

covered entity to obtain written assurance from a business associate receiving the transmission that it will provide an adequate level of protection to the information. For the business associate provisions, see § 164.308(b) and § 164.314(a) of this final rule.

f. *Comment:* One commenter asked what security standards a vendor having access to a covered entity's health information during development, testing, and repair must meet and wanted to know whether the rule anticipates having a double layer of security compliance (one at the user level and one at the vendor level). If so, the commenter believes this will cause duplication of work.

*Response:* In the situation described, the vendor would be acting as a business associate. The covered entity must require the business associate to implement reasonable and appropriate security protections of electronic protected health information. This requirement, however, does not impose detailed requirements for how that level of protection must be achieved. The resulting flexibility should permit entities and their business associates to adapt their security safeguards in ways that make sense in their particular environments.

g. *Comment:* A number of commenters requested sample contract language or models of contracts. We also received one comment that suggested that we should not dictate the contents of contracted agreements.

*Response:* We will consider developing sample contract language as part of our guideline development.

#### *I. Policies and Procedures and Documentation Requirements (§ 164.316)*

We proposed requiring documented policies and procedures for the routine and nonroutine receipt, manipulation, storage, dissemination, transmission, and/or disposal of health information. We proposed that the documentation be reviewed and updated periodically.

We have emphasized throughout this final rule the scalability allowed by the security standards. This final rule requires covered entities to implement policies and procedures that are reasonably designed, taking into account the size and type of activities of the covered entity that relate to electronic protected health information, and requires that the policies and procedures must be documented in written form, which may be in electronic form. This final rule also provides that a covered entity may change its policies and procedures at any time, provided that it documents

and implements the changes in accordance with the applicable requirements. Covered entities must also document designations, for example, of affiliation between covered entities (see § 164.105(b)), and other actions, as required by other provisions of the subpart.

1. *Comment:* One commenter wanted development of written policies regarding such things as confidentiality and privacy rights for access to medical records, and approval of research by a review board when appropriate.

*Response:* These issues are covered in the Privacy Rule (65 FR 82462) (see, in particular, § 164.512(i), § 164.524, and § 164.530(i)).

2. *Comment:* One commenter asked if standards will override agreements that require others to maintain hardcopy documentation (for example, signature on file) and no longer require submitters to maintain hardcopy documentation.

*Response:* The security standards will require a minimum level of documentation of security practices. Any agreements between trading partners for the exchange of electronic protected health information that impose additional documentation requirements will not be overridden by this final rule.

3. *Comment:* One commenter stated that there should be a requirement to document only applications deemed necessary by an applications and data criticality assessment.

*Response:* Electronic protected health information must be afforded security protection under this rule regardless of what application it resides in. The measures taken to protect that information must be documented.

4. *Comment:* One commenter asked how detailed the documentation must be. Another commenter asked what "kept current" meant.

*Response:* Documentation must be detailed enough to communicate the security measures taken and to facilitate periodic evaluations pursuant to § 164.308(a)(8). While the term "current" is not in the final rule, this concept has been adopted in the requirement that documentation must be updated as needed to reflect security measures currently in effect.

5. *Comment:* We received one comment concerning review and updating of implementing documentation suggesting that "periodically" be changed to "at least annually."

*Response:* We believe that the requirement should remain as written, in order to allow individual entities to establish review and update cycles as deemed necessary. The need for review

and update will vary dependent upon a given entity's size, configuration, environment, operational changes, and the security measures implemented.

#### *J. Compliance Dates for Initial Implementation (§ 164.318)*

We proposed that how the security standard would be implemented by each covered entity would be dependent upon industry trading partner agreements for electronic transmissions. Covered entities would be able to adapt the security matrix to meet business needs. We suggested that requirements of the security standard may be implemented earlier than the compliance date. However, we would require implementation to be complete by the applicable compliance date, which is 24 months after adoption of the standard, and 36 months after adoption of the standard for small health plans, as provided by the Act. In the proposed rule, we suggested that an entity choosing to convert from paper to standard EDI transactions, before the effective date of the security standard, consider implementing the security standard at the same time.

In this final rule the dates by which entities must be in compliance with the standards are called "compliance dates," consistent with our practice in the Transactions, Privacy, and Employer Identifier Rules. Section 164.318 in this final rule is also organized consistent with the format of those rules. The substantive requirements, which are statutory, remain unchanged.

Many of the comments received concerning effective dates and compliance dates, including the compliance dates for modifications of standards, were addressed in the Transactions Rule. Those that were not addressed in that publication are presented below.

1. *Comment:* A number of commenters expressed support for the effective dates of the rules and stated that they should not be delayed. In contrast, one commenter stated that we should delay this rule to allow for an open consensus building debate to occur concerning security. One commenter asked that the rule be delayed until after implementation of the ICD-CM changes.

A number of comments were received expressing the opinion that the security regulation should not be published until either the Congress has enacted legislation governing standards with respect to the privacy of individually identifiable health information, or the Secretary of HHS has promulgated final regulations containing these standards. One commenter stated, "we find