

United under HIPAA: a Comparison of Arrangements and Agreements (HIPAA on the Job)

Save to myBoK

by Margret Amatayakul, RHIA, FHIMSS

The HIPAA transactions, security, and privacy regulations identify five agreements and relationships that can be established between healthcare entities to achieve economies of scale and lessen HIPAA's administrative burden. They are:

- affiliated covered entity (ACE)
- business associate contract
- chain of trust agreement
- data use agreement
- organized healthcare arrangement (OHCA)
- trading partner agreement

What are the differences between these agreements and arrangements? What are the similarities? In this article, we'll review each type of arrangement and their accompanying requirements. See "[Comparison of HIPAA Agreements and Arrangements](#)", below for a summary of key characteristics.

Organizational Relationships

In an attempt to remove some of the administrative burden of complying with the HIPAA privacy rule, the rule permits two forms of organizational relationships to be identified and used to achieve economies of scale: the ACE designation and the OHCA.

Affiliated Covered Entity

Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of the HIPAA privacy rule. Under this affiliation, the organizations need only develop and disseminate one notice of privacy practices, comply with one set of policies and procedures, appoint one privacy official, administer common training programs, use one business associate contract, etc.

To be an ACE, the separate covered entities must be under common ownership or control. For example, an integrated delivery network that owns several hospitals, medical groups, and long-term care facilities may designate these entities as one ACE for HIPAA. The designation must be formally documented.

If the ACE combines the functions of a health plan, healthcare provider, and/or healthcare clearinghouse, it must comply with the standards applicable to each separate covered entity. For example, providers only need to provide the notice of privacy practices once, but health plans must do so every three years. Furthermore, a covered entity that performs multiple covered functions may use or disclose the protected health information of individuals who receive the covered entity's services only for purposes related to the appropriate function being performed.

Organized Health Care Arrangement (OHCA)

Because many healthcare settings are clinically integrated but not commonly owned or controlled, the HIPAA privacy rule also permits providers that typically provide healthcare to a common set of patients to designate themselves as an OHCA for purposes of HIPAA. For example, an academic medical center often includes university-affiliated physicians and a hospital or health system. Typically, the university is a separate legal entity, but the patients are treated by the faculty within the hospital or health system.

In addition to some of the economies of scale provided by the ACE, the OHCA assures a seamless approach to HIPAA for the patients being treated by the same providers. The notice of privacy practices, however, must clearly indicate which organizations are included.

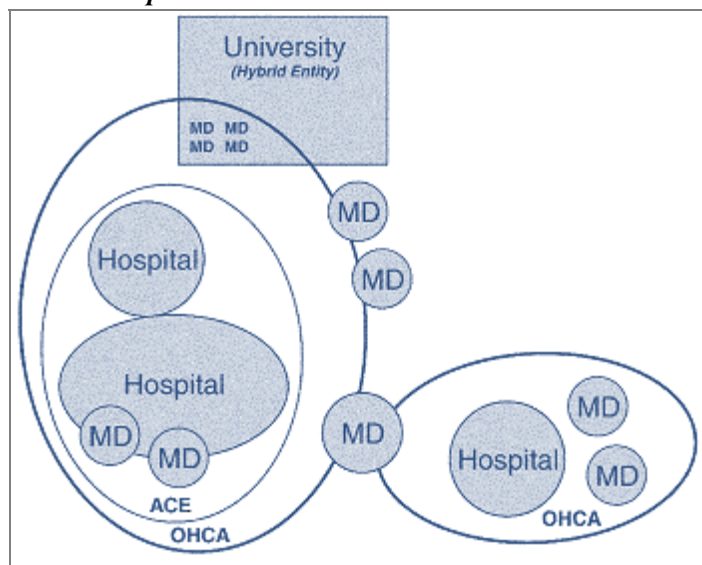
The OHCA is a helpful designation because it permits the use of a joint notice of privacy practices and provides the ability to share protected health information throughout the OHCA for treatment, payment, and healthcare operations.

There are specific requirements for designation as an OHCA. For providers, the organizations must hold themselves out to the public as participating in a joint arrangement and they must jointly perform utilization review, quality assessment and improvement activities, or payment activities. (Health plans may also designate themselves as an OHCA if they meet certain specified criteria.) Interestingly, HIPAA does not require documentation of the OHCA designation, although it would be a good practice to do so. All components of an OHCA must agree on and comply with the content of the notice of privacy practices.

One potential disadvantage of the OHCA is that if provider components of one OHCA also belong to another OHCA, complying with the notice of privacy practices of each OHCA may become complicated (see "[Relationships between ACEs and OCHAs](#)," below). Medical groups that are not owned by a health system and enter into an OHCA with the system must create their own separate notice of privacy practices for patients they treat outside the umbrella of the health system. They must also comply with the separate, different notice of any other OHCA to which they belong (e.g., if they have admitting privileges at more than one hospital).

It is extremely important to emphasize that the purpose of the OHCA is solely for compliance with HIPAA. Each component continues to be responsible for its own actions. In other words, separate entities, separate risk.

Relationships between ACEs and OCHAs



Agreements and Contracts

Each of the HIPAA transactions, privacy, and security rules also references agreements or contracts among organizational entities—some of which are covered entities and some of which are organizations providing services to covered entities.

