

*Response:* Upon review of the matrix and regulations text, we agree with the commenter, because this requirement involves an administrative decision at the highest levels of who should be responsible for ensuring security measures are implemented and maintained. Assigned security responsibility has been removed from "Physical safeguards" and is now located under "Administrative safeguards" at § 164.308.

### 3. Workforce Security (§ 164.308(a)(3)(i))

We proposed implementation of a number of features for personnel security, including ensuring that maintenance personnel are supervised by a knowledgeable person, maintaining a record of access authorizations, ensuring that operating and maintenance personnel have proper access authorization, establishing personnel clearance procedures, establishing and maintaining personnel security policies and procedures, and ensuring that system users have proper training.

In this final rule, to provide clarification and reduce duplication, we have combined the "Assure supervision of maintenance personnel by authorized, knowledgeable person" implementation feature and the "Operating, and in some cases, maintenance personnel have proper access authorization" feature into one addressable implementation specification titled "Authorization and/or supervision."

In a related, but separate, requirement entitled "Termination procedures," we proposed implementation features for the ending of an employee's employment or an internal or external user's access. These features would include things such as changing combination locks, removal from access lists, removal of user account(s), and the turning in of keys, tokens, or cards that allow access.

In this final rule, "Termination procedures" has been made an addressable implementation specification under "Workforce security." This is addressable because in certain circumstances, for example, a solo physician practice whose staff consists only of the physician's spouse, formal procedures may not be necessary.

The proposed "Personnel security policy/procedure" and "record of access authorizations" implementation features have been removed from this final rule, as they have been determined to be redundant. Implementation of the balance of the "Workforce security" implementation specifications and the

other standards contained within this final rule will result in assurance that all personnel with access to electronic protected health information have the required access authority as well as appropriate clearances.

a. *Comment:* The majority of comments concerned the supervision of maintenance personnel by an authorized knowledgeable person. Commenters stated this would not be feasible in smaller settings. For example, the availability of technically knowledgeable persons to ensure this supervision would be an issue. We were asked to either reword this implementation feature or delete it.

*Response:* We agree that a "knowledgeable" person may not be available to supervise maintenance personnel. We have accordingly modified this implementation specification so that, in this final rule, we are adopting an addressable implementation specification titled, "Authorization and/or supervision," requiring that workforce members, for example, operations and maintenance personnel, must either be supervised or have authorization when working with electronic protected health information or in locations where it resides (see § 164.308(a)(3)(ii)(A)). Entities can decide on the feasibility of meeting this specification based on their risk analysis.

b. *Comment:* The second largest group of comments requested assurance that, with regard to the proposed "Personnel clearance procedure" implementation feature, having appropriate clearances does not mean performing background checks on everyone. We were asked to delete references to "clearance" and use the term "authorization" in its place.

*Response:* We agree with the commenters concerning background checks. This feature was not intended to be interpreted as an absolute requirement for background checks. We retain the use of the term "clearance," however, because we believe that it more accurately conveys the screening process intended than does the term "authorization." We have attempted to clarify our intent in the language of § 164.308(a)(3)(ii)(B), which now reads, "Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate." The need for and extent of a screening process is normally based on an assessment of risk, cost, benefit, and feasibility as well as other protective measures in place. Effective personnel screening processes may be applied in a way to allow a range of implementation, from minimal procedures to more stringent procedures

based on the risk analysis performed by the covered entity. So long as the standard is met and the underlying standard of § 164.306(a) is met, covered entities have choices in how they meet these standards. To clarify the intent of this provision, we retitle the implementation specification "Workforce clearance procedure."

c. *Comment:* One commenter asked that we expand the implementation features to include the identification of the restrictions that should be placed on members of the workforce and others.

*Response:* We have not adopted this comment in the interest of maintaining flexibility as discussed in § 164.306. Restrictions would be dependent upon job responsibilities, the amount and type of supervision required and other factors. We note that a covered entity should consider in this regard the applicable requirements of the Privacy Rule (see, for example, § 164.514(d)(2) (relating to minimum necessary requirements), and § 164.530(c) (relating to safeguards).

*Comment:* One commenter believes that the proposed "Personnel security" requirement was reasonable, since an administrative determination of trustworthiness is needed before allowing access to sensitive information. Two commenters asked that we delete the requirement entirely. A number of commenters requested that we delete the implementation features. Another commenter stated that all the implementation features may not be applicable or even appropriate to a given entity and should be so qualified.

*Response:* While we do not believe this requirement should be eliminated, we agree that all the implementation specifications may not be applicable or even appropriate to a given entity. For example, a personal clearance may not be reasonable or appropriate for a small provider whose only assistant is his or her spouse. The implementation specifications are not mandatory, but must be addressed. This final rule has been changed to reflect this approach (see § 164.308(a)(3)(ii)(B)).

e. *Comment:* The majority of commenters on the "Termination procedures" requirement asked that it be made optional, stating that it may not be applicable or even appropriate in all circumstances and should be so qualified or posed as guidelines. A number of commenters stated that the requirement should be deleted. One commenter stated that much of the material covered under the "Termination procedures" requirement is already covered in "Information access control." A number of commenters stated that this requirement