

Privacy regulations (HIPAA, state, and other federal) for researchers and research staff

**Prepared by
Office of Research and Sponsored Programs
Georgia State University**

Summary

The purpose of this module is to provide researchers with the information they will need to comply with the Privacy Rule associated with HIPAA, the Health Insurance Portability and Accountability Act, and other relevant state and federal laws.

The module will cover:

- 1. types of protected health information: de-identified data, limited data sets, and individually identified health information;**
- 2. authorization (consent) requirements and how to obtain waivers of authorization;**
- 3. research subjects' rights;**
- 4. research subject recruitment;**
- 5. authorization templates; and**
- 6. additional resources.**

Under HIPAA, researchers will have to:

- provide more detailed information to the Institutional Review Board about data storage, re-disclosure and destruction; and**
- provide more information to research subjects in the consent and authorization process about how information about them will be used.**

Definitions

•Research: For GSU, "research" means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. Activities that meet this definition constitute "research" whether or not they are supported or funded under a program that is considered research for other purposes. For example, some "demonstration" and "service" programs may include research activities. This definition includes activities preparatory to the conduct of research; for example, activities conducted in support of grant or proposal preparation, pilot studies, and feasibility studies.

•Covered entity: Covered Entities are health care providers, health plans, and health care clearinghouses. GSU is not a covered entity. GSU is a hybrid entity,

where only portions of the University are covered (i.e., Human Resources, Biology, etc...)

• **Authorization**: is the HIPAA equivalent of consent to use and disclose data.

Definitions (continued)

• **Protected Health Information (PHI)**: Protected health information includes all *individually identifiable* health information transmitted or maintained by an organization covered by the HIPAA regulations (a “covered entity”), regardless of form. Specifically, if it is Individually Identifiable Health Information (IIHI) that:

- is created or received by a health care provider, health plan, employer, or health care clearinghouse);
- relates to:
 - the past, present, or future physical or mental condition,
 - the past, present, or future provision of care to an individual, or
 - the past, present or future payment for provision of health care to an individual, and
- identifies the individual (or there is a reasonable basis to believe that the information can be used to identify the individual).

What kind of research and researchers are affected by the HIPAA regulations?

• Any kind of research conducted under the auspices of the GSU that creates, uses, or discloses protected health information is subject to the HIPAA regulations. This includes such research activities as clinical trials, chart reviews, epidemiological studies, behavioral and social science studies, as well as basic science research activities. It includes research that involves the provision of treatment as well as research that provides neither treatment nor diagnosis.

• All studies involving creation, use, or disclosure of Protected Health Information (PHI) must be reviewed and approved in advance by the GSU Institutional Review Board.

Types of health information: Individually Identifiable Health Information (IIHI)

• There are three categories of health information. The requirements for use are different for each.

Individually Identifiable Health Information (IIHI): includes any subset of health information, including demographic information collected from an individual, that:

• Identifies the individual (or there is a reasonable basis to believe that the information can be used to identify the individual.)

•The general rule is that an authorization signed by the research subject is required for the disclosure of individually identifiable health information. An IRB may waive this requirement.

Types of health information: De-identified data sets

De-Identified Information: Health information is considered de-identified when it does not identify an individual and the covered entity has no reasonable basis to believe that the information can be used to identify an individual. Information is considered de-identified if 18 identifiers are removed from the health information and if the remaining health information could not be used alone, or in combination, to identify a subject of the information. An IRB may waive authorization for the use of de-identified data. The identifiers include:

Information that may NOT be included in de-identified data sets

- names,
- geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code and equivalent geocodes, except for the initial three digits of a zip code to 000,
- 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,
- 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, (14) Web Universal Resource Locator (URL),
- biometric identifiers, including finger or voice prints,
- full face photographic images and any comparable images,
- Internet Protocol address numbers
- any other unique identifying number characteristic or code

Types of health information: Limited data sets

•**Limited Data Set:** A limited data set is information disclosed by a covered entity to a researcher who has no relationship with the individual whose information is being disclosed. The covered entity is permitted to disclose PHI, with direct identifiers

removed, subject to obtaining a data use agreement from the researcher receiving the limited data set. The PHI in a limited data set may not be used to contact subjects. The IRB may waive authorization for use of limited data sets in research.
Types of health information: Limited data sets

Direct identifiers that must be *removed* from the information for a limited data set are:

- (1) name,
- (2) address information (other than city, State, and zip code),
- (3) telephone and fax numbers,
- (4) e-mail address,
- (5) Social Security number,
- (6) certificate/license number,
- (7) vehicle identifiers and serial numbers,
- (8) URLs and IP addresses,
- (9) full face photos and other comparable images,
- (10) medical record numbers, health plan beneficiary numbers, and other account numbers,
- (11) device identifiers and serial numbers,
- (12) biometric identifiers including finger and voice prints.

