IRB Guidelines 1.3
HIPAA Research Implications
Version 1.1: Created 4/20/2016

Overview
The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its regulations, including the Privacy Rule and the Security Rule, as well as the Health Information Technology for Economic and Clinical Health (HITECH) Act, govern the way certain health information is collected, maintained, used, and disclosed. The Privacy Rule establishes a set of safeguards on certain types of health information known as protected health information, or PHI. The Privacy Rule was created to provide a national minimum level of protection for PHI. **Important:** HIPAA does only apply to entities that meet the definition of a covered entity or business associate or involve protected health information (PHI). Likewise, if the PHI is collected directly from participants (e.g. via interviews, surveys, questionnaires, the HIPAA privacy does NOT apply. Instead the stipulations of the HHS Common Rule (45 CFR 46) which requires informed consent DO apply.

Basic Terms and Definitions
The guidelines and the definitions are informed by federal policies (e.g. 45 CFR 46, HIPAA privacy rule), OHRP guidance documents as well as institutional best-practices of other US universities.

Protected Health Information **(PHI Link 1):** The HIPAA Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)." "Individually identifiable health information" is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or
- condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the
- individual,

and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number). Note: The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, FERPA 20 U.S.C. §1232g.

Covered Entities and Business Associates **(PHI Link 2):** The HIPAA Rules apply to covered entities and business associates. Individuals, organizations, and agencies that meet the definition of a covered entity under HIPAA must comply with the Rules' requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information. If a covered entity engages a business associate to help it carry out its health care activities and functions, the covered entity must have a written business associate contract or other arrangement with the business associate that establishes specifically what the business associate has been engaged to do and requires the business associate to comply with the Rules' requirements to protect the privacy and security of protected health information. In addition to these contractual obligations, business associates are directly liable for compliance with certain provisions of the HIPAA Rules. See definitions of "business associate" and "covered entity" at 45 CFR 160.103. A Covered Entity is one of the following:

- a Health Care Provider (e.g. providers such as: doctors, clinics, psychologists, dentists, chiropractors, nursing homes, pharmacies, ... but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.
- a Health Plan (e.g. health insurance companies, HMOs, company health plans, government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs)
- a Health Care Clearinghouse (e.g. this includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa)

De-Identified Health Information (PHI Link 5): De-identified health information, as described in the Privacy Rule, is not PHI, and thus is not protected by the Privacy Rule. There are no restrictions on the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two ways to de-identify information; either: (1) a formal determination by a qualified statistician (The covered entity may obtain certification by "a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable" that there is a "very small" risk that the information could be used by the recipient to identify the individual who is the subject of the information, alone or in combination with other reasonably available information. The person certifying statistical de-identification must document the methods used as well as the result of the analysis that justifies the determination. A covered entity is required to keep such certification, in written or electronic format, for at least 6 years from the date of its creation or the date when it was last in effect, whichever is later); or (2) the removal of 18 specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.

Unique HIPPA Identifiers (PHI Link 6): De-identified datasets must either be created by using unique statistical procedures or removing the following 18 identifiers:

1. Names.
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, except for the initial three digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census:

a. The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people.

b. The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000.

3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
4. Telephone numbers.
5. Facsimile numbers.
6. Electronic mail addresses.
7. Social security numbers.
8. Medical record numbers.
9. Health plan beneficiary numbers.
10. Account numbers.
11. Certificate/license numbers.
12. Vehicle identifiers and serial numbers, including license plate numbers.
13. Device identifiers and serial numbers.

14. Web universal resource locators (URLs).
15. Internet protocol (IP) address numbers. 16. Biometric identifiers, including fingerprints and voiceprints.
17. Full-face photographic images and any comparable images.
18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification.

Limited Data Set: A limited data set is described as health information that excludes certain, listed direct identifiers (see below) but that may include city; state; ZIP Code; elements of date; and other numbers, characteristics, or codes not listed as direct identifiers. The direct identifiers listed in the Privacy Rule's limited data set provisions apply both to information about the individual and to information about the individual's relatives, employers, or household members. The following identifiers must be removed from health information if the data are to qualify as a limited data set:

1. Names.
2. Postal address information, other than town or city, state, and ZIP Code.
3. Telephone numbers.
4. Fax numbers.
5. Electronic mail addresses.
6. Social security numbers.
7. Medical record numbers. and voiceprints.
8. Health plan beneficiary numbers.
9. account numbers
10. Certificate/license numbers.
11. Vehicle identifiers and serial numbers, including license plate numbers
12. Device identifiers and serial numbers.
13. Web universal resource locators (URLs).
14. Internet protocol (IP) address numbers.
15. Biometric identifiers, including fingerprints
16. Full-face photographic images and any 9. Account numbers. comparable images.

