

Enhancing Computer Network Security to Achieve HIPAA Compliance

Secure Computer networks are intrinsic part of the HIPAA strategy to completely convert the national patient health records into an electronic format that can be easily exchanged between different agencies like health care providers, insurance providers, and administrators. As a result the health care organizations can manage documentation process efficiently in minimal time and provide better service to the patients. But the present day computer system is prone to hacking and virus attacks, which steal or destroy the crucial data. To protect the patient health information there are network security rules that need to be followed so that the organization is able to achieve HIPAA compliance.

There are two main sections of HIPAA that relate to computer network security and they are:

Administrative Safeguards:

To achieve HIPAA compliance, it necessary for the provider to identify, guard and report against malicious software program in the system. The infected email carry with them worms, virus and Trojans and there should be a security system in place that checks for such unwanted entry. To manage the computer networks smoothly, it is necessary to maintain a vigil by installing special safeguards mentioned below:

- Gateway and desktop anti-virus products should be used.
- The security gateway should be able carry out, deep-packet-penetration, inspection and provide appropriate web filtering capabilities to the network.
- Signature files that update at every 30 minutes should be used, as they are best form of defense against the fast moving worms.
- All the security services and subsystem should be proactive with IPS (Intrusion Protection System) instead of IDS (Intrusion Detection System). This is necessary to protect the network from being infected with virus.
- The installed firewall should provide protection from the top 50 Dos and DDos well known attacks. The installed security system should register the number time the attacks have been made and counter them effectively.

Security Safeguards:

For a computer network to attain HIPAA compliance it is necessary for the organization to frame security policy that make it mandatory for only the authorized personnel or software programs to have the access rights to protected health information

- The security device should support native form of authentication. For web related applications, Transparent Authentication should be used so that a same user who moves to different secure applications does not have to sign-in, his or her, username and password, every time he or she makes a jump.
- The security system should support email content filtration process with keywords and regular expression string features.

- To prevent, unauthorized access or intercept, of the patient health information when it on journey between sender and receiver, proper encryption techniques should be used. The transport of the PHI to public network should be done in strong encryption mode and received by authenticated users, who should have the requisite deciphering codes.
- The security system should continuously monitor for any unwanted or suspicious deviation from the standard procedure and report anomalous activity immediately to IT manager.
- Special security features like email content filtering application and digital signatures should be added in the system to prohibit dispatch of safe data to unverified receivers.

In the end it is necessary for all the entities that are involved in health care system like, health service providers, insurance companies, transcription service providers, payers, labs, internet service providers, hospitals and billing services to build a chain of trust so that any patient health information routed between them is kept high confidential. This can be done through a network of computer systems that strictly adhere to HIPAA compliance norms to facilitate a safe and secure transmission of confidential health information on public network.

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.