Can door hardware help you meet HIPAA guidelines?

By Ann Geissler Timme, Allegion

HIPAA – the Health Insurance Portability and Accountability Act – legislates how a patient's information is managed, viewed, documented, and transported in both inter- and intra-office settings. The law protects both physical and electronic data and documents. Not only does the law require patients' medical history be protected, but it has also forced organizations with access to this information to assess security needs and gaps, and develop/implement policies, procedures, and practices that will ensure they are meeting their obligations. Both physical and logical security must be included in this process.

Healthcare organizations are accountable for the actions (or inaction) of their employees. This includes:

- Designating a privacy official, the person responsible for your HIPAA compliance program
- Identifying all information that must be protected
- Determining who should have access to documents and data elements
- Defining under what circumstances they may view this information
- Establishing how the information must be protected from inadvertent viewing or disclosure
- Clarifying when and how information may be shared internally and externally
- Providing and documenting training to all staff authorized to use this information
- Testing and identifying security gaps
- Defining how processes will be audited to ensure compliance
- Defining a course of action for incident investigation
- And many other requirements

To accomplish these tasks and assure compliance, employers have implemented extensive training and audit programs and enhanced physical security efforts in many areas.

The buzz word around healthcare provider offices regarding patient document security is HIPAA Compliance. Since HIPAA addresses information security from a comprehensive perspective, every place this information resides or passes through, both physically and electronically, must be protected. The difference between being

HIPAA Compliant and being in violation of these laws could come down to something as simple as the whether or not a door closes and locks properly.

Physical records need to be in secured areas. Doors and locks into these areas should be inspected frequently to assure their functionality. Simply having a lock on a door is not sufficient. The lock must perform as intended. Entry management, whether through the use of keys (high security patented keyways) or electronic access control, should ensure that only authorized personnel have access. Doors should open and close smoothly. Locks must work properly. Access rights need to be managed closely. And hinges should be sturdy and if on the public side of the door, effectively secured. Ensuing that the entire opening is fully functional is one of the foundation elements of compliance.

Not only do openings and their locking mechanisms need to be functioning as intended - but some doors must also be alarmed, viewed by CCTV, or staffed at all times. Your organization's HIPAA compliance officer will determine which areas require enhanced security technology.

User protocols

At the user level, offices need to establish a protocol that covers day-to-day operations. The protocols should be able to identify which employees have access to patient information and to what extent employees are allowed access. Who is allowed to retrieve the information, who is allowed to distribute the information, and who is allowed to transmit the information to other agencies and bodies must be defined.

Access protocols

The protocols need to do more than establish who has access to the information, they need to establish how the information is accessed. Using an advanced key-based solution that have a patented keyway system is a sufficient basic solution. Such a system allows administrators to keep track of key holders and significantly reduces problems associated with unauthorized key duplication.

A more popular and advanced security option is the adoption of an electronic access control system. Electronic security can come in a variety of options. From an offline PIN code lock to a wireless electronic lock or wall reader used with smart cards and connected to an access control system with integrated video cameras. With an electronic solution, administrators can restrict user access to specific days and times. And unlike a key-based system, an electronic system will log user entry through openings. This audit trail can be used by administrators to help ensure compliance or investigate breaches.

Inspect yourself

Proactively monitoring, testing, and updating a facility's hardware, policies, and procedures goes a long way in maintaining HIPAA compliance. Security and compliance is the responsibility of not only the security department or risk assessment office, but of every staff member authorized to access these records. Staff should be expected to identify hardware failures such as doors that do not close or locks that are not working and initiate repair.

Ensuring HIPAA compliance is a complex and continuous process requiring the participation of every staff member. Fully functional doors and locking systems are an important aspect of this effort.

Learn more about HIPAA

For more information about preparing your organization for HIPAA requirements, please contact a professional security consultant in your area by calling **888.758.9823** or fill out the **Contact Us** form on our website at allegion.com.

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 7,800 people and sells products in more than 120 countries across the world. Allegion comprises 23 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®.

For more, visit allegion.com/us

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

009606, Rev. 03/14
allegion.com