HIPAA Highlights for Administrators

Jill D. Moore, UNC School of Government

February 2016

I. Entity Designation: Covered Entities and Hybrid Entities

A. Covered Entity (45 C.F.R. § 160.103)

The HIPAA regulations apply to *covered entities*, a term that is defined to include health plans, health care clearinghouses, and health care providers who transmit health information electronically in connection with one of several HIPAA transactions. (The relevant HIPAA transactions relate primarily to insurance claims – eligibility determinations, submitting a claim for payment, etc.). North Carolina's local health departments[1] satisfy the last part of that definition: they are health care providers, and they submit health information electronically in connection with claims to Medicaid and possibly other insurers as well.

Of course, local health departments also do other things that have nothing to do with the provision of health care, such as their environmental health programs. It may not make sense for those activities to be subject to the HIPAA regulations. Fortunately, there is a way for covered entities to "carve out" functions and activities from regulation by HIPAA: the covered entity can designate itself a hybrid entity.

B. Hybrid Entity (45 C.F.R. §§ 164.103, 164.105)

1. Definitions; designating covered components

A *hybrid entity* is a covered entity that:

- Carries out both covered and non-covered functions, *and*
- Documents its hybrid entity status and designates its covered functions.

Covered functions are the things the entity does that make it a covered entity—in the case of health departments, the provision of health care and the associated transmission of health information electronically in connection with HIPAA transactions. Anything that would not satisfy the definition of covered entity if it were a stand-alone activity is a non-covered function. *However, unless the covered entity creates a hybrid entity designation, the non-covered functions are subject to the HIPAA regulations the same as the covered functions.* This is a tremendously important point for health departments—if the agency doesn't want all of its employees and all of its activities subject to HIPAA regulations, it needs

[1] I am using the term "local health department" to mean county health departments, district health departments, public health authorities, and consolidated human services agencies that provide public health services for a county. This is consistent with how North Carolina law uses the term. G.S. 130A-2(5); 130A-43; 153A-77.

to document that it is a hybrid entity and designate which of its functions, activities, and programs are subject to HIPAA. The functions, activities, or programs that are designated in the hybrid entity document constitute the entity's *covered component*. The HIPAA regulations apply only to the covered component. Anything that is not part of the covered component has effectively been "carved out" of HIPAA coverage.

So what needs to be in the covered component?

First, a covered entity must include its covered functions in its hybrid entity designation. 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 public functions.

Second, the hybrid entity designation must also include in the covered component any functions or activities that would create a business associate relationship if they were carried out by a separate legal entity. For example, if a health department has its own finance office, that office most likely performs activities using or disclosing protected health information (PHI) on behalf of the department's covered components. That would make it a business associate (BA) if it were a wholly separate legal entity, so it needs to be included as a covered component in the hybrid entity designation. However, it may be included only to the extent that it is involved in BA-like activities – it is not necessary to extend HIPAA to everything a BA-like agency component does.

Finally, a hybrid entity is allowed to include non-covered functions in its covered component if it wants to. It doesn't have to do this but there may be reasons for making this choice—for example, if the entity wants to enable freer flow of information to a particular program that is a neither a covered function nor a BA-like component per the HIPAA definitions, but that nevertheless works with PHI.

2. *County vs. agency as the 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 hybrid entity designation, as it is likely *the county itself is the covered entity* rather than the department, because the department is not a legal entity in its own right. 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 likely will 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 as well, such as an EMS agency, which should be included in the hybrid entity designation. It is also likely that different county departments carry out business associate-like functions for the health department—departments such as finance, human resources, or legal—and 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 too should create hybrid entity designations if they do not wish to have all of their functions and activities subject to the HIPAA regulations.

3. Documenting, retaining, and updating the hybrid entity designation

There is no requirement that the HIPAA hybrid entity designation be filed with anyone—the document simply needs to be retained in the entity's own files. However, this should not be misconstrued to suggest that the document is unimportant. To the contrary, the entity designation is a critical core document that drives multiple other HIPAA determinations and policies. Agency leaders should be familiar with what's in the document, know where to find it, and review it periodically to make sure it is still up-to-date.

