

However, we have relocated material that relates to both security and privacy (including definitions) to the general section of part 164.

q. Comment: One commenter asked that data retention be addressed more specifically, since this will become a significant issue over time. It is recommended that a national work group be convened to address this issue.

Response: The commenter's concern is noted. While the documentation relating to Security Rule implementation must be retained for a period of 6 years (see § 164.316(b)(2)), it is not within the scope of this final rule to address data retention time frames for administrative or clinical records.

r. Comment: One commenter stated that requiring provider practices to develop policies, procedures, and training programs and to implement record keeping and documentation systems would be tremendously resource-intensive and increase the costs of health care.

Response: We expect that many of the standards of this final rule are already being met in one form or another by covered entities. For example, as part of normal business operations, health care providers already take measures to protect the health information in their keeping. Health care providers already keep records, train their employees, and require employees to follow office policies and procedures. Similarly, health plans are already frequently required by State law to keep information confidential. While revisions to a practice's or plan's current activities may be necessary, the development of entirely new systems or procedures may not be necessary.

s. Comment: One commenter stated that there is no system for which risk has been eliminated and expressed concern over phrases such as covered entities must "assure that electronic health information pertaining to an individual remains secure."

Response: We agree with the commenter that there is no such thing as a totally secure system that carries no risks to security. Furthermore, we believe the Congress' intent in the use of the word "ensure" in section 1173(d) of the Act was to set an exceptionally high goal for the security of electronic protected health information. However, we note that the Congress also recognized that some trade-offs would be necessary, and that "ensuring" protection did not mean providing protection, no matter how expensive. See section 1173(d)(1)(A)(ii) of the Act. Therefore, when we state that a covered entity must ensure the safety of the information in its keeping, we intend

that a covered entity take steps, to the best of its ability, to protect that information. This will involve establishing a balance between the information's identifiable risks and vulnerabilities, and the cost of various protective measures, and will also be dependent upon the size, complexity, and capabilities of the covered entity, as provided in § 164.306(b).

E. Administrative Safeguards (§ 164.308)

We proposed that measures taken to comply with the rule be appropriate to protect the health information in a covered entity's care. Most importantly, we proposed to require that both the measures taken and documentation of those measures be kept current, that is, reviewed and updated periodically to continue appropriately to protect the health information in the care of covered entities. We would have required the documentation to be made available to those individuals responsible for implementing the procedure.

We proposed a number of administrative requirements and supporting implementation features, and required documentation for those administrative requirements and implementation features.

In this final rule, we have placed these administrative standards in § 164.308. We have reordered them, deleted much of the detail of the proposed requirements, as discussed below, and omitted two of the proposed sets of requirements (system configuration requirements and a requirement for a formal mechanism for processing records) as discussed in paragraph 10 of the discussion of § 164.308 of section III.E. of this preamble. Otherwise, the basic elements of the administrative safeguards are adopted in this final rule as proposed.

1. Security Management Process (§ 164.308(a)(1)(i))

We proposed the establishment of a formal security management process to involve the creation, administration, and oversight of policies to address the full range of security issues and to ensure the prevention, detection, containment, and correction of security violations. This process would include implementation features consisting of a risk analysis, risk management, and sanction and security policies.

We also proposed, in a separate requirement under administrative procedures, an internal audit, which would be an in-house review of the records of system activity (for example,

logins, file accesses, and security incidents) maintained by an entity.

In this final rule, risk analysis, risk management, and sanction policy are adopted as required implementation specifications although some of the details are changed, and the proposed internal audit requirement has been renamed as "information system activity review" and incorporated here as an additional implementation specification.

a. Comment: Three commenters asked that this requirement be deleted. Two commenters cited this requirement as a possible burden. Several commenters asked that the implementation features be made optional.

Response: This standard and its component implementation specifications form the foundation upon which an entity's necessary security activities are built. See NIST SP 800-30, "Risk Management Guide for Information Technology Systems," chapters 3 and 4, January 2002. An entity must identify the risks to and vulnerabilities of the information in its care before it can take effective steps to eliminate or minimize those risks and vulnerabilities. Some form of sanction or punishment activity must be instituted for noncompliance. Indeed, we question how the statutory requirement for safeguards "to ensure compliance * * * by a [covered entity's] officers and employees" could be met without a requirement for a sanction policy. See section 1176(d)(2)(C) of the Act. Accordingly, implementation of these specifications remains mandatory. However, it is important to note that covered entities have the flexibility to implement the standard in a manner consistent with numerous factors, including such things as, but not limited to, their size, degree of risk, and environment. We have deleted the implementation specification calling for an organizational security policy, as it duplicated requirements of the security management and training standard.

We note that the implementation specification for a risk analysis at § 164.308(a)(1)(ii)(A) does not specifically require that a covered entity perform a risk analysis often enough to ensure that its security measures are adequate to provide the level of security required by § 164.306(a). In the proposed rule, an assurance of adequate security was framed as a requirement to keep security measures "current." We continue to believe that security measures must remain current, and have added regulatory language in § 164.306(e) as a more precise way of communicating that security measures