Table of Contents

What is meant by "use" and "disclosure" in reference to PHI?

"Use" – refers to PHI that is used ***within*** an institution or covered entity such as Yale.
"Disclosure"- refers to PHI that is disclosed to others ***outside*** an institution or covered entity.

HIPAA allows the covered entity certain uses and disclosures of PHI, primarily those related to treatment and payment. Other uses or disclosures are limited to a defined list of activities or with a patient's authorization. Patients are notified of these uses at the time of treatment through Yale's Notice of Privacy Practices (NOPP, see HIPAA Policy and Procedure 5001). For example, we can disclose PHI to insurers in the course of billing for clinical services without obtaining a signed authorization for each billing.

Note that disclosures can occur both by sharing information with individuals who are not affiliated with Yale as well as sharing with individuals who are affiliated with Yale but are not within the covered entity. For example, YSM sharing PHI with the Anthropology Department would constitute a disclosure.

What research activities are subject to the HIPAA Privacy Rule?

Research activities that take place within the Yale covered entity and which involve PHI are subject to the HIPAA Privacy Rule. This includes not only studies where data is collected from research subjects on site but also studies where PHI is collected elsewhere and stored and/or analyzed within the Yale covered entity.

What HIPAA privacy requirements relate to research?

HIPAA does not create explicit requirements for research per se. Instead, HIPAA limits how identified health information can be accessed, used, and disclosed. The HIPAA privacy requirements do not replace or eliminate the requirements of the federal Common Rule (e.g. IRB approval of human subject research) but rather add certain new requirements such as:

- The use or disclosure of PHI for research purposes requires a signed Research Authorization Form from the research subject unless an exception under HIPAA applies.
- Unlike the Common Rule, HIPAA also applies to research on decedents or studies determined to be exempt from IRB review.
- HIPAA requires that only the "minimum necessary" PHI be used.

What is meant by the "minimum necessary" standard in research?

HIPAA requires that only the minimum necessary PHI needed to accomplish the research initiative and the intended purpose of the use and/or disclosure of the PHI be accessed. Information which is not directly related to the research and which is not indicated in the IRB approved protocol should not be accessed or collected.

Do all types of research fall under the HIPAA Privacy Rule?

The types of research that do not fall under the HIPAA Privacy Rule are:

- Research that does not involve health information
- Research using de-identified data, i.e., data that contains none of the 18 HIPAA identifiers.
- Research conducted by an individual who is not part of a HIPAA covered entity and that does not require access to information held by a HIPAA covered entity.

What is the difference between De-identified data and anonymous data?

"De-identified" is a term used in the HIPAA Privacy Rule and is defined as information that does not identify an individual and with respect to which there is no reasonable basis to believe that

the information can be used to identify an individual. The Privacy Rule then defines 18 identifiers which must be removed from a data set for that data set to be deemed "de-identified." When all 18 identifiers are removed, the data is no longer identifiable and thus no longer PHI which means that HIPAA no longer applies.

"Anonymous" is not defined in either the Privacy Rule or Common Rule but has been used by IRBs to refer to data which does not meet the Common Rule standard of individually identifiable private information. The Common Rule does not define what constitutes an identifier; rather it defines individually identified private information as that for which the identity of the subject is or may readily be ascertained by the investigator or associated with the information.

Because the Privacy Rule is more prescriptive of what constitutes an identifier than the Common Rule, it is possible to have data which would be considered "anonymous" by an IRB but not meet the HIPAA standards for de-identification. In such cases, the Common Rule may not apply or the study qualifies for exemption but HIPAA would still be applicable. For example, a data set which included dates of service for a large sample size is identified under HIPAA but may be deemed anonymous under the Common Rule.

Can de-identified data or anonymous data also be coded?

HIPAA allows disclosure of de-identified data that is coded as long as the code is not derived from identifiers and the code is not disclosed with the data. Researcher A or Hospital A can therefore create a coded de-identified data set for use by Researcher B as long as the code isn't also shared. Researcher B's work with the data is not covered by HIPAA as Researcher B does not have PHI. Researcher A has both the data and the code and hence is subject to the HIPAA requirements.