Identifiers that are *allowed* in the limited data set are:

- (1) admission, discharge and service dates,
- (2) birth date,
- (3) date of death,
- (4) age (including age 90 or over),
- (5) geographical subdivisions such as state, county, city, precinct and five digit zip code.

Authorization requirements

•HIPAA regulations use the term “authorization” to describe the process through which a patient allows researchers to access protected health information. Blanket authorizations for research to be conducted in the future are not permitted. Each new use requires a specific authorization. The authorization for disclosure and use of protected health information may be combined with the consent form that a research subject signs before agreeing to be in a study. It may also be a separate form. In either case, the information must include:

Authorization requirements: elements

- a description of the information to be used for research purposes;

- who may use or disclose the information
- who may receive the information
- purpose of the use or disclosure
- expiration date of authorization (90 days in Washington state)
- how long the data will be retained with identifiers
- individual's signature and date
- right to revoke authorization
- right to refuse to sign authorization (if this happens, the individual may be excluded from the research and any treatment associated with the research)
- if relevant, that the research subject's access rights are to be suspended *while the clinical trial is in progress*, and that the right to access PHI will be reinstated at the conclusion of the clinical trial.
- that information disclosed to another entity in accord with an authorization may no longer be protected by the rule

Waiver of authorization for research

The GSU Institutional Review Board uses these criteria in approving requests for a waiver of authorization for research:

- the use or disclosure of protected health information must involve no more than minimal risk to the privacy, safety, and welfare of the individual;
- the research could not practicably be conducted without the waiver or alteration; and
- the research could not practicably be conducted without access to the protected health information.

The Institutional Review Board must also consider if the researcher has provided:

- an adequate plan to protect the identifiers from improper use or disclosure;
- an adequate plan to destroy the identifiers at the earliest opportunity, unless retention of identifiers is required by law or is justified by research or health issues; and
- adequate written assurance that the PHI will not be used or disclosed to a third party except as required by law or permitted by an authorization signed by the research subject.

What information researchers will have to provide to the IRB?

Researchers will have to provide more detailed information about the types of information they will use in their research, how it will be used, who will have access to it, and when it will be destroyed. Specifically, they will be asked:

- What risks are posed by the use of the data and how have they been minimized?
- What is the justification for access to the data and why are they necessary to conduct the research?
- What plan does the researcher have to protect identifiers from improper use or disclosure?
- What is the researcher's plan to destroy the identifiers? If it is not possible to destroy the identifiers, what is the health, legal, or scientific justification?
- Has the researcher provided adequate written assurance that the PHI will not be used or disclosed to a third party except as required by law or permitted by an authorization signed by the research subject?

Researchers requesting waivers of authorization will need to explain

(The IRB has a Request for Waiver of Authorization Form available for this purpose)

- that the use or disclosure poses no more than minimal risk to the subject;
- that the research could not practicably be conducted without the waiver; and
- that the research could not practicably be conducted without access to the protected health information.

Research subjects' rights

•**Right to an accounting:** When a research subject signs an authorization to disclose PHI, the covered entity is not required to account for the authorized disclosure. Nor is an accounting required when the disclosed PHI was contained in a limited data set or is released to the researcher as de-identified data. However, an accounting is required for research disclosures of identifiable information obtained under a waiver or exception of authorization. Research subjects may request an accounting of disclosures going back for up to six years.

•**Right to revoke authorization:** A research subject has the right to revoke his or her authorization unless the researcher has already acted in reliance on the original authorization. Under the authorization revocation provision, covered entities may continue to use or disclose PHI collected prior to the revocation as necessary to maintain the integrity of the research study. Examples of permitted disclosures include submissions of marketing applications to the FDA, reporting of adverse events, accounting of the subject's withdrawal from the study and investigation of scientific misconduct.

Research subject recruitment

•Recruitment of subjects for research is subject to the general authorization requirements. The Privacy Rule classifies recruitment as "research" rather than as health care operations or marketing. Because development or use of research databases falls within the definition of "research," a covered entity may disclose PHI in a database to sponsors for subject recruitment only after an authorization from the research subject or a waiver from the GSU Institutional Review Board has been obtained.