HIPAA Research Implications

The following section discusses how HIPAA affects different research activities as well as what types of documents/information will be required from the principle investigator (PI) as a part of the IRB application. Unless the research involves certain research activities (e.g. preparatory research, limited data set research, decedent research), the researcher needs to use a privacy authorization form to negotiate access to the PHI (see IRB Form 1.1).

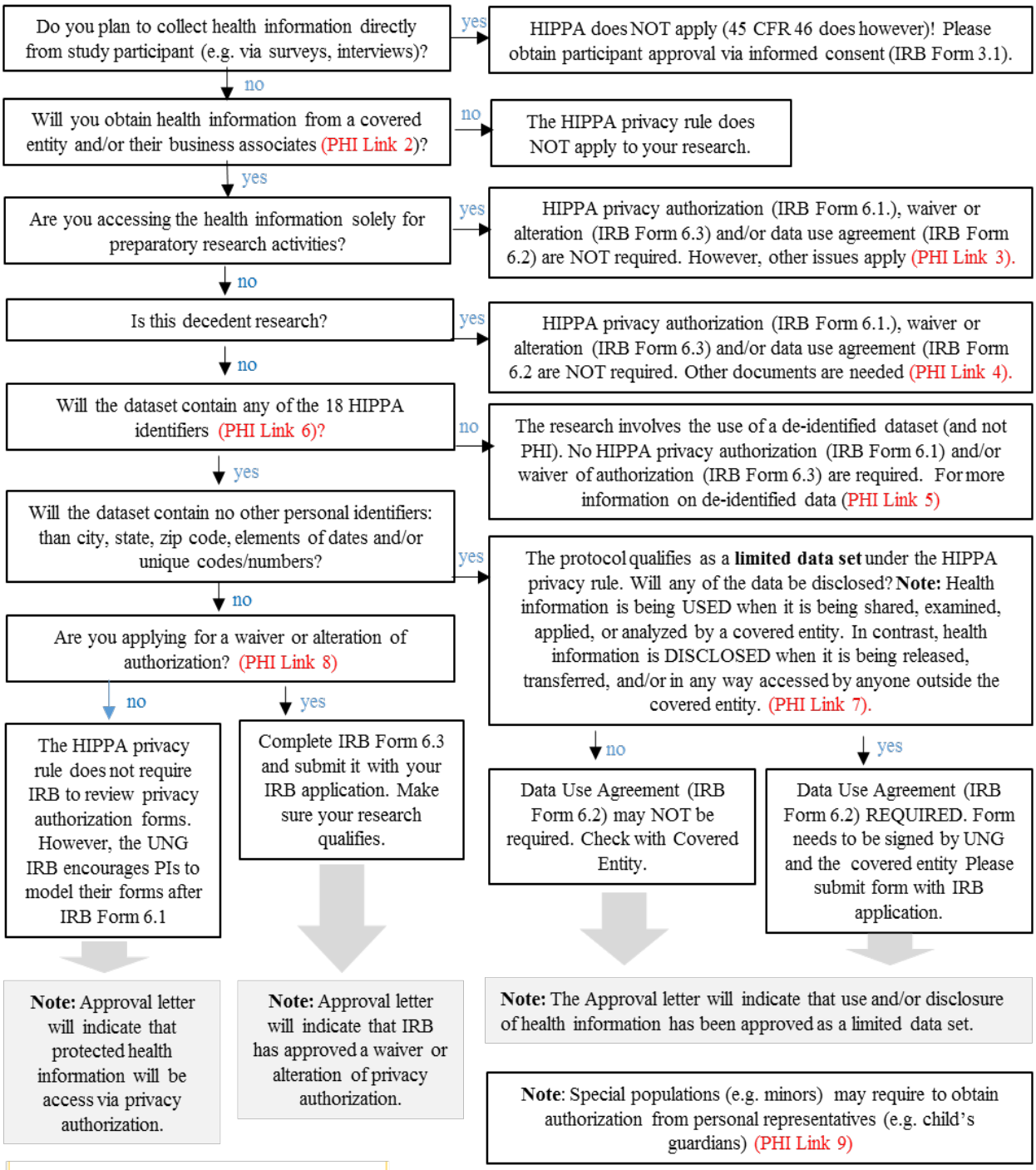
Forms/Templates for HIPAA-Related Research

