

costs must be factored into any base year calculations for the proposed prospective payment system. Without an adjustment, this will be another regulatory mandate that comes at the cost of patient care.

Response: Costs included in the prospective payment system are legislatively mandated. The Congress did not direct the inclusion of HIPAA costs into the system, so they are not included. However, the Department believes that the HIPAA standards will provide savings to the provider community over the next 10 years.

g. Comment: One commenter suggested that we include requirements for how a compliant business could dually operate—(1) in a HIPAA compliant manner; and (2) in their former noncompliant manner in order to accommodate doing business with other organizations that are not yet compliant.

Response: The statute imposes a 2-year implementation period between the adoption of the initial standards and the date by which covered entities (except small health plans) must be in compliance. An entity may come into compliance at any point in time during the 2 years. Therefore, the rule does not require a covered entity to comply before the established compliance date. Those entities that come into compliance before the 2-year deadline should decide how best to deal with entities that are not yet compliant. Further, we note that, generally speaking, compliance by a covered entity with these security rules will not hinge on compliance by other entities.

h. Comment: One commenter stated that privacy legislation could impose significant changes to written policies and procedures on authorization, access to health information, and how sensitive information is disclosed to others. The commenter believes these changes could mean the imposition of security requirements different from those contained in the proposed rule, and money spent complying with the security provisions could be ill spent if significant new requirements result from the privacy legislation.

Response: The privacy standards at subpart E of 42 CFR part 164 are now in effect, and this final rule is compatible with them. If, in the future, the Congress passes a law whose provisions differ from these standards, the standards would have to be modified.

i. Comment: One commenter stated that the private sector should develop educational tools or models in order to assist physicians, other providers, and health plans to comply with the security regulations.

Response: We agree. The health care industry is striving to do this. HHS is also considering provider outreach and education activities.

IV. Provisions of the Final Regulation

We have made the following changes to the provisions of the August 12, 1998 proposed rule. Specifically, we have—

- 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 § 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