BECAUSE WE CARE, WE'RE HIPAA AWARE

HIPAA ADVISOR

AUGUST 25 , 2017 JOYCE HIBEN, PRIVACY OFFICER VOLUME 1 WEEK 2

OSWEGO COMMUNITY HOSPITAL
HIPAA NEWSLETTER

Greetings Colleagues,
This edition of the weekly HIPAA Advisor will provide feedback from the Physical Access Control and Validation Procedures Checklist that was completed last week and explain what our organization must do to comply with the associated federal laws and the HIPAA Omnibus STANDARD.

Background

An important step in protecting electronic health information (EPHI) is to implement reasonable and appropriate physical safeguards for information systems and related equipment and facilities. As we learned last week, 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 intrusions". The Physical Access Control and Validation Procedures Checklist that was completed last week provided an evaluation of the security controls already in place and an opportunity to address the physical vulnerabilities identified.

Questions to consider?

Are policies and procedures developed and implemented that address allowing authorized and limiting unauthorized physical access to electronic information systems and the facility or facilities in which they are housed?

Do the policies and procedures identify individuals (workforce members, business associates, contractors, etc.) with authorized access by title and/or job function?

Do the policies and procedures specify the methods used to control physical access such as door locks, electronic access control systems, security officers, or video monitoring?

DO WE HAVE POLICIES?...We will

HIPAA GUARD

REBOOT INC
KEEPING COMPUTING SIMPLE

Our organization must create and maintain a Facility Security Plan that documents the procedures to safeguard access to the facilities, information systems, and equipment used to store EPHI. The plan is to outline access to areas within the facility by job description, give special attention the security of the server room, and outline methods used to ensure that PHI and EPHI are not viewable to visitors.

The Facility Security Plan addresses Contingency Operations that allow access during emergencies that supports our Disaster Recovery Plan, Access Control and Validation procedures for workforce members, Physical Access Controls to limit access based on need to view and restrict access to software for testing and revision, and to ensure that all maintenance records for the facility, such as repairs and modifications are documented and maintained.

"I heard the new HIPAA Omnibus Rules are a whole lot tougher on business associates."

Breach Example

An employee lost a mobile computer drive resulting in a breach of protected health information (PHI) affecting 600 individuals. The types of PHI involved in the breach included names, addresses, dates of birth, social security numbers, and clinical information. Following the breach, the CE sanctioned the responsible employee, retrained employees about security awareness and implemented administrative and technical safeguards, including malware protection and encryption. As a result of OCR's investigation, the CE completed a thorough risk analysis and developed a risk management plan.