

d. *Comment:* One commenter stated that this requirement should address suspected misuse also.

Response: We agree that security incidents include misuse of data; therefore, this requirement is addressed.

e. *Comment:* Several commenters asked that this requirement be deleted. One commenter asked that we delete the implementation features.

Response: As indicated above, we have adopted the proposed standard and combined the implementation specifications.

7. Contingency Plan (§ 164.308(a)(7)(i))

We proposed that a contingency plan must be in effect for responding to system emergencies. The plan would include an applications and data criticality analysis, a data backup plan, a disaster recovery plan, an emergency mode operation plan, and testing and revision procedures.

In this final rule, we make the implementation specifications for testing and revision procedures and an applications and data criticality analysis addressable, but otherwise require that the contingency features proposed be met.

a. *Comment:* Several commenters suggested the contingency plan requirement be deleted. Several thought that this aspect of the proposed regulation went beyond its intended scope. Another believed that more discussion and development is needed before developing regulatory guidance on contingency plans. Others wanted this to be an optional requirement. In contrast, one commenter requested more guidance concerning contingency planning. Still others wanted to require that a contingency plan be in place but stated that we should not regulate its contents. One comment stated that data backup, disaster recovery, and emergency mode operation should not be part of this requirement.

Response: A contingency plan is the only way to protect the availability, integrity, and security of data during unexpected negative events. Data are often most exposed in these events, since the usual security measures may be disabled, ignored, or not observed.

Each entity needs to determine its own risk in the event of an emergency that would result in a loss of operations. A contingency plan may involve highly complex processes in one processing site, or simple manual processes in another. The contents of any given contingency plan will depend upon the nature and configuration of the entity devising it.

While the contingency plan standard must be met, we agree that the proposed

testing and revision implementation feature should be an addressable implementation specification in this final rule. Dependent upon the size, configuration, and environment of a given covered entity, the entity should decide if testing and revision of all parts of a contingency plan should be done or if there are more reasonable alternatives. The same is true for the proposed applications and data criticality analysis implementation feature. We have revised the final rule to reflect this approach.

b. *Comment:* One commenter believed that adhering to this requirement could prove burdensome. Another stated that testing of certain parts of a contingency plan would be burdensome, and even infeasible, for smaller entities.

Response: Without contingency planning, a covered entity has no assurance that its critical data could survive an emergency situation. Recent events, such as September 11, 2001, illustrate the importance of such planning. Contingency planning will be scalable based upon, among other factors, office configuration, and risk assessment. However, in response to the scalability issue raised by the commenter, we have made the testing and revision implementation specification addressable (see § 164.308(a)(7)(ii)).

c. *Comment:* Two commenters considered a 2-year implementation time frame for this requirement inadequate for large health plans. Another commenter stated that implementation of measures against natural disaster would be too big an issue for this regulation.

Response: The statute sets forth the compliance dates for the initial standards. The statute requires that compliance with initial standards is not later than 2 years after adoption of the standards for all covered entities except small health plans for which the compliance date is not later than 3 years after adoption.

The final rule calls for covered entities to consider how natural disasters could damage systems that contain electronic protected health information and develop policies and procedures for responding to such situations. We consider this to be a reasonable precautionary step to take since in many cases the risk would be deemed to be low.

d. *Comment:* A commenter requested clarification of the term "Emergency mode" with regard to the proposed "Emergency mode operation plan" implementation feature.

Response: We have clarified the "Emergency mode operations plan" to

show that it only involves those critical business processes that must occur to protect the security of electronic protected health information during and immediately after a crisis situation.

8. Evaluation (§ 164.308(a)(8))

We proposed that certification would be required and could be performed internally or by an external accrediting agency. We solicited input on appropriate mechanisms to permit an independent assessment of compliance. We were particularly interested in input from those engaging in health care electronic data interchange (EDI), as well as independent certification and auditing organizations addressing issues of documentary evidence of steps taken for compliance; need for, or desirability of, independent verification, validation, and testing of system changes; and certifications required for off-the-shelf products used to meet the requirements of this regulation. We also solicited comments on the extent to which obtaining external certification would create an undue burden on small or rural providers.

In this final rule, we require covered entities to periodically conduct an evaluation of their security safeguards to demonstrate and document their compliance with the entity's security policy and the requirements of this subpart. Covered entities must assess the need for a new evaluation based on changes to their security environment since their last evaluation, for example, new technology adopted or responses to newly recognized risks to the security of their information.

a. *Comment:* We received several comments that certification should be performed externally. A larger group of commenters preferred self-certification. The majority of the comments, however, were to the effect that external certification should be encouraged but not mandated.

A number of commenters thought that mandating external certification would create an undue financial burden, regardless of the size of the entity being certified. One commenter stated that external certification would not place an undue burden on a small or rural provider.

Response: Evaluation by an external entity is a business decision to be left to each covered entity. Evaluation is required under § 164.308(a)(8), but a covered entity may comply with this standard either by using its own workforce or an external accreditation agency, which would be acting as a business associate. External evaluation may be too costly an option for small entities.