IRB Form 6.1 - HIPAA Data Use Agreement
IRB Form 6.2 - HIPAA Privacy Authorization
IRB Form 6.3 - HIPAA Waiver Application

Activities Preparatory to Research (PHI Link 3)

For activities involved in preparing for research, covered entities may use or disclose PHI to a researcher without an individual's Authorization, a waiver or an alteration of Authorization, or a data use agreement. However, the covered entity must obtain from a researcher representation that (1) the use or disclosure is requested solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research, (2) the PHI will not be removed from the covered entity in the course of review, and (3) the PHI for which use or access is requested is necessary for the research. The covered entity may

IRB Application Process: How Does HIPAA Affect my Research?



UNG UNIVERSITY of NORTH GEORGIA

Created: 2-19-2016

Sources for the Flowchart

https://privacyruleandresearch.nih.gov/pdf/HIPAA_Privacy_Rule_Booklet.pdf
http://www.hhs.gov/sites/default/files/privacysummary.pdf
http://irb.wayne.edu/policies/10-2_hipaa_flowchart.pdf
https://www.umaryland.edu/media/umb/oaa/hrp/documents/study-tools-docs/hipaaflowchart.pdf

permit the researcher to make these representations in written or oral form. The preparatory to research provision permits covered entities to use or disclose protected health information for purposes preparatory to research, such as to aid study recruitment. However, the provision at 45 CFR 164.512(i)(1)(ii) does not permit the researcher to remove protected health information from the covered entity's site. As such, a researcher who is an employee or a member of the covered entity's workforce could use protected health information to contact prospective research subjects [emphasis added]. The preparatory research provision would allow such a researcher to identify prospective research participants for purposes of seeking their Authorization to use or disclose protected health information for a research study. Researchers should note that any preparatory research activities involving human subjects research as defined by the HHS Protection of Human Subjects Regulations, which are not otherwise exempt, must be reviewed and approved by an IRB and must satisfy the informed consent requirements of HHS regulations.

Research on Decedent's Protected Health Information (PHI Link 4)

To use or disclose PHI of the deceased for research, covered entities are not required to obtain Authorizations from the personal representative or next of kin, a waiver or an alteration of the Authorization, or a data use agreement. However, the covered entity must obtain from the researcher who is seeking access to decedents' PHI

(1) oral or written representations that the use and disclosure is sought solely for research on the PHI of decedents,
(2) oral or written representations that the PHI for which use or disclosure is sought is necessary for the research purposes, and
(3) documentation, at the request of the covered entity, of the death of the individuals whose PHI is sought by the researchers.

Working with Limited Data Sets (PHI Link 7)

The Privacy Rule permits a covered entity, without obtaining an Authorization or documentation of a waiver or an alteration of Authorization, to use and disclose PHI included in a limited data set. A covered entity may use and disclose a limited data set for research activities conducted by itself, another covered entity, or a researcher who is not a covered entity if the disclosing covered entity and the limited data set recipient enter into a data use agreement. Limited data sets may be used or disclosed only for purposes of research, public health, or health care operations. Because limited data sets may contain identifiable information, they are still PHI. Note: Health information is being considered to USED when it is shared, examined, applied, or analyzed by a covered entity. In contrast, health information is considered to be DISCLOSED when it is released, transferred, or in any wat accessed by anyone outside the covered entity.

A data use agreement is the means by which covered entities obtain satisfactory assurances that the recipient of the limited data set will use or disclose the PHI in the data set only for specified purposes. Even if the person requesting a limited data set from a covered entity is an employee or otherwise a member of the covered entity's workforce, a written data use agreement meeting the Privacy Rule's requirements must be in place between the covered entity and the limited data set recipient. If PHI are being disclosed as a limited data set, the principle investigator should submit a IRB Form 6.2.

