Research and HIPAA Privacy Protections

Content Author

- **Reid Cushman, PhD**
  CITI Program

This module is for educational purposes only. It is not designed to provide legal advice or legal guidance. You should consult with your organization's attorneys if you have questions or concerns about the relevant laws and regulations discussed in this module.

Introduction

This module discusses data protection requirements for human subjects research that creates, obtains, uses, or discloses health data, principally the protections that derive from the Health Insurance Portability and Accountability Act (HIPAA).

Though HIPAA is the most prominent source, protections for individuals' health information are required by many federal laws and regulations. Additionally, most (if not all) U.S. states also have their own requirements; so do private accreditation organizations, such as the Joint Commission (The Joint Commission used to be JCAHO) If you have access to any individually identifiable health information for any purpose, it is required that you understand these constraints. If you use such health information for human subjects research, you need to know the specific limitations that apply to that activity, deriving from HIPAA and other regulations like 45 CFR 46, Subpart A (also known as the Common Rule).

HIPAA's relatively new data-focused protections, which took effect starting in 2003, work together with the Common Rule and FDA protections; they are not a replacement. Institutional Review Board (IRB) protocol reviews using Common Rule and FDA criteria remain as before, including aspects related to data protection. As will be discussed, IRBs may share responsibilities for addressing some of HIPAA's additional requirements in their reviews when those apply; or some responsibilities may be allocated to another kind of body that HIPAA permits (a **Privacy Board**) or to an institutional official that HIPAA requires (a **privacy officer**). These federal rules and regulations provide a minimum standard of practice, complemented by states' and accreditation bodies' additional requirements.

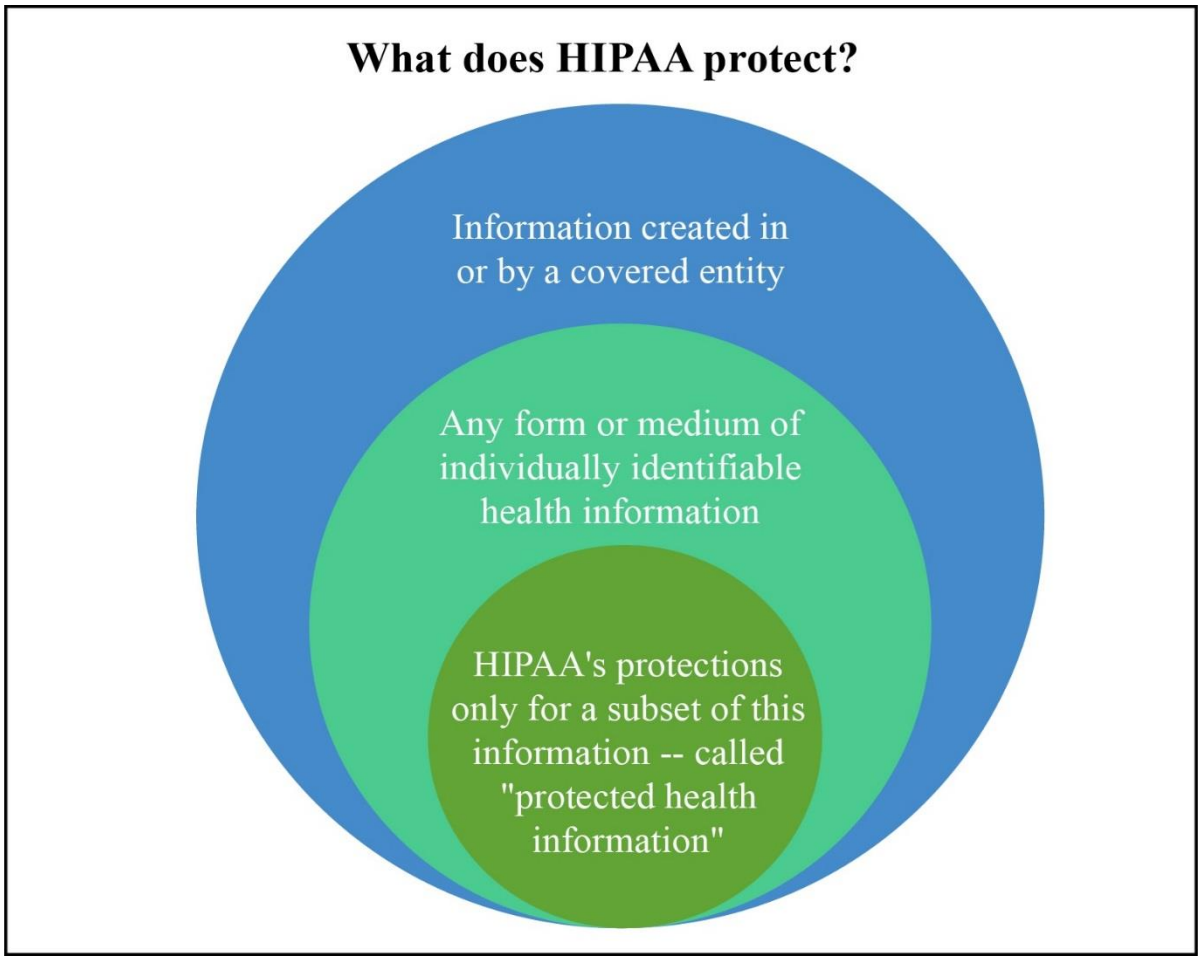
Learning Objectives

By the end of this module, you should be able to:

- Summarize HIPAA's additional privacy protections for individually identifiable health data that are used for human subjects research, including authorizations and accountings of disclosures.

