

Several thought this requirement could result in a significant resource and monetary burden to develop and maintain formal procedures. Two asked for an explanation of the benefit to be derived from this requirement.

One asked that covered entities be required to document processes that create a security risk only and suggested that a risk assessment would determine the need for this documentation.

*Response:* We agree with the commenters that the standard is ambiguous, and upon review, is unnecessary because the remaining standards, for example, device and media controls, provide adequate safeguards. Accordingly, this requirement is not adopted in this final rule.

#### F. Physical Safeguards (§ 164.310)

We proposed requirements and implementation features for documented physical safeguards to guard data integrity, confidentiality, and availability. We proposed to require safeguards in the following areas: Assigned security responsibility; media controls; physical access controls; policies and guidelines on workstation use; a secure workstation location; and security awareness training. A number of specific implementation features were proposed under the media controls and physical access controls requirements.

In § 164.310 of this final rule, most of the proposed implementation features are adopted as addressable implementation specifications. The proposed requirements for the assigned security responsibility and security awareness training requirements are relocated in § 164.308.

##### 1. General Comments

a. *Comment:* Several commenters made suggestions to modify the language to more clearly describe “Physical safeguards.”

*Response:* In response to comments, we have revised the definition of “Physical safeguards” to read as follows: “Physical safeguards are security measures to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.”

b. *Comment:* One commenter was concerned that electronic security systems could not be used in lieu of physical security systems.

*Response:* This final rule does not preclude the use of electronic security systems in lieu of, or in combination with, physical security systems to meet a “Physical safeguard” standard.

##### 2. Facility Access Controls (§ 164.310(a)(1))

We proposed, under the “Physical access controls” requirement, formal, documented policies and procedures for limiting physical access to an entity while ensuring that properly authorized access is allowed. These controls would include the following implementation features: disaster recovery, emergency mode operation, equipment control (into and out of site), a facility security plan, procedures for verifying access authorizations before physical access, maintenance records, need-to-know procedures for personnel access, sign-in for visitors and escort, if appropriate, and testing and revision.

In § 164.310(a)(2) below, we combine and restate these as addressable implementation specifications. These are contingency operations, facility security plan, access control and validation procedures, and maintenance records.

a. *Comment:* Many commenters were concerned because the proposed language would require implementation of all physical access control features. Other commenters were concerned that the language did not allow entities to use the results of their risk assessment and risk management process to arrive at the appropriate solutions for them.

*Response:* We agree that implementation of all implementation specifications may not be appropriate in all situations. While the facility access controls standard must be met, we agree that the implementation specifications should not be required in all circumstances, but should be addressable. In this final rule, all four implementation specifications are addressable.

We have also determined, based on “level of detail” comments requesting consolidation of the list of implementation features, that the proposed implementation feature “Equipment control (into and out of site)” was redundant. “Equipment control” is already covered under the “Device and media controls” standard at § 164.310(d)(1). Accordingly, we have eliminated it as a separate implementation specification.

b. *Comment:* One commenter raised the issue of a potential conflict of authority between those having access to the data and those responsible for checking and maintaining access controls.

*Response:* Any potential conflicts should be identified, addressed, and resolved in the policies and procedures developed according to the standards under § 164.308.

c. *Comment:* Several commenters questioned whether “Physical Access Controls” was a descriptive phrase to describe a technology to be used, or whether the phrase referred to a facility.

*Response:* We agree that the term “Physical” may be misleading; to remove any confusion, the requirement is reflected in this final rule as a standard titled “Facility access controls.” We believe this is a more precise term to describe that the standard, and its associated implementation specifications, is applicable to an entity’s business location or locations.

d. *Comment:* Several commenters requested that the disaster recovery and emergency mode operations features be moved to “Administrative safeguards.” Other commenters recommended that disaster recovery and emergency mode operations should be replaced by, and included in, a “Contingency Operations” implementation feature.

*Response:* The “Administrative safeguards” section addresses the contingency planning that must be done to contend with emergency situations. The placement of the disaster recovery and emergency mode operations implementation specifications in the “Physical safeguards” section is also appropriate, however, because “Physical safeguards” defines the physical operations (processes) that provide access to the facility to implement the associated plans, developed under § 164.308. We agree, however, that the term “contingency operations” better describes, and would include, disaster recovery and emergency mode operations, and have modified the regulation text accordingly (see § 164.310(a)(1)).

e. *Comment:* Commenters were concerned about having to address in their facility security plan the exterior/interior security of a building when they are one of many occupants rather than the sole occupant. Additional commenters were concerned that the responsibility for physical security of the building could not be delegated to a third party when the covered entity shares the building with other offices.

*Response:* The facility security plan is an addressable implementation specification. However, the covered entity retains responsibility for considering facility security even where it shares space within a building with other organizations. Facility security measures taken by a third party must be considered and documented in the covered entity’s facility security plan, when appropriate.