



Using ISO17799 for Your HIPAA Security Compliance Program

Even though the final rule for HIPAA security is still two months away, mapping your effort to ISO17799 will move you significantly closer towards compliance. ISO17799 is a detailed security standard that focuses on the confidentiality, integrity, and availability of information and is organized into ten major sections: asset classification and control, access control, physical and environmental security, business continuity management, system development and maintenance, compliance, personnel security, organizational security, communications and operations management, and security policy. Utilizing ISO17799 as a guideline for your HIPAA Security Compliance Program is smart business. Let's take a look.

HIPAA security is grouped into four categories: Administrative procedures - documented, formal practices to manage the selection and execution of security measures to protect data and the conduct of staff relative to the protection of data; Technical security services - control and monitor information access; Technical security mechanisms and electronic signatures - prevent unauthorized access to data that is transmitted over a network; and Physical safeguards - protect physical computer systems, related buildings and equipment.

HIPAA Security Administrative Procedures - (maps to ISO17799 Organizational Security, Security Policy, Compliance, Personnel Security, Business Continuity Management) – As stated in ISO17799, corporate security policy must be driven from the top. This ensures a broad approach and demonstrates the senior level commitment necessary to succeed. An overall security policy with clear objectives and intent needs to be crafted. This document should include the corporate principles for security, guidelines, standards and regulatory/legislative compliance requirements that pertain to the organization. It should also discuss internal organization cooperation, auditing procedures, training and awareness policies, roles and responsibilities, background checks and screening, confidentiality and employment agreements, disciplinary process, business continuity and disaster recovery policies and procedures, malicious software and hacking prevention, detection, and response, as well as how to deal with security violations. This high level document is supplemented by other more specifically detailed policies and procedures (developed by legal, human resources, IT) that includes all relevant statutory, legislative, regulatory, and contractual requirements. These administrative procedures must be communicated, supported and physically demonstrated from the top. They must have independent review from an objective, knowledgeable, third party. ISO17799 defines the groundwork necessary for a solid approach to the administrative procedures.

HIPAA Technical Security Services and Security Mechanisms - (maps to ISO17799 Asset Classification and Control, Access Control, Communications and Operations Management, & Systems Development and Maintenance) – If you don't know what information assets you have how can you ensure they receive an appropriate level of protection? Once asset inventory is complete, it is time to utilize information security policies to classify this information. This includes the consideration of business needs for the sharing of information, restrictions upon information, and the impact unauthorized access or disclosure will have upon you, your organization and your patient. Information needs to be labeled based upon sensitivity while keeping integrity and availability in mind. ISO17799 recommends that you consider the following “What must be generally forbidden unless expressly permitted,” when defining access control rules and rights for all internal personnel and groups. Unauthorized access to information should be controlled and prevented. If penetration does occur, detection and the ability to act quickly and effectively can minimize the damage.

In order to prevent the loss, modification and/or misuse of patient information, security must be a part of and built into your operational systems. Systems failure risk must be assessed to ensure the availability and integrity of patient information. All projects need to follow a standard secure project methodology as a norm. This is needed in every aspect of handling information throughout the company, in software development and deployment in order to minimize risks. The pervasive nature of information security needs to be recognized and practiced as defined in ISO17799. The processing of this information must prevent loss, modification or misuse during the intended exchanges between organizations. Proper security of any type of data transmission or information exchange must be deployed. ISO17799 provides a common basis for effective technical services and mechanisms.

HIPAA Physical Safeguards (maps to ISO17799 Physical and Environmental Security) - Physical security concerns are instituted to prevent unauthorized access, damage and interference to business premises and information as well as the loss, damage or compromise of assets and interruption to business activities. ISO17799 physical security guidelines address the potential compromise or theft of information, and information processing facilities. Sensitive patient information should be housed in secure areas, protected by a defined perimeter, with appropriate security barriers and entry controls. Once the risks associated with this sensitive information are identified, the proper protection can be employed. ISO17799 delivers the information necessary to physically protect patient data against internal and external threats.

Employing ISO17799 standards to the four HIPAA security categories provides a synergistic and layered approach to protecting information assets. It is internationally accepted, proven, comprehensive, and the intense roadmap you need for HIPAA security compliance. It is amazing how much patient information is shared. Ensure you protect it. Use ISO17799.

Jeff Bardin is the chairman and CTO of Treadstone 71. Jeff can be reached at jbardin@treadstone71.com