Hybrids and BAs and Workforce – Oh My! A Guide to Who and What is Covered[1]

Jill Moore, JD, MPH

Critical Updates for HIPAA Officers in Local Public Health Agencies

September 2017

I. Covered entity[2]

A *covered entity* is:

- A health plan, or
- A health care clearinghouse, or
- A health care provider that transmits health information electronically in connection with a HIPAA transaction.

A *health plan* is an individual or group plan that provides or pays the cost of medical care. This includes health insurance companies, HMOs, company health plans, and public insurance programs such as Medicare or Medicaid.

A *health care clearinghouse* is a company/entity that receives health information from another entity and processes nonstandard information into standard formats or vice versa. This includes entities such as billing services that do this kind of processing.

A *health care provider* is a provider of medical or health services, or any other person, business, or agency that furnishes or receives payment for health care in the normal course of business. The term is very broad and includes dentists, pharmacies, chiropractors, long-term care facilities, and others, as well as medical care providers and facilities. A health care provider is a covered entity only if the provider transmits health information electronically in connection with a transaction for which there is a HIPAA standard (also known as a HIPAA transaction or a covered transaction). At present, there are HIPAA standards for the following transactions:

- Health care claims or equivalent encounter information
- Eligibility for a health plan
- Referral certification or authorization
- Health care claim status
- Enrollment and disenrollment in a health plan
- Health care payment and remittance advice
- Health plan premium payments
- Coordination of benefits
- Medicaid pharmacy subrogation

---

[1] This document is a handout developed to support a training workshop held in Asheville, NC on September 26, 2017. It is not an academic paper and it is not a comprehensive treatment of all issues related to covered entities, hybrid entities, business associates, or workforce.

[2] Italicized terms in this document have specific definitions in the HIPAA regulations. 45 CFR 160.103. This document provides abbreviated descriptions of the terms, which are derived from the regulatory definitions, plus the additional guidance information provided by the U.S. Department of Health & Human Services through its HIPAA website, https://www.hhs.gov/hipaa/for-professionals/index.html.

II. Hybrid entity

A covered entity may designate itself a *hybrid entity* if it is a single legal entity whose business activities include both covered and non-covered functions. A *covered function* is a function the entity performs that makes it a health plan, a health care clearinghouse, or a health care provider. For example, the provision of health care by a local health department is a covered function. Local health departments in North Carolina are eligible to designate themselves hybrid entities because they also do things that are not covered functions, such as permitting on-site wastewater systems.

In order to be a hybrid entity, the covered entity must document its status as a hybrid entity and designate its *health care component*, which is the part or parts of the hybrid entity that are covered by HIPAA.

The HIPAA regulations specify that the health care component must include:

- **Covered functions** – The entity must include all its covered functions in the health care component. If a particular program or division has some covered functions and some non-covered functions, it may be designated as covered only to the extent that it is performing covered functions.
- **Business associate-like functions** – The entity must also include any functions or activities that would create a business associate relationship if they were carried out by a separate legal entity.

A hybrid entity is allowed to include non-covered functions in its health care component if it chooses. This is optional.

While the hybrid entity designation must be documented, there is no requirement that it be filed with anyone—the document simply needs to be retained in the entity's own files. However, this does not mean the document is unimportant. To the contrary, the entity designation is a core document that drives multiple other HIPAA policies and procedures. Agency leaders and HIPAA officers should be familiar with what is in the document, and should review it periodically to be sure it is still up-to-date.

A hybrid entity must treat its non-covered components as if they were entirely separate entities when using or disclosing protected health information (PHI). Technology, policies, and practices need to enable the agency and its workforce to adhere to this obligation.

