

to providers. We received an equal number of comments stating that there is no need to define these terms. One commenter stated that definitions for these terms would be necessary only if special exemptions existed for small and rural providers. Several commenters suggested initiation of a study to determine limitations and potential barriers small and rural providers will have in implementing these regulations.

Response: The statute requires that we address the needs of small and rural providers. We believe that we have done this through the provisions, which require the risk assessment and the response to be assessment based on the needs and capabilities of the entity. This scalability concept takes the needs of those providers into account and eliminates any need to define those terms.

c. *Comment:* In the proposed rule, we proposed the following definition for the term "Access control": "A method of restricting access to resources, allowing only privileged entities access. Types of access control include, among others, mandatory access control, discretionary access control, time-of-day, classification, and subject-object separation." One commenter believed the proposed definition is too restrictive and requested revision of the definition to read: "Access control refers to a method of restricting access to resources, allowing access to only those entities which have been specifically granted the desired access rights." Another commenter wanted the definition expanded to include partitioned rule-based access control (PRBAC).

Response: We agree with the commenter who suggested that the definition as proposed seemed too restrictive. In this case, as in many others, a number of commenters believed the examples given in the proposed rule provided the only acceptable compliance actions. As previously noted, in order to clarify that the examples listed were not to be considered all-inclusive, we have generalized the proposed requirements in this final rule. In this case, we have also generalized the requirements and placed the substantive provisions governing access control at § 164.308(a)(4), § 164.310(a)(1), and § 164.312(a)(1). With respect to PRBAC, the access control standard does not exclude this control, and entities should adopt it if appropriate to their circumstances.

D. General Rules (§ 164.306)

In the proposed rule, we proposed to cover all health information maintained or transmitted in electronic form by a covered entity. We proposed to adopt, in § 142.308, a nation-wide security standard that would require covered entities to implement security measures that would be technology-neutral and scalable, and yet integrate all the components of security (administrative procedures, physical safeguards, technical security services, and technical security mechanisms) that must be in place to preserve health information confidentiality, integrity, and availability (three basic elements of security). Since no comprehensive, scalable, and technology-neutral set of standards currently exists, we proposed to designate a new standard, which would define the security requirements to be fulfilled.

The proposed rule proposed to define the security standard as a set of scalable, technology-neutral requirements with implementation features that providers, plans, and clearinghouses would have to include in their operations to ensure that health information pertaining to an individual that is electronically maintained or electronically transmitted remains safeguarded. The proposed rule would have required that each affected entity assess its own security needs and risks and devise, implement, and maintain appropriate security to address its own unique security needs. How individual security requirements would be satisfied and which technology to use would be business decisions that each entity would have to make.

In the final rule we adopt this basic framework. In § 164.306, we set forth general rules pertaining to the security standards. In paragraph (a), we describe the general requirements. Paragraph (a) generally reflects section 1173(d)(2) of the Act, but makes explicit the connection between the security standards and the privacy standards (see § 164.306(a)(3)). In § 164.306(a)(1), we provide that the security standards apply to all electronic protected health information the covered entity creates, receives, maintains, or transmits. In paragraph (b)(1), we provide explicitly for the scalability of this rule by discussing the flexibility of the standards, and paragraph (b)(2) of § 164.306 discusses various factors covered entities must consider in complying with the standards.

The provisions of § 164.306(c) provide the framework for the security standards, and establish the requirement that covered entities must comply with the standards. The administrative,

physical, and technical safeguards a covered entity employs must be reasonable and appropriate to accomplish the tasks outlined in paragraphs (1) through (4) of § 164.306(a). Thus, an entity's risk analysis and risk management measures required by § 164.308(a)(1) must be designed to lead to the implementation of security measures that will comply with § 164.306(a).

It should be noted that the implementation of reasonable and appropriate security measures also supports compliance with the privacy standards, just as the lack of adequate security can increase the risk of violation of the privacy standards. If, for example, a particular safeguard is inadequate because it routinely permits reasonably anticipated uses or disclosures of electronic protected health information that are not permitted by the Privacy Rule, and that could have been prevented by implementation of one or more security measures appropriate to the scale of the covered entity, the covered entity would not only be violating the Privacy Rule, but would also not be in compliance with § 164.306(a)(3) of this rule.

Paragraph (d) of § 164.306 establishes two types of implementation specifications, required and addressable. It provides that required implementation specifications must be met. However, with respect to implementation specifications that are addressable, § 164.306(d)(3) specifies that covered entities must assess whether an implementation specification is a reasonable and appropriate safeguard in its environment, which may include consideration of factors such as the size and capability of the organization as well as the risk. If the organization determines it is a reasonable and appropriate safeguard, it must implement the specification. If an addressable implementation specification is determined not to be a reasonable and appropriate answer to a covered entity's security needs, the covered entity must do one of two things: implement another equivalent measure if reasonable and appropriate; or if the standard can otherwise be met, the covered entity may choose to not implement the implementation specification or any equivalent alternative measure at all. The covered entity must document the rationale behind not implementing the implementation specification. See the detailed discussion in section II.A.3.

Paragraph (e) of § 164.306 addresses the requirement for covered entities to maintain the security measures