HIPAA Waiver or Alteration of Privacy Authorization (PHI Link 8)

A waiver or alteration of the PHI authorization process may be granted if the following criteria are met:

(1) The use or disclosure of the PHI involves no more than minimal risk to the privacy of individuals based on, at least, the presence of the following elements:
    a. An adequate plan to protect health information identifiers from improper use and disclosure.

b. An adequate plan to destroy identifiers at the earliest opportunity consistent with conduct of the research (absent a health or research justification for retaining them or a legal requirement to do so).

c. Adequate written assurances that the PHI will not be reused or disclosed to (shared with) any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of the PHI would be permitted under the Privacy Rule.

(2) The research could not practicably be conducted without the waiver or alteration.

(3) The research could not practicably be conducted without access to and use of the PHI.

For multi-site studies there is usually only one IRB or privacy approval per covered entity needed (however, some covered entities may require approvals for all IRBs). To apply for a HIPAA waiver or alteration of privacy authorization please submit IRB Form 6.3.

De-Identifying Protected Health Information

Under the first method, unique identifying numbers, characteristics, or codes must be removed if the health information is to be considered de-identified. However, the Privacy Rule permits a covered entity to assign to, and retain with, the health information a code or other means of record identification if that code is not derived from or related to the information about the individual and could not be translated to identify the individual. The covered entity may not use or disclose the code or other means of record identification for any other purpose and may not disclose its method of re-identifying the information. For example, a randomly assigned code that permits re-identification through a secured key to that code would not make the information to which it is assigned PHI, because a random code would not be derived from or related to information about the individual and because the key to that code is secure. A covered entity is permitted to de-identify PHI or engage a business associate to de-identify PHI. For example, a researcher may be a covered entity him/herself performing, or may be hired as a business associate to perform, the de-identification. In most cases, the covered entity must have a written contract with the business associate containing the provisions required by the Privacy Rule before it provides PHI to the business associate. In addition, a covered entity, if a hybrid entity, could designate in its health care component(s) portions of the entity that conduct business associate-like functions, such as de-identification. De-identifying PHI according to HIPAA Privacy Rule may enable many research activities; for example, it permits a covered entity to use and disclose protected health information for research purposes, without an individual's authorization, provided the covered entity obtains either:

(1) documentation that an alteration or waiver of individuals' authorization for the use or disclosure of protected health information about them for research purposes has been approved by an Institutional Review Board or Privacy Board;

(2) representations from the researcher that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purpose preparatory to research, that the researcher will not remove any protected health information from the covered entity, and that protected health information for which access is sought is necessary for the research; or

(3) representations from the researcher that the use or disclosure sought is solely for research on the protected health information of decedents, that the protected health information sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is sought.38 A covered entity also may use or disclose, without an individuals' authorization, a limited data set of protected health information for research purposes

Personal Representatives and Minors (PHI Link 9)

Personal Representatives. The Privacy Rule requires a covered entity to treat a "personal representative" the same as the individual, with respect to uses and disclosures of the individual's protected health information, as well as the individual's rights under the Rule 84. A personal representative is a person

legally authorized to make health care decisions on an individual's behalf or to act for a deceased individual or the estate. The Privacy Rule permits an exception when a covered entity has a reasonable belief that the personal representative may be abusing or neglecting the individual, or that treating the person as the personal representative could otherwise endanger the individual. Special case: Minors. In most cases, parents are the personal representatives for their minor children. Therefore, in most cases, parents can exercise individual rights, such as access to the medical record, on behalf of their minor children. In certain exceptional cases, the parent is not considered the personal representative. In these situations, the Privacy Rule defers to State and other law to determine the rights of parents to access and control the protected health information of their minor children. If State and other law is silent concerning parental access to the minor's protected health information, a covered entity has discretion to provide or deny a parent access to the minor's health information, provided the decision is made by a licensed health care professional in the exercise of professional judgment.

References

https://privacyruleandresearch.nih.gov/pdf/HIPAA_Privacy_Rule_Booklet.pdf
http://www.hhs.gov/sites/default/files/privacysummary.pdf
http://irb.wayne.edu/policies/10-2_hipaa_flowchart.pdf
https://www.umaryland.edu/media/umb/oaa/hrp/documents/study-tools-docs/hipaaflowchart.pdf

If you need this document in another format, please email irbchair@ung.edu or call 706-867-2969.