Special consideration for county departments – county vs. agency as relevant entity

Most of North Carolina's local health departments are departments of counties—they are either a county health department or a county consolidated human services agency. These agencies should work with their counties on the hybrid entity designation, as it is likely the county itself is the covered entity, rather than the individual department. This is because a department of a county is not a legal entity in its own right; rather, it is part of a larger legal entity—the county. In some places, the HIPAA regulations use the term "single legal entity" to refer to a covered entity. While this term is not defined, in context it implies something that is recognized as an autonomous entity for other legal purposes, such as determining its own budget, or being authorized to sue and be sued. County departments do not have those qualities. When a health department is a county department, ideally the county itself will create a hybrid entity designation. (The health department

will likely have its own designation as well, with the recognition that it is a hybrid department of a larger hybrid entity.) This allows the county to address the likelihood that the county has other HIPAA-covered functions that should be included in the hybrid entity designation. For example, a county EMS agency would probably need to be included in the county's designation. It is also likely that different county departments (such as finance, human resources, or legal) carry out business associate-like functions for the health department. Those too should be included in the county's hybrid entity designation to the extent they are using or disclosing PHI to perform work on behalf of covered components.

District health departments and public health authorities have the characteristics of a single legal entity and may consider themselves covered entities in their own right. They should create hybrid entity designations if they do not wish to have all of their functions subject to HIPAA.

III. Business associates

A *business associate* is a person or entity that is not a member of the covered entity's workforce, and that does something that fits into one of the following categories:

1. Performs or assists in performing, on behalf of a covered entity:
    - A function or activity that involves the use or disclosure of PHI, including (but not limited to) claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
    - Any other function or activity that is regulated by HIPAA.
2. Performs any one or more of the following specific services for a covered entity, when those services require the use or disclosure of PHI:
    - Legal services
    - Actuarial services
    - Accounting services
    - Consulting services
    - Management services
    - Administrative services
    - Accreditation services
    - Financial services

Business associate contracts (also known as business associate agreements) are required by both the Privacy and the Security Rule. The basic requirements for the terms of the agreement are set out in the Privacy Rule. The agreement must establish when the business associate (BA) is permitted to use or disclose PHI, and must include provisions that the BA will:

- Refrain from using or disclosing PHI except as permitted or required by the BA agreement or as required by law.
- Use appropriate safeguards to prevent the unauthorized use or disclosure of PHI.
- Notify the covered entity if the BA becomes aware of a use or disclosure of PHI that is not permitted by the BA agreement.
- Ensure that its agents or subcontractors comply with the same restrictions and conditions that apply to the BA.
- Make PHI available to the covered entity so that the covered entity may comply with the provisions of the Privacy Rule that give individuals the right to access their PHI, the right to amend PHI, and the right to obtain an accounting of disclosures of PHI.

- Incorporate amendments to PHI when notified to do so by the covered entity.
- Make documents and other information available to the federal oversight agency when needed to ensure the covered entity's compliance with HIPAA.
- Upon termination of the agreement, return or destroy all PHI to the covered entity, if feasible. If it is not feasible, extend the protections of the BAA and limit further uses or disclosures to the purposes that make the return or destruction of the PHI not feasible.

The Security Rule adds that a BA agreement must include provisions that the BA will:

- Comply with the Security Rule.
- Ensure that any of the BA's subcontractors that create, receive, maintain, or transmit electronic PHI on the BA's behalf will comply with the security rule. The BA must do this by treating its subcontractors as its own BAs with whom a BA agreement is required.
- Report to the covered entity any security incidents that it becomes aware of, including breaches that require notification under HIPAA's breach notification rule. (The breach rule has a specific section setting out the duties of BAs that discover breaches. 45 CFR 164.310.)

A BA agreement may not authorize a BA to use or disclose PHI in a way that would violate the Privacy Rule, nor may a BA agreement be used to attempt to create a "business associate" relationship where none exists in order to support a desired disclosure.

IV. Workforce

For HIPAA purposes, an entity's *workforce* includes employees, volunteers, trainees, and other persons whose conduct in the performance of work for a covered entity is under the direct control of the covered entity, regardless of whether they are paid.

If the covered entity is a hybrid entity, then the workforce is composed of the employees, volunteers, trainees, and other persons whose work is performed for the entity's health care component.

It is important for covered entities to be able to identify all members of the workforce for purposes of complying with HIPAA regulations. For example, the rules require members of the workforce to receive training in HIPAA policies and procedures.