

**CAL HIPAA
Modifications to the HIPAA Proposed Security Rule
February 20, 2003**

The following changes were made to the provisions of the August 12, 1998 proposed rule.

- Changed the CFR part from 142 to 164.
- Removed information throughout the document pertaining to electronic signature standards. Electronic signature standards will be published in a separate final rule.
- Replaced the word "requirement," when referring to a standard, with "standard." Replaced "Implementation feature" with "Implementation specification."
- Made minor modifications to the text throughout the document for purposes of clarity.
- Modified numerous implementation features so that they are now addressable rather than mandatory.
- Removed the word "formal" when referring to documentation.
- Revised the phrase "health information pertaining to an individual" to "electronic protected health information."
- Added the following definitions to § 160.103: "Disclosure," "Electronic protected health information," "Electronic media," "Organized health care arrangement," and "Use."
- Removed proposed § 142.101 as this information is conveyed in § 160.101 and § 160.102 of the Privacy Rule (65 FR 82798). Removed proposed § 142.102 as it is redundant.
- Removed the following definitions from proposed § 142.103 since they are pertinent to other administrative simplification regulations and are defined elsewhere: code set, health care clearinghouse, health care provider, health information, health plan, medical care, small health plan, standard, and transaction.
- Moved the following definitions from § 164.501 to § 164.103 (proposed § 142.103): "Plan sponsor" and "Protected health information." Added definitions of "Covered functions" and "Required by law."
- Removed proposed § 142.104, "General requirements for health plans," and proposed § 142.105, "Compliance using a health care clearinghouse," since these sections are not pertinent to the security standards.
- Removed proposed § 142.106, "Effective dates of a modification to a standard or implementation specification," since this information is covered in the "Standards for Electronic Transactions" final rule (65 FR 50312).
- Moved proposed § 142.302 to § 164.302. Changed the section heading from "Applicability and scope" to "Applicability." Modified language to state that covered entities must comply with the security standards.
- Moved proposed § 142.304 to § 164.304. Modified language to remove definitions of words and concepts not used in this final rule: "Access control," "Contingency plan," "Participant," "Role-based access control," "Token," and "User-based access."
- Moved proposed § 142.304 to § 164.304. Modified language to add definitions requested by commenters; previously published in Addendum 2 but not in the draft regulation itself; or necessitated

by the change of scope to electronic protected health information and alignment with the Privacy Rule to include: "Administrative safeguards," "Availability," "Confidentiality," "Data," "Data authentication Code," "Integrity," "Electronic protected health information," "Facility," "Information System," "Security or security measures," "Security incident," "Technical safeguards," "User," and "Workstation."

