COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 24, Number 2. February 08, 2024 When It Comes to Security Compliance, Don't Neglect Facilities; Audits Can Help

By Nina Youngstrom

Ransomware may grab the headlines but covered entities (CEs) should also be sensitive to physical security vulnerabilities and relevant requirements in the HIPAA Security Rule.

"Physical safeguards are part of the three-legged stool—physical, technical and administrative safeguards," said Robert Trusiak, an attorney in Buffalo, N.Y. Technical safeguards get the most attention because they relate to the "electronic security that you're wrapping your cybersecurity infrastructure around," he said. "Everyone talks about technical and to a lesser extent administrative safeguards, and often people don't spend any time on physical safeguards. But you need to be mindful of it."

Hospitals are also vulnerable because of the paper they still have lying around and the continued use of fax machines that are unencrypted, said attorney Sharon Klein with Blank Rome in Irvine, Calif. Suppose an unauthorized person gains access by tailgating their way through the front door or steals an access card. They may be able to get their hands on protected health information, she said.

"You walk into institutions and there's paper everywhere and there's fax machines that are unencrypted," Klein said. The HIPAA headlines are about digital failures and hacks, but "most hospitals can't get rid of paper. The boxes of paper should be shredded."

Piedmont Healthcare conducts annual audits of its physical security safeguards, according to Debra Harris and Lisa Anderson, senior IT internal auditors at the Georgia health system. The audits are performed with the physical security and safety departments at every Piedmont facility on a rotating basis, according to the audit plan. The environment for physical security changes all the time, Harris and Anderson noted, and everybody at every organization is responsible for protecting it.

Piedmont's audits are guided by an internal control questionnaire that employees complete to assist the person in charge of this business area in conducting a self-assessment of the adequacy of internal controls in place to ensure adequate monitoring procedures for physical security.[2] In addition, the following are items they look for during audits:

- "Site exterior is landscaped to facilitate natural surveillance and deter crime.
- "Warning signs or notices are posted to serve as a psychological deterrent to criminals lurking around the property.
- "Vehicular and pedestrian traffic into nonpublic areas of the site is restricted and controlled.

- "Fences are erected to deter intruders from gaining access to the site from outside the site's exterior perimeters.
- "Critical areas are well illuminated to deter crime and loitering around the facility.
- "Security guards regularly patrol theperimeters of the site and critical assets in public areas to watch for suspicious activities and deter intruders.
- "Site perimeters are equipped with physical intrusion detection and alarm systems that automatically detect suspicious activities and alert monitoring personnel/systems to take immediate action.
- "Walls, doors and windows are hardened to prevent forced entry and other types of threats (such as projectiles and blasts).
- "ID badges (and other types of ID tokens) are used to identify individuals, associate access authority with the identified person and control access through integration with physical access devices.
- "Authorization is required for entry to all nonpublic areas within the facility.
- "Physical access devices (card readers, biometric devices, etc.) have been implemented to allow access to authorized personnel while keeping out unauthorized personnel.
- "Physical intrusion detection systems are utilized to detect unauthorized entry to and/or presence in security areas that require protection.
- "Individuals, vehicles or delivery packages entering/leaving restricted or sensitive areas of the facility are searched for possible concealed, prohibited items.
- Surveillance systems are used to monitor sensitive/controlled work areas for unauthorized/inappropriate actions or suspicious behaviors.
- "Classification schema based on security profiles of different workspace areas is used.
- "How is staffing determined? Are there staffing concerns? What improvements can be made? This is determined by having discussions with various security personnel."

Contact Anderson at lisa.anderson@piedmont.org, Harris at debra.harris1@piedmont.org, Trusiak at robert@trusiaklaw.com and Klein at sharon.klein@blankrome.com.

A version of this story originally appeared in *Report on Medicare Compliance*, *RPP*'s sister publication. For more information, visit hcca-info.org/RMC.