- Describe situations where full HIPAA privacy protections are required, and those which can qualify for waivers, alterations, or exemptions with more limited requirements.
- Explain the responsibilities of researchers and organizations for meeting these privacy requirements, and for appropriate data security protections that are necessary to protect privacy.

HIPAA's Regulatory Scope



HIPAA's protections focus on "individually identifiable health information," which HIPAA defines as information in "any form or medium" that "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of health care to an individual" (Security and Privacy 2013).

HIPAA's protections reach only a subset of individually identifiable health information -- formally called **protected health information** or simply "PHI" -- created in or by what HIPAA calls covered entities. **Covered entities** include individual healthcare providers, healthcare provider organizations, health plans, and health information clearinghouses that engage in

electronic healthcare transactions (see Health and Human Services Covered Entity Decision Charts). HIPAA's protections for PHI extend to non-U.S. citizens' data as well.

Some identifiable health information used for research originates outside of covered entities, and so may not be covered by HIPAA. However, you must check with your organization's privacy authorities before assuming your situation falls outside HIPAA's scope.

What Kinds of Users and Uses Are Covered?

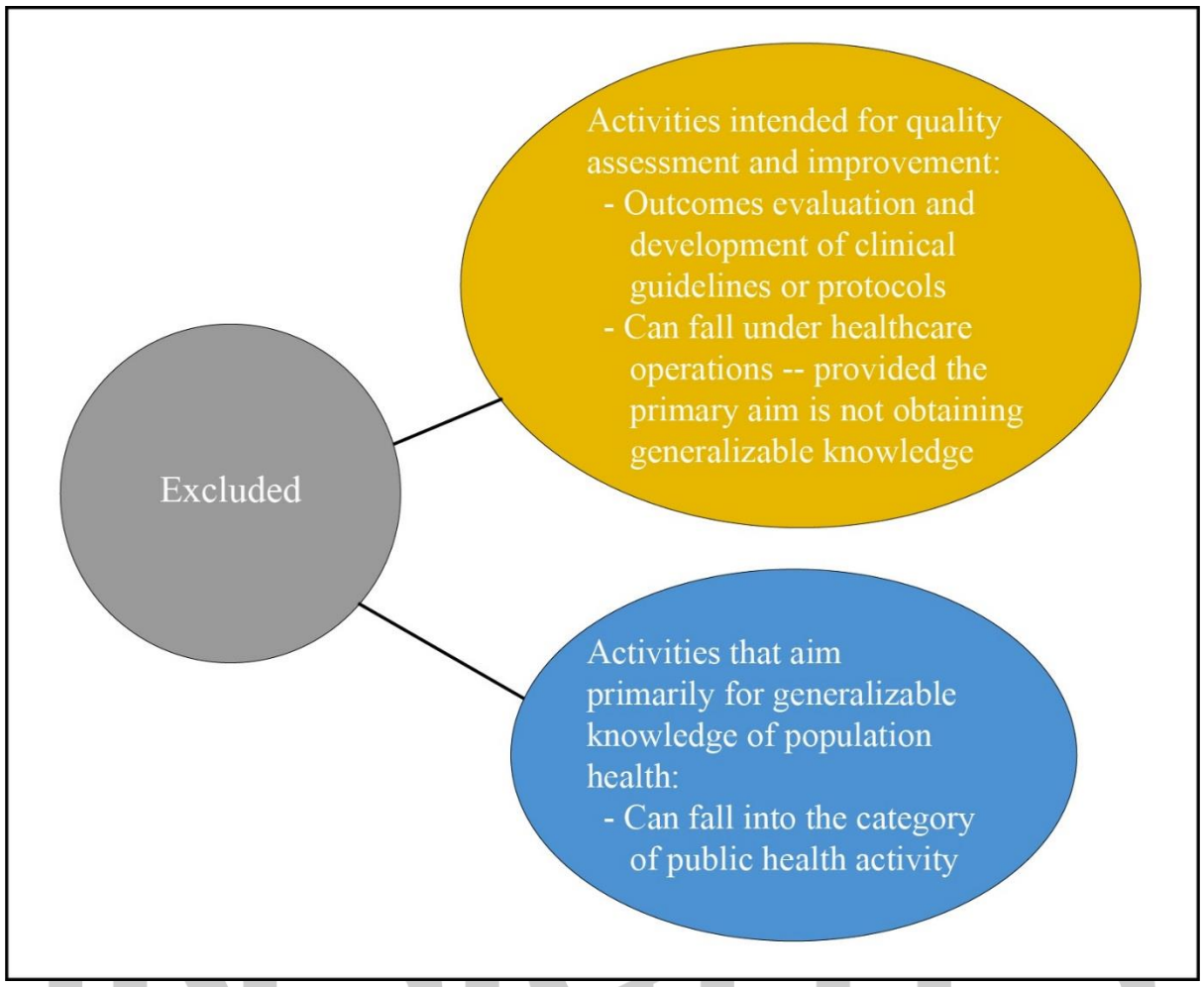
HIPAA regulations set requirements for use and disclosure of PHI by covered entities, and by extension on all members of a covered entity's **workforce** that have contact with PHI. HIPAA's data protection requirements also apply "in the same manner" to **business associates** (and by extension to the workforce of such business associates) that perform functions using PHI on a covered entity's behalf.