Trading Partner Agreement

The transaction rule describes the use of a trading partner agreement, which is a contract between two parties—generally each covered entities—that exchange the financial and administrative transactions (i.e., claims, eligibility verification, remittances, etc.), such as between a provider and a clearinghouse or a provider and a health plan.

The trading partner agreement would specify various technical requirements for communications protocols, such as how the transactions are to be addressed, what character set must be used, whether receipt will be acknowledged, and more.

The transaction rule does not require a trading partner agreement, but if one is used, the rule specifies what may not be included in such an agreement. Specifically, the trading partner agreement cannot:

- change any definition, data condition, or use of a data element
- add any data elements or segments to the maximum defined data set
- require use of any codes or data elements that are marked "not used" or not in the implementation guide
- change the meaning or intent of the standard's implementation specification

Business Associate Contract

The business associate contract is the most well-known of the agreements and contracts identified in HIPAA. It is required by the privacy rule for use between covered entities and business associates, some of whom may be other covered entities.

A business associate is an individual or organization that performs a function involving use or disclosure of individually identifiable health information for a covered entity or OHCA. One covered entity may be a business associate of another covered entity if it performs such services for the other covered entity.

The covered entity or OHCA requesting the services must have a contract with the business associate to establish the permitted and required uses and disclosures of individually identifiable health information by the business associate.

There are several requirements with respect to the content of the business associate contract. They are:

- the business associate must have appropriate safeguards to prevent use or disclosure of information other than as provided for by its contract
- the business associate must report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware
- the business associate must ensure that any agents or subcontractors agree to the same restrictions and conditions that apply to the business associate with respect to the individually identifiable health information being processed
- the business associate must also make available protected health information for patient access and amendment, must make any amendment provided to it from the covered entity, and provide an accounting of disclosures
- the business associate must make its internal practices, books, and records relating to the use and disclosure of protected health information available to HHS for purposes of determining the covered entity's compliance
- at termination of the contract, the business associate must return or destroy all protected health information. The contract must also authorize termination of the contract if the business associate is in material violation

Sample contract provisions for the business associate contract are provided in the appendix to the preamble to the final privacy rule modification.

Data Use Agreement

New to the privacy rule modification is also the requirement for a data use agreement if the covered entity discloses a limited data set of protected health information to another entity. The limited data set is protected health information from which many, but not all of the data elements for de-identifying data have been removed. The data use agreement is very similar to the business associate contract, in which the recipient of the data set would agree to limit the use of the data for the purposes for which it was given to ensure the security of the data and not to identify the information or use it to contact any individual.

Chain of Trust Agreement

The chain of trust agreement was identified in HIPAA's proposed security rule. If individually identifiable health information is processed through a third party, the security rule would require that the parties enter into a chain of trust agreement.

The chain of trust agreement was described as a contract in which the parties agree to electronically exchange data and to protect the transmitted data. (The security rule did not specify the nature of these transactions.) The sender and receiver are required to and depend on each other to maintain the integrity and confidentiality of the transmitted information. Multiple two-party contracts may be involved in moving information from the originating party to the ultimate receiving party. For example, a

provider may contract with a clearinghouse to transmit claims to the clearinghouse. The clearinghouse, in turn, may contract with another clearinghouse or with a payer for the further transmittal of those claims. The agreements provide for the same level of security to be maintained at all links in the chain when information moves from one organization to another.

It remains to be seen whether the final security rule will require a chain of trust agreement separate from the business associate contract. If it does, the contractual language could potentially become a part of a trading partner agreement.

A Common Goal

HIPAA's transactions, privacy, and security rules call for contractual obligations to afford confidentiality, data integrity, and availability to protected health information among both covered entities and otherwise. After examining each relationship, consider which ones would be appropriate for your healthcare organization to simplify the transition to HIPAA compliance.

Comparison of HIPAA Arrangements and Agreements

	Affiliated Covered Entity	Business Associate Contract	Chain of Trust Agreement	Data Use Agreement	Organized Health Care Arrangement	Trading Partner Agreement
Applicable rule	Privacy	Privacy	Security	Privacy	Privacy	Transactions
Required?	No	Yes	To be determined in final rule	Yes	No	No
Purpose	Economies of scale	Protection	Protection	Protect limited data set	Economies of scale	Communication
Originated by	Covered entities	Covered entity	Covered entity	Covered entity	Covered providers	Health plan or clearinghouse (typically)
With whom	Commonly owned covered entities	Business associates	Organizations receiving data	Recipient of limited data set	Non-owned providers	Provider (typically)

Final Privacy Rule Released

The Department of Health and Human Services Office of Civil Rights released the final revisions to the HIPAA privacy rule in the August 14 *Federal Register*. For AHIMA's complete analysis of the rule, go to www.ahima.org.

Margret Amatayakul (margretcpr@aol.com) is president of Margret\A Consulting, an independent consulting firm in Schaumburg, IL.

Article citation:

Amatayakul, Margret. "United Under HIPAA: a Comparison of Arrangements and Agreements" (HIPAA on the Job series). *Journal of AHIMA* 73, no.8 (2002): 24A-D.

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.