

in general that must be periodically reassessed and updated as needed.

The risk analysis implementation specification contains other terms that merit explanation. Under § 164.308(a)(1)(ii)(A), the risk analysis must look at risks to the covered entity's electronic protected health information. A thorough and accurate risk analysis would consider "all relevant losses" that would be expected if the security measures were not in place. "Relevant losses" would include losses caused by unauthorized uses and disclosures and loss of data integrity that would be expected to occur absent the security measures.

b. *Comment:* Relative to the development of an entity's sanction policy, one commenter asked that we describe the sanction penalties for breach of security. Another suggested establishment of a standard to which one's conduct could be held and adoption of mitigating circumstances so that the fact that a person acted in good faith would be a factor that could be used to reduce or otherwise minimize any sanction imposed. Another commenter suggested sanction activities not be implemented before the full implementation and testing of all electronic transaction standards.

Response: The sanction policy is a required implementation specification because—(1) the statute requires covered entities to have safeguards to ensure compliance by officers and employees; (2) a negative consequence to noncompliance enhances the likelihood of compliance; and (3) sanction policies are recognized as a usual and necessary component of an adequate security program. The type and severity of sanctions imposed, and for what causes, must be determined by each covered entity based upon its security policy and the relative severity of the violation.

c. *Comment:* Commenters requested the definitions of "risk analysis" and "breach."

Response: "Risk analysis" is defined and described in the specification of the security management process standard, and is discussed in the preamble discussion of § 164.308(a)(1)(ii)(A) of this final rule. The term breach is no longer used and is, therefore, not defined.

d. *Comment:* One commenter asked whether all health information is considered equally "sensitive," the thought being that, in determining risk, an entity may consider the loss of a smaller amount of extraordinarily sensitive data to be more significant than the loss of a larger amount of routinely collected data. The commenter

stated that common reasoning would suggest that the smaller amount of data would be considered more sensitive.

Response: All electronic protected health information must be protected at least to the degree provided by these standards. If an entity desires to protect the information to a greater degree than the risk analysis would indicate, it is free to do so.

e. *Comment:* One commenter asked that we add "threat assessment" to this requirement.

Response: We have not done this because we view threat assessment as an inherent part of a risk analysis; adding it would be redundant.

f. *Comment:* We proposed a requirement for internal audit, the in-house review of the records of system activity (for example, logins, file accesses, and security incidents) maintained by an entity. Several commenters wanted this requirement deleted. One suggested the audit trail requirement should not be mandatory, while another stated that internal audits would be unnecessary if physical security requirements are implemented.

A number of commenters asked that we clarify the nature and scope of what an internal audit covers and what the audit time frame should be. Several commenters offered further detail concerning what should and should not be required in an internal audit for security purposes. One commenter stated that ongoing intrusion detection should be included in this requirement. Another wanted us to specify the retention times for archived audit logs.

Several commenters had difficulty with the term "audit" and suggested we change the title of the requirement to "logging and violation monitoring."

A number of commenters stated this requirement could result in an undue burden and would be economically unfeasible.

Response: Our intent for this requirement was to promote the periodic review of an entity's internal security controls, for example, logs, access reports, and incident tracking. The extent, frequency, and nature of the reviews would be determined by the covered entity's security environment. The term "internal audit" apparently, based on the comments received, has certain rigid formal connotations we did not intend. We agree that the implementation of formal internal audits could prove burdensome or even unfeasible, to some covered entities due to the cost and effort involved. However, we do not want to overlook the value of internal reviews. Based on our review of the comments and the text to which they refer, it is clear that this

requirement should be renamed for clarity and that it should actually be an implementation specification of the security management process rather than an independent standard. We accordingly remove "internal audit" as a separate requirement and add "information system activity review" under the security management process standard as a mandatory implementation specification.

2. Assigned Security Responsibility (§ 164.308(a)(2))

We proposed that the responsibility for security be assigned to a specific individual or organization to provide an organizational focus and importance to security, and that the assignment be documented. Responsibilities would include the management and supervision of (1) the use of security measures to protect data, and (2) the conduct of personnel in relation to the protection of data.

In this final rule, we clarify that the final responsibility for a covered entity's security must be assigned to one official. The requirement for documentation is retained, but is made part of § 164.316 below. This policy is consistent with the analogous policy in the Privacy Rule, at 45 CFR 164.530(a), and the same considerations apply. See 65 FR 82744 through 87445. The same person could fill the role for both security and privacy.

a. *Comment:* Commenters were concerned that delegation of assigned security responsibility, especially in large organizations, needs to be to more than a single individual. Commenters believe that a large health organization's security concerns would likely cross many departmental boundaries requiring group responsibility.

Response: The assigned security responsibility standard adopted in this final rule specifies that final security responsibility must rest with one individual to ensure accountability within each covered entity. More than one individual may be given specific security responsibilities, especially within a large organization, but a single individual must be designated as having the overall final responsibility for the security of the entity's electronic protected health information. This decision also aligns this rule with the final Privacy Rule provisions concerning the Privacy Official.

b. *Comment:* One commenter disagreed with placing assigned security responsibility as part of physical safeguards. The commenter suggested that assigned security responsibility should be included under the Administrative Procedures.