

implemented by reviewing and modifying the measures as needed to continue the provision of reasonable and appropriate protections, for example, as technology moves forward, and as new threats or vulnerabilities are discovered.

#### 1. Scope of Health Information Covered by the Rule (§ 164.306(a))

We proposed to cover health information maintained or transmitted by a covered entity in electronic form. We have modified, by narrowing, the scope of health information to be safeguarded under this rule from that which was proposed. The statute requires the privacy standards to cover individually identifiable health information. The Privacy Rule covers all individually identifiable information except for: (1) Education records covered by the Family and Educational Rights and Privacy Act (FERPA); (2) records described in 20 U.S.C. 1232g(a)(4)(B)(iv); and (3) employment records. (see the Privacy Rule at 65 FR 82496. See also 67 FR 53191 through 53193). The scope of information covered in the Privacy Rule is referred to as "protected health information." Based upon the comments we received, we align the requirements of the Security and Privacy Rules with regard to the scope of information covered, in order to eliminate confusion and ease implementation. Thus, this final rule requires protection of the same scope of information as that covered by the Privacy Rule, except that it only covers that information if it is in electronic form.

We note that standards for the security of all health information or protected health information in nonelectronic form may be proposed at a later date.

a. *Comment:* One commenter stated that the rule should apply to aggregate information that is not identifiable to an individual. In contrast, another commenter asked that health information used for statistical analysis be exempted if the covered entity may reasonably expect that the removed information cannot be used to re-identify an individual.

*Response:* As a general proposition, any electronic protected health information received, created, maintained, or transmitted by a covered entity is covered by this final rule. We agree with the second commenter that certain information, from which identifiers have been stripped, does not come within the purview of this final rule. Information that is de-identified, as defined in the Privacy Rule at § 164.502(d) and § 164.514(a), is not

"individually identifiable" within the meaning of these rules and, thus, does not come within the definition of "protected health information." It accordingly is not covered by this final rule. For a full discussion of the issues of de-identification and re-identification of individually identifiable health information see 65 FR 82499 and 82708 through 82712 and 67 FR 53232 through 53234.

b. *Comment:* Several commenters asked whether systems that determine eligibility of clients for insurance coverage under broad categories such as medical coverage groups are considered health information. One commenter asked that we specifically exclude eligibility information from the standards.

*Response:* We cannot accept the latter suggestion. Eligibility information will typically be individually identifiable, and much eligibility information will also contain health information. If the information is "individually identifiable" and is "health information," (with three very specific exceptions noted in the general discussion above) and it is in electronic form, it is covered by the security standards if maintained or transmitted by a covered entity.

c. *Comment:* Several commenters requested clarification as to whether the standards apply to identifiable health information in paper form. Some commenters believed the rule should be applicable to paper; others argued that it should apply to all confidential, identifiable health information.

*Response:* While we agree that protected health information in paper or other form also should have appropriate security protections, the proposed rule proposing the security standards proposed to apply those standards to health information in electronic form only. We are, accordingly, not extending the scope in this final rule.

We may establish standards to secure protected health information in other media in a future rule, in accordance with our statutory authority to do so. See discussion, *supra*, responding to a comment on the definition of "health information" and "individually identifiable health information."

d. *Comment:* The proposed rule would have excluded "telephone voice response" and "faxback" systems from the security standards, and we specifically solicited comments on that issue. A number of commenters agreed that telephone voice response and faxback should be excluded from the regulation, suggesting that the privacy standards rather than the security standards should apply. Others wanted

those systems included, on the grounds that inclusion is necessary for consistency and in keeping with the intent of the Act. Still others specifically wanted personal computer-fax transmissions included. One commenter asked for clarification of when we would cover faxes, and another commenter asked why we were excluding them. Several commenters suggested that the other security requirements provide for adequate security of these systems.

*Response:* In light of these comments, we have decided that telephone voice response and "faxback" (that is, a request for information from a computer made via voice or telephone keypad input with the requested information returned as a fax) systems fall under this rule because they are used as input and output devices for computers, not because they have computers in them. Excluding these features would provide a huge loophole in any system concerned with security of the information contained and/or processed therein. It should be noted that employment of telephone voice response and/or faxback systems will generally require security protection by only one of the parties involved, and not the other. Information being transmitted via a telephone (either by voice or a DTMP tone pad) is not in electronic form (as defined in the first paragraph of the definition of "electronic media") before transmission and therefore is not subject to the Security Rule. Information being returned via a telephone voice response system in response to a telephone request is data that is already in electronic form and stored in a computer. This latter transmission does require protection under the Security Rule.

Although most recently made electronic devices contain microprocessors (a form of computer) controlled by firmware (an unchangeable form of computer program), we intend the term "computer" to include only software programmable computers, for example, personal computers, minicomputers, and mainframes. Copy machines, fax machines, and telephones, even those that contain memory and can produce multiple copies for multiple people are not intended to be included in the term "computer." Therefore, because "paper-to-paper" faxes, person-to-person telephone calls, video teleconferencing, or messages left on voice-mail were not in electronic form before the transmission, those activities are not covered by this rule. See also the definition of "electronic media" at § 160.103.