Report on Medicare Compliance Volume 32, Number 35. October 02, 2023

HIPAA Physical Security May Be Ripe for Audit Despite Fewer Cases

By Nina Youngstrom

Ransomware may grab the headlines in the HIPAA security world, but covered entities also should 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, New York. 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.” If the HHS Office for Civil Rights (OCR) investigates a breach sparked by malware, for example, “it will focus on all three safeguards.”

The HIPAA Security Rule requires covered entities to have physical safeguards. They’re defined as “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,” according to HHS.[1] They cover facility access controls, workstation use, workstation security and device and media controls. “This may extend outside of an actual office, and could include workforce members’ homes or other physical locations where they access EPHI [electronic protected health information].”

This document is only available to subscribers. Please log in or purchase access.

Purchase Login

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website’s Terms of Use.