

was too detailed and some of the requirements excessive.

Response: Based upon the comments received, we agree that termination procedures should not be a separate standard; however, consideration of termination procedures remains relevant for any covered entity with employees, because of the risks associated with the potential for unauthorized acts by former employees, such as acts of retribution or use of proprietary information for personal gain. We further agree with the reasoning of the commenters who asked that these procedures be made optional; therefore, "Termination procedures" is now reflected in this final rule as an addressable implementation specification. We also removed reference to all specific termination activities, for example, changing locks, because, although the activities may be considered appropriate for some covered entities, they may not be reasonable for others.

f. *Comment:* One commenter asked whether human resource employee termination policies and procedures must be documented to show the types of security breaches that would result in termination.

Response: Policies and procedures implemented to adhere to this standard must be documented (see § 164.316 below). The purpose of termination procedure documentation under this implementation specification is not to detail when or under which circumstances an employee should be terminated. This information would more appropriately be part of the entity's sanction policy. The purpose of termination procedure documentation is to ensure that termination procedures include security-unique actions to be followed, for example, revoking passwords and retrieving keys when a termination occurs.

4. Information Access Management (§ 164.308(a)(4))

We proposed an "information access control" requirement for establishment and maintenance of formal, documented policies and procedures defining levels of access for all personnel authorized to access health information, and how access is granted and modified. In § 164.308(a)(4)(ii)(B) and (C) below, the proposed implementation features are made addressable specifications. We have added in § 164.308(a)(4)(ii)(A), a required implementation specification to isolate health care clearinghouse functions to address the provisions of section 1173(d)(1)(B) of the Act which related to this area.

a. *Comment:* One commenter asked that the requirement be deleted, expressing the opinion that this requirement goes beyond "reasonable boundaries" into regulating common business practices. In contrast, another asked that we expand this requirement to identify participating parties and access privileges relative to specific data elements.

Response: We disagree that this requirement improperly imposes upon business functions. Restricting access to those persons and entities with a need for access is a basic tenet of security. By this mechanism, the risk of inappropriate disclosure, alteration, or destruction of information is minimized. We cannot, however, specifically identify participating parties and access privileges relative to data elements within this regulation. These will vary depending upon the entity, the needs within the user community, the system in which the data resides, and the specific data being accessed. This standard is consistent with § 164.514(d) in the Privacy Rule (minimum necessary requirements for use and disclosure of protected health information), and is, therefore, being retained.

b. *Comment:* Several commenters asked that we not mandate the implementation features, but leave them as optional, a suggested means of compliance. The commenters noted that this might make the rules more scalable and flexible, since this approach would allow providers to implement safeguards that best addressed their needs. Along this line, one commenter expressed the belief that each organization should implement features deemed necessary based on its own risk assessment.

Response: While the information access management standard in this final rule must be met, we agree that the implementation specifications at § 164.308(a)(4)(ii)(B) and (C) should not be mandated but posed as a suggested means of compliance, which must be addressed. These specifications may not be applicable to all entities based on their size and degree of automation. A fully automated covered entity spanning multiple locations and involving hundreds of employees may determine it has a need to adopt a formal policy for access authorization, while a small provider may decide that a desktop standard operating procedure will meet the specifications. The final rule has been revised accordingly.

c. *Comment:* Clarification was requested concerning the meaning of "formal."

Response: The word "formal" has caused considerable concern among commenters, as it was thought "formal" carried the connotation of a rigidly defined structure similar to what might be found in the Department of Defense instructions. As used in the proposed rule, this word was not intended to convey such a strict structure. Rather, it was meant to convey that documentation should be an official organizational statement as opposed to word-of-mouth or cryptic notes scratched on a notepad. While documentation is still required (see § 164.316), to alleviate confusion, the word "formal" has been deleted.

d. *Comment:* One commenter asked that we clarify that this requirement relates to both the establishment of policies for the access control function and to access control (the implementation of those policies).

Response: "Information access management" does address both the establishment of access control policies and their implementation. We use the term "implement" to clarify that the procedures must be in use, and we believe that the requirement to implement policies and procedures requires, as an antecedent condition, the establishment or adaptation of those policies and procedures.

5. Security Awareness and Training (§ 164.308(a)(5)(i))

We proposed, under the requirement "Training," that security training be required for all staff, including management. Training would include awareness training for all personnel, periodic security reminders, user education concerning virus protection, user education in the importance of monitoring login success/failure, and how to report discrepancies, and user education in password management.

In this final rule, we adopt this proposed requirement in modified form. For the standard "Security awareness and training," in § 164.308(a)(5), we require training of the workforce as reasonable and appropriate to carry out their functions in the facility. All proposed training features have been combined as implementation specifications under this standard. Specific implementation specifications relative to content are addressable. The "Virus protection" implementation feature has been renamed "protection from malicious software," because we did not intend by the nomenclature to exclude coverage of malicious acts that might not come within the prior term, such as worms.

a. *Comment:* One commenter believes that security awareness training for all