

b. *Comment:* Several commenters stated that the certification should cover all components of the proposed rule, not just the information systems.

*Response:* We agree. We have revised this section to reflect that evaluation would be both technical and nontechnical components of security.

c. *Comment:* A number of commenters expressed a desire for the creation of certification guides or models to complement the rule.

*Response:* We agree that creation of compliance guidelines or models for different business environments would help in the implementation and evaluation of HIPAA security requirements and we encourage professional associations and others to do so. We may develop technical assistance materials, but do not intend to create certification criteria because we do not have the resources to address the large number of different business environments.

d. *Comment:* Some commenters asked how certification is possible without specifying the level of risk that is permissible.

*Response:* The level of risk that is permissible is specified by § 164.306(a). How such risk is managed will be determined by a covered entity through its security risk analysis and the risk mitigation activities it implements in order to ensure that the level of security required by § 164.306 is provided.

e. *Comment:* Several commenters requested creation of a list of Federally “certified” security software and off-the-shelf products. Several others stated that this request was not feasible. Regarding certification of off-the-shelf products, one commenter thought this should be encouraged, but not mandated; several thought this would be an impractical endeavor.

*Response:* While we will not assume the task of certifying software and off-the-shelf products for the reason described above, we have noted with interest that other Government agencies such as the National Institute of Standards and Technology (NIST) are working towards that end. The health care industry is encouraged to monitor the activity of NIST and provide comments and suggestions when requested (see <http://www.niap.nist.gov>).

f. *Comment:* One commenter stated, “With HCFA’s publishing of these HIPAA standards, and their desire to retain the final responsibility for determining violations and imposing penalties of the statute, it also seems appropriate for HCFA to also provide certifying services to ensure security compliance.”

*Response:* In view of the enormous number and variety of covered entities, we believe that evaluation can best be handled through the marketplace, which can develop more usable and targeted evaluation instruments and processes.

#### 8. Business Associate Contracts or Other Arrangements (§ 164.308(b)(1))

In the proposed rule § 142.308(a)(2) “Chain of trust” requirement, we proposed that covered entities be required to enter into a chain of trust partner agreement with their business partners, in which the partners would agree to electronically exchange data and protect the integrity, confidentiality, and availability of the data exchanged. This standard has been modified from the proposed requirement to reflect, in § 164.308(b)(1) “Business associate contracts and other arrangements,” the business associate structure put in place by the Privacy Rule.

In this final rule, covered entities must enter into a contract or other arrangement with persons that meet the definition of business associate in § 160.103. The covered entity must obtain satisfactory assurances from the business associate that it will appropriately safeguard the information in accordance with these standards (see § 164.314(a)(1)).

The comments received on the proposed chain of trust partner agreements are discussed in section 2 “Business associate contracts and other arrangements” of the discussion of § 164.314 below.

#### 9. Proposed Requirements Not Adopted in This Final Rule

##### a. Security Configuration Management

We proposed that an organization would be required to implement measures, practices, and procedures regarding security configuration management. They would be coordinated and integrated with other system configuration management practices for the security of information systems. These would include documentation, hardware and/or software installation and maintenance review and testing for security features, inventory procedures, security testing, and virus checking.

*Comment:* Several commenters asked that the entire requirement be deleted. Several others asked that the inventory and virus checking implementation features be removed as they believe those features are not germane to security configuration management. A number of commenters requested that

security testing be deleted because this implementation feature is too detailed, unreasonable, impractical, and beyond the scope of the legislation. Others stated that the testing would be very complex and expensive. Others wanted more clarification of what we intend by security testing, and how much would be enough. A number of commenters asked that all of the implementation features be deleted. Others asked that the implementation features be made optional. Several commenters wanted to know the scope of organizational integration required. Several others asked if what we meant by Security Configuration Management was change or version control.

*Response:* Upon review, this requirement appears unnecessary because it is redundant of other requirements we are adopting in this rule. A covered entity will have addressed the activities described by the features under this proposed requirement by virtue of having implemented the risk analysis, risk management measures, sanction policies, and information systems criticality review called for under the security management process. The proposed documentation implementation feature has been made a separate standard (see § 164.316). As a result, the Security Configuration Management requirement is not adopted in this final rule.

##### b. Formal Mechanism for Processing Records

The proposed rule proposed requiring a formal mechanism for processing records, and documented policies and procedures for the routine and nonroutine receipt, manipulation, storage, dissemination, transmission, and/or disposal of health information. This requirement has not been adopted in the final rule.

*Comment:* Several commenters thought this requirement concerned the regulation of formal procedures for how an entity does business and stated that such procedures should not be regulated. Others asked for additional clarification of what is meant by this requirement. One commenter thought the requirement too ambiguous and asked for clarification as to whether we meant such things as “the proper handling of storage media, databases, transmissions,” or “the clinical realm of processes.”

Two commenters asked how extensive this requirement would be and whether systems’ user manuals and policies and procedures for handling health information would suffice and what level of detail would be expected.