- Moved definitions related to privacy from § 164.504 to new § 164.103: "Common control," "Common ownership," "Health care component," "Hybrid entity."
- Moved proposed § 142.306, "Rules for the security Standard," to § 164.306. Modified language to more clearly state the general requirements of the final rule relative to the standards and implementation specifications contained therein. Retitled the section as "Security standards: General Rules."
- Moved proposed § 142.308 to § 164.308. Where this section was proposed to contain all of the security standards in paragraphs (a) through (d), it now encompasses the Administrative safeguards.
- Moved and reorganized proposed § 142.308(a) through (d) requirements to § 164.308, § 164.310, and § 164.312.
- Moved proposed § 142.308(a)(1), "Certification," to § 164.308(a)(8). Modified language to indicate both technical and nontechnical evaluation is involved and renamed "Evaluation".
- Moved proposed § 142.308(a)(2), "Chain of trust," to 195 § 164.308(b)(1), renamed to "Business associate contracts and other arrangements," and revised language to redefine who must enter into a contract under this rule for the protection of electronic protected health information.
- Moved proposed § 142.308(a)(3), "Contingency plan," to § 164.308(a)(7)(i). Modified language to state that two implementation specifications, "Applications and data criticality analysis" and "Testing and revision procedures," are addressable.
- Removed "Formal mechanism for processing records" (proposed § 142.308(a)(4)) since this requirement was determined to be in part intrusive into business functions and in part redundant.
- Moved proposed § 142.308(a)(5), "Information access control," to § 164.308(a)(4)(i) and renamed as "Information access management." Removed the word "formal" from description. Modified language to state that two implementation specifications ("Access Authorization" and Access Establishment and Modification") are addressable.
- Moved proposed § 142.308(a)(6), "Internal audit," to § 164.308(a)(1)(ii)(D) as an implementation specification under the "Security management process" standard since this was determined to be a more logical 196 placement of this item. Retitled, for clarity, "Information system activity review."
- Moved proposed § 142.308(a)(7), "Personnel security," to § 164.308(a)(3)(i) and retitled "Workforce security." Modified language to state that implementation specifications are addressable.
- Combined proposed § 142.308(a)(7)(i), and § 142.308(a)(7)(iii) ("Assuring supervision of maintenance personnel by an authorized, knowledgeable person" and "Assuring that operations and maintenance personnel have proper access authorization,") under § 164.308(a)(3)(ii)(A) and renamed to "Authorization and/or supervision." Modified description for clarity.
- Moved proposed § 142.308(a)(7)(iv), "Personnel clearance procedure," to § 164.308(a)(3)(ii)(B), renamed to "Workforce clearance procedure," and modified description for clarity.
- Removed proposed § 142.308(a)(7)(v), "Personnel security policies and procedures," as this feature was determined to require redundant effort.

- Removed proposed § 142.308(a)(7)(vi), "Security awareness training." Information concerning this subject has been incorporated under § 164.308(a)(5)(i), "Security 197 awareness and training."
- Removed proposed § 142.308(a)(8), "Security configuration management," and all implementation features, except "Documentation" (hardware and/or software installation, Inventory, Security testing, and Virus checking), since this requirement was determined to be redundant. "Documentation" has been made a discrete standard at § 164.316.
- Moved proposed § 142.308(a)(9), "Security incident procedures," to § 164.308(a)(6)(i) and reworded for clarity. Combined "Report procedures" and "Response procedures" features into a single required implementation specification, named "Response and Reporting" at § 164.308(a)(6)(ii).
- Moved proposed § 142.308(a)(10), "Security management process," to § 164.308(a)(1).
- Moved proposed § 142.308(a)(10)(i), "Risk analysis," to § 164.308(a)(1)(ii)(A).
- Moved proposed § 142.308(a)(10)(ii), "Risk management," to § 164.308(a)(1)(ii)(B).
- Moved proposed § 142.308(a)(10)(iii), "Sanction policy," to § 164.308(a)(1)(ii)(C).
- Removed proposed § 142.308(a)(10)(iv), "Security policy," since this requirement was determined to be redundant.
- Moved proposed § 142.308(a)(11), "Termination," to § 164.308(a)(3)(ii)(C) as an addressable implementation specification under the "Workforce security" standard, and renamed as "Termination procedures". Removed "Termination" implementation features (changing locks, removal from access lists, removal of user accounts, turning in of keys, tokens, or cards) since these were determined to be too specific.
- Moved proposed § 142.308(a)(12), "Training," to § 164.308(a)(5)(i) and renamed as "Security awareness and training." Language modified to incorporate all training information under this one standard. Revised and made addressable all implementation specifications under this standard.
- Moved proposed § 142.308(b), "Physical safeguards to guard data integrity, confidentiality and availability," to § 164.310 and renamed as "Physical safeguards." Removed specific reference to locks and keys.
- Moved proposed § 142.308(b)(1), "Assigned security responsibility requirement," to § 164.308(a)(2) since this has been determined to be an administrative procedure. Modified language to clarify that responsibility could be assigned to more than one individual.
- Moved proposed § 142.308(b)(2), "Media controls," to § 164.310(d)(1) and renamed as "Device and media controls." Removed the word "formal." Added "Media re-use" as a required implementation specification at § 164.310(d)(2)(ii).
- Removed proposed § 142.308(b)(2)(i), "Access control," implementation feature as it was determined to be redundant.
- Moved proposed § 142.308(b)(2)(ii), "Accountability" implementation feature to § 164.310(d)(2)(iii), and made it an addressable implementation specification.
- Combined proposed § 142.308(b)(2)(iii), "Data backup," implementation feature with proposed § 142.308(b)(2)(iv), "Data storage" implementation feature, renamed as "Data backup and storage", moved to § 164.310(d)(2)(iv), and made it an addressable implementation specification.

