

well as technical practices and procedures.

*Response:* We agree. Section 164.308 of this final rule describes administrative safeguards that address these topics. Section 164.308 requires covered entities to implement standards and required implementation specifications, as well as consider and implement, when appropriate and reasonable, addressable implementation specifications. For example, the security management process standard requires implementation of a risk analysis, risk management, a sanction policy, and an information system activity review. The information access management standard requires consideration, and implementation where appropriate and reasonable, of access authorization and access establishment and modification policies and procedures. Other areas addressed are assigned security responsibility, workforce security, security awareness and training, security incident procedures, contingency planning, business associate contracts, and evaluation.

*h. Comment:* One commenter stated that internal and external security requirements should be separated and dealt with independently.

*Response:* The presentation of the standards within this final rule could have been structured in numerous ways, including by addressing separate internal and external security standards. We chose the current structure as we considered it a logical breakout for purposes of display within this final rule. Under our structure a covered entity may apply a given standard to internal activities and to external activities. Had we displayed separately the standards for internal security and the standards for external security, we would have needed to describe a number of the standards twice, as many apply to both internal and external security. However, a given entity may address the standards in whatever order it chooses, as long as the standards are met.

*i. Comment:* Two commenters stated that the standards identified in Addendum 3 of the proposed rule may not all have matured to implementation readiness.

*Response:* Addendum 3 of the proposed rule cross-referred individual requirements on the matrix to existing industry standards of varying levels of maturity. Addendum 3 was intended to show what we evaluated in searching for existing industry standards that could be adopted on a national level. No one standard was found to be comprehensive enough to be adopted, and none were proposed as the

standards to be met under the Security Rule.

*j. Comment:* One commenter suggested we include a revised preamble in the final publication. Another questioned how clarification of points in the preamble will be handled if the preamble is not part of the final regulation.

*Response:* Preambles to proposed rules are not republished in the final rule. The preamble in this final rule contains summaries of the information presented in the preamble of the proposed rule, summaries of the comments received during the public comment period, and responses to questions and concerns raised in those comments and a summary of changes made. Additional clarification will be provided by HHS on an ongoing basis through written documents and postings on HHS's websites.

*k. Comment:* One commenter asked that we clarify that no third party can require implementation of more security features than are required in the final rule, for example, a third party could not require encryption but may choose to accept it if the other party so desires.

*Response:* The security standards establish a minimum level of security to be met by covered entities. It is not our intent to limit the level of security that may be agreed to between trading partners or others above this floor.

*l. Comment:* One commenter asked how privacy legislation would affect these rules. The commenter inquired whether covered entities will have to reassess and revise actions already taken in the spirit of compliance with the security regulations.

*Response:* We cannot predict if or how future legislation may affect the rules below. At present, the privacy standards at subpart E of 42 CFR part 164 have been adopted, and this final rule is compatible with them.

*m. Comment:* One commenter stated that a data classification policy, that is a method of assigning sensitivity ratings to specific pieces of data, should be part of the final regulations.

*Response:* We did not adopt such a policy because this final rule requires a floor of protection of all electronic protected health information. A covered entity has the option to exceed this floor. The sensitivity of information, the risks to and vulnerabilities of electronic protected health information and the means that should be employed to protect it are business determinations and decisions to be made by each covered entity.

*n. Comment:* One commenter stated that this proposed rule conflicts with previously stated rules that acceptable

“standards” must have been developed by ANSI-recognized Standards Development Organizations (SDOs).

*Response:* In general, HHS is required to adopt standards developed by ANSI-accredited SDOs when such standards exist. The currently existing security standards developed by ANSI-recognized SDOs are targeted to specific technologies and/or activities. No existing security standard, or group of standards, is technology-neutral, scaleable to the extent required by HIPAA, and broad enough to be adopted in this final rule. Therefore, this final rule adopts standards under section 1172(c)(2)(B) of the Act, which permits us to develop standards when no industry standards exist.

*o. Comment:* One commenter stated that this regulation goes beyond the scope of the law, unjustifiably extending into business practices, employee policies, and facility security.

*Response:* We do not believe that this regulation goes beyond the scope of the law. The law requires HHS to adopt standards for reasonable and appropriate security safeguards concerning such matters as compliance by the officers and employees of covered entities, protection against reasonably anticipated unauthorized uses and disclosures of health information, and so on. Such standards will inevitably address the areas the commenter pointed to.

The intent of this regulation is to provide standards for the protection of electronic protected health information in accordance with the Act. In order to do this, covered entities are required to implement administrative, physical, and technical safeguards. Those entities must ensure that data are protected, to the extent feasible, from inappropriate access, modification, dissemination, and destruction. As noted above, however, this final rule has been modified to increase flexibility as to how this protection is accomplished.

*p. Comment:* One commenter stated that all sections regarding confidentiality and privacy should be removed, since they do not belong in this regulation.

*Response:* As the discussion in section III.A above of this final rule makes clear, the privacy and security standards are very closely related. Section 1173(d)(2) of the Act specifically mentions “confidentiality” and authorizes uses and disclosures of information as part of what security safeguards must address. Thus, we cannot omit all references to confidentiality and privacy in discussions of the security standards.