TMA Privacy Office Information Paper

# Integrity Standards

HIPAA Security◆ November 2003

**Standard Requirement**

The integrity standard of the technical safeguards addresses "policies and procedures to protect electronic protected health information (EPHI) from improper alteration or destruction." Covered entities assure data integrity through a combination of many controls including administrative, physical and technical policies and procedures. For example, the administrative policies and procedures for training and information access stipulate that only authorized and trained personnel should review, enter, or modify protected health information. Technical policies and procedures for access control, virus protection, and encryption help protect the integrity of data stored and processed on an automated information system by implementing and enforcing administrative policies in the system. This standard requires covered entities to deploy and use technical policies and procedures to enforce and/or implement all policies and procedures that protect data integrity. There is one addressable implementation specification associated with data integrity, mechanism to authenticate data.

Implementation Specification

The standard has one implementation specification which is addressable rather than required: "Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner." Because this requirement is "addressable", compliance depends on the outcome of a covered entity's risk assessment. A covered entity must evaluate the need for technical mechanisms to authenticate the integrity of protected health information in its automated information system. The covered entity's risk analysis must address what data should be authenticated, and to what degree of assurance. A covered entity must describe and justify its approach to this problem in its risk management plan. The proposed rule includes examples of methods such as check sums, message authentication codes, and digital signatures. Inclusion of these examples was not meant to restrict a services' or MTFs' choice of methods to use. Covered entities may deploy other methods of data authentication as long as they provide appropriate levels of data integrity.

See also:

45 CFR 164.312(c)(1)

Federal and DoD regulations that support this standard

DoD 8510.1-M

DoDI 8500.2