

standard for electronic signatures. This final rule adopts only security standards. All comments concerning the proposed electronic signature standard, responses to these comments, and a final rule for electronic signatures will be published at a later date. A detailed discussion of the provisions of the August 12, 1998 proposed rule can be found at 63 FR 43245 through 43259.

We originally proposed to add part 142, entitled "Administrative Requirements," to title 45 of the Code of Federal Regulations (CFR). It has now been determined that this material will reside in subchapter C of title 45, consisting of parts 160, 162, and 164. Subpart A of part 160 contains the general provisions applicable to all the Administrative Simplification rules; other subparts of part 160 will contain other requirements applicable to all standards. Part 162 contains the standards for transactions and code sets and will contain the identifier standards. Part 164 contains the standards relating to privacy and security. Subpart A of part 164 contains general provisions applicable to part 164; subpart E contains the privacy standards. Subpart C of part 164, which is adopted in this final rule, adopts standards for the security of electronic protected health information.

### III. Analysis of, and Responses to, Public Comments on the Proposed Rule

We received approximately 2,350 timely public comments on the August 12, 1998 proposed rule. The comments came from professional associations and societies, health care workers, law firms, health insurers, hospitals, and private individuals. We reviewed each commenter's letter and grouped related comments. Some comments were identical. After associating like comments, we placed them in categories based on subject matter or based on the section(s) of the regulations affected and then reviewed the comments.

In this section of the preamble, we summarize the provisions of the proposed regulations, summarize the related provisions in this final rule, and respond to comments received concerning each area.

It should be noted that the proposed Security Rule contained multiple proposed "requirements" and "implementation features." In this final rule, we replace the term "requirement" with "standard." We also replace the phrase "implementation feature" with "implementation specification." We do this to maintain consistency with the use of those terms as they appear in the statute, the Transactions Rule, and the Privacy Rule. Within the comment and

response portion of this final rule, for purposes of continuity, however, we use "requirement" and "implementation feature" when we are referring specifically to matters from the proposed rule. In all other instances, we use "standard" and "implementation specification."

The proposed rule would require that each covered entity (as now described in § 160.102) engaged in the electronic maintenance or transmission of health information pertaining to individuals assess potential risks and vulnerabilities to such information in its possession in electronic form, and develop, implement, and maintain appropriate security measures to protect that information. Importantly, these measures would be required to be documented and kept current.

The proposed security standard was based on three basic concepts that were derived from the Administrative Simplification provisions of HIPAA. First, the standard should be comprehensive and coordinated to address all aspects of security. Second, it should be scalable, so that it can be effectively implemented by covered entities of all types and sizes. Third, it should not be linked to specific technologies, allowing covered entities to make use of future technology advancements.

The proposed standard consisted of four categories of requirements that a covered entity would have to address in order to safeguard the integrity, confidentiality, and availability of its electronic health information pertaining to individuals: administrative procedures, physical safeguards, technical security services, and technical mechanisms. The implementation features described the requirements in greater detail when that detail was needed. Within the four categories, the requirements and implementation features were presented in alphabetical order to convey that no one item was considered to be more important than another.

The four proposed categories of requirements and implementation features were depicted in tabular form along with the electronic signature standard in a combined matrix located at Addendum 1. We also provided a glossary of terms, at Addendum 2, to facilitate a common understanding of the matrix entries, and at Addendum 3, we mapped available existing industry standards and guidelines to the proposed security requirements.

#### A. General Issues

The comment process overwhelmingly validated our basic

assumptions that the entities affected by this regulation are so varied in terms of installed technology, size, resources, and relative risk, that it would be impossible to dictate a specific solution or set of solutions that would be useable by all covered entities. Many commenters also supported the concept of technological neutrality, which would afford them the flexibility to select appropriate technology solutions and to adopt new technology over time.

#### 1. Security Rule and Privacy Rule Distinctions

As many commenters recognized, security and privacy are inextricably linked. The protection of the privacy of information depends in large part on the existence of security measures to protect that information. It is important that we note several distinct differences between the Privacy Rule and the Security Rule.

The security standards below define administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. The standards require covered entities to implement basic safeguards to protect electronic protected health information from unauthorized access, alteration, deletion, and transmission. The Privacy Rule, by contrast, sets standards for how protected health information should be controlled by setting forth what uses and disclosures are authorized or required and what rights patients have with respect to their health information.

As is discussed more fully below, this rule narrows the scope of the information to which the safeguards must be applied from that proposed in the proposed rule, electronic health information pertaining to individuals, to protected health information in electronic form. Thus, the scope of information covered in this rule is consistent with the Privacy Rule, which addresses privacy protections for "protected health information." However, the scope of the Security Rule is more limited than that of the Privacy Rule. The Privacy Rule applies to protected health information in any form, whereas this rule applies only to protected health information in electronic form. It is true that, under section 1173(d) of the Act, the Secretary has authority to cover "health information," which, by statute, includes information in other than electronic form. However, because the proposed rule proposed to cover only health information in electronic form, we do not include security standards for health information in non-electronic form in this final rule.