

SUNY New Paltz Policy and Procedure on Research Subjects' Right to Privacy

PART I: Introduction

The privacy regulations (The Privacy Rule) that have been promulgated by the federal Office of Civil Rights under the Health Insurance Portability and Accountability Act (HIPAA) impact research involving human subjects. These regulations define conditions where certain health information may be used or disclosed in research activities. Further, the regulations define conditions where 'authorization' must be obtained from the patient. The full text of these regulations, is available at www.hhs.gov/ocr/hipaa .

PART II: Definitions pertaining to Privacy in Research

1. **Health Care:** means care, services, or supplies related to the health of an individual. It includes, but is not limited to: preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body.

2. **Health Care Provider:** A researcher is a covered health care provider (and must comply fully with HIPAA privacy regulations) if he or she furnishes health care services to individuals, including the subjects of research, and transmits any health information in electronic form in connection with a transaction covered by the federal Transaction Rule (involving e.g., health care claims and payments, health plan eligibility, enrollment and disenrollments etc.; see 64 CFR 102 and 103 for specifics).

3. **Health Information:** any information, whether oral or recorded in any form or medium, that is created or received by an investigator, and relates to the past, present, or future physical or mental health or condition of an individual. To assist you in making the determination of what constitutes 'health information', this definition includes physical or mental information regarding the diagnosis, treatment and/or prevention of physical or mental conditions of the type that is now (or could be in the future) covered by health insurance.

4. **Individually identifiable health information (IIHI):** is a subset of health information, including demographic information collected from an individual that identifies the individual (either directly, or through codes/identifiers)

5. **De-identified Health Information:** health information can be considered de-identified if, EITHER:

a) The investigator provides to SUNY New Paltz IRB a written attestation by an expert in de-identification methods, that there is a very small risk that the information could be used by others to identify the subject.

The preamble to the Privacy Rule provides guidance (see, e.g., <http://www.fcsm.gov/working-papers/wp22.html> and http://www.fcsm.gov/docs/checklist_799.doc) for what would be required in this regard, e.g., removing all direct identifiers, for reducing the number of variables on which a match might be made, and for limiting the distribution of records, etc.

OR

b) The investigator certifies to the IRB (via the HIPAA De-identification Certification Form) that all of the following 18 identifiers are removed, and the investigator has no actual knowledge that the remaining information could be used, alone or in combination, to identify a specific subject. This is referred to as the Safe Harbor method. The 18 identifiers are name, address (street address, city, county, zip code -with certain exceptions), dates (e.g., birth date, admission date, discharge date, date of death) and individual ages if over 89, telephone #'s, fax #'s, electronic mail addresses, social security #'s, medical record numbers, health plan beneficiary #'s, account #'s, certificate/license #'s, vehicle identifiers and serial #'s, license plate #'s, device identifiers and serial #'s, Web Universal Resource Locators (URL's), Internet Protocol (IP) address #'s, Biometric identifiers (including finger and voice prints), Full face photographic images and any comparable images, and any other unique identifying #, characteristic, or code.

De-identified health information is NOT subject to the special authorization and disclosure accounting requirements addressed in this document. However, the application and approval process for the research use of such 'anonymous' health information remains the same as is currently in place, and is not impacted by the privacy regulations (except for the need to complete the additional HIPAA form).

PART III: Policy

A. **All** investigators who conduct research where individually identifiable health information is used, generated, or disclosed are required to protect their research subjects' right to privacy of their health information, using procedures as outlined in Part 4. This policy, and these procedures, are in addition to provisions already in place under the Common Rule at 45 CFR 46.

According to the Privacy Rule, researchers are performing a function specifically covered under HIPAA (and are, therefore, considered health care providers under the rule) if they

a) provide health care as part of their research, **and**

b) are involved in standard electronic transactions (involving e.g., health care claims and payments, health plan eligibility, enrollment and disenrollments etc.; see 64 CFR 102 and 103 for specifics). **SUNY at New Paltz, therefore, requires that research investigators meeting both of these 2 criteria comply with all provisions of the privacy regulations and upcoming security regulations.**

Part IV: Procedures

The procedures below must be followed in addition to IRB submission and approval requirements detailed in the SUNY at New Paltz IRB Manual.

A) Research Databases/Registries

The collection of health information for 'private' research registries is allowable if either:

1. authorization is obtained from the subject (i.e., for prospective collections) or
2. authorization is not obtained from the subjects (e.g., for retrospective collections) if :

a) the health information is either in de-identified form (in accordance with HIPAA specifications) or

b) the health information is in the form of a limited data set where the recipient of the data enters into a data use agreement with the provider of the data. If the latter, only the minimum necessary information may be released as necessary to achieve the purpose of the database/registry.

If an investigator wishes to obtain data from a registry for research purposes, the usual IRB application and approval requirements must be met (including assessment of consent/authorization waivers etc.)

