



February 2002
OSD(HA), TMA, TMI&S

HIPAA - SECURITY

TRICARE Management Activity, Information Assurance Program Office, February 2002

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

Highlights

- ◆ HIPAA Overview
- ◆ Security Rule
- ◆ Administrative Procedures
- ◆ Physical Safeguards
- ◆ Technical Security Services and Mechanisms
- ◆ Resources

Overview

As a result of the enactment of HIPAA, healthcare entities in the United States will be required to substantially alter the way they transmit and protect the medical records of their patients and members. In general terms, HIPAA is not a voluntary initiative but is a mandate to protect the confidentiality, integrity, and availability of individual health information.

HIPAA contains three sets of administrative simplification standards (transactions and code sets, privacy and security and unique health identifiers). The rules governing transactions and code sets

and privacy have been finalized and published. Rules for a national provider identifier and national employer identifier have been proposed and are under review. Rules for a national health plan identifier and unique individual health identifier have been discussed but not proposed. The proposed security rule, in final coordination, is expected to be published in late Spring 2002. Following its publication in the Federal Register, healthcare entities will have 26 months to become compliant with the *HIPAA Security Rule*.

HIPAA compliance begins at the organizational level, and

in recognition of this the three Surgeons General have recommended that each Military Treatment Facility (MTF) form an interdisciplinary team, the Medical Information Security Readiness Team (MISRT).

MISRTs can utilize a DoD available risk assessment tool (Operationally Critical Threat Asset and Vulnerability Evaluationsm (OCTAVEsm)) and the provided training to assess and develop plans to manage threats and vulnerabilities to their MTF's critical information assets.

More information at: <http://www.tatrc.org/rimr>

HIPAA Security Rule

The HIPAA Security Rule has a different scope and purpose than the rules that deal with standard transactions and code sets. The security rule is designed to provide protection for all individually identifiable health information that is maintained, transmitted, or received in electronic form, not just the information in the standard transactions.

All clearinghouses and health plans must comply with HIPAA, while a provider must become

compliant only after having used one of the standard transactions. However, once a provider uses a standard transaction, they must continue to comply with the security rule even if they never use another standard transaction.

The security rule is divided into four categories:

- ◆ Administrative Procedures
- ◆ Physical Safeguards
- ◆ Technical Security Services
- ◆ Technical Security Mechanisms

Each category includes mandatory requirements and two types of implementation feature: mandatory and addressable. Grouping requirements and implementation features under a major rule elucidates the rule's intent and how it should be met.

The Golden Rule is you *must document everything!* What is documented must reflect what you actually do and it must be kept current and accurate.



TRICARE Management Activity

Technology Management,
Integration & Standards

INFORMATION ASSURANCE PROGRAM OFFICE

Skyline 5, Suite 810
5111 Leesburg Pike
Falls Church, VA
22041-3206

PHONE:
703-681-6866

FAX:
703-681-8814

E-MAIL:
hipaamail@tma.osd.mil

We're on the Web!

See us at:

[www.tricare.osd.mil/
imtr/default.htm](http://www.tricare.osd.mil/imtr/default.htm)



Synopsis

The Defense Health Information Assurance Program and its Policies, Procedures, and Practices (P3) Work Group have been working steadily to assess HIPAA's impact and comparability to current DoD and Service regulations. They have developed tools, provided basic OCTAVESM training and ensured advanced training is available to support the MISRTs. The membership has laid the groundwork for the MHS Security Working Integrated Project Team (WIPT) to plan the implementation.

In a nutshell, the proposed HIPAA security rule delineates administrative requirements and supporting implementation features. It requires that procedures be documented, periodically reviewed and made available to individuals responsible for implementing the procedures or content. It also allows some flexibility in how it is implemented but requires the rationale for any deviation to be documented.

Administrative Procedures

The "Administrative Procedures" category addresses the business processes that allow access to and protect the individually identifiable health information electronically maintained, transmitted, and/or received.

Of the eighteen major requirements dictated in the rule, half are in this category. This category emphasizes HIPAA as an organizational view of security. In order to be HIPAA compliant, information security must involve all of the ways that people handle and access the information found in the information technology systems.

Physical Safeguards

This category covers the use of administrative measures and other mechanisms to control physical access to computer systems and facilities. The "Physical Safeguards" category focuses on protecting buildings, computer rooms and computer hardware from the threats of fire and other natural and environmental hazards, intrusion, and physical destruction or damage by humans.

There exists some overlap with the "Administrative Procedures" category, however, this category emphasizes the facility and physical security aspects of those procedures.

Technical Security Services & Mechanisms

Both of these categories differ from the safeguards identified under "Administrative Procedures" because they generally function as technical security controls in concert with automated information systems. They usually entail computer execution of a security task as well as human implementation of a policy.

They differ from one another in that "Technical Security Services" involve protecting the information as it is being processed or maintained within the system, data at rest. "Technical Security Mechanisms" guard against unauthorized access to data that is transmitted over a communication network, data in transit.

To Find Out More...

Websites:

<http://www.tricare.osd.mil/hipaa>

<http://aspe.hhs.gov/admsimp>

<http://snip.wedi.org>