Similarly, the Common Rule does not pertain to research that does not involve human subjects, e.g. does not involve intervention or interaction or which does not involve identifiable private information. Data can be coded and not be considered to involve human subjects as long as the code is not provided to the researcher and the code itself does not identify the individuals. In the example above, when data is provided to Researcher B with a code and Researcher B agrees in writing to not obtain the code, then the coded data is not covered by the Common Rule. Similarly, if the data owner has policies and procedures which prohibit release of the code, then the data can also be deemed to not involve human subjects and hence not subject to the Common Rule requirements. Determinations regarding whether or not a study involves human subjects as defined under the regulations should be done in consultation with the IRB.

Under the HIPAA Privacy Rule is a research authorization needed?

As a general rule, in order to use PHI in research it is necessary to obtain a signed authorization form from each research subject prior to creating, using or disclosing PHI. The requirement for a HIPAA authorization is in addition to the requirements for informed consent, although in some cases the two can be combined (see below). Yale has developed a Research Authorization Form

(RAF) and compound authorization template which include the specific elements mandated by the HIPAA Privacy Rule.

See: HIPAA Policy and Form 5032.

Does a new RAF need to be submitted each year with the protocol renewal application?

No. Unless there is a change to the project which necessitates a change in the RAF, such as when a new collaborating institution is to be provided access to the PHI, the RAF does not have to be submitted for continuing review by the IRB.

Must the Yale University RAF/Compound Authorization template always be used?

The Yale University Research Authorization Form (RAF) and the Compound Authorization Template provide standard language for the required HIPAA Privacy Rule research authorization. PIs using either of these forms need only specify to whom and where PHI will be sent and what type of PHI will be disclosed. Authorization forms not based on the Yale template or that modify or remove language from the template are subject to review by the Privacy Office and IRB to ensure that they are valid under HIPAA's requirements.

What if the PI needs to disclose PHI to a person or organization not listed in the original signed RAF?

Permissible uses and disclosures are limited to those detailed in the original signed RAF and in the case of studies that also involve treatment, in the Yale Notice of Privacy Practices (NOPP, see HIPAA Policy and Procedure 5001). Note that the NOPP describes permissible disclosures related to our providing health care and does not substitute the need for a RAF in the research context. The NOPP does however allow disclosure for payment in the case of trials which will bill insurers for health care services. If a researcher needs to disclose PHI to a person or organization not listed in the signed RAF for research related purposes, the researcher should obtain an additional written RAF from the subject or apply to the IRB for a waiver of Authorization. Disclosure of PHI without patient authorization requires that the disclosure be logged in the accounting for disclosure log.

When is a RAF waiver needed? (HIPAA Authorization)

If PHI is to be used or disclosed and no written authorization has been or is planned to be obtained from the research subject, a researcher must submit a request for a waiver of authorization to the IRB. The waiver will be approved if **all** of the following conditions exist:

- The research could not practicably be conducted without the waiver
- The research could not be practicably conducted without access to and use of the PHI

- A written assurance is provided to the IRB that the PHI will not be re-used or disclosed except as required by law, for authorized oversight of the research, or for other IRB-approved research
- Uses and disclosures of PHI will be limited to the "minimum necessary" standard
- Disclosure involves no more than minimal privacy risk to the individual.

If a waiver of authorization is not approved, the PHI cannot be used or disclosed as planned in the described research and a signed RAF must be obtained from each research subject. Disclosures of PHI that are made in connection with research conducted pursuant to a Waiver of HIPAA Authorization must be tracked in the event the subject requests an accounting of disclosures of their PHI.

Is a signed RAF needed when recruiting participants?

The recruitment procedure frequently requires access to a limited amount of health information and therefore the PI must comply with HIPAA requirements of obtaining either a signed RAF from the patient or a Waiver of HIPAA Authorization approved by the IRB prior to using PHI to determining eligibility or recruitment activities. When the RAF is waived for recruitment only, it is referred to as a ***"partial waiver"*** because following recruitment a RAF will need to be signed by the research subjects.

Do I need a waiver if the authorization will be done orally?

Yes. HIPAA does not have provisions for authorization to be provided in any way other than a written form signed by the patient/subject. For example, if the information will be read to the subject over the phone or presented on-line at the start of a survey, a waiver of authorization is required to accommodate the lack of signature.

What is the difference between an informed consent and a RAF?

Simply stated, informed consent refers to the subject agreeing to participate in the research, while a RAF refers to the subject (or research participant) giving permission to use and disclose their PHI (protected health information). The requirements of the RAF under HIPAA are different from the Common Rule consent form requirements; for example, the consent form does not require the specificity of who will have access to the data. On the other hand, the RAF does not need to explain the non-privacy risks of the research. The two do overlap and can often be combined in a compound authorization.