Researchers may be part of the workforce of a covered entity, or may be covered entities themselves if they are also healthcare providers. If so, they are directly affected by the HIPAA's research rules. Researchers who meet neither of these conditions are still indirectly affected by HIPAA rules if a covered entity is the source of their data and those data meet the definition of PHI.

HIPAA's rules on use and disclosure are generally "**purpose-based**" -- that is, the intended use sets the rules more than the type of data itself. The research rules discussed here are different than those for, say, treatment or treatment-related payments (relatively liberal), or for marketing or fundraising (relatively strict). A few types of data, such as psychotherapy notes do receive special protection under HIPAA. State laws also often have many categories of data with special protections, with which you should be familiar (or be in contact with an organizational official who has that knowledge).

What Constitutes "Research"?

Like the Common Rule, HIPAA defines research as a "systematic investigation, including research development, testing, and evaluation, designed to develop and contribute to generalizable knowledge" (Protection of Human Subjects 2009; Security and Privacy 2013). Note that some kinds of investigative activities that use patient data are excluded in this definition. For example:



The regulations are complex. So, as with the covered entity status, a determination by an organization's IRB, designated privacy official(s), or legal counsel is usually required to assure that an activity is "not research" and therefore subject to different HIPAA rules.

Who Enforces the HIPAA Research Protections?

A covered entity may choose to rely on an IRB to assess compliance with both the FDA and Common Rule requirements and HIPAA research requirements. Alternatively, HIPAA provides that covered entities may create a Privacy Board to handle some research-related issues, notably determinations about eligibility for waivers, alterations, and exemptions from authorization processes. A covered entity may also leave some decisions about compliance with the research provisions of HIPAA to its designated privacy officer. It is critical that you understand the allocation of responsibilities at your organization.

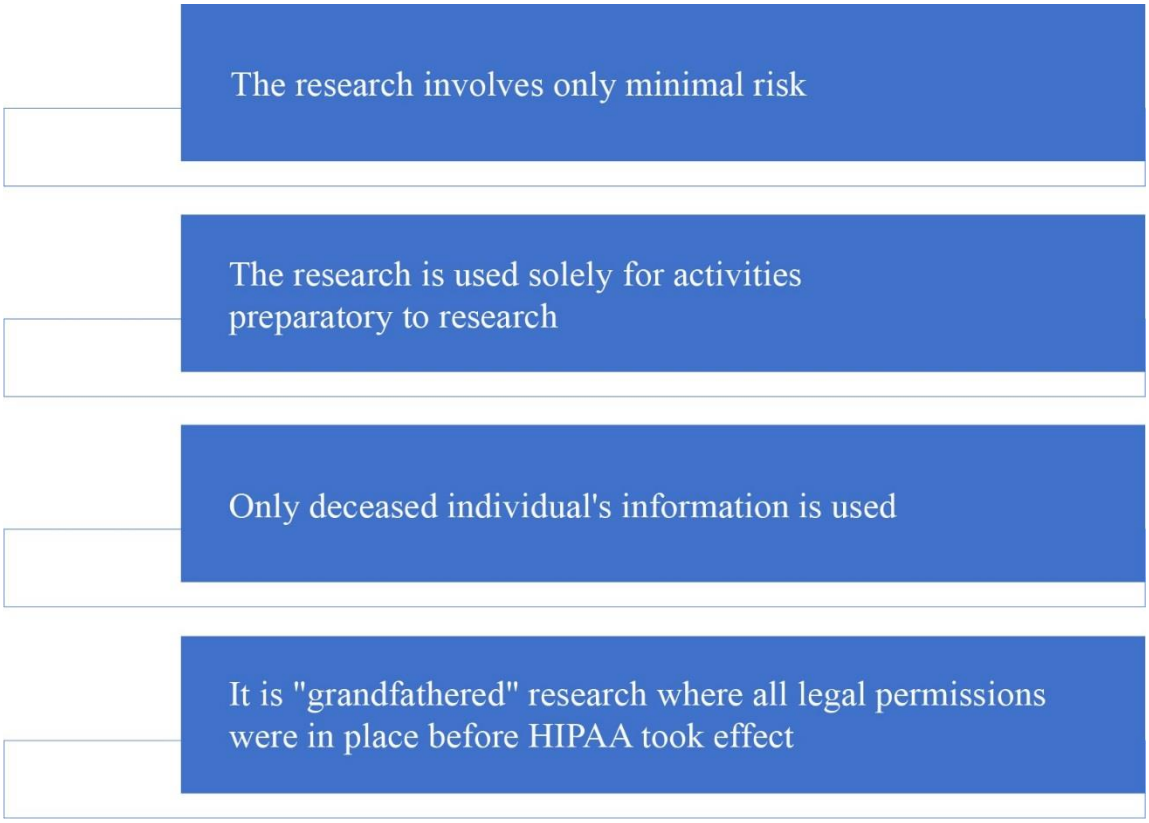
Research subjects, like patients generally, have recourse to both your organization's authorities and to federal and state agencies in the event they wish to file complaints about or have questions regarding an organization's protective efforts.

