Last Revised: September 11, 2009

HIPAA Basics

When we work with Protected Health Information (PHI) covered under the Health Insurance Portability and Accountability Act (HIPAA), we have to make sure we understand the impact of HIPAA. Its impact will depend on the nature of the project, what we are using for identifiers, and our relationship to the Covered Entity. Depending on these factors, the compliance requirements for your project may have big implications for its cost and even its feasibility. That's why we need to identify HIPAA issues early in the process, when we still have time to design our work to minimize or avoid the cost of HIPAA, or price our work to reflect the additional costs that go along with using PHI.

This TIPSHEET provides a basic overview of some key HIPAA terms to help you know a HIPAA issue when you see one, as well as some options for study design that have implications for how HIPAA applies to you. Another **TIPSHEET**, **HUMAN SUBJECTS AND HIPAA**, helps you sort through the range of compliance requirements that might apply to your work, depending on whether or not your study also involves research.

Summarizing laws can be tricky. They are often too complex to be summarized and there are usually nuances in how to interpret them that are only apparent when the law is applied to the specific facts in a particular situation. That's why this TIPSHEET is not intended to give you answers, only enough information to go on to ask the right questions. The University of Maine System Counsel is the only person authorized to say whether or how HIPAA applies to your project.

The Basics

In our world, spotting HIPAA issues requires a working knowledge of three key terms: Basically, we need to make sure we understand when we are using **Protected Health Information (PHI)** that has been created by a **Covered Entity** or by a **Business Associate** working on behalf of the Covered Entity. Each of these terms is explained more fully below, in the context of the work that we do at the Muskie School.

What's a Covered Entity?

In many cases, spotting a Covered Entity should be pretty easy. Now that HIPAA's been around so long, the people working for the Covered Entity should be able to tell you if they're covered or not. However, that's not always the case and even if it were, you still need to know when to ask the question, because the sooner you ask, the sooner you know what you need to do to comply.

The definition of a Covered Entity identifies three types of entities that fall within HIPAA's reach: a health plan, a health care provider, or a health care clearinghouse. You can read more about how these

terms are defined in the Box on the next page. These definitions capture some very obvious candidates for health plan Covered Entities: the MaineCare Program, Dirigo, Anthem Blue Cross are some examples of health plans that we might work with here at the Muskie School. The definition of health care provider can also be pretty straightforward: a hospital, a medical practice, a nursing service, mental health providers, and substance abuse treatment providers, all seem to be obvious candidates. We also need to take a close at case management agencies and other social service agencies that we work with. Depending on the nature of their services, these agencies may also be a "health care provider" within the meaning of HIPAA.

When it Gets Complicated. Sometimes, however, it's not so easy to know when you're dealing with a Covered Entity. Listed below are some of the confusing situations you should be looking for. And to play it safe, *ask when you don't know*.

On the Border. Because HIPAA defines health care very broadly (see Box), in some cases, it might not seem obvious we're working with a health care provider. For example, a homemaker agency or a supported employer provider might not sound like they have anything to do with health care but could still be a Covered Entity. You might not know until you ask, but if you are obtaining individually identifiable information about the people they serve, you should *definitely ask*.

Hybrids. Some large, complex organizations have some organizational units that are covered under HIPAA (*i.e.*, a "covered component") and others that are not. The Maine Department of Health and Human Services is a familiar example of a "hybrid." It includes several components that each qualify as a Covered Entity, several offices that are partially treated as a Covered Entity, and several that do not. In hybrid organizations like this, not everyone working for the organization is necessarily aware of which component is covered and which is not. When working with a large organization like DHHS, if you don't already know, *you need to ask* whether or not you are working with a covered component.

Covered Entities

Health Plan: A health plan is an individual or group plan that provides or pays the cost of medical care. A health plan includes an employer sponsored plan. The Medicaid program, the State Child Health Program (SCHIP) and other government-funded health plans are also included.

