

## Human Subjects & HIPAA

How you are using Protected Health Information (PHI) is important for determining what your obligations are under both HIPAA and federal regulations governing human subjects research protections. Depending on whether you are conducting research, acting as a Business Associate, doing both, or doing neither, the impact of HIPAA is different. This **TIPSHEET** summarizes the way these two sets of laws can interact and builds on two other **TIPSHEETS: HIPAA BASICS** and **WHAT'S 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 University's Institutional Review Board (IRB), through the Office of Research Compliance (ORC), is the only entity authorized to say whether or not your project involves research.

### Types of Studies Involving PHI

The studies we conduct involving PHI might be research, might be a Business Associate function regulated under HIPAA, might involve both, or might involve neither.

**Research.** Human Subjects regulations govern the rights and protections afforded individuals participating in a research study. Human Subjects regulations apply if your study is creating generalizable knowledge and the IRB has determined that it is human subjects research or, although your study is not currently intended to be research, you've asked for an exemption so you can preserve the option of using the data for research at another point in time. See the **TIPSHEET: WHAT'S RESEARCH?** for more information about what kinds of studies are considered research.

The only direct interaction between human subjects regulations and HIPAA regulations is limited to those instances when the research involves PHI. In those cases, the researcher can only access the PHI if the Covered Entity has obtained the individual's authorization to disclose the PHI; the University's Institutional Review Board has granted a waiver of the authorization requirement; or through a Limited Data Set governed by a Data Use Agreement with the Covered Entity providing the data. (See **TIPSHEET: HIPAA BASICS** for more information about Limited Data Sets.) Individual authorization is easier to obtain when the study involves only a small number of people and you have a way of obtaining the authorization (*e.g.*, the Covered Entity can request the authorization in a regular service encounter).

**Business Associate Functions.** When your study is a function conducted on behalf of a Covered Entity or a service provided for a Covered Entity, you are very likely performing a Business Associate function. For example, you are likely to be a Business Associate if you are conducting a focus group or a survey to help a Covered Entity evaluate the effectiveness of a particular service or program. Or, if you are

analyzing data to give a Covered Entity a better understanding of expenditures and utilization, or the clinical characteristics of the people it serves. The actual determination of whether or not you are conducting a Business Associate function will depend on the relationship between the Muskier School, the Covered Entity, and the Project Funder, if different. See the [TIPSHEET: HIPAA BASICS](#) for more information about Business Associates and HIPAA.

If you are acting as a Business Associate you must enter into a Business Associate’s Agreement with the Covered Entity.

*Note:* You are not a Business Associate if you are conducting public health activities under contract to a public health authority or health oversight activities under contract to a health oversight agency (see [Neither Fish Nor Fowl](#) below).

### **Both Research and Business Associate Functions.**

In many cases, we are acting as both a Business Associate and a researcher at the same time. While our study is directly responding to the needs of the Covered Entity, we want to design it so that what we learn can be applied more generally to other programs and population groups (or we at least want to preserve the option by obtaining an exemption from IRB review). In these situations, usually we will have to comply with both Business Associate requirements and human subjects regulations.

HIPAA adds a little wrinkle to this analysis: if the *primary* purpose of our study is to create generalizable knowledge, *i.e.*, conduct research, then your study is treated as research only. This “wrinkle” is unlikely to apply when your study involves a program or services administered by the Covered Entity who is also funding the project. See the [BOX](#) for more on how to sort out the “primary” purpose of your study.

HIPAA also allows a Covered Entity to enter into a Business Associate Agreement with a researcher to develop the Limited Data Set that the researcher will use for research purposes. In these cases the researcher will need a Business Associate Agreement and Data Use Agreement (or a combination of both) to govern these two uses. Now that the Business Associate

#### What’s the “Primary” Purpose of Your Project?

Unfortunately, HIPAA does not provide any guidance on how to decide what the primary purpose of a study is. Because we need to be prepared to defend our decision if it should ever be challenged, the University has to use good faith in making that determination. Bluntly put, this determination is not based on what’s most appealing or most convenient, but on the facts of the particular study you are conducting.