As with any other planned activity related to protected health information, research must be mentioned in a **privacy notice** that HIPAA requires be provided by covered entities to their patients/customers. The privacy notice must include the ways in which data subjects may register complaints and report problems, either locally or with federal authorities. Every researcher should be familiar with their organization's privacy notice, particularly the persons or departments it identifies as enforcement authorities for the organization.

HIPAA Research-Related Rules

If the data in question meet the definition of PHI and are being used for purposes that fall within HIPAA's definition of research, HIPAA generally requires explicit written **authorization** (consent) from the data subject for research uses.

However, HIPAA allows for research-related access to individuals' identifiable health data without authorization under certain circumstances:



Data that do not identify individuals can be used for research without specific authorization if:

1. Only fully de-identified data are used.
2. A "limited data set" is used, under an approved "data use agreement."

Each of these conditions is described in the sections below.

Waivers of Alterations of Authorization Requirement Due to Minimal Risk

An organization's IRB or Privacy Board (and in some organizations a designated privacy official) may determine that a waiver or alteration of the authorization requirement is appropriate. The conditions are modeled on the criteria for a waiver of informed consent in the Common Rule.

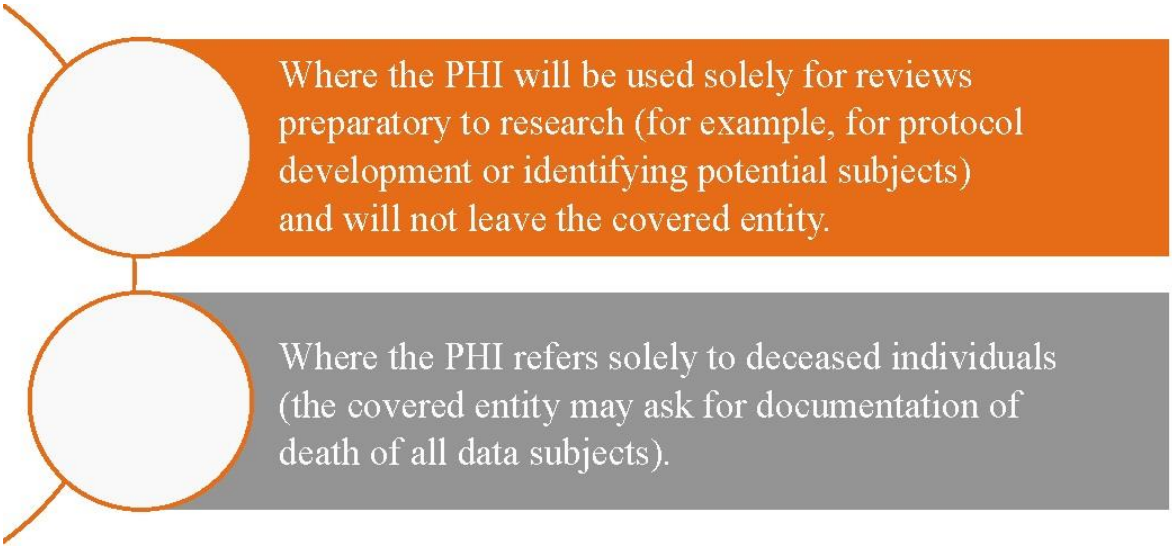
Use or disclosure of the PHI must involve no more than minimal risk to the privacy of the research subjects, and include the following elements:

- An adequate plan to protect any data identifiers from improper use and disclosure.
- An adequate plan to destroy data identifiers at the earliest opportunity consistent with conduct of the research (unless there is a health or research justification for retaining the identifiers, or such retention is otherwise required by law).
- Adequate written assurances that the PHI will not be reused or disclosed to any other individual or entity, except as required by law for authorized oversight of the research project, or for other research for which the use or disclosure of PHI would be permitted by HIPAA.
- The research could not practicably be conducted without access to and use of the PHI.
- The research could not practicably be conducted without the waiver or alteration to the authorization.

More about what counts as a **data identifier** is provided in the sections below on de-identified data and limited data sets.

Activities Preparatory to Research; Decedents' Information Exceptions

HIPAA provides for two more exceptions to the authorization requirement for identifiable data:



In each case, the researcher must make a written or oral representation to the covered entity's designated officials that such access is necessary for the research purposes -- someone from the IRB, the Privacy Board, or a privacy officer / designee -- who would then determine the appropriateness of the request.

Grandfathered Research

If all informed consents and other legal permissions required at the time were in place before HIPAA took effect (April 2003 in most cases), and have not changed since, a new HIPAA authorization is not required even for identified data. Obviously, this is no longer a commonly used pathway to bypass authorizations.

De-identified Data

A researcher may use fully **de-identified** health data without any authorization from individual data subjects.

