COSMOS
Navigate the Compliance Universe

Health Care Privacy Compliance Handbook, 3rd Edition
3. HIPAA Vendor Relations

By David B. Nelson, CHRC, CHPC, CISSP[1]

Introduction

Vendors play a critical function in helping healthcare entities deliver services. The array of services available are extensive, as they might be direct or indirect. Services available could be physicians, temporary nurses, billing, legal, research, data retention—right down to educational pamphlets, paper clips, and watercoolers jugs. The range is between relatively simple to extremely complex, and they all must be reflected in the description of the business relationship between the covered entity (CE) and the vendor.

The Health Insurance Portability and Accountability Act (HIPAA) describes several types of business relationships, and there are mandates placed on the CE if a vendor has anything to do with client information. While a cleaning service does not "use or disclose" client information, its employees may be in the same space as information, which would point to the need for physical controls for privacy and security of the space. The "function" and where it performs the service usually requires one of the specific HIPAA solutions for privacy and security. The trick is to identify the correct solution.

The most familiar relationship for sharing information is the business associate (BA), controlled through the contractual business associate agreement (BAA). However, there are other solutions for sharing information beyond just getting client authorization, which are described in the Transactions and Code Sets, Privacy, and Security rules. They are affiliated entities, organized healthcare arrangements (OHCAs), trading partner agreements, and assurances. By splitting these into two groups, administrative and contractual, it is easier to grasp which fits a vendor function.

Author's Note: In some instances, I have included a citation to a definition or explanation of the topic. I have done this where possible to reduce the length of this chapter, as this handbook is an introduction to topics, not a definitive source. While it would be prudent to include many definitions at the point where referenced, I suggest the reader create their own definitions document. In this way you will have, at your fingertips, all of the terms that you use regularly (e.g., HIPAA, 42 C.F.R. Part 2 , FERPA, state regulation definitions, your entity policy terms). I have included some definitions as they make a specific point for discussion and are relatively short.

Administrative Solutions

Administrative solutions require just as much work as any contract solution, but they fit specific business relationships or definitions.

1) Affiliated Covered Entity (Affiliated CEs)

> **Affiliated Covered Entities.** Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of this part.[2]

In simplistic terms, an Affiliated CE would look like one entity with corporate control of multiple CEs, sometimes

in multiple jurisdictions. Usually these entities have a centralized corporate office that provides many administrative functions, such as human resources, legal, infrastructure maintenance, and intranet support, and it could provide some corporate privacy or security functions. The deciding factor on declaring the affiliated status is "legally separate covered entities." While an Affiliated CE could have a general Notice of Privacy Practice from the corporate level, it might have to include the local (read: state preemption) mandates that do not apply to all jurisdictions.

The declaration of affiliated status also declares *specifically* what information is shared between any of the corporate pieces. Remember, this is a healthcare mandate placed on CEs, yet if the separate entities are part of a larger organization, information from each CE may need to move to the corporate level or between the healthcare operations in individual legal jurisdictions. This is a corporate administrative solution that meets the letter of the law. However, some information is firewalled from certain corporate functions. A hospital in Reno, Nevada, could share some information with a corporate office in Sacramento, California, as long as the shared content is in the Affiliated CE declaration. For example, personal health information of employees in one jurisdiction should not be shared with the corporate building maintenance function. It is the declaration documents that control the information, and allowable transfers must be stated prior to sharing.

Note: For privacy compliance without confusion, declaring content prior to information sharing is much easier to explain to auditors than relying on justifications or arguing over the meaning of technical terms after the fact. If you are going to "go left" the majority of the time, say, "We are going to go left." You can add an exclusion clause that says "unless there is a documented reason to go right." This documents how you will normally operate, *unless* you have a documented reason. The much looser, "We may go left," begs the question: "Why did you go left this time and not that time?" You end up explaining multiple situations, rather than the one-off that you documented.

There are specific implementation standards at 45 C.F.R. § 164.504(d) that you must address if you are going to choose the affiliated administrative solution for sharing information.

I also recommend you read the discussion on page 82,503 of the *Federal Register*.[3] It explains what the Department of Health and Human Services was trying to achieve under this designation.

2) Organized Healthcare Arrangements

Similar in some ways to the Affiliated CE is the Organized Healthcare Arrangement (OHCA). It differs principally by being separate CEs, but *not* under the control of one entity. Specifically, OHCA means:

> 1. A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;
> 2. An organized system of health care in which more than one covered entity participates and in which the participating covered entities:
>   i. Hold themselves out to the public as participating in a joint arrangement; and
>   ii. Participate in joint activities that include at least one of the following:
>   A. Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

B. Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

C. Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

3. A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

4. A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

5. The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.[4]

Often the OHCA designation is used where multiple entities are on one campus or located relatively close to each other. A hospital may not own the pharmacy on the first floor, the radiology clinic across the parking lot, or the outpatient substance use disorder clinic just down the street. Yet, they may all service the same client or refer to each other frequently. Or, the hospital billing department could process all of the claims for each entity, thus reducing the collective expense AND providing oversight so that duplicate billing does not occur. The OHCA declaration may be used for the simplification of administrative activities, and it must clearly state what information is shared back and forth. But remember, the "system of care" OHCA members *must* perform one of the three mandates under the definition in section 2(ii) of the OHCA definition in 45 C.F.R. § 160.103 .

Another example is when a large organization has multiple healthcare plans for employees and the necessary information sharing is easily facilitated by an OHCA declaration. Again, they can state what information will be shared between the plans. Be wary that state employment laws come into play with this OHCA. This will probably block OHCA activities from other human resources functions, as OHCA activities fall under the HIPAA health plan mandates, not just employment law.

Note: A shorthand definition for OHCA: Clinically integrated or organized healthcare systems that, at times, include not *just* clinical elements, such as multiple health plans and the various activities they perform. The key is an "integrated" relationship. While the OHCA is frequently driven by a principal player in the arrangement, the principal player *is not* controlling the other players. This is unlike the Affiliated CE.