

ourselves in the difficult position of reacting to proposed rules setting the standards for how information should be physically and electronically protected, without having reached agreement on the larger issues of consent for and disclosure of individual medical information.”

Response: The effective date of the final rule is 60 days after this final rule is published in the **Federal Register**. The statute sets forth the compliance dates for the standards. Covered entities must comply with this final rule no later than 24 months (36 months for small plans) after the effective date.

The final Privacy Rule has already been published. We note that numerous comments concerning the timing of the adoption of privacy and security standards were also received in the privacy rulemaking and are discussed in the Privacy Rule at 65 FR 82752.

2. *Comment:* One commenter asked that proposed § 142.312 be rewritten to separate the effective dates for the Security Rule and the Transactions Rule.

Response: The proposed rule incorporated general language applicable to all the proposed Administrative Simplification standards. Language concerning standards other than Security is not included in § 164.318. Because this final rule is adopted after the Transactions Rule was adopted, the compliance dates for the security standards differ from those for the transactions standards. Comments concerning general effective dates were addressed in the Transactions Rule. Comments specific to the security standards are addressed here.

3. *Comment:* Several commenters suggested that we not allow early implementation of the Security Rules. A number of others asked that we allow, but not require, early implementation by willing trading partners. Another commenter suggested that early implementation by willing trading partners be allowed as long as the data content transmitted is equal to that required by statute. Another commenter requested that it be stipulated that entities cannot implement less than 1 year from the date of this final rule and then only after successful testing, and that a “start testing by” date be defined.

Response: Whether or not to implement before the compliance date is a business decision that each covered entity must make. Moreover, the vast majority of the standards address internal policies and procedures that can be implemented at any time without any impact on trading partners.

4. *Comment:* One commenter asked us to establish a research site or test laboratory for a trial implementation.

Response: The concept of a “trial implementation” that would have widespread relevance is inconsistent with our basic principles of flexibility, scalability, and technology-neutrality.

5. *Comment:* One commenter stated that the 2-year time frame for implementation of a contingency plan is too short for health plans that serve multiple regions of the country.

Response: The Congress mandated that entities must be in compliance 2 years from the initial standard’s adoption date (3 years for small plans).

K. Appendix

The proposed rule contained three addenda. Addendum 1 set out in matrix form the proposed requirements and related implementation features of the proposed rule. Addendum 2 set out in list form a glossary of terms with citations to the sources of those terms. Addendum 3 identified and mapped areas of overlap in the proposed security standard and implementation features.

This final rule retains only the first proposed addendum, the matrix, as an appendix, that is modified to reflect the changes in the administrative, physical, and technical safeguard portions of the rule below. Numerous terms in the glossary now appear in the rule below, typically (but not always) as definitions.

1. *Comment:* Over two-thirds of the comments received on this topic asked that the matrix be incorporated into the final rule. One commenter asked that a simplified version be made part of the final rule. Six commenters wanted it kept in this final rule as an addendum. One commenter stated that it should be in an appendix to the rule, while others stated that it should not be included in this final rule.

Response: Since a significant majority of commenters requested retention of the matrix, it has been incorporated into this final rule as an appendix. The matrix displays, in tabular form, the administrative, physical, and technical safeguard standards and relating implementation specifications described in this final rule in § 164.308, § 164.310, and § 164.312. It should be noted that the requirements of § 164.105, § 164.314, and § 164.316 are not presented in the matrix.

2. *Comment:* A large majority of commenters stated that the glossary located in Addendum 2 of the proposed rule should be included as part of the final rule. Several commenters asked that it be incorporated into the definitions section of the final rule. One

commenter stated that the glossary should not be part of this final rule.

Response: The terms defined in the glossary in Addendum 2 of the proposed rule are found throughout this final rule, either as part of the text of § 164.306 through § 164.312 or under § 164.304, as appropriate. We included only terms relevant to the particular standards and implementation specifications being adopted.

3. *Comment:* Several commenters requested that the mapped matrix located in Addendum 3 of the proposed rule be included in this final rule, either as part of the rule or as an addendum, while others stated that it should not be part of this final rule. Several commenters cited items to be added to the mapped matrix.

Response: The mapped matrix was merely a snapshot of current standards and guidelines that the implementation team was able to obtain for review during the development of the security and electronic signature requirements and was provided in the proposed rule as background material. Since this matrix has not been fully populated or kept up-to-date, it is not being published as part of this final rule. Where relevant, we do reference various standards and guidelines indicated in the matrix in this preamble.

L. Miscellaneous Issues

1. Preemption

The statute requires generally that the security standards supersede contrary provisions of State law including State law requiring medical or health plan records to be maintained or transmitted in written rather than electronic formats. The statute provides certain exceptions to the general rule; section 1178(a)(2) of the Act identifies conditions under which an exception applies. The proposed rule did not provide for a process for making exception determinations; rather, a process was proposed in the privacy rulemaking and was adopted with the Privacy Rule (see part 160, subpart B). This process applies to exception determinations for all of the Administrative Simplification rules, including this rule.

a. *Comment:* Several commenters stated that the proposed rule does not include substantive protections for the privacy rights of patients’ electronic medical records, while the rule attempts to preempt State privacy laws with respect to these records. Comments stated that, by omitting a clarification of State privacy law applicability, the proposed rule creates confusion. They believe that the rule must contain