

HIPAA SECURITY STANDARDS

The purpose of the Security Standards is to implement national safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. The safeguards are designed to protect stored information from the risks of improper access and to prevent interception during electronic transmission. The deadline for compliance is April 20, 2005.

The security requirements include administrative, physical, and technical safeguards. A summary of the standards and some of the required specifications for implementation are listed below:

STANDARDS	IMPLEMENTATION SPECIFICATONS
ADMINISTRATIVE SAFEGUARDS	
Security management process Policies and procedures to prevent, detect, contain, correct security violations	~ Risk analysis Assess vulnerabilities, threats ~ Risk management - Implement security measures to reduce identified threats ~ Sanction policy - Apply sanctions against policy violators ~ Information system activity (ISA) review - Review records of ISA – audit logs, security incident tracking reports, access reports
Assign security responsibility	~ Identify a security officer
Workforce security	~ Policies and procedures to allow appropriate access to workforce as indicated by job duties
Information access management	~ Policies for authorizing and granting access to electronic PHI
Security awareness and training	~ Provide security training to all workforce
Security incident procedures Policies to address security incidents, violations or breaches	~ Response and reporting – Identify and respond to security incidents. Document incidents and their outcomes.
Contingency plan Policies for responding to an emergency that damages systems containing electronic PHI	~ Data back-up plan ~ Disaster recovery plan ~ Emergency mode operation plan
Evaluation	~ Perform periodic technical and non-technical evaluation
Business associates contract	~ Obtain satisfactory assurance that BA will appropriately safeguard electronic PHI
PHYSICAL SAFEGUARDS	
Facility access controls	~ Policies to appropriately limit or allow physical access to electronic information systems
Workstation use	~ Procedures to specify workstation functions and the manner the functions are to be performed
Workstation security	~ Implement physical safeguards to restrict access to authorized users
Device and media controls	~ Disposal - Policies on final disposition of electronic PHI and hardware or electronic media on which it is stored ~ Media Re-use – Procedures for removal of electronic PHI from electronic media before re-using the media
TECHNICAL SAFEGUARDS	
Access control Technical policies to allow access only to users who have been granted access	~ Unique user identification – Assign a unique name &/or number for identifying and tracking user identity. ~ Emergency access procedures – Procedures for obtaining needed electronic PHI during an emergency.
Audit controls	~ Implement hardware, software, or procedural mechanisms that record and examine activity in information systems containing or using PHI
Integrity	~ Protections from improper alteration or destruction of electronic PHI
Person or entity authentication	~ Procedures to verify person seeking entry into electronic PHI system is the one claimed

Transmission security	~ Guards against unauthorized access to PHI being transmitted over network
POLICIES AND PROCEDURES & DOCUMENTATION REQUIREMENTS	
Policies and procedures	~ Implement reasonable and appropriate policies addressing compliance with standards and implementation specifications
Documentation Maintain written records of assessments, activities, or actions and policies and procedures related to security rule compliance	<ul style="list-style-type: none"> ~ Time limit – 6 years from date of its creation or from its last effective date (whichever is later) ~ Availability – Available to persons responsible for implementation ~ Updates – Review documentation periodically and update in response to changes affecting the security of electronic PHI
Source: <u>Federal Register</u> , "DHHS, 45 CFR Parts 160, 162, and 164 - Health Insurance Reform: Security Standards; Final Rule," February 20, 2003, pp. 8334 – 8381.	