> As the name implies, de-identified information must have all direct and indirect identifiers removed, to eliminate (or at least make highly improbable) re-identification using statistical techniques.

De-identified information is no longer considered PHI, because by definition it is no longer individually identifiable.

HHS issued its *Guidance Regarding Methods for De-identification of Protected Health Information* in 2012. This guidance provides a detailed description of alternative methods, and should be considered required reading for anyone contemplating a de-identification strategy.

Under the HIPAA regulations, successful de-identification may be based on an "Expert Determination" by an "individual with appropriate knowledge" of statistical techniques who has analyzed the data set and can attest that the risk of re-identification is "very small." (Very small is not defined in the regulations.) Alternatively, covered entities may use the "Safe Harbor" method of removing 18 types of identifying elements specified in the HIPAA regulations. In either case, the covered entity must have no actual knowledge that re-identification is possible or likely, for example by linking to other known data sets.

Limited Data Sets and Data Use Agreements

De-identification trades privacy protection for research productivity. Sometimes the trade-off is too steep, and a fully de-identified data set will not meet a research need. As an alternative, a covered entity may disclose PHI in a **limited data set (LDS)** to a researcher who has entered into an appropriate **data use agreement**.

> A LDS must have all direct identifiers removed; however, it may still include information that could "indirectly" identify the subject using statistical methods.

That is, the disclosure risk is greater than "very small."

The data use agreement for an LDS must:

- Delineate the permitted uses and disclosures of such information by the recipient, consistent with the purposes of research;
- Limit the individuals that can use or receive the data; and
- Require the recipient to agree not to re-identify the data or contact the individuals.

Minimum Necessary Uses and Disclosures

Uses and disclosures of data for research that are allowed to bypass the authorization requirement are still subject to the **minimum necessary standard** -- that is, the uses/disclosures must be no more than the minimum required for the described research purpose. A covered entity may rely on a researcher's documentation -- or the assessment of an IRB or Privacy Board -- that the information requested is the minimum necessary for the research purpose.

By contrast, research information obtained using an authorization is not bound by the minimum necessary standard -- on the theory that the data subject has given explicit permission in accordance with the signed authorization. However, be aware that while HIPAA may not require a minimum necessary justification at all times, an IRB's evaluation of risks and burdens on human research subjects arguably does.

Disclosure Accounting

Individuals whose health information is covered by HIPAA have the right to an "accounting of disclosures" of their PHI. In this context, a "disclosure" occurs when PHI is communicated to an outside individual or entity, including another covered entity. Access within the covered entity -- for example, by members of a research team who are all part of the same organization's workforce -- is considered a "use" not a disclosure. There is no accounting requirement for these internal uses for research.

In addition to being limited to external disclosures, disclosure accounting is not required for:

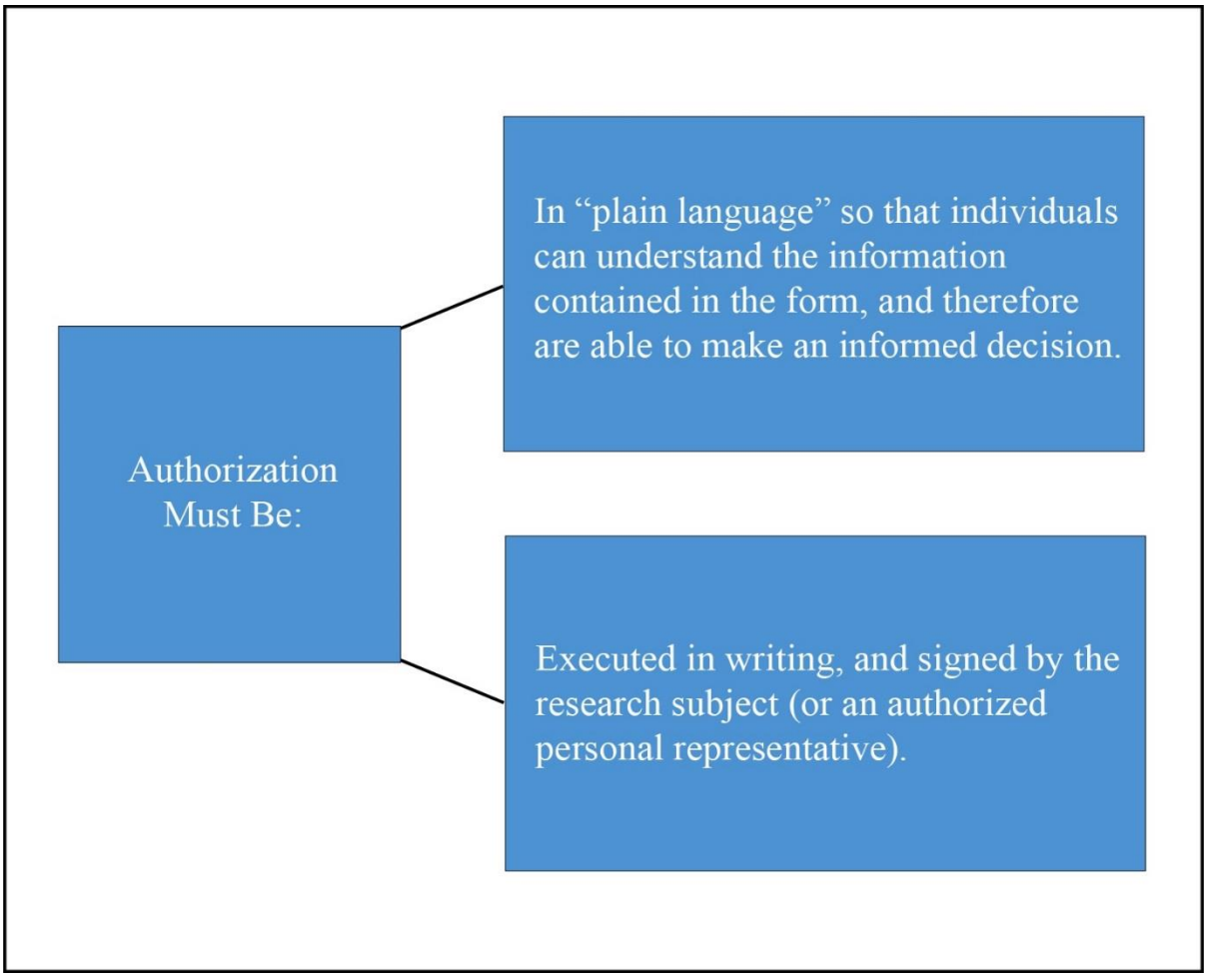
- Disclosures made under authority of a consent/authorization, on the theory that individuals are aware of what they have expressly permitted for that research.
- Disclosures to the individual directly about him/herself.
- Limited data set disclosures subject to a data use agreement.
- De-identified information that no longer qualifies as PHI.

