

requirements, a “chain of trust” agreement does not add to overall security. Compliance with the regulation should be sufficient.

*Response:* We believe the commenters are correct that the rule as proposed would—(1) not allow for scalability; and (2) would lead an entity to believe it is responsible, and liable, for making sure all entities down the line maintain the same level of security. The confusion here seems to come from the phrase “same level of security.” Our intention was that each trading partner would maintain reasonable and appropriate safeguards to protect the information. We did not mean that partners would need to implement the same security technology or measures and procedures.

We have replaced the proposed “Chain of trust” standard with a standard for “Business associate contracts and other arrangements.”

When another entity is acting as a business associate of a covered entity, we require the covered entity to require the other entity to protect the electronic protected health information that it creates, receives, maintains or transmits on the covered entity’s behalf. The level of security afforded particular electronic protected health information should not decrease just because the covered entity has made the business decision to entrust a business associate with using or disclosing that information in connection with the performance of certain functions instead of doing those functions itself. Thus, the rule below requires covered entities to require their business associates to implement certain safeguards and take other measures to ensure that the information is safeguarded (see § 164.308(b)(1) and § 164.314(a)(1)).

The specific requirements of § 164.314(a)(1) are drawn from the analogous requirements at 45 CFR 164.504(e) of the Privacy Rule, although they have been adapted to reflect the objectives and context of the security standards. Compare, in particular, 45 CFR 164.504(e)(2)(ii) with § 164.314(a)(1). We have not imported all of the requirements of 45 CFR 164.504(e), however, as many have no clear analog in the security context (see, for example, 45 CFR 164.504(e)(2)(i) regarding permitted and required uses and disclosures made by a business associate). HHS had previously committed to reconciling its security and privacy policies regarding business associates (see 65 FR 82643). The close relationship of many of the organizational requirements in section 164.314 with the analogous requirements of the Privacy Rule should facilitate the implementation and

coordination of security and privacy policies and procedures by covered entities.

In contrast, when another entity is not acting as a business associate for the covered entity, but rather is acting in the capacity of some other sort of trading partner, we do not require the covered entity to require the other entity to adopt particular security measures, as previously proposed. This policy is likewise consistent with the general approach of the Privacy Rule (see the discussion in the Privacy Rule at 65 FR 82476). The covered entity is free to negotiate security arrangements with its non-business associate trading partners, but this rule does not require it to do so.

A similar approach underlies § 164.314(b) below. These provisions are likewise drawn from, and intended to support, the analogous privacy protections provided for by 45 CFR 164.504(f) (see the discussion of § 164.504(f) of the Privacy Rule at 65 FR 82507 through 82509, and 82646 through 82648). As with the business associate contract provisions, however, they are imported and adapted only to the extent they make sense in the security context. Thus, for example, the requirement at § 164.504(f)(2)(ii)(C) prohibits the plan documents from permitting disclosure of protected health information to the plan sponsor for employment-related purposes. As this prohibition goes entirely to the permissibility of a particular type of disclosure, it has no analog in § 164.314(b).

*c. Comment:* Several commenters stated that if security features are determined by agreements established between “trading partners,” as stated in the proposed regulations, there should be some guidelines or boundaries for those agreements so that extreme or unusual provisions are not permitted.

*Response:* This final rule sets a baseline, or minimum level, of security measures that must be taken by a covered entity and stipulates that a business associate must also implement reasonable and appropriate safeguards. This final rule does not, however, prohibit a covered entity from employing more stringent security measures or from requiring a business associate to employ more stringent security measures. A covered entity may determine that, in order to do business with it, a business associate must also employ equivalent measures. This would be a business decision and would not be governed by the provisions of this rule. Security mechanisms relative to the transmission of electronic protected health information between entities may need to be agreed upon by

both parties in order to successfully complete the transmission. However, the determination of the specific transmission mechanisms and the specific security features to be implemented remains a business decision.

*d. Comment:* Several commenters asked whether existing contracts could be used to meet the requirement for a trading partner agreement, or does the rule require entry into a new contract specific to this purpose. Also, the commenters want to know about those whose working agreements do not involve written contractual agreement: Do they now need to set up formal agreements and incur the additional expense that would entail?

*Response:* This final rule requires written agreements between covered entities and business associates. New contracts do not have to be entered into specifically for this purpose, if existing written contracts adequately address the applicable requirements (or can be amended to do so).

*e. Comment:* Several commenters asked whether covered entities are responsible for the security of all individual health information sent to them, or only information sent by chain of trust partners. They also asked if they can refuse to process standard transactions sent to them in an unsecured fashion. In addition, they inquired if they can refuse to send secured information in standard transactions to entities not required by law to secure the information. One commenter asked if there is a formula for understanding in any particular set of relationships where the ultimate responsibility for compliance with the standards would lie.

*Response:* Pursuant to the Transactions Rule, if a health plan receives an unsecured standard transaction, it may not refuse to process that transaction simply because it was sent in an unsecured manner. The health plan is not responsible under this rule, for how the transaction was sent to it (unless the transmission was made by a business associate, in which case different considerations apply); however, once electronic protected health information is in the possession of a covered entity, the covered entity is responsible for the security of the electronic protected health information received. The covered entity must implement technical security mechanisms to guard against unauthorized access to electronic protected health information that is transmitted over an electronic communication network. In addition, the rule requires the transmitting