HIPAA Rules and Regulations: Security

The Security Standards were issued on February 20, 2003 but went into effect on April 21, 2003 with a compliance date of April 21. The Privacy Rule pertains to all Protected Health Information (PHI) including paper and electronic, the Security Rule deals specifically with Electronic Protected Health Information (ePHI). HIPAA Rules and Regulations lay out three types of security safeguards required for compliance: administrative, physical, and technical. For each of these types, the Rule identifies security standards, and for each standard, it names both required and addressable implementation specifications. Required specifications must be adopted and administered as dictated by the Rule. Addressable specifications are more flexible. Individual covered entities can evaluate their own situation and determine the best way to implement addressable specifications. The HIPAA Rules and Regulations standards and specifications are as follows:

- Administrative Safeguards – Policies and procedures designed to clearly show how the entity will comply with the act

- Covered entities must adopt a written set of privacy procedures and designate a privacy officer to be responsible for developing and implementing all required policies and procedures.
- The policies and procedures must reference management oversight and organizational buy-in to compliance with the documented security controls.
- Procedures should clearly identify employees or classes of employees who will have access to electronic protected health information ePHI. Access to ePHI must be restricted to only those employees who have a need for it to complete their job function.
- The procedures must address access authorization, establishment, modification, and termination.
- Entities must show that an appropriate ongoing training program regarding the handling of PHI is provided to employees performing health plan administrative functions.
- Covered entities that out-source some of their business processes to a third party must ensure that their vendors also have a framework in place to comply with HIPAA requirements. Companies typically gain this assurance through clauses in the contracts stating that the vendor will meet the same data protection requirements that apply to the covered entity. Care must be taken to determine if the vendor further out-sources any data handling functions to other vendors and monitor whether appropriate contracts and controls are in place.
- A contingency plan should be in place for responding to emergencies. Covered entities are responsible for backing up their data and having disaster recovery procedures in place. The plan should document data priority and failure analysis, testing activities, and change control procedures.
- Internal audits play a key role in HIPAA compliance by reviewing operations with the goal of identifying potential security violations. Policies and procedures should specifically document

the scope, frequency, and procedures of audits. Audits should be both routine and event-based.
- Procedures should document instructions for addressing and responding to security breaches that are identified either during the audit or the normal course of operations.

- Physical Safeguards – controlling physical access to protect against inappropriate access to protected data:

- Controls must govern the introduction and removal of hardware and software from the network. When equipment is taken out of service it must be disposed of properly to ensure that PHI is not compromised.

- Access to equipment containing health information should be carefully controlled and monitored.
- Access to hardware and software must be limited to properly authorized individuals.
- Required access controls consist of facility security plans, maintenance records, and visitor sign-in and escorts.
- Policies are required to address proper workstation use. Workstations should be removed from high traffic areas and monitor screens should not be in direct view of the public.
- If the covered entities utilize contractors or agents, they too must be fully trained on their physical access responsibilities.

- Technical Safeguards – controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient.

- Information systems housing PHI must be protected from intrusion. When information flows over open networks, some form of encryption must be utilized if deemed appropriate and possible. If closed systems/networks are utilized, existing access controls are considered sufficient and encryption is optional.
- Data integrity must be maintained, including the use of check sum, double-keying, message authentication, and digital signature may be used to ensure data integrity.
- Covered entities must also authenticate entities with which they communicate to include: password systems, two or three-way handshakes, telephone callback, and token systems.
- Covered entities must make documentation of their HIPAA practices available to the government to determine compliance.
- In addition to policies and procedures and access records, information technology documentation should also include a written record of all configuration settings on the components of the network s.
- Documented risk analysis and risk management programs are required. Covered entities must carefully consider the risks of their operations as they implement systems to comply with the act.