

We note that this guidance differs from the guidance regarding the applicability of the Transactions Rule to faxback and voice response systems. HHS has stated that faxback and voice response systems are not required to follow the standards mandated in the Transactions Rule. This new guidance refers only to this rule.

e. *Comment:* One commenter asked whether there is a need to implement special security practices to address the shipping and receiving of health information and asked that we more fully explain our expectations and solutions in the final rules.

Response: If the handling of electronic protected health information involves shipping and receiving, appropriate measures must be taken to protect the information. However, specific solutions are not provided within this rule, as discussed in section III.A.3 of this final rule. The device and media controls standard under § 164.310(d)(1) addresses this situation.

f. *Comment:* One commenter wanted the "HTML" statement reworded to eliminate a specific exemption for HTML from the regulation.

Response: The Transactions Rule did not adopt the proposed exemption for HTML. The use of HTML or any other electronic protocol is not exempt from the security standards. Generally, if protected health information is contained in any form of electronic transmission, it must be appropriately safeguarded.

g. *Comment:* One commenter asked to what degree "family history" is considered health information under this rule and what protections apply to family members included in a patient's family history.

Response: Any health-related "family history" contained in a patient's record that identifies a patient, including a person other than the patient, is individually identifiable health information and, to the extent it is also electronic protected health information, must be afforded the security protections.

h. *Comment:* Two commenters asked that the rule prohibit re-identification of de-identified data. In contrast, several commenters asked that we identify a minimum list or threshold of specific re-identification data elements (for example, name, city, and ZIP) that would fall under this final rule so that, for example, the rule would not affect numerous systems, for example, network adequacy and population-based clinical analysis databases. One commenter asked that we establish a means to use re-identified information if the entity already has access to the

information or is authorized to have access.

Response: The issue of re-identification is addressed in the Privacy Rule at § 164.502(d) and § 164.514(c). The reader is referred to those sections and the related discussion in the preamble to the Privacy Rule (65 FR 82712) and the preamble to the Privacy Modifications (67 FR 53232 through 53234) for a full discussion of the issues of re-identification. We note that once information in the possession (or constructive possession) of a covered entity is re-identified and meets the definition of electronic protected health information, the security standards apply.

2. Technology-Neutral Standards

Comment: Many commenters expressed support for our efforts to develop standards for the security of health information. A number of comments were made in support of the technology-neutral approach of the proposed rule. For example, one commenter stated, "By avoiding prescription of the specific technologies health care entities should use to meet the law's requirements, you are opening the door for industry to apply innovation. Technologies that don't currently exist or are impractical today could, in the near future, enhance health information security while minimizing the overall cost." Several other commenters stated that the requirements should be general enough to withstand changes to technology without becoming obsolete. One commenter anticipates no problems with meeting the standards.

In contrast, one commenter suggested that whenever possible, specific technology recommendations should provide sufficient detail to promote systems interoperability and decrease the tendency toward adoption of multiple divergent standards. Several commenters stated that by letting each organization determine its own rules, the rules impose procedural burdens without any substantive benefit to security.

Response: The overwhelming majority of comments supported our position. We do not believe it is appropriate to make the standards technology-specific because technology is simply moving too fast, for example, the increased use and sophistication of internet-enabled hand held devices. We believe that the implementation of these rules will promote the security of electronic protected health information by (1) providing integrity and confidentiality; (2) allowing only authorized individuals

access to that information; and (3) ensuring its availability to those authorized to access the information. The standards do not allow organizations to make their own rules, only their own technology choices.

3. Miscellaneous Comments

a. *Comment:* Some commenters stated that the requirements and implementation features set out in the proposed rule were not specific enough to be considered standards, and that the actual standards are delegated to the discretion of the covered entities, at the expense of medical record privacy. Several commenters stated that it was inappropriate to balance the interests of those seeking to use identifiable medical information without patient consent against the interest of patients. Several other commenters believe that allowing covered entities to make their own decisions about the adequacy and balance of security measures undermined patient confidentiality interests, and stated that the proposed rule did not appear to adequately consider patient concerns and viewpoints.

Response: Again, the overwhelming majority of commenters supported our approach. This final rule sets forth requirements with which covered entities must comply and labels those requirements as standards and implementation specifications. Adequate implementation of this final rule by covered entities will ensure that the electronic protected health information in a covered entity's care will be as protected as is feasible for that entity.

We disagree that covered entities are given complete discretion to determine their security policies under this rule, resulting in effect, in no standards. While cost is one factor a covered entity may consider in determining whether to implement a particular implementation specification, there is nonetheless a clear requirement that adequate security measures be implemented, see 45 CFR 164.306(b). Cost is not meant to free covered entities from this responsibility.

b. *Comment:* Several commenters requested we withdraw the regulations, citing resource shortages due to Y2K preparation, upcoming privacy legislation, and/or the "excessive micro-management" contained in the rules. One commenter stated that, to insurers, these rules were onerous, not necessary, and not justified as cost-effective, as they already have effective practices for computer security and are subject to rigorous State laws for the safeguarding of health information. Another