When an accounting is required, it must include disclosures during the six years prior to the data subject's request, and include certain types of information depending on the size of the protocol.

While HIPAA may not require it, many organizations will require that researchers maintain logs of all disclosures from research data collections as a security measure, including transfers to other individuals within the covered entity. Electronic data storage will increasingly offer this capability cheaply and automatically; older collections will require manual logging.

Characteristics of Authorizations

If a research activity meets none of the bypassing criteria above, an authorization (consent) is required. When they are required:



Authorizations must include a specific description of the PHI to be used or disclosed, the name(s) or other identification of individuals involved in the research, and description of each purpose of the requested use or disclosure.

HIPAA authorizations are normally required to have an explicit expiration date. In the context of research, it is sufficient to specify an expiration "event" -- such as "the end of the study." A research authorization can also have no expiration date at all, as would be the case for a research database or repository, or other future use, though this absence must be clearly indicated.

HIPAA authorizations cannot normally be combined with other types of documents (such as a privacy notice). However, HIPAA research authorizations can be combined with any other legal permission related to the study, including an informed consent that meets Common Rule or FDA regulations or another type of authorization.

As with any informed consent document, researchers are strongly urged to rely on standard models rather than creating their own authorization forms, lest they make a critical error in format or content. Most organizations will already have standard documents available; check with your IRB, Privacy Board, or privacy officer.

If there are multiple documents that limit information use or disclosure, the most restrictive one applies. Whether in a single instrument or several, the core requirement is to provide enough information for the data subject to make an informed choice.

Revocations of Authorizations

Like other kinds of HIPAA authorizations, those for research may be revoked by the subject at any time, provided that the revocation is in writing. Revocation of an authorization is not valid to the extent that the covered entity has taken actions relying on it, such as in the provision of prior treatment. Such revocations may be limited "as necessary to maintain the integrity of the research study."

Recruiting into Research

It is still permissible under HIPAA to discuss recruitment into research with patients for whom such involvement might be appropriate. This common practice is considered to fall within the definition of treatment, at least when the conversation is undertaken by one of the patient's healthcare providers.

Remember, however, that a data subject's information cannot generally be disclosed to a third party -- even another care provider -- for a research use without an authorization from the individual or an approved waiver, alteration, or exception to authorization.

HHS guidance on HIPAA has affirmed that recruitment efforts can qualify as a "preparatory to research" activity that would allow a researcher to identify potential research participants, and even contact them for purposes of seeking their authorization (HHS 2004). However, such