4. The requirement for a "firewall" between covered and non-covered components

The HIPAA Privacy Rule requires a hybrid entity to treat its non-covered components as if they were entirely separate entities when using or disclosing PHI. This means that information about health department patients may not be disclosed to or used by the health department's non-covered components unless the patient gives written authorization, or the use or disclosure is otherwise allowed by the HIPAA privacy rule. (HIPAA's general rule is that written authorization is required, so it's best to start with the assumption that authorization is needed, and stick with that assumption until you can identify the HIPAA provision that allows use or disclosure without it.) We sometimes refer to this as a requirement that there be a "firewall" between the covered and non-covered components. Technology, policies and practices need to enable the agency and its employees to adhere to this obligation.

II. HIPAA Officers

Covered entities must designate a privacy official and a security official. The privacy official is responsible for developing and implementing the policies and procedures required by the HIPAA Privacy Rule. 45 C.F.R. § 164.530(a). Similarly, the security official is responsible for developing and implementing the policies and procedures required by the HIPAA Security Rule. 45 C.F.R. § 164.308(a)(2)). These may be separate individuals, or the same person may serve in both roles. Depending on the needs and resources of the entity, there may also be deputy or assistant privacy or security officials. For example, a county may have a chief officer who is responsible for HIPAA throughout the county, but then deputy or assistant officials for privacy, security, or both in the departments that constitute the county's covered components.

III. Business Associates

Every covered entity has business associates (BAs). HIPAA has a detailed definition of "business associate" (see below), but in general, these are individuals or entities who need access to PHI in order to perform functions or activities on the covered entity's behalf.

A covered entity must have a business associate agreement (BAA) with its business associates. The overarching purpose of the BAA is to ensure that PHI is protected in accordance with HIPAA's requirements. Since 2013, business associates have been directly responsible for HIPAA compliance and directly liable to federal HIPAA oversight agencies for any failures in this regard. However, covered entities still are required to enter BAAs with their business associates.

"Do I need a business associate agreement?" is a very frequently asked question. The short answer is that a BAA is required only if a person or entity is a BA. It's not quite as simple as that sounds, but the short answer tells us where to start figuring out: by looking at the definition of business associate and determining if the person or entity we're talking about fits.

A. Definition of Business Associate (45 C.F.R. § 160.103)

A business associate is a person or entity that is not a member of the covered entity's workforce,[2] but who 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 the HIPAA regulations.
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
    - Data aggregation services
    - Management services
    - Administrative services
    - Accreditation services
    - Financial services

[2] Workforce is defined to include employees, volunteers, trainees, and other persons whose conduct in the performance of work for the covered entity is under the direct control of the covered entity, regardless of whether they are paid.

B. Business Associate Agreements (Contracts) (45 C.F.R. §§ 164.318, 164.5

Both the Privacy Rule and the Security Rule require BAAs and specify what the agreements must include. The basic requirements for the terms of the agreement are set out in the Privacy Rule. The agreement must establish when the BA is permitted or required 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 BAA 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 BAA.
- 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 BAA 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 BAA 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 notification rule has a specific section setting out the duties of BAs that discover breaches. 45 C.F.R. § 164.410.)

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

A sample business associate agreement is available from the US Department of Health & Human Services (the HIPAA enforcement agency), at http://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.

C. BAA Not Required to Disclose PHI to a Health Care Provider for Treatment Purposes

When a health department discloses PHI to a health care provider *for treatment purposes only*, a BAA is not required.

It is possible for a health care provider to be a BA, and indeed it is a BA if it has a relationship with the covered entity that involves one of the activities covered by the BA definition. The point here is simply that disclosures made to health care providers *for treatment purposes only* do not create a BA relationship requiring a BAA. This is probably the most frequently asked question I get about BAs.