But sorting through the facts doesn’t always give you a cut and dried answer. When we are trying to serve the needs of a Covered Entity as well as our own interests in contributing to a field of knowledge, which is the “primary” purpose?

One way to answer this question is to ask yourself whether, but for the Covered Entity’s interest in evaluating its own program, would the Covered Entity be funding this project as a research project? If we would not have the funding to conduct the research side of the project, but for our commitment to perform the Business Associate function, the primary purpose of the study is the Business Associate function.

In general, where the Covered Entity is also the Project Funder there is a strong presumption that “but for” the Business Associate function, we would not be conducting the study.

relationship brings along so much more risk than it used to, there will need to be a good reason for using this approach, unless we are already operating under a Business Associate Agreement with that Covered Entity.

**Neither Fish Nor Fowl.** In some unusual cases your study might not be research or a Business Associate function, though you are still using PHI. Examples of these include:

- ✦ You have a grant from a foundation to conduct an evaluation of a program. Your relationship is with the foundation, which has been determined to not be a Covered Entity and your report will be presented to a collaborative overseeing the development of the program. At the same time, the IRB has determined your study is for the benefit of the collaborative that is overseeing the development of the program, but is not designed to create generalizable knowledge. If your evaluation involves obtaining PHI from a provider that has been determined to be a Covered Entity, the Covered Entity still needs to obtain authorization to disclose PHI to you. In these cases, the University's counsel will need to review the authorization.
- ✦ You are accessing a Limited Data Set for the purpose of a public health activity.
- ✦ You are under contract with a health oversight agency to conduct health oversight activities (*e.g.*, data collection activities related to provider licensing)
- ✦ You are under contract with a public health authority to conduct public health activities (*e.g.*, data collection activities for public health surveillance).

The grid on page 6 maps out the range of compliance requirements you face when working with PHI, depending on the characteristics of your study: Is it research? Are you performing a Business Associate function?

