

system users would be too difficult to do in a large organization.

*Response:* We disagree with the commenter. Security awareness training is a critical activity, regardless of an organization's size. This feature would typically become part of an entity's overall training program (which would include privacy and other information technology items as well). For example, the Government Information Systems Reform ACT (GISRA) of 2000 requires security awareness training as part of Federal agencies' information security programs, including Federal covered entities, such as the Medicare program. In addition, National Institute of Standards and Technology (NIST) SP 800-16, *Information Technology Security Training Requirements, A role and performance base model*, April 1998, provides an excellent source of information and guidance on this subject and is targeted at industry as well as government activities. We also note that covered entities must have discretion in how they implement the requirement, so they can incorporate this training in other existing activities. One approach would be to require this training as part of employee orientation.

b. *Comment:* A number of commenters asked that this requirement be made optional or used as a guideline only. Several commenters stated that this requirement is too specific and is burdensome. Several asked that the implementation features be removed.

Several others stated that this requirement is not appropriate for agents or contractors. One commenter asked how to apply this requirement to outsiders having access to data. Another asked if this requirement included all subcontractor staff. Others stated that contracts, signed by entities such as consultants, that address training should be sufficient.

*Response:* Security training remains a requirement because of its criticality; however, we have revised the implementation specifications to indicate that the amount and type of training needed will be dependent upon an entity's configuration and security risks. Business associates must be made aware of security policies and procedures, whether through contract language or other means. Covered entities are not required to provide training to business associates or anyone else that is not a member of their workforce.

c. *Comment:* Several commenters questioned why security awareness training appeared in two places, under "Physical safeguards" as well as "Administrative safeguards." Others questioned the appropriateness of

security awareness training under "Physical safeguards."

*Response:* We reviewed the definitions of the proposed "Awareness training for all personnel" ("Administrative safeguards") implementation feature and the proposed "Security awareness training" ("Physical safeguards") requirement. We agree that, to avoid confusion and eliminate redundancy, security awareness and training should appear in only one place. We believe the appropriate location for it is under "Administrative safeguards," as such training is essentially an administrative function.

d. *Comment:* Several commenters objected to the blanket requirement for security awareness training of individuals who may be on site for a limited time period (for example, a single day).

*Response:* Each individual who has access to electronic protected health information must be aware of the appropriate security measures to reduce the risk of improper access, uses, and disclosures. This requirement does not mean lengthy training is appropriate in every instance; there are alternative methods to inform individuals of security responsibilities (for example, provisions of pamphlets or copies of security policies, and procedures).

e. *Comment:* One commenter asked that "training" be changed to "orientation."

*Response:* We believe the term "training," as presented within this rule is the more appropriate term. The rule does not contemplate a one-time type of activity as connoted by "orientation," but rather an on-going, evolving process as an entity's security needs and procedures change.

f. *Comment:* Several commenters asked how often training should be conducted and asked for a definition of "periodic," as it appears in the proposed implementation feature "Periodic security reminders." One asked if the training should be tailored to job need.

*Response:* Amount and timing of training should be determined by each covered entity; training should be an on-going, evolving process in response to environmental and operational changes affecting the security of electronic protected health information. While initial training must be carried out by the compliance date, we provide flexibility for covered entities to construct training programs. Training can be tailored to job need if the covered entity so desires.

6. Security Incident Procedures (§ 164.308(a)(6))

We proposed a requirement for implementation of accurate and current security incident procedures: formal, documented report and response procedures so that security violations would be reported and handled promptly. We adopt this standard in the final rule, along with an implementation specification for response and reporting, since documenting and reporting incidents, as well as responding to incidents are an integral part of a security program.

a. *Comment:* Several commenters asked that we further define the scope of a breach of security. Along this same line, another commenter stated that the proposed security incident procedures were too vague as stated. We were asked to specify what a security incident would be, what the internal chain for reporting procedures would be, and what should be included in the documentation (for example, hardware/software, personnel responses).

*Response:* We define a security incident in § 164.304. Whether a specific action would be considered a security incident, the specific process of documenting incidents, what information should be contained in the documentation, and what the appropriate response should be will be dependent upon an entity's environment and the information involved. An entity should be able to rely upon the information gathered in complying with the other security standards, for example, its risk assessment and risk management procedures and the privacy standards, to determine what constitutes a security incident in the context of its business operations.

b. *Comment:* One commenter asked what types of incidents must be reported to outside entities. Another commented that we clarify that incident reporting is internal.

*Response:* Internal reporting is an inherent part of security incident procedures. This regulation does not specifically require any incident reporting to outside entities. External incident reporting is dependent upon business and legal considerations.

c. *Comment:* One commenter stated that network activity should be included here.

*Response:* We see no reason to exclude network activity under this requirement. Improper network activity should be treated as a security incident, because, by definition, it represents an improper instance of access to or use of information.