

HIPAA Security Compliance: Protects Confidential Patient Health Information

The stringent HIPAA security compliance norms make it mandatory for all the entities like hospitals, insurance providers, payers, billing services, insurance plans and medical personnel to strictly adhere to the laws relating to the safe transfer and storage of confidential patient health information. To achieve HIPAA security compliance it is necessary to implement few steps that have been categorized below:

Establish Physical Safeguards:

Computer networks play a crucial role in processing, storage and exchange of health records of patients between different health care entities. The physical access to crucial information can be safely managed by following these steps:

- ❖ Creating and implementing a policy that authorizes only limited and trusted people to access the confidential patient health data.
- ❖ Installing workstations and computers in safe areas of the facility, which is accessed by authorized personnel. Devices like computers, fax, printers and copiers should be placed in such a manner so that unwanted people view data inside them.
- ❖ All the computer programs should be protected by passwords and user ids to prevent, unauthorized access. The passwords should be securely managed so that unwanted people cannot access them.
- ❖ A security system should be in place so that it manages passwords efficiently and guarantees the safety of patient health information when the staff members change positions or somebody leaves the organization.
- ❖ All the storage devices, backup tapes and computer equipment should be accounted for by maintaining a proper log book that keeps track on them.
- ❖ All paper documents that contain critical information, but not needed in the office should be shredded so that no body else can lay hand on it.

Enhance Computer Network Security

It is necessary to maintain a proper record of the hardware and software employed in the facility, and understand their role in processing the patient health information, safely. Risk analysis should be done by creating a flow diagram of the work process so that loopholes in the system can be identified and removed. The computer network should be protected from virus attack or hacking by adopting some security measures mentioned below:

- ❖ Appropriate gateway security with capacity to deeply inspect the web content and filter out unwanted elements like debilitating software and virus should be, placed.
- ❖ Anti virus solutions, digital signatures, firewalls should be in place to negate any debilitating online threat.
- ❖ Proper encryption procedure should be followed, while sending out crucial health data from the organization network to the public network. The information should be strongly encrypted to protect it from unauthorized access or intercept.

- ❖ The network security system should continuously monitor the network for any suspicious activity that indicates an unexplained deviation from the standard procedure and raise an alarm.

Educate Staff on HIPAA Security Compliance

A well trained staff forms the backbone of the successful organization. It is of utmost importance for an organization to increase the awareness about the importance of safe handling the patient health information. It protects the healthcare facility from lawsuits due to non compliance of HIPAA norms by an employee or employees. The organization should:

- ❖ Provide staff access to HIPAA compliant training courses and seminars to increase awareness about importance of compliance norms.
- ❖ Provide training in password management and virus protection.
- ❖ Train on how to efficiently maintain logs and audits
- ❖ Carry out periodic review of employee's HIPAA security compliance and update their training to hone their skills in managing safely, the patient health information.
- ❖ Provide training on operating the backup system as per contingency plan in case of natural or manmade disaster with the aim to protect the health data and keep crucial operations running.

Hence for an organization to achieve the requisite HIPAA security compliance, it is necessary to integrate smoothly the software, hardware and personnel so all of them work in a cohesive manner, ably guided by an administration that continuously monitors, provides feedback and places safeguards to ensure safe handling of the crucial health information of the patient.

About emPower

emPower e-learning solutions, with offices in US and India, provides end-to-end e-learning services, with strong focus on quality assured online compliance training content for the healthcare professionals. We provide a Learning Management System (LMS) and an array of courses including those mandated by government and other regulatory bodies such as OSHA (Occupational Safety and Health Administration), HIPAA (Health Insurance Portability and Accountability Act), Joint Commission and Red Flag Rule.