•Neither an authorization nor a waiver is required to disclose PHI contained in a limited data set or as de-identified data. Limited data sets will make it easier to create databases of potential subjects to see if it is feasible to conduct a clinical trial or to perform epidemiological research.

•There are a couple of important limitations on the use of PHI in a limited data set for subject recruitment. The PHI may not be used to contact subjects, and, because telephone numbers, internet provider addresses, and email addresses are not part of a limited data set, this information may not be collected by researchers from prospective subjects.

•When researchers want to approach potential subjects to participate in a study whom they have identified using PHI under a waiver of authorization, they must use an approach method that has been approved in advance by the Human Subjects Review Committee. Examples of approach mechanisms include using an intermediary such as the patient's primary care provider or a member of the medical staff actually caring for that patient, or sending the potential subject a letter signed by the patient's provider.

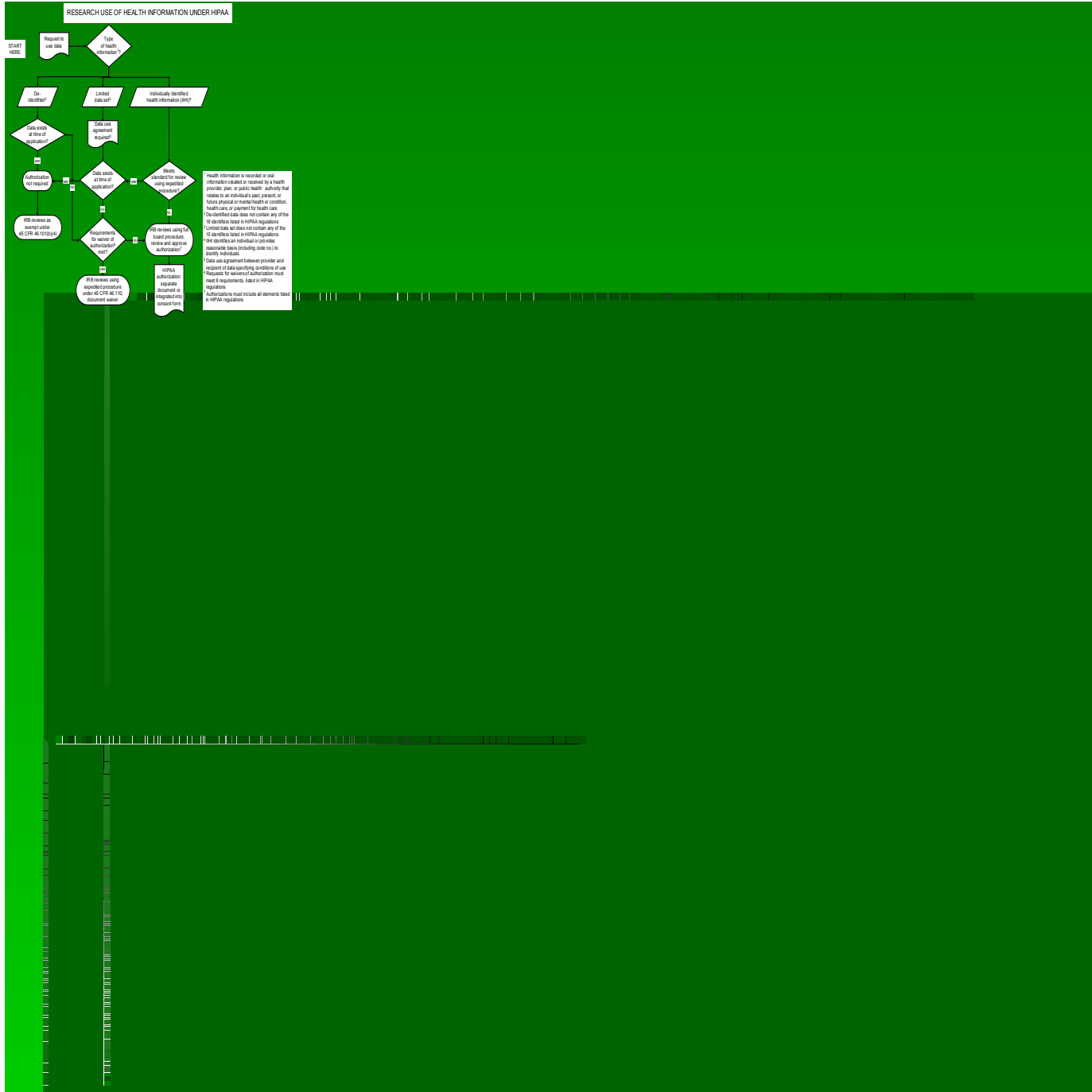
What will researchers have to do to request a waiver of authorization?