B) Research involving De-identified data:

Along with the standard IRB application requirements for 'anonymous' data collection, one of the methods detailed in Part 2 above must be detailed for assuring that the data are de-identified. The HIPAA De-identification form must be completed if the 18 listed identifiers are to be removed to satisfy HIPAA standards.

C) Research Use or Disclosure of IIHI without Subject Authorization:

1. The IRB can waive the requirement to obtain authorization for use or disclosure of IIHI if one of the 4 following conditions apply:

a. The IRB finds and documents that all of the following criteria are addressed and met in the application submission (PI completes a HIPAA Waiver of Authorization form):

i) The use or disclosure of IIHI for the research involves no more than minimal risk to the privacy of individuals, based on:

- a. an adequate plan to protect identifiers from improper use
- b. an adequate plan to destroy identifiers at the earliest opportunity, and
- c. adequate written assurances that health information will be protected (e.g., not re-used/disclosed to any other person or entity except as required by law, for authorized oversight, etc.)

ii) The research could not practicably be conducted without the waiver or alteration; and

iii) The research could not be practicably be conducted without access to and use of the health information.

b. The proposed activity is solely for the purpose of creating a protocol preparatory to research (documented via the "Request for Permission to Access Identifiable Health Information for Reviews Preparatory to Research")

Using the example of a medical record review to be conducted through a covered entity, an investigator can review IIHI of patients as necessary to assist in the development of a research hypothesis, or to prepare a research protocol, or to assess whether covered entity has a patient population that would meet the eligibility criteria for enrollment into a proposed research study. But the investigator may only record de-identified information; no other health information can be removed from the medical record. **Further, SUNY at New Paltz does not permit this method to be used for recruitment purposes, i.e., as a means to specifically screen and contact patients as potential research subjects, unless a) the investigator has a treatment relationship with the patient and b) this method of recruitment is described and approved by the IRB via the standard application process.**

c. The proposed activity is for research on a deceased person's IIHI (documented via the "Request for Permission to Access Identifiable Health Information of Deceased Individuals")
Investigators must provide representation that :

- 1) the use of disclosure sought is solely for research on the IIHI of (verifiably) deceased individuals, and
- 2) the IIHI for which use or disclosure is sought is necessary for the research purposes.

d. The proposed use of health information is via a 'limited data set'.

A limited data set (LDS) contains information that is not completely de-identified as defined above (e.g., an LDS can contain dates of admission and discharge, dates of birth and death, dates of procedures, city, state, zip codes...it must exclude certain direct identifiers such as names, addresses, telephone #'s, e-mail addresses etc.). To use a Limited Data Set, a Data Use Agreement (DUA) must first be in place with the recipient of the information, and a HIPAA Limited Data Set (LDS) form must be on file with SUNY at New Paltz IRB. If, for example, an investigator receives a LDS derived from covered entity's medical records, the DUA would be generated through the covered entity. The Data Use Agreement defines the permissible uses/disclosures of the LDS by the recipient, defines who can use or receive the data, and require the recipient to assure that data will not be re-identified and that individuals will not be contacted.

2. Minimum Necessary Requirement/Accounting for Disclosures Requirement

With the exception of limited data sets obtained under a data use agreement, disclosure of IIHI without authorization (i.e., a waiver of authorization was granted, or the disclosure involved record review preparatory to research, or the disclosure involved the IIHI of deceased individuals) made after April 14, 2003 requires that:

a) The disclosure of health information be kept to the minimum necessary to meet the purpose of the study,

and

b) The HIPAA disclosure accounting requirement must be met by the covered entity. This means that a patient/subject must be able to request, and be provided with, a list of all individuals or entities to which their IIHI was disclosed without their authorization. **The researcher must keep track of each instance where s/he has provided an entity outside of the original covered entity with subjects' IIHI without that subject's authorization. Researchers are to comply with all of the requirements of the covered entity relative to disclosure of and accounting for IIHI.**

In consideration of the federal accounting requirement, and the associated workload, it is strongly urged that the investigator either obtain an authorization, or utilize a limited data set prior to disclosure of his/her subjects' IIHI.

D) Research Use of Health Information with Subject Authorization*

Under the HIPAA regulations, a patient coming into a doctor's office or hospital for clinical treatment will sign a consent, basically allowing the physician's office (or hospital etc) to use or disclose his or her for treatment, payment and health care operations purposes.

In the research setting, it is clear that health information could be generated and used or disclosed during the course of a research study. It is also clear that health information could be derived from research activities where the procedure involves a simple blood draw from which

genetic information can be obtained. It is thus important to assess the proposed research protocol for need to access health information, and the potential for producing health information. If either is possible, then the HIPAA regulations will likely apply.

It is important to remember, that subjects can revoke their authorization for use of their health information at any time during the research. However, health information that was obtained prior to when authorization was revoked can continue to be used and disclosed if its inclusion is important to maintain the integrity of the research study. For example, health information could be reported to account for a subject's withdrawal from the study, to be used as part of a marketing application to the FDA, to conduct investigations of scientific misconduct, or to report adverse events.