Preventing Security Breaches With Physical Safeguards

Data breaches in healthcare are increasingly common and costly, and it is well known that patient health records — with their wealth of information — are a valuable asset for identity thieves and cybercriminals.

Discussions about data breaches often focus on technology-based safeguards for preventing loss or theft of protected health information (PHI) and electronic PHI (ePHI). However, physical safeguards also are a critical component of a sound security strategy and a requirement under the HIPAA Security Rule.

The HIPAA Security Rule stipulates that covered entities and business associates must "Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users."[1] Workstations include desktop computers and portable electronic devices (e.g., laptops, tablets, and smartphones). Additionally, electronic media is covered as part of the HIPAA Security Rule.[2]

In a cybersecurity newsletter, the U.S. Department of Health and Human Services Office for Civil Rights stated that, "While the latest security solutions to combat new threats and vulnerabilities get much deserved attention, appropriate physical security controls are often overlooked. Yet physical security controls remain essential and often cost-effective components of an organization's overall information security program."[3]

The risk tips in this publication focus on strategies for physically safeguarding PHI and ePHI as well as other proprietary information. For more information about technology-based solutions for preventing data breaches, see *Risk Tips: Preventing Security Breaches With Technology-Based Safeguards*.

1. As part of your organization's security risk assessment, review physical security measures to determine potential areas of vulnerability. (**Note:** HIPAA requires covered entities and their business associates to conduct risk assessments.[4])

2. Include physical security measures in your organization's written security plan as well as staff accountabilities for implementing and following policies related to physical safeguards.

3. Keep an up-to-date inventory of all electronic devices, where they are located, and their function. Move devices that are located in areas that might be vulnerable to theft or where inadvertent disclosure of information might occur.

4. Lock any storage areas that house electronic equipment and media that contain proprietary and sensitive information. Determine who is authorized to access these areas and who will maintain the keys or access codes.

5. Strictly prohibit employees from sharing passwords and placing written passwords in easily accessible locations (e.g., taped to a computer monitor or placed in an unlocked desk drawer).

6. Implement physical security features, such as cameras, alarms, door and file locks, and privacy screens for computer monitors. Position monitors so that they face away from public view.

7

Document implementation of physical security features as well as repairs, upgrades, or changes to physical aspects of the facility that are associated with security.

8

Ensure that your organization's policies clearly prohibit employees from removing devices containing ePHI (e.g., laptops, tablets, etc.) from the facility, unless specifically required. The policy also should stipulate that when employees remove devices from the facility with approval, they should never leave the devices in vehicles.

9

Develop protocols for disposal of electronic devices, media, and hardcopy records and information. Ensure staff members are aware of the protocols and best practices, and monitor for compliance.

10

Limit the number of people who have keys or access codes to the facility or restricted areas of the facility; do not give keys to employees who have not passed probationary periods.

11

Restrict entry to areas of the facility where patient data can be accessed; implement these restrictions during times when the areas are not in use or outside of business hours.

12

Stipulate the return of keys and facility-issued identification or access badges from employees who quit or are terminated. Employees who are fired should turn in their keys and badges immediately upon termination, and badges should be deactivated. They should not be given the opportunity to access any patient- or business-related information.

13

Change locks and access codes on facility doors if any former employees pose legitimate concerns about unauthorized access.

14

Post signs to remind employees, patients, and visitors about security policies and monitoring as well as the organization's commitment to privacy and confidentiality.

15

Include physical security as part of the organization's overall security training for employees, contractors, vendors, and volunteers during orientation and in-service trainings.

16

Periodically audit organizational security policies for compliance, and take corrective action as needed.

Endnotes

[1] 45 C.F.R. § 164.310(c)

[2] 45 C.F.R. § 164.304

[3] U.S. Department of Health and Human Services, Office for Civil Rights. (2018, May). *Workstation security: Don't forget about physical security*. Retrieved from www.hhs.gov/sites/default/files/cybersecurity-newsletter-may-2018-workstation-security.pdf

[4] The Office of the National Coordinator for Health Information Technology. (n.d.). *Privacy, security, and HIPAA: Security risk assessment tool.* Retrieved from www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment