered under this requirement.

3. Automatic logoff: Systems and workstations must utilize automatic logoff to thwart unauthorized access to ePHI and critical organizational data. "Failure to implement automatic logoff not only increases the risk of unauthorized access and potential alteration or destruction of ePHI, it also impedes an organization's ability to properly investigate such unauthorized access because it would appear to originate from an authorized user,” OCR says.

4. Encryption and decryption: These technical tools allow CEs and BAs to secure ePHI - it's just that simple. Encryption scrambles data, making it unusable and unreadable to unauthorized users while decryption takes that indecipherable text and transforms it back into plaintext. These techniques are particularly important to employ on mobile devices as they are often lost or stolen, OCR counsels.

Bottom line: Taking a two-pronged approach to stopping both inside jobs and external theft of your ePHI is the best way forward, experts insist. The first approach is to apply the technical securities that will help prevent a threat to your

information systems, "and the other is to require good authentication of individuals when providing services or supplying information," advises **Jim Sheldon-Dean**, founder and director of compliance services at Lewis Creek Systems LLC in Charlotte, Vermont.

Resources: Check out the Varonis report at https://info.varonis.com/hubfs/Files/docs/research_reports/2021-Healthcare-Data-Risk-Report.pdf. Review Verizon's study at www.verizon.com/business/resources/reports/dbir/. Find OCR's summer 2021 edition of the Cybersecurity Newsletter at www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-summer-2021/index.html#footnote10_ar7ppha.