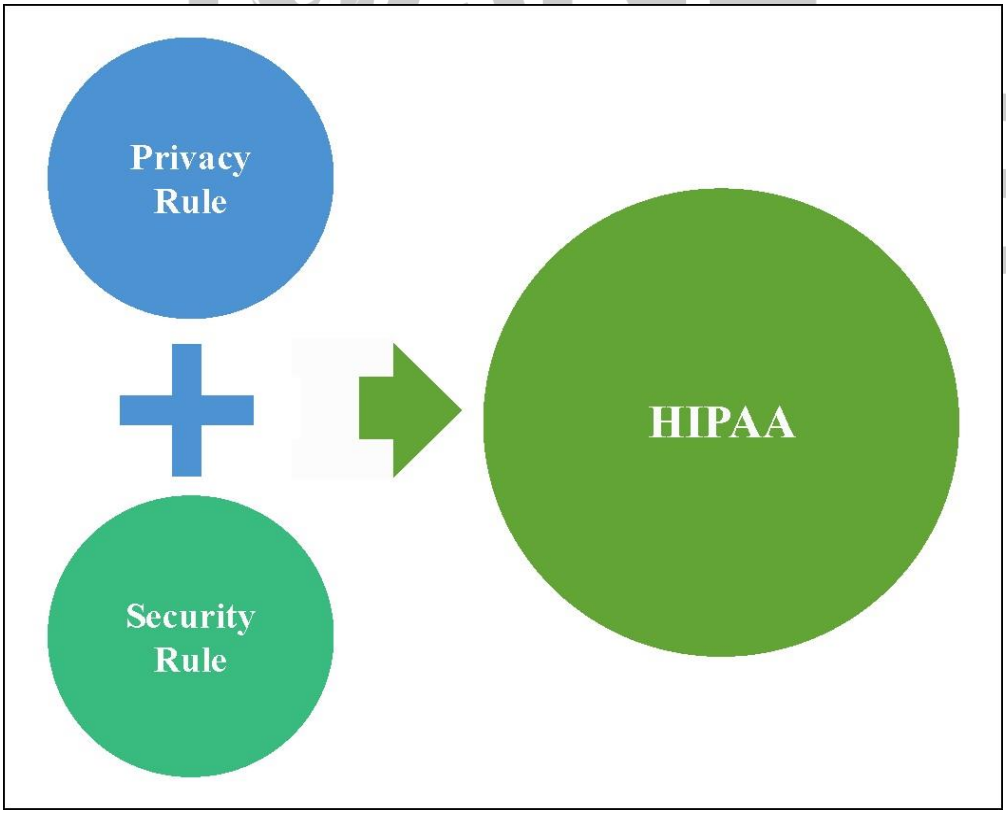
efforts must be approved, and the PHI used for this purpose cannot leave the covered entity during this activity.

"Retrospective" Research

As electronic health data collections grow in scale and scope it is an increasingly common practice to "browse" them, looking for interesting patterns that could translate into research possibilities. Indeed, bio-repositories of tissue and data created just for this purpose are increasingly common, and the scope and scale of such repositories grow daily. (Retrospective analysis of paper charts hasn't gone away either.)

Use or disclosure of PHI for retrospective research studies may be done only with patient authorization -- or with a waiver, alteration, or exception determination from an IRB or Privacy Board. It should not be difficult to meet one of the criteria for the latter for such exploratory efforts. Alternatively, the data collection itself may have been created with an explicit authorization from subjects for future research. However, remember that you generally cannot proceed on your own without some approval from an IRB, Privacy Board, or other designated governing entity.

Security Rule



Research and HIPAA Privacy Protections

Efforts to meet the Common Rule, FDA, and HIPAA regulations' privacy requirements are only part of the researcher's task. HIPAA also has a **Security Rule** that complements its Privacy Rule. The Security Rule requires that PHI collections receive appropriate information security protections for as long as they exist. If you do not know how to do that, find a resource at your organization that does. In addition to a privacy officer, HIPAA requires designation of a **security official**, who should be able to help assure appropriate data protection.

It is important to note that HIPAA's requirements include reporting of security breaches and data exposures. In addition to notifying affected individuals, HHS must be notified of exposures of PHI; in addition to potentially triggering an investigation, exposures involving more than 500 persons are posted on the HHS "Breach Portal" website for all the world to see. State laws may also include breach-reporting requirements.

Case Study

BIO HIPAA

Dr. McMahon is an oncologist at Central Suffolk Hospital who is interested in conducting a research study that attempts to correlate patient smoking history with development and treatment of different types of pancreatic cancer. She proposes to have patients who are being admitted to the hospital for treatment of their pancreatic cancer complete a detailed questionnaire regarding their smoking habits. She would access their medical records over five years for information concerning cancer type, treatment, and survival.

- Does the activity Dr. McMahon proposed to conduct invoke HIPAA research requirements?

  Yes. Dr. McMahon will be accessing and generating individually identifiable health information for research purposes.

- If yes, how can Dr. McMahon satisfy HIPAA requirements in order to conduct this study?

  Accessing a patient's individually identifiable health information from the medical chart and utilizing the detailed questionnaire for reasons other than treatment, payment, or operations requires consideration of HIPAA research provisions. In this instance, the prospective and longitudinal (for example, following the subjects over time) nature of the study would require a signed

HIPAA authorization from the subject to use their health information in this way.

