TMA Privacy Office Information Paper

HIPAA and the Acquisition Process

45 CFR §164.316

Compliance with the Health Information Portability and Accountability Act (HIPAA) Security Rule requires the integration of people, processes, policies and procedures, and products into an organizational system designed to protect the confidentiality, integrity and availability of the electronic protected health information (ePHI) the Military Health System (MHS) collects, uses and maintains. Ensuring the automated information systems (AIS) purchased by MHS support and enable compliance with the HIPAA Security requirements is essential to meeting that goal. This paper provides guidance to ensure that technical security requirements which support HIPAA compliance are included in the acquisition process.

CHARACTERISTICS OF HIPAA TECHNICAL STANDARDS

The standards and implementation specifications found in the HIPAA Security Rule and the Department of Defense (DoD) documents promulgated to implement that rule, are designed to be flexible and scalable. Those included under the technical safeguards category enforce the policies and procedures developed to implement the administrative safeguards. They are non-technology specific. They tell you what to do; not how to do it. This allows for differences in platforms, infrastructure, business needs and processes. As the technical environment continues to change and develop new capabilities, the characteristics of the HIPAA technical standards allow you to adopt new technology to meet your changing business and security needs and still remain compliant with the HIPAA requirements.

CHOOSING TECHNICAL REQUIREMENTS TO SUPPORT HIPAA COMPLIANCE

Services and their Military Treatment Facilities (MTFs) must evaluate their approach to security compliance in light of the mission, budget, other relevant laws and regulations and good information assurance practices. Protection strategies and tactics may vary in organizations depending on size, complexity and capabilities, the hardware and software security capabilities of the technical infrastructure, the cost of security measures and the probability and criticality of potential risks. The DoD Health Information Security Regulation, the draft regulation implementing the HIPAA Security Rule, emphasizes the important role of risk assessments in establishing compliance with the HIPAA data security rules. This regulation was in coordination for signature at the time this paper was posted.

The first step in determining your specific technical requirements is to identify the risks to the information that will be collected, processed, transmitted or maintained by the

HIPAA and the Acquisition Process

45 CFR §164.316

acquired AIS. Identify a range of safeguards or controls that will mitigate those risks. Include controls that are required by other DoD and Service regulations and associate those controls with the appropriate HIPAA technical standards and implementation specifications as expressed in the DoD Health Information Security Regulation. Evaluate the controls' ability to mitigate the identified risks. For requirements identified as "addressable", evaluate whether the controls are reasonable and appropriate. If not, consider alternative safeguards that will achieve the same protection. Choose additional controls to reduce identified risks to an acceptable level and satisfy the requirements as needed. Include requirements for the chosen controls in the request for proposal (RFP) and other acquisition requirements documents. Finally, retain all documentation including the risk assessment, the identified requirements, how they satisfy the technical security standards presented below, and the rationale behind their selection for a period of six years.

HIPAA TECHNICAL SECURITY REQUIREMENTS

There are five technical standards and seven implementation specifications associated with those standards. They are:

Access Control Standard: Implement technical policies and procedures for information systems and electronic devices containing PHI that allows access only to those persons or software programs that have been granted access rights as specified in the policies implementing the information access management standard under the HIPAA Security Rule.

Unique User Identification Implementation Specification: Assign a unique name and/or number for identifying and tracking user identity.

Emergency Access Procedure Implementation Specification: Establish and implement, as needed procedures for obtaining necessary electronic PHI during an emergency.

Automatic Logoff Implementation Specification (Addressable): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Encryption and Decryption Implementation Specification (Addressable): Implement a mechanism to encrypt and decrypt electronic PHI at rest and during transmission as a means of controlling access to the electronic PHI.

HIPAA and the Acquisition Process

45 CFR §164.316

Audit Control Standard: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.

Integrity Standard: Implement policies and procedures to protect electronic PHI from improper or unauthorized access, use, disclosure, modification, alteration or destruction.

Mechanism to Authenticate Electronic PHI Implementation Specification: Implement electronic mechanisms to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner.

Person or Entity Authentication Standard: Implement procedures to verify that a person or entity needing access to electronic PHI is the one claimed. Install and use technical procedures that verify the identification and authentication of human users and other machines that transfer or request information.

Transmission Security Standard: Implement technical security mechanisms to guard against unauthorized access, use, disclosure, modification, alteration, or destruction to PHI that is being transmitted over an electronic communications network.

Integrity Controls Implementation Specification: Implement security mechanisms to ensure that electronically transmitted PHI is not improperly modified without detection.

Encryption Implementation Specification (Addressable): Encrypt electronic PHI in transit to protect the confidentiality and integrity of the data during transmission over a network or other electronic means.