Health Care Provider: A health care provider is any person or organization that furnishes, bills or is paid for *health care* who also electronically transmits health information in connection with certain transactions (e.g., claims, benefits eligibility inquiries, authorization requests). Providers who use a third party to perform these transactions are also included. ("***Health care***" is defined very broadly and includes "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….") An individual can be a Covered Entity if the individual meets all of the criteria (including electronically transmitting health information in connection with certain transactions).

Health Care Clearinghouse: A health care clearinghouse processes nonstandard information received from another entity into a standard (*i.e.*, standard format and content), or vice versa. Examples include billing services or community health management information systems.

Who's Providing the Data. You also need to focus on who is giving you the information. Is it your partner or a Covered Entity in contract with your partner? For example, your partner might be a correctional facility that reports it's not a Covered Entity. But you still have a HIPAA issue if you're obtaining health information from a contracted health service providing care to inmates.

Schools. In some cases, an elementary or secondary school provides health care to its students through a student health clinic. While technically the school might be a Covered Entity under HIPAA, if it maintains the health information as part of the educational record, the school complies with the Federal Educational Rights and Privacy Act (FERPA), not HIPAA. If you are trying to access health information created by a school health clinic, consult with the school to determine if its health information is protected under HIPAA or FERPA. If it's protected under FERPA, consult with the school to determine the best way to access the records. *Note*: The review of any agreement for acquiring protected information from an external source, including one governed by FERPA, would go through the same review process as required for a BAA or DUA governed under HIPAA.

What's Protected Health Information?

Protected Health Information is based on the definition of individually identifiable health information[1] which:

- Is created or received by a health care provider, a health plan, an employer, or health care clearinghouse, or a Business Associate acting on behalf of a Covered Entity.
- 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; (See a partial definition of "health care" in the Box on the previous page.)
- Is "individually Identifiable" when the individual can be identified either by name or other specified identifiers, or because there is a reasonable basis to believe the information can be used to identify the individual. (See DESIGN OPTIONS below for some guidance on the meaning of "identifiable" under HIPAA.)

At the Muskie School we can either:

- *Obtain* PHI from a Covered Entity (*e.g.*, the names and contact information of MaineCare members that you use to recruit participants for a survey, or data you use for data analysis), or

[1]HIPAA excludes certain types of individually identifiable health information from the definition of Protected Health Information: information in education records covered under Federal Educational Rights and Privacy Act (FERPA); certain records for students at post-secondary educational institutions maintained by a physician or another professional in connection with treatment; or employment records held by a Covered Entity in its role as an employer.

- *Create* PHI on behalf of a Covered Entity when we are acting as a Business Associate (*e.g.*, information that you obtained from focus group participants when you were conducting a program evaluation on behalf of a Covered Entity).

Design Options. HIPAA makes some important distinctions in how much protection health information requires depending on how identifiable it is. If you can design your project so you don't need identifiable health information at all (*i.e.*, it's "de-identified" as defined by HIPAA), then you don't have to worry about HIPAA. Also, if you don't need directly identifiable information, you might be able to avoid the highest level of HIPAA protections (and liability). Below explains the way HIPAA distinguishes identifiable PHI:

Fully Identifiable PHI. PHI that directly identifies an individual (*e.g.*, with a name, social security, date of birth, etc.) or for which there is a reasonable basis to believe it could be used to identify an individual requires the highest level of security.

Limited Data Set. Partially identifiable PHI with direct identifiers removed in compliance with HIPAA. This PHI is known as a Limited Data Set. See the grid on page 7 for more on Limited Data Sets. (*Note*: a Limited Data Set is only available for public health, research, and health care operation purposes.)

De-Identified Health information. De-identified health information is only de-identified when all identifiers are removed, as defined by HIPAA. See the grid on page 7 for more on De-Identified Data.

IMPORTANT

Under HIPAA if you *can* design your project to not require PHI, you *must* design your project to not require PHI. Design your study to include only the individual identifiers and other information that you need in order to achieve your study objectives. If you need linked data (combining data from more than one Covered Entity) explore whether another entity can link the data and provide you with de-identified linked data.