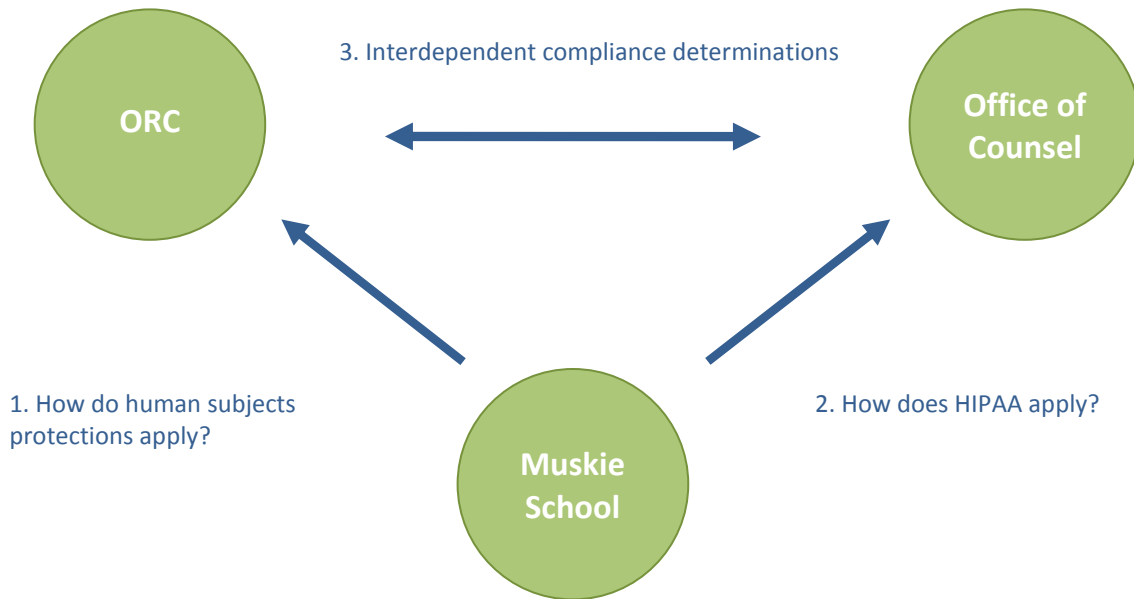
## Design Options

To the degree that you have options in how you design your study, you should consider how these different options impact your compliance requirements. The grid on page 7 is provided as an example of how your choice of strategies for recruiting study participants has different implications for the way HIPAA and HSRP regulations come into play.

## Getting Answers

Well, now that you know the relationship between HIPAA and human subjects regulations is complicated, you're probably wondering how to figure out what you need to do. As explained above, only the University's Institutional Review Board, through the Office of Research Compliance (ORC), can determine whether or how your study has to comply with human subjects regulations. And only the University's attorney can answer whether or how HIPAA applies to your study. In some cases, their answers are interdependent and require communication across three points in a triangle: ORC, UMS Counsel and us.

## The Research Compliance Triangle for Human Subjects and HIPAA



**Accurate and Relevant Information.** The Project Director plays a very important role in this process. It's your job to make sure that the other points in the triangle each have access to all the relevant and accurate information about your project, so that they can make legally sound determinations. That's why, before you start, you should be prepared to answer the following questions:

- ✦ Have you confirmed that a Covered Entity is involved in this study?
- ✦ What is the Covered Entity's role in the study? What is our relationship to the Covered Entity? Who is the Project Funder? Do we have a contract with the Covered Entity that requires us to conduct the study? Are we accountable to the Covered Entity for producing a report on the study results?
- ✦ Will the results of the study be a direct benefit to the Covered Entity? Is the study intended to create generalizable knowledge? See [TIPSHEET: WHAT'S RESEARCH?](#) for more information about "generalizable knowledge."
- ✦ Does the study design require that a Covered Entity share individual health information with us? Does the success of the study require access to direct identifiers or can it be designed to minimize or eliminate the need for identifiable health information? If identifiers are involved, what are they? See [TIPSHEET: HIPAA BASICS](#) for more on PHI and individual identifiers.

**Where to Start.** Once you've done your homework (developed your study design, gathered the relevant HIPAA information, obtained any necessary internal review and approvals), your pathway to all necessary research compliance approvals proceeds this way:

RESEARCH COMPLIANCE ✦ CUTLER INSTITUTE FOR HEALTH AND SOCIAL POLICY ✦ MUSKIE SCHOOL OF PUBLIC SERVICE

**Start with ORC.** The ORC/IRB can make the determination of whether or not the study is research. ORC can also help to spot some of the HIPAA issues that you might have missed. When there are HIPAA issues, before you can obtain IRB approval of a research protocol, or exemption from IRB review, you will be required to consult with UMS Counsel to ensure compliance with HIPAA.

**Consult with UMS Counsel.** UMS Counsel can determine how HIPAA applies to you. Are you acting as a Business Associate? If not, what are the legal means by which you can obtain and use PHI? (A **TIPSHEET** describing the approval process for these different mechanisms for obtaining PHI will be developed.)

**Keep ORC in the Loop.** If your IRB approval is conditioned on approval from UMS Counsel, make sure that ORC is copied on key correspondence documenting UMS Counsel (and CIO, where relevant) determinations.

