

express and specific exemptions of State laws with respect to medical privacy.

*Response:* The Privacy Rule establishes standards for the rights of patients in regard to the privacy of their medical records and for the allowable uses and disclosures of protected health information. The identified concerns were discussed in the Privacy Rule (see 65 FR 82587 through 82588). The security standards do not specifically address privacy but will safeguard electronic protected health information against unauthorized access or modification.

b. *Comment:* One commenter asked how these regulations relate to confidentiality laws, which vary from State to State.

*Response:* It is difficult to respond to this question in the abstract without the benefit of reference to a specific State statute. However, in general, these security standards will preempt contrary State laws. Per section 1178(a)(2) of the Act, this general rule would not hold if the Secretary determines that a contrary provision of State law is necessary for certain identified purposes to prevent fraud and abuse; to ensure appropriate State regulation of insurance and health plans; for State reporting on health care delivery costs; or if it addresses controlled substances. See 45 CFR part 160 subpart B. In such case, the contrary provision of State law would preempt a Federal provision of these security standards. State laws that are related but not contrary to this final rule, will not be affected.

Section 1178 of the Act also limits the preemptive effect of the Federal requirements on certain State laws other than where the Secretary makes certain determinations. Section 1178(b) of the Act provides that State laws for reporting of disease and other conditions and for public health surveillance, investigation, or intervention are not invalidated or limited by the Administrative Simplification rules. Section 1178(c) of the Act provides that the Federal requirements do not limit States' abilities to require that health plans report or provide access to certain information.

c. *Comment:* Several commenters stated that allowing State law to establish additional security restrictions conflicts with the purpose of the Federal rule and/or would make implementation very difficult. One commenter asked for clarification as to whether additional requirements tighter than the requirements outlined in the proposed rule may be imposed.

*Response:* The general rule is that the security standards in this final rule supersede contrary State law. Only where the Secretary has granted an exception under section 1178(a)(2)(A) of the Act, or in situations under section 1178(b) or (c) of the Act, will the general rule not hold true. Covered entities may be required to adhere to stricter State-imposed security measures that are not contrary to this final rule.

## 2. Enforcement

The proposed rule did not contain specific enforcement provisions. This final rule likewise does not contain specific enforcement provisions; it is expected that enforcement provisions applicable to all Administrative Simplification rules will be proposed in a future rulemaking.

a. *Comment:* One commenter voiced support for the proposed rule's approach. Another stated that the process is poorly defined. One commenter stated that fines should be eliminated, or the scope of activity subject to fines should be more narrowly defined.

While a number of commenters were of the opinion that HHS must retain enforcement responsibility, stating that it would be unconstitutional to give it to a private entity, several others stated that it may not be practical for HHS to retain the responsibility for determining violations and imposing penalties specified by the statute. A concern was voiced over HHS's ability to fairly and consistently apply the rules due to budget constraints. Several commenters support industry solutions to enforcement with some level of government involvement. One commenter recommended a single audit process using accrediting bodies already in place. Another stated that entities providing accreditation services should not be involved in enforcement as this would result in a conflict of interest.

Clarification was requested, including the use of examples, concerning what constitutes a violation, and how a penalty applies to a "person." Commenters asked if the term "person" referred to the people responsible for the system and how penalties would apply to corporations and other entities.

*Response:* It is expected that enforcement of HIPAA standards will be addressed in regulations to be issued at a later date.

b. *Comment:* Several commenters stated that enforcement of the security standards will be arbitrarily delegated to private businesses that compete with physicians and with each other.

*Response:* These comments are premature for the reasons stated above.

## 3. Comment Period

The comment period on the proposed rule was 60 days.

*Comment:* We received comments suggesting that significant changes to the standards could occur in the final rule as a result of changes made in response to comments. The commenter believes such changes could adversely affect payers and providers, and suggested that the rule should be republished as a proposed rule with a new comment period to allow additional comments concerning any changes. A "work-in-progress" approach was also suggested, to give all stakeholders time to read, analyze, and comment upon evolving versions of a particular proposed rule.

*Response:* We have not accepted these suggestions. The numerous comments received were thoughtful, analytical, detailed, and addressed every area of the proposed rule. This response to the proposed rule indicates that the public had ample time to read, analyze, and comment upon the proposed rule. If we were to treat the rule as a "work-in-progress" and issue evolving versions, allowing for comments to each version, we would never implement the statute and achieve administrative simplification as directed by the Congress.

## M. Proposed Impact Analysis

The preamble to the Transactions Rule contains comments and responses on the impact of all the administrative simplification standards in general except privacy. Comments and responses specific to the relative impact of implementing this final rule are presented below.

a. *Comment:* Several commenters stated that the proposed security standards are complex, costly, administratively burdensome, and could result in decreased use of EDI. One commenter stated that this rule runs counter to the explicit intent of Administrative Simplification that requires, "any standard adopted under this part shall be consistent with the objective of reducing the administrative costs of providing and paying for health care."

Several commenters expressed concern that there was no cost benefit analysis provided for these proposed regulations, stating that, faced with increasingly limited resources, it is essential that a security standards cost/benefit analysis for all health care trading partners be provided. Another said an independent cost estimate by the General Accounting Office (GAO) should be performed on these rules and