HIPAA and DSS:
Covered Entities? Hybrid Entities? Business Associates?

Aimee Wall
UNC School of Government

This paper will address the foundational questions that county departments of social services must understand and answer when evaluating whether the department or a component of the department must comply with the HIPAA privacy and security regulations. It will not explore details of either of the regulations, such as when use and disclosure of protected health information is allowed. If a county DSS, or a component of DSS, determines that it must comply with HIPAA, the next step will be to evaluate the intersection of the HIPAA regulations with other confidentiality laws that apply to the information used and disclosed by the department and develop appropriate policies and procedures.

1. Do the HIPAA privacy and security regulations apply to county departments of social services?

A county DSS is subject to the HIPAA privacy and security regulations if, and to the extent that, the social services department is a

- covered entity,
- a covered health care component of a hybrid entity, or
- a business associate of a covered entity.

There are three types of "covered entities under HIPAA:

- health plans
- health care clearinghouses
- health care providers who transmit any health information in electronic form in connection with a HIPAA-covered transaction

A county DSS almost certainly is not a health plan or a health care clearinghouse (see Appendix for definitions). It may, however, be a health care provider. Unpacking and understanding the definitions of the terms "health care provider," "health care," and "health information" is key to determining whether the county DSS – or a small part of the county DSS – is a covered health care provider. The next question will explore these terms and concepts in more detail.

2. When is a county DSS a covered health care provider?

Does any component of the county DSS, in the normal course of business, furnish health care* to an individual?

NO ➔ The county DSS is not a covered health care provider.

YES

Does the county DSS or another entity transmit health information** electronically in connection with a HIPAA transaction on behalf of a county DSS component that furnishes health care to an individual?

NO ➔ The county DSS is not a covered health care provider.

YES

Has the county designated itself as a hybrid entity?

NO ➔ The county DSS is a covered entity and all components of the county DSS must comply with the HIPAA regulations.

YES

The county is a hybrid entity, which means that it is a HIPAA covered entity and it must designate covered health care components. Any DSS component that is a covered health care provider must be included within a covered health care component and therefore must comply with the HIPAA regulations. In addition, any DSS component that is performing a function or activity that would make it a business associate of the covered component if the two were separate legal entities must comply with the HIPAA regulations.

***Health care** means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body…

****Health information** means any information, including genetic information, whether oral or recorded in any form or medium, that is created or received by a health care provider… and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

3. What is a hybrid entity and why does it matter?

If a covered entity has a mix of functions, the HIPAA regulations allow the covered to designate itself a hybrid entity. This means that the "single legal entity" draws invisible lines throughout its organization to separate covered and non-covered components.

The covered components must include:

(1) Any component that would be a covered entity if it was a separate legal entity, and

(2) Any component that would be considered a business associate of the covered function.

The term "business associate" will be discussed in more detail below.

The county is the "single legal entity" and therefore it must make the first important decision: is it a hybrid entity? It is responsible for making the designation – which simply means documenting the decision to call itself a hybrid entity. It is not required to report this decision to anyone at the federal level but it must document it.

The county DSS must be prepared to make a careful evaluation of its operations to determine which pieces of the department should be included in the health care component. It may well be that the answer is *none.*

If, however, there is a covered health care provider in the department, DSS will need to (1) draw some lines around that component and (2) identify any "business associates" (both internal and external) of that component. If the business associate is internal (i.e., an employee/agency/department of the county), the business associate *must* be included in the "health care component" of the hybrid entity (see further discussion below). If the business associate is external, the county must ensure that it has "satisfactory assurances" that the associate will comply with HIPAA, which likely will require entering into a business associate agreement.

Once the covered health care component is defined, the covered entity must ensure that there are firewalls in place to prevent inappropriate use and disclosure across components. In addition, staff within the covered component must comply with all of the other requirements of the HIPAA privacy and security regulations, including drafting detailed policies and procedures, providing training, establishing safeguards, and distributing notices of privacy practices.

4. What is a business associate and why does it matter?

In short, a business associate is a person or entity that is not a member of a covered entity's workforce who uses protected health information in order to help or support a covered entity. Examples of functions or services that a business associate might provide include:

- Claims processing and administration;
- Quality assurance;
- Data analysis;
- Billing; and
- Providing legal, accounting, consulting, and financial services.

The HIPAA regulations require that a covered entity have "satisfactory assurances" that the business associate will protect the information and comply with other administrative requirements. These assurances are typically part of a contract referred to as a "business associate agreement." The business associate is has two layers of legal responsibility; it is

- (1) Required to comply with HIPAA regulations and may be subject to enforcement actions in the same way a covered entity would be and
- (2) Responsible to the covered entity pursuant to the contract.

For a *regular* health care provider, these relationships may be fairly straightforward. The provider hires a billing company. The provider enters into a business associate agreement with the billing company. Easy.

For a county DSS that is part of hybrid entity, the application of the concept may be more complex. The county may have some external business associates – these would look just like the billing company described above. It may be a contract with an outside organization to provide some consulting services that requires disclosure of some protected health information, for example. In this case, the county would enter into a business associate agreement with the consulting group.

The county may have some internal components that are performing business associate-like functions for one or more health care components within the county. For example, the county's finance office may be managing all of the billing for the provision of health care by DSS, the health department, and emergency management services. If the finance office was not included within the county, it would be considered a business associate. Since it is within the county and the county is a hybrid entity, the county must include the finance office as part of its covered health care component. In other words, the county *must* include any business-associate like functions in its health care component.

It is possible to include a business associate-like function in the health care component "only to the extent that it performs covered functions." This means that, in our example above, not every staff person in the finance office would need to be trained to comply with the HIPAA regulations but only those staff members who work with protected health information for the

covered health care component. In addition, not all records in the office would be subject to all of the HIPAA restrictions on use and disclosure. This may be helpful but it also could be tricky to execute depending upon the size of the organization and the number of people and activities o functions involved. A county may simply decide that, for ease of administration, all staff and records within a business associate-like component will comply with the HIPAA regulations.

Appendix: Key Definitions

Definitions can be found in 45 CFR 160.102, 45 CFR 164.103.

Business associate (1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

> (i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or
>
> (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity may be a business associate of another covered entity.

(3) *Business associate* includes:

> (i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.
> (ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.
> (iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(4) *Business associate* does not include:

> (i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance HIPAA Administrative Simplification Regulation Text March 2013 issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.
(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.
(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

Covered entity means

(1) A health plan
(2) A health care clearinghouse.
(3) A health care provider who transmits health information in electronic form in connection with a transaction covered by this subchapter [HIPAA regulations].

Health care means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following:

(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health care provider means…any…other person or organization that furnishes, bills, or is paid for health care in the normal course of business.

Health information means any information, including genetic information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan…; and
(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Health plan means an individual or group plan that provides, or pays the cost of, medical care. [This includes Medicaid and Health Choice, but only at the state level]. The definition excludes … A government-funded program

(1) whose principal purpose is other than providing, or paying the cost of, health care; or
(2) whose principal activity is
    (a) the direct provision of health care to persons; or
    (2) the making of grants to fund the direct provision of health care to persons.

Hybrid entity means a single legal entity

(1) That is a covered entity;
(2) Whose business activities include both covered and non-covered functions; and
(3) That designates health care components in accordance with §164.105(a)(2)(iii)(D).