

We received a number of comments that pertained to privacy issues. These issues were considered in the development of the Privacy Rule and many of these comments were addressed in the preamble of the Privacy Rule. Therefore, we are referring the reader to that document for a discussion of those issues.

2. Level of Detail

We solicited comments as to the level of detail expressed in the required implementation features; that is, we specifically wanted to know whether commenters believe the level of detail of any proposed requirement went beyond what is necessary or appropriate. We received numerous comments expressing the view that the security standards should not be overly prescriptive because the speed with which technology is evolving could make specific requirements obsolete and might in fact deter technological progress. We have accordingly written the final rule to frame the standards in terms that are as generic as possible and which, generally speaking, may be met through various approaches or technologies.

3. Implementation Specifications

In addition to adopting standards, this rule adopts implementation specifications that provide instructions for implementing those standards.

However, in some cases, the standard itself includes all the necessary instructions for implementation. In these instances, there may be no corresponding implementation specification for the standard specifically set forth in the regulations text. In those instances, the standards themselves also serve as the implementation specification. In other words, in those instances, we are adopting one set of instructions as both the standard and the implementation specification. The implementation specification would, accordingly, in those instances be required.

In this final rule, we adopt both "required" and "addressable" implementation specifications. We introduce the concept of "addressable implementation specifications" to provide covered entities additional flexibility with respect to compliance with the security standards.

In meeting standards that contain addressable implementation specifications, a covered entity will ultimately do one of the following: (a) Implement one or more of the addressable implementation specifications; (b) implement one or more alternative security measures; (c)

implement a combination of both; or (d) not implement either an addressable implementation specification or an alternative security measure. In all cases, the covered entity must meet the standards, as explained below.

The entity must decide whether a given addressable implementation specification is a reasonable and appropriate security measure to apply within its particular security framework. This decision will depend on a variety of factors, such as, among others, the entity's risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. Based upon this decision the following applies:

(a) If a given addressable implementation specification is determined to be reasonable and appropriate, the covered entity must implement it.

(b) If a given addressable implementation specification is determined to be an inappropriate and/or unreasonable security measure for the covered entity, but the standard cannot be met without implementation of an additional security safeguard, the covered entity may implement an alternate measure that accomplishes the same end as the addressable implementation specification. An entity that meets a given standard through alternative measures must document the decision not to implement the addressable implementation specification, the rationale behind that decision, and the alternative safeguard implemented to meet the standard. For example, the addressable implementation specification for the integrity standard calls for electronic mechanisms to corroborate that data have not been altered or destroyed in an unauthorized manner (see 45 CFR 164.312(c)(2)). In a small provider's office environment, it might well be unreasonable and inappropriate to make electronic copies of the data in question. Rather, it might well be more practical and afford a sufficient safeguard to make paper copies of the data.

(c) A covered entity may also decide that a given implementation specification is simply not applicable (that is, neither reasonable nor appropriate) to its situation and that the standard can be met without implementation of an alternative measure in place of the addressable implementation specification. In this scenario, the covered entity must document the decision not to implement the addressable specification, the rationale behind that decision, and how the standard is being met. For example, under the

information access management standard, an access establishment and modification implementation specification reads: "implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process" (45 CFR 164.308(a)(4)(ii)(c)). It is possible that a small practice, with one or more individuals equally responsible for establishing and maintaining all automated patient records, will not need to establish policies and procedures for granting access to that electronic protected health information because the access rights are equal for all of the individuals.

a. *Comment:* A large number of commenters indicated that mandating 69 implementation features would result in a regulation that is too burdensome, intrusive, and difficult to implement. These commenters requested that the implementation features be made optional to meet the requirements. A number of other commenters requested that all implementation features be removed from the regulation.

Response: Deleting the implementation specifications would result in the standards being too general to understand, apply effectively, and enforce consistently. Moreover, a number of implementation specifications are so basic that no covered entity could effectively protect electronic protected health information without implementing them. We selected 13 of these mandatory implementation specifications based on (1) the expertise of Federal security experts and generally accepted industry practices and, (2) the recommendation for immediate implementation of certain technical and organizational practices and procedures described in Chapter 6 of *For The Record: Protecting Electronic Health Information*, a 1997 report by the National Research Council (NRC). These mandatory implementation specifications are referred to as required implementation specifications and are reflected in the NRC report's recommendations. Risk Analysis and Risk management are found in the NRC recommendation title System Assessment; Sanction Policy is required in the Sanctions recommendation; Information system Activity Review is discussed in Audit Trails; Response and Reporting circumstances.

In addition, a number of voluntary national and regional organizations have been formed to address HIPAA implementation issues and to facilitate