## Related Tipsheets

- ✦ What is Research?
- ✦ HIPAA Basics

## Still Have Questions?

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

## The Range of Possibilities: Compliance with HIPAA & Human Subjects

The Key Questions		Are you Performing a Business Associate Function?	
		YES	NO
Is it Research?	YES	<p>You will need to obtain a Business Associate Agreement for the Business Associate function.</p> <p>You will need IRB approval of your research protocol. Obtaining PHI will involve:</p> <ul style="list-style-type: none"> <li>✦ Obtaining individual authorization from your study participants;</li> <li>✦ A waiver of the authorization requirement from the IRB; or</li> <li>✦ Obtaining a Data Use Agreement for accessing a Limited Data Set</li> </ul>	<p>You will need IRB approval of your research protocol. Obtaining PHI will involve:</p> <ul style="list-style-type: none"> <li>✦ Obtaining individual authorization from your study participants;</li> <li>✦ A waiver of the authorization requirement from the IRB; or</li> <li>✦ Obtaining a Data Use Agreement for accessing a Limited Data Set</li> </ul>
	NO	<p>You need to obtain a Business Associate's Agreement.</p>	<p>If you are using PHI, obtaining the PHI will involve:</p> <ul style="list-style-type: none"> <li>✦ Obtaining individual authorization from your study participants;</li> <li>✦ Obtaining a Data Use Agreement for accessing a Limited Data Set ; (Here, this option is only available for the purpose of conducting public health activities.)</li> <li>✦ Complying with HIPAA requirements for conducting public health activities; or</li> <li>✦ Complying with HIPAA requirements for conducting health oversight activities</li> </ul>

# Recruitment Strategies and HIPAA

Recruitment Strategies	How to Comply with HIPAA When Your Project Is...			
	RESEARCH ONLY	BA FUNCTION ONLY	RESEARCH & BA FUNCTION	NOT RESEARCH OR BA FUNCTION
A Covered Entity invites clients to participate in your study, compiles the names of those who are willing to participate, and shares those names with you.	You need a waiver of the authorization requirement from the IRB or the Covered Entity must obtain authorization from the study participants before their names or any other PHI can be disclosed to you.	You must obtain a Business Associate's Agreement to govern the Business Associate function.	You need a waiver of the authorization requirement from the IRB or the Covered Entity must obtain authorization from the study participants before their names or any other PHI can be disclosed to you.  You must obtain a Business Associate's Agreement to govern the Business Associate function.	The Covered Entity must obtain authorization from the study participants before their names or any other PHI can be disclosed to you.
A Covered Entity shares its client list with you so you can develop a sample for conducting a survey.	You need a waiver of the authorization requirement from the IRB or the Covered Entity must obtain authorization from the study participants before their names or any other PHI can be disclosed to you. In this situation it's probably not practical for the Covered Entity to obtain individual authorization from each of the study participants sharing their	You must obtain a Business Associate's Agreement to govern the Business Associate function.	You need a waiver of the authorization requirement from the IRB or the Covered Entity must obtain authorization from the study participants before their names or any other PHI can be disclosed to you. In this situation it's probably not practical for the Covered Entity to obtain individual authorization from each of the study participants sharing their	The Covered Entity must obtain individual authorization from the study participants before their names or any other PHI can be disclosed to you.

	PHI. If that's the case, waiver of the authorization requirement from the IRB is your best option.		PHI. If that's the case, waiver of the authorization requirement from the IRB is your best option.  You must obtain a Business Associate's Agreement to govern the Business Associate function.	
A Covered Entity invites clients to participate in your study, tells them how to get in touch with you and you compile the names of willing participants.	In this case, the Covered Entity is not sharing information with you, the individual is. HIPAA does not come into play and you do not need an authorization, a waiver of authorization, or a BAA.	You must obtain a Business Associate's Agreement to govern the Business Associate function. (Even though you are not obtaining PHI in order to recruit participants, you will, in the course of conducting the study, be creating PHI on behalf of the Covered Entity. The BAA will cover the PHI you create.)	You must obtain a Business Associate's Agreement to govern the Business Associate function. (Even though you are not obtaining PHI in order to recruit participants, you will, in the course of conducting the study, be creating PHI on behalf of the Covered Entity. The BAA will cover the PHI you create.)	In this case, the Covered Entity is not sharing information with you, the individual is. HIPAA does not come into play and you do not need an authorization, a waiver of authorization, or a BAA.