Security and PHI. The identifiers included in your data determine what you level of security is attached to your data. The grid on page 8 identifies the different conditions HIPAA places on acquiring health information, and the different level of security attached, depending on the identifiers that are included.

What's a Business Associate?

A Business Associate is a person or entity that performs certain ***functions*** or activities that involve the use or disclosure of PHI on behalf of, or provides ***services*** to, a Covered Entity.

Functions. A Business Associate might perform these and other functions on behalf of a Covered Entity: data analysis, processing or administration; rate setting; quality assurance; quality assessment or improvement; population based activities relating to improving health or reducing health care costs, or protocol development; evaluating practitioner and provider performance or

health plan performance; and conducting training programs in which students, trainees or practitioners learn under supervision to improve their skills.[2]

Services. Services that might be provided to a Covered Entity include data aggregation (combining data from one Covered Entity with that of another to permit data analysis of the operations of both), consulting, administrative, management, legal, actuarial, accreditation or financial services.

Risks and Responsibilities. When we serve as a Business Associate we take on a lot more risk and responsibility than when we acquire health information in other ways. In particular:

- We have to comply with HIPAA privacy and security standards;
- We are liable for civil and criminal penalties when we fail to comply with HIPAA privacy and security standards;
- We have to report our breaches. In some cases, we will have to report breaches by the Covered Entity we're working with, including if necessary to the federal government;
- Our violations (when more than 500 people are affected) will be published in the media and on the ("wall of shame") website for the federal Office of Civil Rights within the U.S. Department of Health and Human Services. In addition to discrediting the Muskie School and the University with our partners, this public exposure invites more scrutiny and challenges from people who might want to claim a breach.

It is What it Is. Given this increased level of risk, we have an obvious incentive to avoid being a Business Associate whenever possible. Obtaining a Business Associate's Agreement will be harder and complying with a Business Associate Agreement will mean higher costs, more responsibility for the Project Director, and more restrictions on how the information is used. But wishing to avoid the Business Associate relationship doesn't mean we do; and failing to obtain a Business Associate's Agreement when you need one only creates major problems down the road.

Ultimately, avoiding a Business Associate relationship comes down to your project design:

- Can you design your study so that so that you require only a Limited Data Set or, better, de-identified data (see PROTECTED HEALTH INFORMATION above)?
- Can you design your study so that performing a function on behalf of or providing a service to a Covered Entity is not the primary purpose of your study?[3]

If you can answer "yes" to either one of these questions, you can spare yourself a lot of extra work and spare your partner some extra expense.

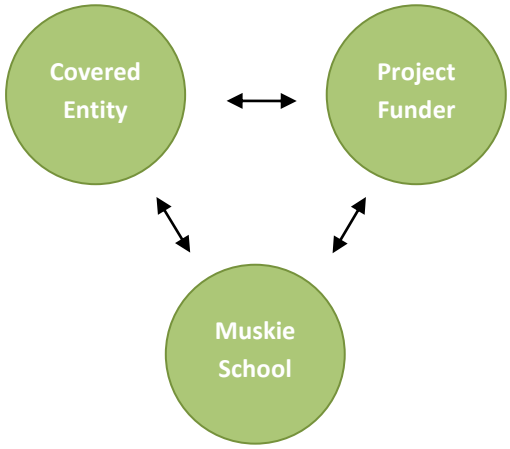
---

[2] See 45 CFR §160.103 for a definition of Business Associate, which lists more of the functions that might be delegated to a Business Associate. You should also refer to the definition of "health care operations" (45 CFR §164.501) for other operational functions that a Covered Entity might delegate.

[3] Answering this question involves an understanding of the relationship between a business associate function and research. See TIPSHEET HUMAN SUBJECTS AND HIPAA.

