

Encryption; Alarm; Audit trails; Entity authentication; and Event reporting.

In this final rule, we consolidate these provisions into § 164.312. That section now includes standards regarding access controls, audit controls, integrity (previously titled data authentication), person or entity authentication, and transmission security. As discussed below, while certain implementation specifications are required, many of the proposed security implementation features are now addressable implementation specifications. The function of authorization control has been incorporated into the information access management standard under § 164.308, Administrative safeguards.

1. Access Control (§ 164.312(a)(1))

In the proposed rule, we proposed to require that the access controls requirement include features for emergency access procedures and provisions for context-based, role-based, and/or user-based access; we also proposed the optional use of encryption as a means of providing access control. In this final rule, we require unique user identification and provision for emergency access procedures, and retain encryption as an addressable implementation specification. We also make “Automatic logoff” an addressable implementation specification. “Automatic logoff” and “Unique user identification” were formerly implementation features under the proposed “Entity authentication” (see § 164.312(d)).

a. *Comment:* Some commenters believe that in specifying “Context,” “Role,” and “User” based controls, use of other controls would effectively be excluded, for example, “Partition rule-based access controls,” and the development of new access control technology.

Response: We agree with the commenters that other types of access controls should be allowed. There was no intent to limit the implementation features to the named technologies and this final rule has been reworded to make it clear that use of any appropriate access control mechanism is allowed. Proposed implementation features titled “Context-based access,” “Role-based access,” and “User-based access” have been deleted and the access control standard at § 164.312(a)(1) states the general requirement.

b. *Comment:* A large number of comments were received objecting to the identification of “Automatic logoff” as a mandatory implementation feature. Generally the comments asked that we not be so specific and allow other forms of inactivity lockout, and that this type

of feature be made optional, based more on the particular configuration in use and a risk assessment/analysis.

Response: We agree with the comments that mandating an automatic logoff is too specific. This final rule has been written to clarify that the proposed implementation feature of automatic logoff now appears as an addressable access control implementation specification and also permits the use of an equivalent measure.

c. *Comment:* We received comments asking that encryption be deleted as an implementation feature and stating that encryption is not required for “data at rest.”

Response: The use of file encryption is an acceptable method of denying access to information in that file. Encryption provides confidentiality, which is a form of control. The use of encryption, for the purpose of access control of data at rest, should be based upon an entity’s risk analysis. Therefore, encryption has been adopted as an addressable implementation specification in this final rule.

d. *Comment:* We received one comment stating that the proposed implementation feature “Procedure for emergency access,” is not access control and recommending that emergency access be made a separate requirement.

Response: We believe that emergency access is a necessary part of access controls and, therefore, is properly a required implementation specification of the “Access controls” standard. Access controls will still be necessary under emergency conditions, although they may be very different from those used in normal operational circumstances. For example, in a situation when normal environmental systems, including electrical power, have been severely damaged or rendered inoperative due to a natural or man-made disaster, procedures should be established beforehand to provide guidance on possible ways to gain access to needed electronic protected health information.

2. Audit Controls (§ 164.312(b))

We proposed that audit control mechanisms be put in place to record and examine system activity. We adopt this requirement in this final rule.

a. *Comment:* We received a comment stating that “Audit controls” should be an implementation feature rather than the standard, and suggesting that we change the title of the standard to “Accountability,” and provide additional detail to the audit control implementation feature.

Response: We do not adopt the term “Accountability” in this final rule

because it is not descriptive of the requirement, which is to have the capability to record and examine system activity. We believe that it is appropriate to specify audit controls as a type of technical safeguard. Entities have flexibility to implement the standard in a manner appropriate to their needs as deemed necessary by their own risk analyses. For example, see NIST Special Publication 800–14, *Generally Accepted Principles and Practices for Securing Information Technology Systems* and NIST Special Publication 800–33, *Underlying Technical Models for Information Technology Security*.

b. *Comment:* One commenter recommended that this final rule state that audit control mechanisms should be implemented based on the findings of an entity’s risk assessment and risk analysis. The commenter asserted that audit control mechanisms should be utilized only when appropriate and necessary and should not adversely affect system performance.

Response: We support the use of a risk assessment and risk analysis to determine how intensive any audit control function should be. We believe that the audit control requirement should remain mandatory, however, since it provides a means to assess activities regarding the electronic protected health information in an entity’s care.

c. *Comment:* One commenter was concerned about the interplay of State and Federal requirements for auditing of privacy data and requested additional guidance on the interplay of privacy rights, laws, and the expectation for audits under the rule.

Response: In general, the security standards will supercede any contrary provision of State law. Security standards in this final rule establish a minimum level of security that covered entities must meet. We note that covered entities may be required by other Federal law to adhere to additional, or more stringent security measures. Section 1178(a)(2) of the statute provides several exceptions to this general rule. With regard to protected health information, the preemption of State laws and the relationship of the Privacy Rule to other Federal laws is discussed in the Privacy Rule beginning at 65 FR 82480; the preemption provisions of the rule are set out at 45 CFR part 160, subpart B.

It should be noted that although the Privacy Rule does not incorporate a requirement for an “audit trail” function, it does call for providing an accounting of certain disclosures of protected health information to an