- Moved proposed § 142.308(b)(2)(v), "Data disposal," implementation feature to § 164.310(d)(2)(i) and made it a required implementation specification.
- Moved proposed § 142.308(b)(3), "Physical access controls," to § 164.310(a)(1) and renamed as "Facility access controls." Removed word "formal."
- Moved proposed § 142.308(b)(3)(i), "Disaster recovery," implementation feature to § 164.310(a)(2)(i). It is now part of the "Contingency operations" implementation specification.
- Moved proposed § 142.308(b)(3)(ii), "Emergency mode operations," implementation feature to § 164.310(a)(2)(i). It is now part of the "Contingency operations" implementation specification.
- Removed proposed § 142.308(b)(3)(iii), "Equipment control (into and out of site)," as this information is now covered under § 164.310(d)(1), "Device and media controls."
- Moved proposed § 142.308(b)(3)(iv), "A facility security plan," to § 164.310(a)(2)(ii).
- Moved proposed § 142.308(b)(3)(v), "Procedure for verifying access authorizations," to § 164.310(a)(2)(iii) and renamed as "Access control and validation procedures." Removed the word "formal" from text.
- Moved proposed § 142.308(b)(3)(vi), "Maintenance records," to § 164.310(a)(2)(iv).
- Moved proposed § 142.308(b)(3)(vii), "Need to know procedures for personnel access," to § 164.310(a)(2)(iii) and renamed as "Access control and validation procedures."
- Moved proposed § 142.308(b)(3)(viii), "Procedures to sign in visitors and provide escort, if appropriate," to § 164.310(a)(2)(iii) and renamed as "Access control and validation procedures."
- Moved proposed § 142.308(b)(3)(ix), "Testing and revision," to § 164.310(a)(2)(iii) and renamed as "Access control and validation procedures."
- Moved proposed § 142.308(b)(4), "Policy and guidelines on workstation use," to § 164.310(b) and renamed as "Workstation use."
- Moved proposed § 142.308(b)(5), "Secure work station location," to § 164.310(c) and renamed as "Workstation security."
- Removed proposed § 142.308(b)(6), "Security awareness training," as a separate requirement. This requirement has been incorporated under § 164.308(a)(5)(i), "Security awareness and training."
- Combined and moved proposed § 142.308(c) and § 142.308(d), "Technical security services to guard data integrity, confidentiality and availability" and "Technical security mechanisms," to § 164.312 and renamed as "Technical safeguards."
- Removed proposed § 142.308(c)(1) since it is no longer pertinent.
- Moved proposed § 142.308(c)(1)(i), "Access control," to § 164.312(a)(1).
- Moved proposed § 142.308(c)(1)(i)(A), "Procedure for emergency access," to § 164.312(a)(2)(ii), and renamed as "Emergency access procedures."
- Removed proposed § 142.308(c)(1)(i)(B).

