

Guide to Proposed Security Regulation

142 ADMINISTRATIVE REQUIREMENTS

Subpart A – General Provisions

142.101 Statutory basis and purpose

142.102 Applicability

142.103 Definitions

142.104 General requirements for health plans

142.105 Compliance using a health care clearinghouse

142.106 Effective dates of a modification to a standard or implementation specification

Subpart B – [Reserved]

Subpart C – Security and Electronic Signature Standards

142.302 Applicability and scope

142.304 Definitions

142.306 Rules for the security standard

142.308 Security standard

documented, formal practices to manage the selection and execution of security measures to protect data, and to manage the conduct of personnel in relation to the protection of data

- (a) *Administrative procedures* – include:
 - (1) certification
 - (2) chain of trust partner agreement
 - (3) contingency plan – includes:
 - (i) applications and data criticality analysis
 - (ii) data backup plan
 - (iii) disaster recovery plan
 - (iv) emergency mode operation plan
 - (v) testing and revision procedures
 - (4) formal mechanism for processing records
 - (5) information access control – includes:
 - (i) access authorization
 - (ii) access establishment
 - (iii) access modification
 - (6) internal audit
 - (7) personnel security – includes:
 - (i) assuring supervision of maintenance personnel
 - (ii) maintaining a record of access authorizations
 - (iii) proper access authorization for operating and maintenance personnel
 - (iv) personnel clearance procedures

- (v) personnel security policies and procedures
 - (vi) security awareness training
 - (8) Security configuration management – includes:
 - (i) documentation on all components of entity's security
 - (ii) hardware and software installation and maintenance review and testing
 - (iii) inventory of hardware and software assets
 - (iv) security testing
 - (v) virus checking
 - (9) security incident procedures – include:
 - (i) report procedures
 - (ii) response procedures
 - (10) security management process
 - (i) risk analysis
 - (ii) risk management
 - (iii) sanction policies and procedures
 - (iv) security policy
 - (11) termination procedures – include:
 - (i) changing locks
 - (ii) removal from access lists
 - (iii) removal of user account(s)
 - (iv) turning in of keys, tokens, or cards that allow access
 - (12) training – includes:
 - (i) awareness training
 - (ii) periodic security reminders
 - (iii) user education concerning virus protection
 - (iv) user education on monitoring log-ins and reporting discrepancies
 - (v) user education in password management
- (b) *Physical safeguards* – include:
- (1) assigned security responsibility
 - (2) media controls – include:
 - (i) access control
 - (ii) accountability
 - (iii) data backup
 - (iv) data storage
 - (v) disposal
 - (3) physical access controls – include:
 - (i) disaster recovery
 - (ii) emergency mode operation
 - (iii) equipment control
 - (iv) facility security plan
 - (v) procedures for verifying access authorizations
 - (vi) maintenance records for physical components
 - (vii) need-to-know procedures for personnel access
 - (viii) procedures to sign in visitors and provide escorts, if appropriate
 - (4) policy and guidelines on work station use
 - (5) secure work station location
 - (6) security awareness training
- (c) *Technical security services to guard data integrity, confidentiality, and availability*
- (1) technical security services must include:
 - (i) access control that includes:
 - (A) procedure for emergency access
 - (B) at least one of the following implementation features:
 - (1) Context-based access
 - (2) Role-based access

- (3) User-based access
 - (C) optional use of encryption
 - (ii) audit controls
 - (iii) authorization control – includes:
 - (A) automatic logoff
 - (B) unique user identifier
 - (C) at least one of the following implementation features:
 - (1) biometric identification
 - (2) password
 - (3) personal identification number (PIN)
 - (4) telephone callback procedure
 - (5) token
 - (2) [Reserved]
- (d) *Technical security mechanisms*
 - (1) If an entity uses communications or network controls, must include:
 - (i) following implementation features:
 - (A) integrity controls
 - (B) message authentication
 - (ii) one of the following implementation features:
 - (A) access controls
 - (B) encryption
 - (2) if an entity uses network controls, must include:
 - (i) alarm
 - (ii) audit trail
 - (iii) entity authentication
 - (iv) event reporting

142.310 Electronic signature standard

- (a) General rule
- (b) Standard
- (c) Required implementation features
- (d) Optional implementation features

142.312 Effective date of the initial implementation of the security and electronic signature standards

- (a) General rules
- (b) Small health plans