In completing the application to the GSU Institutional Review Board, the researcher must:

- Explain how the use of PHI involves no more than minimal risk to individuals**
- Explain why such a waiver will not adversely affect privacy rights or welfare of individuals in the study**
- Explain why the study could not practicably be conducted without a waiver**
- Explain why it is necessary to access and use protected health information to conduct this research**
- Explain how the risks to privacy posed by use of PHI in this research are reasonable in relation to the anticipated benefits**
- Explain the plan to protect identifiers from re-disclosure**

—Explain the plan to destroy identifiers. Provide a date by which this will take place. If identifiers must be retained, provide the reason (scientific, health, or other) why this is necessary.

—Confirm that the PHI will not be reused or disclosed to anyone else.



HIPAA Waiver of Authorization Form

Researchers must fill out the GSU HIPAA Waiver of Authorization Form (can be downloaded from www.gsu.edu/irb) and submit it with their IRB application to the Office of Research at G-76 Alumni Hall.

Elements and sample text

- **A description of the information: minimum necessary**

“We will review your medical record for information about diagnosis and treatment of your breast cancer.”

- **Who may use or disclose the information**

“The researcher and research team members will have access to this information.”

- **Who may receive the information**

“We may give the sponsor of this research, the Food and Drug Administration, the laboratory, and the Institutional Review Board access to this information.”

- **Purpose of the use or disclosure**

**“We will use this information to make sure it is safe for you to be in this study,” or,
“We will use this information to make sure you are eligible to be in this study.”**

- **Expiration date**

“This authorization will expire in 90 days. That means we cannot obtain new information about you after that time.

- **How long identifiable data will be retained**

“We will keep information about you linked to your name until [INSERT DATE].”

- **Individual’s signature and date:**

subject or subject’s personal representative or legally authorized surrogate must receive copy; researcher must retain copy for at least 3 years or per applicable policy

- **Right to revoke authorization**

“You have the right to change your mind about allowing us to have access to this information. If you do....”

- **Right to refuse to sign authorization**

“You have the right to refuse to allow us access to this information. If you do....”

- **Loss of privacy protection once information is re-disclosed.**

“If we disclose information about you to anyone outside of this study, you will lose your privacy protections.

- **If the research subject’s access rights are to be suspended *while the clinical trial is in progress*, the consent form must include an agreement to this denial of access.**

“While you are in this study you will not be able to have access to any of your medical records related to this study.”

- **The consent form must inform the research participant that the right to access PHI will be reinstated at the conclusion of the clinical trial.**

“When the study is over, you will have the right to access your medical records again.”

- **The consent form must state that if the information is disclosed by the researcher to another entity that the information may no longer be protected by the Privacy Rule.**

“If we disclose information about you to someone else, it may no longer be protected by this privacy law.”

Quiz questions

1. **What types of Protected Health Information may be used in research without specific authorization from patients?**
 - a. **Individually Identifiable Health Information**
 - b. **Limited Data Set**
 - c. **De-Identified Data**
 - d. **all of the above**
 - e. **none of the above**

2. **How should researchers who access Individually Identifiable Health Information under a waiver of authorization from the IRB invite the potential subjects they have identified to take part in their research?**
 - a. the researchers can telephone the subjects directly
 - b. the researchers can send a letter to the subjects directly
 - c. the researchers can email the subjects directly
 - d. the researchers can ask the potential subject's health care provider to invite the subject to be in the study

3. **Accounting of disclosures of PHI to patients is NOT required when::**
 - a. the disclosure was conducted with the authorization of the patient
 - b. the disclosure was conducted under a waiver of authorization
 - c. the disclosure was made for research purposes
 - d. the disclosure was about a deceased person

4. **The requirement that a patient provide written authorization to disclose PHI to a researcher can be waived when:**
 - a. the data are de-identified
 - b. the data are part of a Limited Data Set
 - c. the researcher determines that the research is "exempt" from IRB review
 - d. the IRB determines that a waiver request meets HIPAA requirements

Where to go for additional information

GSU Office of Research and Sponsored Programs

G-76 Alumni Hall

(404) 651-4350

<http://www.gsu.edu/~wwwosp/Compliance2002/web-irb/index.htm>

Department of Health and Human Services

Office for Civil Rights – HIPAA

<http://www.hhs.gov/ocr/hipaa/>

Department of Health and Human Services, Office of the Assistant Secretary for Planning and Evaluation, Administrative Simplification

<http://aspe.os.dhhs.gov/admsimp/>