- Removed proposed § 142.308(c)(1)(i)(B)(1), "Context-based access," § 142.308(c)(1)(i)(B)(2), "Role-based access," and § 142.308(c)(1)(i)(B)(3), "User-based access," since these features were deemed too specific and were perceived as the only options permissible.
- Moved proposed § 142.308(c)(1)(i)(C), "Optional use of encryption," to § 164.312(a)(2)(iv) and retitled "Encryption and decryption."
- Moved proposed § 142.308(c)(1)(ii), "Audit controls," to § 164.312(b).
- Removed proposed § 142.308(c)(1)(iii), "Authorization control," and all implementation features (Role-based access, User-based access) since this function has been incorporated into § 164.308(a)(4), "Information access management."
- Moved proposed § 142.308(c)(1)(iv), "Data authentication," to § 164.312(c)(1), and retitled as "Integrity." Reworded part of description and placed in § 164.312(c)(2), "Mechanism to authenticate data," a new, addressable implementation specification. Removed reference to double keying.
- Moved proposed § 142.308(c)(1)(v), "Entity authentication," to § 164.312(d) and retitled as "Person or entity authentication."
- Moved proposed § 142.308(c)(1)(v)(A), "Automatic logoff," to § 164.312(a)(2)(iii).
- Moved proposed § 142.308(c)(1)(v)(B), "Unique user identification," to § 164.312(a)(2)(i).
- Removed proposed § 142.308(c)(1)(v)(C) since text is no longer pertinent.
- Removed proposed § 142.308(c)(1)(v)(C)(2), "Password," as too specific.
- Removed proposed § 142.308(c)(1)(v)(C)(3), "PIN," as too specific.
- Removed proposed § 142.308(c)(1)(v)(C)(4), "Telephone callback," as too specific.
- Removed proposed § 142.308(c)(1)(v)(C)(5), "Token," as too specific.
- Removed proposed § 142.308(c)(2), as no longer relevant.
- Moved proposed § 142.308(d)(1), "Communications or network controls," to § 164.312(e)(1) and renamed as "Transmission security."
- Removed proposed § 142.308(d)(1)(i), since it is no longer pertinent.
- Moved proposed § 142.308(d)(1)(i)(A), "Integrity controls," to § 164.312(e)(2)(i) and reworded for clarity.
- Removed proposed § 142.308(d)(1)(i)(B), "Message authentication," since this subject is now covered under § 164.312(e)(2)(i), "Integrity controls."
- Removed proposed § 142.308(d)(1)(ii) text since it is no longer pertinent.
- Removed proposed § 142.308(d)(1)(ii)(A), "Access controls."
- Moved proposed § 142.308(d)(1)(ii)(B), "Encryption," to § 164.312(e)(2)(ii) and reworded to enhance flexibility and scalability.

- Removed proposed § 142.308(d)(2) text regarding: "Network controls," and all implementation features ("Alarm," "Audio trail," "Entity authentication," "Event reporting").
- Removed proposed § 142.310, "Electronic signature," and all subheadings. This section will be issued as a separate future regulation.
- Moved proposed § 142.310 "Electronic signature Standard," to § 164.310. Where this section was proposed to contain the electronic signature standard, it now encompasses the "Physical safeguards."
- Moved proposed § 142.312, "Effective date of the implementation of the security and electronic signature standards," to § 164.318 and retitled as "Compliance dates for the initial implementation of the security standards." Reworded and retitled subsections.
- Added § 164.105, "Organizational requirements," with two standards, "Health care component and "Affiliated covered entities" with related implementation specifications.
- Added § 164.310(d)(2)(ii), "Media re-use procedures," implementation specification.
- Added § 164.312, "Technical safeguards," encompassing the combined technical services and technical mechanisms standards (proposed § 142.308 (c) and (d)).
- Added § 164.314, "Organizational requirements."
- Added § 164.314(a)(1), "Business associate contracts or other arrangements" standard and related implementation specifications.
- Added § 164.314(b)(1), "Requirements for group health plans" standard and related implementation specifications.
- Added § 164.316, "Policies and procedures and documentation requirements."
- Added § 164.316(a), "Policies and procedures" standard.
- Added § 164.316(b)(1), "Documentation" standard and related implementation specifications.
- Added § 164.318, "Compliance dates for the initial implementation of the security standards."
- Renamed Addendum 1 as Appendix A.
- Removed Addendum 2. Definitions of terms used in this final rule are now incorporated into § 164.103 and § 164.304, or within the rule itself.
- Removed Addendum 3.