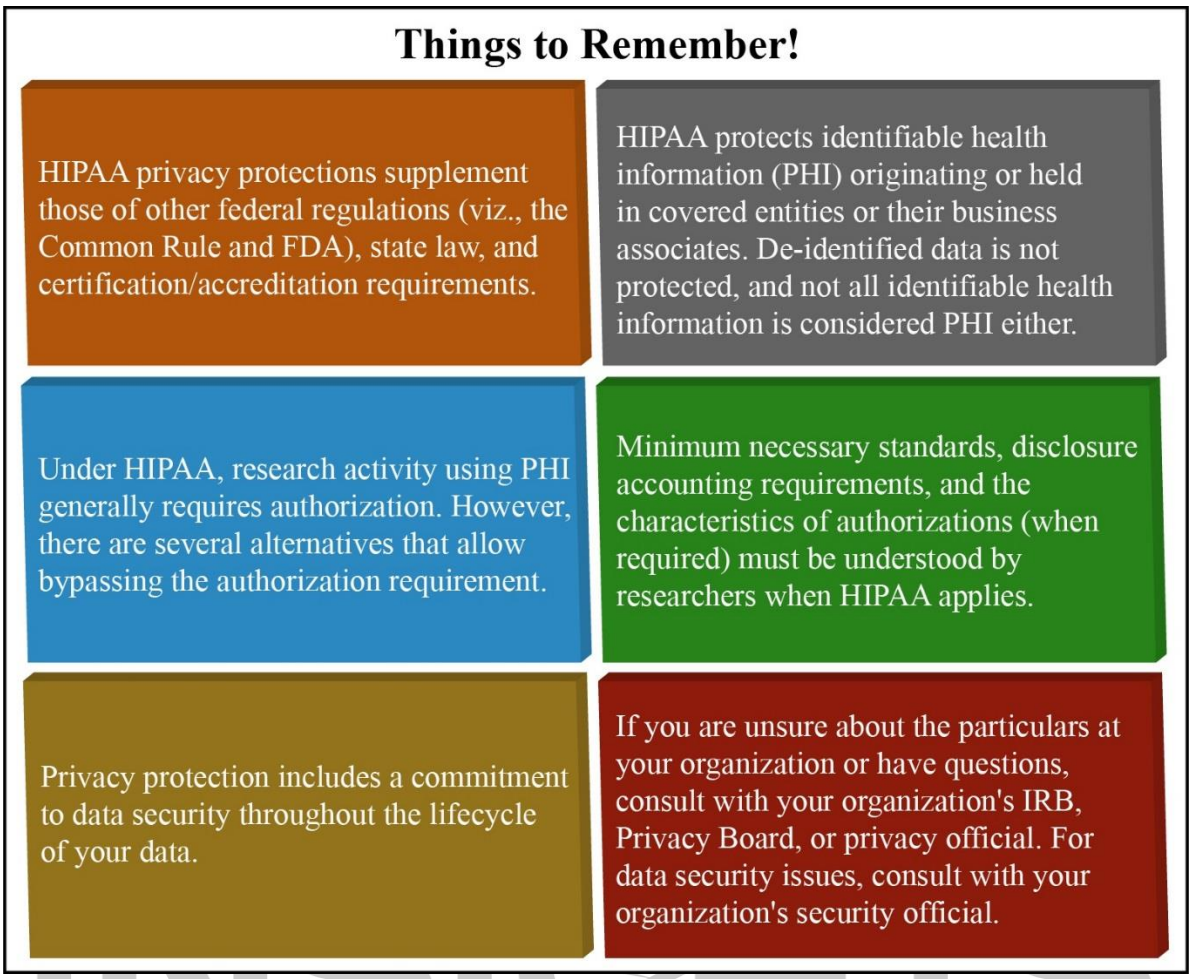
IRB approval, including informed consent from subjects, would be required because this activity qualifies as research. The study results would be generalizable to pancreatic cancer patients beyond those who are being studied at Central Suffolk Hospital.

Summary

Although the specifics are lengthy, the net administrative burden that HIPAA adds to existing Common Rule and FDA regulations is generally not a large one. Compared to protocol approval generally -- and the details of informed consent particularly -- a HIPAA authorization is relatively easy. Additionally, as noted, there are several pathways around the authorization requirement.

To approve a study under the Common Rule and FDA requirements, IRBs have long been required to determine that there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data. Where researchers are meeting those requirements, HIPAA should change very little beyond the additional "paperwork."

As noted, HIPAA applies to covered entities and their business associates, and to the PHI that originates in or by them. Research conducted by organizations that do not qualify as such, using data that does not derive from any covered entity source, is not reached by HIPAA. In such cases, the requirements of the Common Rule and FDA remain as protections for human subjects' privacy and other interests. The issue then is not "PHI" but what the Common Rule defines as identifiable "private information."



Acknowledgements

The author would like to thank the following individuals for their editorial and content review of this and prior versions: Jaime Arango, Evelyne Bital, Helenemarie Blake, Joey Casanova, Anita Cava, Amanda Coltes-Rojas, Ken Goodman, Karen Hansen, Margaret Rankovic, Daniel Smith, and Sally Mann.

References

- Protection of Human Subjects, 45 CFR § 46 (2009).
- Security and Privacy, 45 CFR § 160, 162, and 164 (2013).
- U.S. Department of Health and Human Services (HHS). 2004. "Clinical Research and the HIPAA Privacy Rule." Last modified February 5.
- U.S. Department of Health and Human Services (HHS). 2013. "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule." *Federal Register* 78(17):5566-702.

Additional Resources

- U.S. Department of Health and Human Services (HHS). 2012. "Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule." Accessed April 14, 2016.
- U.S. Department of Health and Human Services (HHS). 2013a. "Combined Regulation Text of All Rules." Accessed April 14, 2016.
- U.S. Department of Health and Human Services (HHS). 2013b. "Research." Accessed April 14, 2016.
- U.S. Department of Health and Human Services (HHS). 2016. "HIPAA for Professionals" Accessed April 14.

Original Release: July 2006
Last Updated: November 2017