

2. *Comment:* Several commenters recommended expansion of applicability, either to other specific entities, or to all entities involved in health care. Others wanted to know whether the standards apply to entities such as employers, public health organizations, medical schools, universities, research organizations, plan brokers, or non-EDI providers. One commenter asked whether the standards apply to State data organizations operating in capacities other than as plans, clearinghouses, or providers. Still other commenters stated that it was inappropriate to include physicians and other health care professionals in the same category as plans and clearinghouses, arguing that providers should be subject to different, less burdensome requirements because they already protect health information.

*Response:* The statute does not cover all health care entities that transmit or maintain individually identifiable health information. Section 1172(a) of the Act provides that only health plans, health care clearinghouses, and certain health care providers (as discussed above) are covered. With respect to the comments regarding the difference between providers and plans/clearinghouses, we have structured the Security Rule to be scalable and flexible enough to allow different entities to implement the standards in a manner that is appropriate for their circumstances. Regarding the coverage of entities not within the jurisdiction of HIPAA, see the Privacy Rule at 82567 through 82571.

3. *Comment:* One commenter asked whether the standards would apply to research organizations, both to those affiliated with health care providers and those that are not.

*Response:* Only health plans, health care clearinghouses, and certain health care providers are required to comply with the security standards. Researchers who are members of a covered entity's work force may be covered by the security standards as part of the covered entity. See the definition of "workforce" at 45 CFR 160.103. Note, however, that a covered entity could, under appropriate circumstances, exclude a researcher or research division from its health care component or components (see § 164.105(a)). Researchers who are not part of the covered entity's workforce and are not themselves covered entities are not subject to the standards.

4. *Comment:* Several commenters stated that internal networks and external networks should be treated differently. One commenter asked for further clarification of the difference

between what needs to be secured external to a corporation versus the security of data movement within an organization. Another stated that complying with the security standards for internal communications may prove difficult and costly to monitor and control. In contrast, one commenter stated that the existence of requirements should not depend on whether use of information is for internal or external purposes.

Another commenter argued that the regulation goes beyond the intent of the law, and while communication of electronic information between entities should be covered, the law was never intended to mandate changes to an entity's internal automated systems. One commenter requested that raw data that are only for the internal use of a facility be excluded, provided that reasonable safeguards are in place to keep the raw data under the control of the facility.

*Response:* Section 1173(d)(2) of the Act states: Each person described in section 1172(a) who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards—(A) to ensure the integrity and confidentiality of the information; (B) to protect against any reasonably anticipated—(i) threats or hazards to the security or integrity of the information; and (ii) unauthorized uses or disclosures of the information; and (C) otherwise to ensure compliance with this part by the officers and employees of such person.

This language draws no distinction between internal and external data movement. Therefore, this final rule covers electronic protected health information at rest (that is, in storage) as well as during transmission.

Appropriate protections must be applied, regardless of whether the data are at rest or being transmitted. However, because each entity's security needs are unique, the specific protections determined appropriate to adequately protect information will vary and will be determined by each entity in complying with the standards (see the discussion below).

5. *Comment:* Several commenters found the following statement in the proposed rule (63 FR 43245) at section II.A. confusing and asked for clarification: "With the exception of the security standard, transmission within a corporate entity would not be required to comply with the standards."

*Response:* In the final Transactions Rule, we revised our approach concerning the transaction and code set exemptions, replacing this concept with

other tests that determine whether a particular transaction is subject to those standards (see the discussion in the Transactions Rule at 65 FR 50316 through 50318). We also note that the Privacy Rule regulates a covered entity's use, as well as disclosure, of protected health information.

6. *Comment:* One commenter stated that research would be hampered if proposed § 142.306(a) applied. The commenter believes that research uses of health information should be excluded or the standard should be revised to allow appropriate flexibility for research depending on the risk to patients or subjects (for example, if the information is anonymous, there is no risk, and it would not be necessary to meet the security standards).

*Response:* If electronic protected health information is de-identified (as truly anonymous information would be), it is not covered by this rule because it is no longer electronic protected health information (see 45 CFR 164.502(d) and 164.514(a)). Electronic protected health information received, created, or maintained by a covered entity, or that is transmitted by covered entities, is covered by the security standards and must be protected. To the extent a researcher is a covered entity, the researcher must comply with these standards with respect to electronic protected health information. Otherwise, the conditions for release of such information to researchers is governed by the Privacy Rule. See, for example, 45 CFR 164.512(i), 164.514(e) and 164.502(d). These standards would not apply to the researchers as such in the latter circumstances.

7. *Comment:* One commenter asked to what extent individual patients are subject to the standards. For example, some telemedicine practices support the use of diagnostic systems in the patient's home, which can be used to conduct tests and send results to a remote physician. In other cases, patients may be responsible for the filing of insurance claims directly and will need the ability to verify facts, confirm receipt of claims, and so on. The commenter asked if it is the intent of the rule to include electronic transmission to or from the patient.

*Response:* Patients are not covered entities and, thus, are not subject to these standards. With respect to transmissions from covered entities, covered entities must protect electronic protected health information when they transmit that information. See also the discussion of encryption in section III.G.