HIPAA Authorizations vs Common Rule Consent

	Common Rule	HIPAA
Statement that study involves research	X	
Purpose of the research/disclosure	X	X
Duration of participation	X	
Description of procedures	X	

Description of risk	X	
Description of benefits	X	
Description of alternate procedures/treatments	X	
Degree of confidentiality	X	
Description of compensation/treatment for injury	X	
Who to contact for research questions	X	
Who to contact for questions about their rights	X	
Who to contact in case of injury	X	
Statement of voluntary participation/no loss of benefits/treatment if don't participate	X	X
Ability to withdraw/revoke and any exceptions	X	X
Potential for unknown risks	X	
Potential to be withdrawn from study by PI	X	
Costs of participating	X	
Consequences of subject withdrawing from study	X	
Promise to provide additional information during the course of the study	X	
Number of subjects	X	
No exculpatory language	X	
Signature	X	X
Date		X
Specific description of information to be used/disclosed	X	X
Who is authorized to use/disclose the information		X
To whom the information can be used/disclosed		X
Expiration date of authorization (not of form)		X
Potential for re-disclosure and no longer protected		X

What is a compound authorization?

A compound authorization combines the required elements of the Common Rule consent form and those required in a HIPAA Research Authorization form (RAF) into a single document.

When can you use a compound authorization?

Since RAFs are sometimes used to authorize release of subject medical records, they can end up filed in a medical record. When a compound authorization is used, both the consent information and RAF information end up in the medical record. Consent forms generally provide more detailed information which may be inappropriate for inclusion in a medical record. In such cases, separate consent and authorization forms should be used. A compound authorization can be utilized when the privacy risks associated with using a document containing both consent and authorization information are minimal.

Can banking of specimens obtained from research be included in a compound authorization?

The HIPAA Privacy Rule considers the creation and maintenance of a research repository or database as a specific research activity which can be authorized via the RAF, which in some cases may be a compound authorization. In cases where the banking of biological specimens is in addition to the current research protocol, subjects should be given the ability to consent to the research but not to the banking. This can be achieved using checkboxes on the compound authorization which allow the subject to specify whether or not they are consenting to both the study and the banking.

When is the "Request for Access to PHI for Research Purposes" form used?

The "Request Access to Protected Health Information for a Research Purpose" document, located with HIPAA Policy 5032, Use and Disclosure of PHI for Research Purposes at: http://hipaa.yale.edu/policies-procedures-forms is meant for use by investigators requesting access to protected health information for research purposes including activities preparatory to research. Once completed, it should be submitted with the supporting documentation (described on the form) and given to the entity responsible for the PHI of interest. Both Yale University and Yale New Haven Hospital (YNHH) have approved this form and it can be uploaded into the documents tab of Epic.

What is a limited data set?

A limited data set is PHI that excludes "direct identifiers" of the individual, relatives of the individual, employers, or household members of the individual and excludes psychotherapy notes. Limited data sets do not meet the strict HIPAA definition of "de-identified" data but present only minimal potential for identifying the participants. Limited data sets are afforded exception from HIPAA's accounting for disclosure requirement and are a useful way to minimize the HIPAA burden on research when used appropriately.
In contrast to de-identified data, limited data sets can have geographic areas and elements of dates, for example: Epidemiology research studies may have data where the subject names are not needed but geographic locations are relevant and a limited data set may be used.

A limited data set can only be used for purposes of research, public health, or health care operations and if the covered entity providing the data and the recipient of the data first enter into a Data Use Agreement.

What is a data use agreement?

A data use agreement is an agreement between a covered entity (the holder of the PHI) and the recipient of the PHI (such as a research investigator) in which the covered entity discloses a limited data set for purposes of research, public health or healthcare operations. Data use agreements outline permissible uses and disclosures of PHI and prohibit re-identifying or using the PHI to contact individuals.

What is an internal data use agreement?

An internal use data use agreement is used for passing limited data sets within Yale or for studies where the HIPAA privacy rules do not apply initially but becomes applicable following data collection. For example, studies conducted at facilities outside of the U.S. or health information collected from an educational record are not governed by HIPAA while the data reside outside the US or in the school. However, once the data are transferred to a HIPAA covered entity, such as YSM, all HIPAA regulations apply. Yale developed the internal data use agreement to allow researchers working internationally to bring limited data sets back to Yale with only a minimal HIPAA burden.