

receives, maintains, or transmits on behalf of the covered entity; (2) ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate safeguards; (3) report to the covered entity any security incident of which it becomes aware; (4) make its policies and procedures, and documentation required by this subpart relating to such safeguards, available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and (5) authorize termination of the contract by the covered entity if the covered entity determines that the business associate has violated a material term of the contract.

When a covered entity and its business associate are both governmental entities, an "other arrangement" is sufficient. The covered entity is in compliance with this standard if it enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of the above-described business associate contract. However, the covered entity may omit from this memorandum the termination authorization required by the business associate contract provisions if this authorization is inconsistent with the statutory obligations of the covered entity or its business associate. If other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of the above-described business associate contract, a contract or agreement is not required. If a covered entity enters into other arrangements with another governmental entity that is a business associate, such arrangements may omit provisions equivalent to the termination authorization required by the business associate contract, if inconsistent with the statutory obligation of the covered entity or its business associate.

If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate in § 160.103 of this subchapter to a covered entity, the covered entity may permit the business associate to receive, create, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of the above-described business associate contract, *provided that* the covered entity attempts in good faith to obtain satisfactory assurances as required by the above described

business associate contract and documents the attempt and the reasons that these assurances cannot be obtained.

We have added a standard for group health plans that parallels the provisions of the Privacy Rule. It became apparent during the course of the security and privacy rulemaking that our original chain of trust approach was both overly broad in scope and failed to address appropriately the circumstances of certain covered entities, particularly the ERISA group health plans. These latter considerations and the solutions arrived at in the Privacy Rule are described in detail in the Privacy Rule at 65 FR 82507 through 82509. Because the purpose of the security standards is in part to reinforce privacy protections, it makes sense to align the organizational policies of the two rules. This decision should also make compliance less burdensome for covered entities than would a decision to have different organizational requirements for the two sets of rules.

Thus, we have added at § 164.314(b) a standard for group health plan that tracks the standard at § 164.504(f) very closely. The purpose of these provisions is to ensure that, except when the electronic protected health information disclosed to a plan sponsor is summary health information or enrollment or disenrollment information as provided for by § 164.504(f), group health plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained or transmitted to or by the plan sponsor on behalf of the group health plan. The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to implement reasonable and appropriate safeguards to protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; ensure that any agents, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate safeguards to protect the information; report to the group health plan any security incident of which it becomes aware; and make its policies and procedures and documentation relating to these safeguards available to the Secretary for purposes of determining the group

health plan's compliance with this subpart.

a. *Comment:* Several commenters expressed confusion concerning the applicability of proposed § 142.104 to security.

Response: The proposed preamble included language generally applicable to most of the proposed standards under HIPAA. Proposed § 142.104 concerned general requirements for health plans relative to processing transactions. We proposed that plans could not refuse to conduct a transaction as a standard transaction, or delay or otherwise adversely affect a transaction on the grounds that it was a standard transaction; health information transmitted and received in connection with a transaction must be in the form of standard data elements; and plans conducting transactions through an agent must ensure that the agent met all the requirements that applied to the health plan. Except for the statement that a plan's agent ("business associate" in the final rule) must meet the requirements (which would include security) that apply to the health plan, this proposed section did not pertain to the security standards and was addressed in the Transaction Rule.

b. *Comment:* The majority of comments concerned proposed rule language stating "the same level of security will be maintained at all links in the chain * * *". Commenters believed the current language will have an adverse impact on one of the security standard's basic premises, which is scalability. It was requested that the language be changed to indicate that, while appropriate security must be maintained, all partners do not need to maintain the same level of security.

A number of commenters expressed some confusion concerning their responsibility for the security of information once it has passed from their control to their trading partner's control, and so on down the trading partner chain. Requests were made that we clarify that chain of trust partner agreements were really between two parties, and that, if a trading partner agreement has been entered into, any given partner would not be responsible, or liable, for the security of data once it is out of his or her control.

In line with this concern, several commenters were concerned that they would have some responsibility to ensure the level of security maintained by their trading partner.

Several commenters believe a chain of trust partner agreement should not be a security requirement. One commenter stated that because covered entities must already conform to the regulation