

incorporated in the access authorization implementation specification under the information access management standard in § 164.308(a)(4). Under the information access management standard, a covered entity must implement, if appropriate and reasonable to its situation, policies and procedures first to authorize a person to access electronic protected health information and then to actually establish such access. These policies and procedures will enable entities to follow the Privacy Rule minimum necessary requirements, which provide when persons should have access to information.

H. Organizational Requirements (§ 164.314)

We proposed that each health care clearinghouse must comply with the security standards to ensure all health information and activities are protected from unauthorized access. If the clearinghouse is part of a larger organization, then unauthorized access by the larger organization must be prevented. We also proposed that parties processing data through a third party would be required to enter into a chain of trust partner agreement, a contract in which the parties agree to electronically exchange data and to protect the transmitted data in accordance with the security standards.

In this final rule, we have adopted the concepts of hybrid and affiliated entities, as previously defined in § 164.504, and now defined in § 164.103, and business associates as defined in § 160.103, to be consistent with the Privacy Rule. General organizational requirements related to affiliated covered entities and hybrid entities are now contained in a new § 164.105. The proposed chain of trust partner agreement has been replaced by the standards for business associate contracts or other arrangements and the standards for group health plans. Consistent with the statute and the policy of the Privacy Rule, this final rule does not require noncovered entities to comply with the security standards.

1. Health Care Clearinghouses

The proposed rule proposed that if a health care clearinghouse were part of a larger organization, it would be required to ensure that all health information pertaining to an individual is protected from unauthorized access by the larger organization; this statement closely tracked the statutory language in section 1173(d)(1)(B) of the Act. Since the point of the statutory language is to ensure that health care information in the possession of a health care

clearinghouse is not inappropriately accessed by the larger organization of which it is a part, this final rule implements the statutory language through the information access management provision of § 164.308(a)(4)(ii)(A).

The final rule, at § 164.105, makes the health care component and affiliated entity standards of the Privacy Rule applicable to the security standards. Therefore, we have not changed those standards substantively. In pertaining to the Privacy Rule, we have simply moved them to a new location in part 164. Any differences between § 164.105 and § 164.504(a) through (d) reflects the addition of requirements specific to the security standards.

The health care component approach was developed in response to extensive comment received principally on the Privacy Rule. See 65 FR 82502 through 82503 and 82637 through 82640 for a discussion of the policy concerns underlying the health care component approach. Since the security standards are intended to support the protection of electronic information protected by the Privacy Rule, it makes sense to incorporate organizational requirements that parallel those required of covered entities by the Privacy Rule. This policy will also minimize the burden of complying with both rules.

a. *Comment:* Relative to the following preamble statement (63 FR 43258): “If the clearinghouse is part of a larger organization, then security must be imposed to prevent unauthorized access by the larger organization.” One commenter asked what is considered to be “the larger organization.” For example, if a clearinghouse function occurs in a department of a larger business entity, will the regulation cover all internal electronic communication, such as e-mail, within the larger business and all external electronic communication, such as e-mail with its owners?

Response: The “larger organization” is the overall business entity that a clearinghouse would be part of. Under the Security Rule, the larger organization must assure that the health care clearinghouse function has instituted measures to ensure only that electronic protected health information that it processes is not improperly accessed by unauthorized persons or other entities, including the larger organization. Internal electronic communication within the larger organization will not be covered by the rule if it does not involve the clearinghouse, assuming that it has designated health care components, of which the health care clearinghouse is

one. External communication must be protected as sent by the clearinghouse, but need not be protected once received.

b. *Comment:* One commenter asked that the first sentence in § 142.306(b) of the proposed rule, “If a health care clearinghouse is part of a larger organization, it must assure all health information is protected from unauthorized access by the larger organization” be expanded to read, “If a health care clearinghouse or any other health care entity is part of a larger organization . . .”

Response: The Act specifically provides, at section 1173(d)(1)(B), that the Secretary must adopt standards to ensure that a health care clearinghouse, if part of a larger organization, has policies and security procedures to protect information from unauthorized access by the larger organization.

Health care providers and health plans are often part of larger organizations that are not themselves health care providers or health plans. The security measures implemented by health plans and covered health care providers should protect electronic protected health information in circumstances such as the one identified by the commenter. Therefore, we agree with the comment that the requirement should be expanded as suggested by the commenter. In this final rule, those components of a hybrid entity that are designated as health care components must comply with the security standards and protect against unauthorized access with respect to the other components of the larger entity in the same way as they must deal with separate entities.

2. Business Associate Contracts and Other Arrangements

We proposed that parties processing data through a third party would be required to enter into a chain of trust partner agreement, a contract in which the parties agree to electronically exchange data and to protect the transmitted data. This final rule narrows the scope of agreements required. It essentially tracks the provisions in § 164.502(e) and § 164.504(e) of the Privacy Rule, although appropriate modifications have been made in this rule to the required elements of the contract.

In this final rule, a contract between a covered entity and a business associate must provide that the business associate must—(1) implement safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates,