Health Information Compliance Alert

Case Study: Make the Physical Security of Your Office a Priority

Break-ins happen more than you think.

The majority of HIPAA breaches are due in part to accidental privacy snafus or IT-related hacks. Most arise from carelessness and can easily be amended with stricter office regulations. The combination of securing the physical premises of your practice while safeguarding your technical tools will help keep your violations in check.

Background: In February, the protected health information (PHI) of 582,174 individuals was compromised when the offices at the California's Department of Developmental Services (DDS) were plundered. The theft was significant, exposing over half a million people as well as the personal information of 15,000 employees, in the largest breach of the year thus far, according to the HHS Office for Civil Rights (OCR) Breach Portal.

"On February 11, 2018, a break-in occurred at the DDS legal and audits offices building in Sacramento," indicates a California DDS release. "The trespassers ransacked files, vandalized and stole state property, and started a fire. The Department has no evidence that personal and health information was compromised due to the incident."

Here's the good news: Though California DDS ascertained that paper documents and CDs were either "displaced or damaged" in the raid, fire, and aftermath, they also conceded that health IT was stolen, the release suggests. However, in light of the theft of electronic devices and hardware, the state agency attributed the diminished loss of PHI to physical safeguards it had in place to protect information. "Twelve state-owned laptop computers were also stolen, but the data on these computers cannot be accessed because they were encrypted to meet the highest federal security standards," notes the California DDS report.

Follow Federal Requirements to Avoid Problems

It's crucial to remember that the HIPAA Security Rule requires all covered entities (CEs) to abide by the "Physical Safeguards" section or risk censure. In fact, "physical security is an important component of the HIPAA Security Rule that is often overlooked," says the OCR in the May 2018 issue of its Cybersecurity Newsletter. The agency stresses, that "what constitutes appropriate physical security controls will depend on each organization and its risk analysis and risk management process."

Nuts and bolts: The HIPAA Security Rule refers not only to the protection of devices but also the actual medical office, too. "Physical safeguards are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion," the OCR guidance reminds.

"Facility access controls, workstation use, workstation security, and device and media controls" are required of CEs in the Rule. These requirements cover a broad range of standards but may include:

- **Device inventories.** Providers must know what devices and hardware are on the premises and being utilized as well as where they are located in the office.
- **Authorization lists.** Who can and cannot access the building, workstations, and mobile devices must be clearly outlined.
- **Physical controls.** This refers to door locks, security guards and companies, alarm systems, secure rooms, encryption and authentication, passwords, and privacy implementations.
- **Policies, monitoring, and repercussions.** A major factor after a breach is evidence that a practice or hospital had HIPAA-compliant policies in place to protect the facility, the technology, and the ePHI.

Warning: Steep penalties may ensue if you don't have your ducks in a row. "Through recent settlements, the OCR has demonstrated its propensity to impose significant fines on entities that fail to implement appropriate safeguards, independent of the number of affected individuals or the content of the protected health information included in a particular breach," reminds attorney **John E. Morrone, Esq.**, a partner at Frier Levitt Attorneys at Law in New York.

Don't Be Fooled - Physical Security Is Still Important

A belief exists that suggests hacking presents a much higher risk of a data breach than physical security problems.

Reality: This is one of the biggest myths when it comes to healthcare security compliance, states **Thomas Lewis, CISSP, CISA, QSA**, shareholder in a blog posting for LBMC Information Security. "Data can be stolen in many ways, not just over a compromised network."

"Hospitals and other large clinical settings are targets of opportunity for thieves looking for personal information," Lewis warns. "Because these facilities are built for public access, protecting the data inside is not their primary objective."

Best bet: Prioritize strengthening physical security controls and network security, including "preventing unauthorized physical access to secure areas as well as preventing outright physical theft," Lewis advises.

To read the details on California's DDS breach, visit www.dds.ca.gov/SecurityNotice/.