

We agree with the commenters that switched, point-to-point connections, for example, dial-up lines, have a very small probability of interception.

Thus, we agree that encryption should not be a mandatory requirement for transmission over dial-up lines. We also agree with commenters who mentioned the financial and technical burdens associated with the employment of encryption tools. Particularly when considering situations faced by small and rural providers, it became clear that there is not yet available a simple and interoperable solution to encrypting e-mail communications with patients. As a result, we decided to make the use of encryption in the transmission process an addressable implementation specification. Covered entities are encouraged, however, to consider use of encryption technology for transmitting electronic protected health information, particularly over the internet.

As business practices and technology change, there may arise situations where electronic protected health information being transmitted from a covered entity would be at significant risk of being accessed by unauthorized entities. Where risk analysis showed such risk to be significant, we would expect covered entities to encrypt those transmissions, if appropriate, under the addressable implementation specification for encryption.

We do not use the term "open network" in this final rule because its meaning is too broad. We include as an addressable implementation specification the requirement that transmissions be encrypted when appropriate based on the entity's risk analysis.

b. Comment: We received comments requesting that the implementation features be deleted or made optional. Three commenters asked that the requirement for an alarm be deleted.

Response: This final rule has been revised to reflect deletion of the following implementation features: (1) The alarm capability; (2) audit trail; (3) entity authentication; and (4) event reporting. These features were associated with a proposed requirement for "Communications/network controls" and have been deleted since they are normally incorporated by telecommunications providers as part of network management and control functions that are included with the provision of network services. A health care entity would not expect to be responsible for these technical telecommunications features. "Access controls" has also been deleted from the implementation features since the consideration of the use of encryption

will satisfy the intent of this feature. We retain as addressable implementation specifications two features: (1) "Integrity controls" and "encryption". "Message authentication" has been deleted as an implementation feature because the use of data authentication codes (called for in the "integrity controls" implementation specification) satisfies the intent of "Message authentication."

c. Comment: A number of comments were received asking that this final rule establish a specific (or at least a minimum) cryptographic algorithm strength. Others recommended that the rule not specify an encryption strength since technology is changing so rapidly. Several commenters requested guidelines and minimum encryption standards for the Internet. Another stated that, since an example was included (small or rural providers for example), the government should feel free to name a specific encryption package. One commenter stated that the requirement for encryption on the Internet should reference the "CMS Internet Security Policy."

Response: We remain committed to the principle of technology neutrality and agree with the comment that rapidly changing technology makes it impractical and inappropriate to name a specific technology. Consistent with this principle, specification of an algorithm strength or specific products would be inappropriate. Moreover, rapid advances in the success of "brute force" cryptanalysis techniques suggest that any minimum specification would soon be outmoded. We maintain that it is much more appropriate for this final rule to state a general requirement for encryption protection when necessary and depend on covered entities to specify technical details, such as algorithm types and strength. Because "CMS Internet Security Policy" is the policy of a single organization and applies only to information sent to CMS, and not between all covered entities, we have not referred to it here.

d. Comment: The proposed definition of "Integrity controls" generated comments that asked that the word "validity" be changed to "Integrity." Commenters were concerned about the ability of an entity to ensure that information was "valid."

Response: We agree with the commenters about the meaning of the word "validity" in the context of the proposed definition of "Integrity controls." We have named "integrity controls" as an implementation specification in this final rule to require mechanisms to ensure that electronically transmitted information is

not improperly modified without detection (see § 164.312(c)(1)).

e. Comment: Three commenters asked for clarification and guidance regarding the unsolicited electronic receipt of health information in an unsecured manner, for example, when the information was submitted by a patient via e-mail over the Internet. Commenters asked for guidance as to what was their obligation to protect data received in this manner.

Response: The manner in which electronic protected health information is received by a covered entity does not affect the requirement that security protection must subsequently be afforded to that information by the covered entity once that information is in possession of the covered entity.

6. Proposed Requirements Not Adopted in This Final Rule

a. Authorization Control

We proposed, under "Technical Security Services to Guard Data Integrity, Confidentiality, and Availability," that a mechanism be required for obtaining consent for the use and disclosure of health information using either "Role-based access" or "User-based access" controls. In this final rule, we do not adopt this requirement.

Comment: We received a large number of comments regarding use of the word "consent." It was pointed out that this could be construed to mean patient consent to the use or disclosure of patient information, which would make this a privacy issue, rather than one of security. Other comments suggested deletion of the requirement in its entirety. We received a comment asking for clarification about the distinction between "Access control" and "Authorizations."

Response: These requirements were intended to address authorization of workforce members and others for the use and disclosure of health information, not patient consent. Upon reviewing the differences between "Access control" and "Authorization control," we found it to be unnecessary to retain "Authorization control" as a separate requirement. Both the access control and the authorization control proposed requirements involved implementation of types of automated access controls, that is, role-based access and user-based access. It can be argued that the process of managing access involves allowing and restricting access to those individuals that have been authorized to access the data. The intent of the proposed authorization control implementation feature is now