

communication among trading partners. These include the Strategic National Implementation Process (SNIP) developed under the auspices of the Workgroup for Electronic Data Interchange (WEDI), an organization named in the HIPAA statute to consult with the Secretary of HHS on HIPAA issues. Some of these organizations have developed white papers, tools, and recommended best practices addressing a number of HIPAA issues, including security. Covered entities may wish to examine these products to determine if they are relevant and useful in their own implementation efforts. A partial list of these organizations can be found at <http://www.wedi/snip.org>. We believe that these and other future industry-developed guidelines and/or models may provide valuable assistance to covered entities implementing these standards but must caution that HHS does not rate or endorse any such guidelines and/or models and the value of its content must be determined by the user.

b. *Comment:* Many commenters asked us to develop guidelines and models to aid in complying with the Security Rule. Several commenters either offered to participate in the development of guidelines and models or suggested entities that should be invited to participate.

Response: We agree that creation of compliance tools and guidelines for different business environments could assist covered entities to implement the HIPAA Security Rule. We plan to issue guidance documents after the publication of this final rule. However, it is critical for each covered entity to establish policies and procedures that address its own unique risks and circumstances.

In addition, a number of voluntary national and regional organizations have been formed to address HIPAA implementation issues and to facilitate communication among trading partners. These include the Strategic National Implementation Process (SNIP) developed under the auspices of the Workgroup for Electronic Data Interchange (WEDI), an organization named in the HIPAA statute to consult with the Secretary of HHS on HIPAA issues. Some of these organizations have developed white papers, tools, and recommended best practices addressing a number of HIPAA issues, including security.

Covered entities may wish to examine these products to determine if they are relevant and useful in their own implementation efforts. A partial list of these organizations can be found at <http://www.snip.wedi.org>. We believe

that these and other future industry-developed guidelines and/or models may provide valuable assistance to covered entities implementing these standards but must caution that HHS does not rate or endorse any such guidelines and/or models and the value of its content must be determined by the user.

4. Examples

Comment: We received a number of comments that demonstrated confusion regarding the purpose of the examples of security solutions that were included throughout the proposed rule. Commenters stated that they could not, or did not wish to, adopt various security measures suggested in examples. Other commenters asked that we include additional options within the examples. Some commenters referred specifically to the example provided in the proposed rule demonstrating how a small or rural provider might comply with the standards. One commenter asked for clarification that the examples are not mandatory measures that are required to demonstrate compliance, but are merely meant as a guide when implementing the security standards. Another commenter expressed support for the use of examples to clarify the intent of text descriptions.

Response: We wish to clarify that examples are used only as illustrations of possible approaches, and are included to serve as a springboard for ideas. The steps that a covered entity will actually need to take to comply with these regulations will be dependent upon its own particular environment and circumstances and risk assessment. The examples do not describe mandatory measures, nor do they represent the only, or even the best, way of achieving compliance. The most appropriate means of compliance for any covered entity can only be determined by that entity assessing its own risks and deciding upon the measures that would best mitigate those risks.

B. Applicability (§ 164.302)

We proposed that the security standards would apply to health plans, health care clearinghouses, and to health care providers that maintain or transmit health information electronically. The proposed security standards would apply to all electronic health information maintained or transmitted, regardless of format (standard transaction or a proprietary format). No distinction would be made between internal corporate entity communication or communication

external to the corporate entity. Electronic transmissions would include transactions using all media, even when the information is physically moved from one location to another using magnetic tape, disk, or other machine readable media. Transmissions over the Internet (wide-open), extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, and private networks would be included. We proposed that telephone voice response and “faxback” systems (a request for information made via voice using a fax machine and requested information returned via that same machine as a fax) would not be included but we solicited comments on this proposed exclusion.

This final rule simplifies the applicability statement greatly. Section 164.302 provides that the security standards apply to covered entities; the scope of the information covered is specified in § 164.306 (see the discussion under that section below regarding the changes and revisions to the scope of information covered).

1. *Comment:* A number of commenters requested clarification of who must comply with the standards. The preamble and proposed § 142.102 and § 142.302 stated: “Each person described in section 1172(a) of the Act who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards.” Commenters suggested that this statement is in conflict with the law, which defines a covered entity as a health plan, a clearinghouse, or a health care provider that conducts certain transactions electronically. The commenters apparently did not realize that section 1172(a) of the Act contains the definition of covered entities.

Response: Section 164.302 below makes the security standards applicable to “covered entities.” The term “covered entity” is defined at § 160.103 as one of the following: (1) A health plan; (2) a health care clearinghouse; (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by part 162 of title 45 of the Code of Federal Regulations (CFR). The rationale for the use and the meaning of the term “covered entity” is discussed in the preamble to the Privacy Rule (65 FR 82476 through 82477).

As that discussion makes clear, the standards only apply to health care providers who engage electronically in the transactions for which standards have been adopted.