Spotting a Business Associate Relationship. If the success of your study requires access to directly identifiable PHI, you have an immediate flag that you might be entering into a Business Associate relationship. Knowing for sure will depend on the relationship between the Project Funder, the Covered Entity providing the PHI, and us:

- Is the Project Funder also a Covered Entity?
- Is the Project Funder the Covered Entity providing the PHI or is the Project Funder in a contractual relationship with the Covered Entity providing the PHI?
- Do we have a contractual relationship with a Covered Entity that requires us to conduct the study? Are we accountable to the Covered Entity for producing a report on the study results? Are we creating generalizable knowledge for the benefit of others?[4]



You will need to follow up with UMS Legal Counsel to confirm how HIPAA applies in your situation. You can make that process go a lot more smoothly if you know the answers to these questions before you do so.

Related Tipsheets

- What is Research?
- Human Subjects and HIPAA

Still Have Questions?

If you have questions about this TIPSHEET or need help, please contact Eileen Griffin at eileeng@usm.maine.edu or 780-4813.

[4] See **TIPSHEETS: HUMAN SUBJECTS AND HIPAA** for more on the relationship of research to the question of whether or not you are performing a Business Associate function.

Limited Data Sets and De-Identified Data

LIMITED DATA SET	DE-IDENTIFIED DATA
To be a **Limited Data Set**, these identifiers must be removed for the individual, as well as relatives, employers, and household members: ✦ Names ✦ Postal address information, other than town or city, State and zipcode; ✦ Telephone numbers ✦ Fax numbers ✦ Electronic mail addresses; ✦ Social security numbers; ✦ Medical record numbers; ✦ Health plan beneficiary numbers; ✦ Account numbers; ✦ Certificate/license numbers; ✦ Vehicle identifiers and serial numbers, including license plate numbers; ✦ Device identifiers and serial numbers; ✦ Web Universal Resource Locators (URLs) ✦ Internet Protocol (IP) addresses ✦ Biometric identifiers (e.g., finger and voice prints); ✦ Full face photographic images and any comparable images; and ✦ Any other unique identifying number, characteristic, or code *Note*: A Limited Data Set may include dates, and some geographical information.	To be **de-identified**, these identifiers must be removed for the individual, as well as relatives, employers, and household members: ✦ Names ✦ Geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes. (The first three digits of a zip code may be used within certain guidelines); ✦ Elements of dates (except year) directly related to an individual (including, *e.g.*, birth date, admission date, discharge date, date of death) (can't use year or other indications of age for people over age 89). ✦ Telephone numbers ✦ Fax numbers ✦ Electronic mail addresses; ✦ Social security numbers; ✦ Medical record numbers; ✦ Health plan beneficiary numbers; ✦ Account numbers; ✦ Certificate/license numbers; ✦ Vehicle identifiers and serial numbers, including license plate numbers; ✦ Device identifiers and serial numbers; ✦ Web Universal Resource Locators (URLs) ✦ Internet Protocol (IP) addresses ✦ Biometric identifiers (e.g., finger and voice prints); ✦ Full face photographic images and any comparable images; and ✦ Any other unique identifying number, characteristic, or code

Acquiring and Securing Protected Health Information

Type of Health Information	How It's Acquired[5]	How We Protect It[6]
Fully Identifiable	Individually identifiable PHI triggers all of the HIPAA protections and can only be disclosed pursuant to: ✦ An authorization, ✦ A waiver of authorization from the IRB, ✦ Under a Business Associate Agreement (discussed below), or ✦ One of the limited exceptions to the authorization requirement under HIPAA. (These are not typically applicable.)	For Muskie, this category of PHI triggers our highest standards for security: on a secure server or an iron key only.
Limited Data Set	A Limited Data Set may be acquired through a Data Use Agreement. This option is only available for the purpose of research, public health, or health care operation activities.	Same as above.
De-Identified	De-identified health information is not PHI and can be disclosed without a BAA or DUA.	De-identified health information does not require security. It may be stored in project folders or on the common drive as appropriate.

[5] A TIPSHEET addressing the approval process for acquiring PHI is forthcoming.
[6] When our security requirements are formalized into policies and procedures (before February 2010) this TIPSHEET will direct you to those.