May 01, 2012

How Door Hardware Helps Hospitals Meet HIPAA Guidelines

Being compliant could come down to whether or not a door closes and locks properly.

Written by: A member of the Allegion Healthcare Marketing Team

The Health Insurance Portability and Accountability Act (HIPAA) legislates how a patient’s information is managed, viewed, documented and transported in both interoffice 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, it has also forced organizations with access to this information to assess security needs and gaps, prodding them to 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 held accountable for the actions (or inactions) of their employees and business partners. This includes:

- Designating a privacy official, the person responsible for the 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

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 phrase around healthcare provider offices regarding patient document security is “HIPAA Compliance.” The difference between being HIPAA compliant and being in violation of these laws could come down to something as simple as whether or not a door closes and locks properly. Since HIPAA addresses information security from a comprehensive perspective, every place this information resides or passes through, both physically and electronically, must be protected.

Physical records need to be in secured areas. Doors and locks to 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 brass keys (high security patented keyways) or electronic access control systems, should ensure that only authorized personnel have access.

Doors should open and close smoothly. Locks must work properly. Hinges should be sturdy and, if on the public side of the door, effectively secured. Ensuring that both doors and locks are fully functional is one of the foundations of compliance.

Not only do openings and their locking mechanisms need to be functioning as intended, some doors must also have the ability to be audited, viewed by CCTV or staffed at all times. The organization’s HIPAA compliance officer will determine which areas require enhanced security technology.

On a 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 guidelines.

Access protocols need to do more than establish who has access to the information; they must establish how the information is accessed. Using an advanced key-based solution that has 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 credential and network options, from offline PIN code locks on the door to wireless locks and card readers. With an electronic solution, administrators can restrict user access to specific days and times. 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 a breach.

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 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.

It’s important that employees understand HIPAA regulations. Periodic training will make the staff aware of what is proper and allowable. They will be able to spot violations of the regulations, knowing what to look for and how to report violations.
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.