



Administrative Safeguards

HIPAA Security ♦ November 2003

TMA Privacy Office Information Paper

Records Management ♦ FOIA ♦ DUAs ♦ HIPAA Compliance ♦ ADP Security ♦ Privacy Act ♦ System of Records ♦ PIAs



General Requirement

HIPAA's [Security Rule](#) divides its protections into three categories: administrative (discussed here), [physical](#) and [technical](#) safeguards. The Rule defines administrative safeguards as “administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect [electronic protected health information \(EPHI\)](#) and to manage the conduct of the [covered entity's](#) workforce in relation to the protection of that information.” Covered entities must implement safeguards that ensure compliance with the standards and implementation specifications included in each category.

What must covered entities do to demonstrate compliance?

Documented policies and procedures are required for compliance with the Security Rule. Comprehensive documentation of security measures is also required. Documentation must be kept current, and a historical record maintained as well. Those two standards are included in the matrix below for completeness, but they apply to all safeguard areas.

How should the matrix be used?

The administrative safeguards' standards and specifications are presented in the matrix below. All standards are required. The implementation specifications associated with some standards provide additional detail when needed and are either required or addressable. For more information on a particular standard and the associated implementation specifications, follow the link in the left column.

Standard(s)	CFR Section	Implementation Specification
All are required	(Code of Federal Regulations)	(r)=required (a)=addressable
security mgmt process	164.308(a)(1)	risk analysis (r) risk management (r) sanction policy (r) information system activity review (r)
assigned security responsibility	164.308(a)(2)	
workforce security	164.308(a)(3)	authorization and/or supervision (a) workforce clearance procedure (a) termination procedures (a)
information access	164.308(a)(4)	isolating health care clearinghouse function (r) access authorization (a) access establishment and modification (a)
Standard(s)	CFR section	Implementation Specification

PrivacyMail@tma.osd.mil ♦ www.tricare.osd.mil/tmaprivacy



Administrative Safeguards

HIPAA Security ♦ November 2003

Standard(s)	CFR Section	Implementation Specification
All are required	(Code of Federal Regulations)	(r)=required (a)=addressable
security awareness and training	164.308(a) (5)	security reminders (a) protection from malicious software (a) log-in monitoring (a) password management (a)
security incident procedures	164.308(a)(6)	response and reporting (r)
contingency plan	164.308.(a)(7)	data backup plan (r) disaster recovery plan (r) emergency mode operation plan (r) testing and revision procedure (a) applications and data criticality analysis (a)
evaluation	164.308(a)(8)	
business associate contracts	164.308(b)(1)	written contract or other arrangement (r)
policies and procedures	164.316(a)	
documentation	164.316(b)(1)	time limit (r) availability (r)updates (r)

Matrix adapted from Appendix A to Subpart C of Part 164.

See also:

[Appendix A to Subpart C of Part 164 Security Rule Applicability](#)

