

individual upon request. There has been a tendency to assume that this Privacy Rule requirement would be satisfied via some sort of process involving audit trails. We caution against assuming that the Security Rule's requirement for an audit capability will satisfy the Privacy Rule's requirement regarding accounting for disclosures of protected health information. The two rules cover overlapping, but not identical information. Further, audit trails are typically used to record uses within an electronic information system, while the Privacy Rule requirement for accounting applies to certain disclosures outside of the covered entity (for example, to public health authorities).

### 3. Integrity (§ 164.312(c)(1))

We proposed under the "Data authentication" requirement, that each organization be required to corroborate that data in its possession have not been altered or destroyed in an unauthorized manner and provided examples of mechanisms that could be used to accomplish this task. We adopt the proposed requirement for data authentication in the final rule as an addressable implementation specification "Mechanism to authenticate data," under the "Integrity" standard.

*a. Comment:* We received a large number of comments requesting clarification of the "Data authentication" requirement. Many of these comments suggested that the requirement be called "Data integrity" instead of "Data authentication." Others asked for guidance regarding just what "data" must be authenticated. A significant number of commenters indicated that this requirement would put an extraordinary burden on large segments of the health care industry, particularly when legacy systems are in use. Requests were received to make this an "optional" requirement, based on an entity's risk assessment and analysis.

*Response:* We adopt the suggested "integrity" terminology because it more clearly describes the intent of the standard. We retain the meaning of the term "Data authentication" under the addressable implementation specification "Mechanism to authenticate data," and provide an example of a potential means to achieve data integrity.

Error-correcting memory and magnetic disc storage are examples of the built-in data authentication mechanisms that are ubiquitous in hardware and operating systems today. The risk analysis process will address what data must be authenticated and

should provide answers appropriate to the different situations faced by the various health care entities implementing this regulation.

Further, we believe that this standard will not prove difficult to implement, since there are numerous techniques available, such as processes that employ digital signature or check sum technology to accomplish the task.

*b. Comment:* We received numerous comments suggesting that "Double keying" be deleted as a viable "Data authentication" mechanism, since this practice was generally associated with the use of punched cards.

*Response:* We agree that the process of "Double keying" is outdated. This final rule omits any reference to "Double keying."

### 4. Person or Entity Authentication (§ 164.312(d))

We proposed that an organization implement the requirement for "Entity authentication", the corroboration that an entity is who it claims to be. "Automatic logoff" and "Unique user identification" were specified as mandatory features, and were to be coupled with at least one of the following features: (1) A "biometric" identification system; (2) a "password" system; (3) a "personal identification number"; and (4) "telephone callback," or a "token" system that uses a physical device for user identification.

In this final rule, we provide a general requirement for person or entity authentication without the specifics of the proposed rule.

*Comment:* We received comments from a number of organizations requesting that the implementation features for entity authentication be either deleted in their entirety or at least be made optional. On the other hand, comments were received requesting that the use of digital signatures and soft tokens be added to the list of implementation features.

*Response:* We agree with the commenters that many different mechanisms may be used to authenticate entities, and this final rule now reflects this fact by not incorporating a list of implementation specifications, in order to allow covered entities to use whatever is reasonable and appropriate. "Digital signatures" and "soft tokens" may be used, as well as many other mechanisms, to implement this standard.

The proposed mandatory implementation feature, "Unique user identification," has been moved from this standard and is now a required implementation specification under "Access control" at § 164.312(a)(1).

"Automatic logoff" has also been moved from this standard to the "Access control" standard and is now an addressable implementation specification.

### 5. Transmission Security (§ 164.312(e)(1))

Under "Technical Security Mechanisms to Guard Against Unauthorized Access to Data that is Transmitted Over a Communications Network," we proposed that "Communications/network controls" be required to protect the security of health information when being transmitted electronically from one point to another over open networks, along with a combination of mandatory and optional implementation features. We proposed that some form of encryption must be employed on "open" networks such as the Internet or dial-up lines.

In this final rule, we adopt integrity controls and encryption, as addressable implementation specifications.

*a. Comment:* We received a number of comments asking for overall clarification as well as a definition of terms used in this section. A definition for the term "open networks" was the most requested action, but there was a general expression of dislike for the manner in which we approached this section, with some comments suggesting that the entire section be rewritten. A significant number of comments were received on the question of encryption requirements when dial-up lines were to be employed as a means of connectivity. The overwhelming majority strongly urged that encryption not be mandatory when using any transmission media other than the Internet, but rather be considered optional based on individual entity risk assessment/analysis. Many comments noted that there are very few known breaches of security over dial-up lines and that nonjudicious use of encryption can adversely affect processing times and become both financially and technically burdensome. Only one commenter suggested that "most" external traffic should be encrypted.

*Response:* In general, we agree with the commenters who asked for clarification and revision. This final rule has been significantly revised to reflect a much simpler and more direct requirement. The term "Communications/network controls" has been replaced with "Transmission security" to better reflect the requirement that, when electronic protected health information is transmitted from one point to another, it must be protected in a manner commensurate with the associated risk.