BECAUSE WE CARE, WE'RE HIPAA AWARE

HIPAA ADVISOR

AUGUST 18 , 2017 JOYCE HIBEN, PRIVACY OFFICER VOLUME 1 WEEK 1

OSWEGO COMMUNITY HOSPITAL
HIPAA NEWSLETTER

Greetings,
This edition of the weekly HIPAA Advisor contains resources and information related to HIPAA Compliance and Physical Security. Please continue reading for details about upcoming steps to improve compliance in our facility.

This week the Privacy Officer, Joyce Hiben, will be conducting a walkthrough of the facility to complete a Physical Access Control Checklist to provide information to our HIPAA GUARD partners related to physical safeguards.

What are HIPAA physical safeguards?

As stated in the HIPAA Security Series, 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."*

What are Facility Access Controls?

The first standard under the Physical Safeguards section is Facility Access Control. It requires covered entities to:

"Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed."

A facility is defined in the rule as *"the physical premises and the interior and exterior of a building(s)".*

HIPAA GUARD

REBOOT INC
KEEPING COMPUTING SIMPLE

"Our HIPAA compliance program made great progress last year. We finally managed to get everyone to spell HIPAA correctly."

What is a FACILITY SECURITY PLAN?

The Facility Security Plan defines and documents the safeguards used by the covered entity to protect the facility or facilities.

Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

"Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft."

To establish the facility security plan, covered entities should review risk analysis data on persons or workforce members that need access to facilities and equipment. This includes staff, patients, visitors and business partners.

Some common controls to prevent unauthorized physical access, tampering, and theft that covered entities may want to consider include:

- Locked doors, signs warning of restricted areas, surveillance cameras, alarms
- Property controls such as property control tags, engraving on equipment
- Personnel controls such as identification badges, visitor badges and/or escorts for large offices
- Private security service or patrol for the facility

What are ACCESS CONTROL AND VALIDATION PROCEDURES?

The Facility Access Controls standard also includes the Access Control and Validation Procedures implementation specification. Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

"Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision."

The purpose of this implementation specification is to specifically align a person's access to information with his or her role or function in the organization.

Breach Example

An employee of the covered entity (CE), Salina Family Healthcare Center, sent an email containing electronic protected health information (ePHI) to a third party as part of a research case study. The types of PHI involved in the breach included names, dates of birth, addresses, chart numbers, and procedure codes affecting approximately 9,640 individuals. The CE provided breach notification to HHS, affected individuals, and the media. The CE responded to the breach by obtaining assurances that the email was destroyed by the third party, and sanctioning the responsible employee. As a result of OCR's investigation, the CE updated and trained staff on its policies relating to the e-mailing of PHI and uses and disclosures of PHI.