

commenter stated that these rules would adversely affect a provider's practice environment.

Response: The HIPAA statute requires us to promulgate a rule adopting security standards for health information. Resource concerns due to Y2K should no longer be an issue. Covered entities will have 2 years (or, in the case of small health plans, 3 years) from the adoption of this final rule in which to comply. Concerns relative to effective and compliance dates and the Privacy Rule are discussed under § 164.318, Compliance dates for initial implementation, below and at 65 FR 82751 through 82752.

We disagree that these standards will adversely affect a provider's practice environment. The scalability of the standards allows each covered entity to implement security protections that are appropriate to its specific needs, risks, and environments. These protections are necessary to maintain the confidentiality, integrity, and availability of patient data. A covered entity that lacks adequate protections risks inadvertent disclosure of patient data, with resulting loss of public trust, and potential legal action. For example, a covered entity with poor facility access controls and procedures would be susceptible to hacking of its databases. A provider with appropriate security protections already in place would only need to ensure that the protections are documented and are reassessed periodically to ensure that they continue to be appropriate and are actually being implemented. Our decision to classify many implementation specifications as addressable, rather than mandatory, provides even more flexibility to covered entities to develop cost-effective solutions. We believe that insurers who already have effective security programs in place will have met many of the requirements of this regulation.

c. *Comment:* One commenter believes the rule is arbitrary and capricious in its requirements without any justification that they will significantly improve the security of medical records and with the likelihood that their implementation may actually increase the vulnerability of the data. The commenter noted that the data backup requirements increase access to data and that security awareness training provides more information to employees.

Response: The standards are based on generally accepted security procedures, existing industry standards and guidelines, and recommendations contained in the National Research Council's 1997 report *For The Record:*

Protecting Electronic Health

Information, Chapter 6. We also consulted extensively with experts in the field of security throughout the health care industry. The standards are consistent with generally accepted security principles and practices that are already in widespread use.

Data backup need not result in increased access to that data. Backups should be stored in a secure location with controlled access. The appropriate secure location and access control will vary, based upon the security needs of the covered entity. For example, a procedure as simple as locking backup diskettes in a safe place and restricting who has access to the key may be suitable for one entity, whereas another may need to store backed-up information off-site in a secure computer facility. The information provided in security awareness training heightens awareness of security anomalies and helps to prevent security incidents.

d. *Comment:* Several commenters suggested that the proposed rule appears to reflect the Medicare program's perspective on security risks and solutions, and that it should be noted that not all industry segments share all the same risks as Medicare. One commenter stated that as future proposed rules are drafted, we should solicit input from those most significantly affected, for example, providers, plans, and clearinghouses.

Others stated that Medicaid agencies were not sufficiently involved in the discussions and debate. Still another stated that States would be unable to perform some basic business functions if all the standards are not designed to meet their needs.

Response: We believe that the standards are consistent with common industry practices and equitable, and that there has been adequate consultation with interested parties in the development of the standards. These standards are the result of an intensive process of public consultation. We consulted with the National Uniform Billing Committee, the National Uniform Claim Committee, the American Dental Association, and the Workgroup for Electronic Data Interchange, in the course of developing the proposed rule. Those organizations were specifically named in the Act to advise the Secretary, and their membership is drawn from the full spectrum of industry segments. In addition, the National Committee on Vital and Health Statistics (NCVHS), an independent advisory group to the Secretary, held numerous public hearings to obtain the views of

interested parties. Again, many segments of the health care industry, including provider groups, health plans, clearinghouses, vendors, and government programs participated actively. The NCVHS developed recommendations to the Secretary, which were relied upon as we developed the proposed rule. Finally, we note that the opportunity to comment was available to all during the public comment period.

e. *Comment:* One commenter stated that there is a need to ensure the confidentiality of risk analysis information that may contain sensitive information.

Response: The information included in a risk analysis would not be subject to the security standards if it does not include electronic protected health information. We agree that risk analysis data could contain sensitive information, just as other business information can be sensitive. Covered entities may wish to develop their own business rules regarding access to and protections for risk analysis data.

f. *Comment:* One commenter expressed concern over the statement in the preamble of the proposed rule (63 FR 43250) that read: "No one item is considered to be more important than another." The commenter suggested that security management should be viewed as most critical and perhaps what forms the foundation for all other security actions.

Response: The majority of comments received on this subject requested that we prioritize the standards. In response, we have regrouped the standards and implementation specifications in what we believe is a logical order within each of three categories: "Administrative safeguards," "Physical safeguards," and "Technical safeguards." In this final rule, we order the standards in such a way that the "Security management process" is listed first under the "Administrative safeguards" section, as we believe this forms the foundation on which all of the other standards depend. The determination of the specific security measures to be implemented to comply with the standards will, in large part, be dependent upon completion of the implementation specifications within the security management process standard (see § 164.308(a)(1)). We emphasize, however, that an entity implementing these standards may choose to implement them in any order, as long as the standards are met.

g. *Comment:* One commenter stated that there is a need for requirements concerning organizational practices (for example, education, training, and security and confidentiality policies), as