

# **SUNY-O Policy and Procedure on Research Subjects' Right to Privacy**

## **-final 5/13/03-**

### **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](http://www.hhs.gov/ocr/hipaa) . Further mandates will follow once the upcoming security regulations are finalized.

#### **Deadlines:**

- **Health Care Providers:** The deadline for health care providers (see definition in part 3) to fully comply with these regulations (i.e., the 'enforcement' date) is **April 14, 2003**.
- **For all other researchers:** If your research requires access to existing health information (e.g., medical records, etc) from a health care entity after 4/13/03, that entity is required to obtain from you either the subject's authorization to access that information about them (via a IRB approved updated consent form), or proof from IRB that one of the mechanisms outlined in Part 4, Section D below has been met to warrant not obtaining such authorization. For this reason, you may need to comply with the 4/14/03 deadline even if you, yourself, are not a health care provider. *If you don't need access to health information as part of your research, the deadline for compliance for non health care providers is the date that your current approval period terms.*

### **PART II: SUNY-O 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 dis-enrollments 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 SUNY-O 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 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](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 SUNY-O investigator certifies to 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 IRB 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** SUNY-O 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-O, therefore, requires that research investigators meeting both of these 2 criteria comply with all provisions of the privacy regulations and upcoming security regulations.** SUNY-O staff members and medical staff members must additionally comply with this, and all SUNY-O policies and procedures pertaining to HIPAA.

If you qualify as a health care provider, and either you or your co-investigators are NOT currently part of SUNY-O staff, you must contact the Office of Research Compliance for additional requirements (e.g., signing of specific privacy and/or confidentiality agreements etc.).

### **Part IV: Procedures**

***The procedures below must be followed in addition to IRB submission and approval requirements detailed in the IRB Handbook for Investigators (Nov 2002).***

**A) Notice of Privacy Practice (NOPP):**

Effective April 14, 2003, all patients encountered in a health care facility (e.g., University Optometric Center) must receive an NOPP. In it, the patients are provided with information concerning how their IIHI may be used and/or disclosed by the facility, details concerning the patients' privacy rights, and the facility's legal responsibilities with respect to IIHI. For subjects who are SUNY-O UH patients, their signing of the research consent form will acknowledge receipt of the NOPP.

**B) Research Databases/Registries (see also Section 18 of the IRB Handbook)**

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 SUNY-O 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.)

**C) 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.

**D) Research Use or Disclosure of IIHI without Subject Authorization:**

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

**a. 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 ORC:HIPAA form: "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 University Optometric Center, 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 UH 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-O 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 IRB via the standard application process.**

**c. The proposed activity is for research on a deceased person's IIHI** (documented via the ORC:HIPAA form: "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 IRB. If, for example, an investigator receives a LDS derived from UH medical records, the DUA would be generated through UH. 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. 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 SUNY-O researcher must keep track of each instance where s/he has provided an entity outside of SUNY-O with subjects' IIHI without that subject's authorization.** (For disclosures from medical records, a mechanism at the University Optometric Center level would provide such accounting. **For disclosures from departmental patient records, sometimes referred to as 'shadow chart', the department must provide such accounting).**

**For disclosures involving less than 50 individuals, the accounting must include:**

- date of the disclosure
- frequency or number of disclosures made during the accounting period
- date of the most recent disclosure
- name of the individual or entity receiving the information (and address, if known)
- brief description of the IIHI disclosed and
- brief statement of the purpose of the disclosure

**For disclosures involving 50 or more individuals, the accounting must include:**

- name of the study or protocol
- description of the purpose of the study
- type of IIHI disclosed
- time frame over which disclosures took place (including the date of the most recent disclosure)
- name, address, and telephone # of the entity sponsoring the research, and of the researchers to whom the information was disclosed.

**In consideration of this 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.**

#### **E) 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 it's 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.

**For research involving IIHI where subject authorization is sought, the confidentiality section of the consent form (or permission form, for parents of minor subjects) is replaced with a combined section below:**

---

—

**Confidentiality/Protecting the Privacy of Your Health Information**

*(Replaces the separate "Confidentiality" and "Protecting your health information" sections in the November 2002 Handbook for Investigators)*

NOTE TO INVESTIGATORS:

*ITALICS=instructions*

**Boldface=boilerplate text; do NOT boldface the text in the consent form.**

*This section describes the extent to which confidentiality and privacy of records that identify the subject will be maintained and protected.*

*The following statement should be used to start this section:*

**The following procedures will be followed in an effort to keep your personal information confidential in this study: Your identity will be held confidential, and all data will be kept in a secured, limited access location. Your identity will not be revealed in any publication or presentation of the results of this research.**

**Confidentiality cannot be guaranteed; your personal information may be disclosed if required by law. This means that there may be rare situations that require us to release personal information about you, e.g., in case a judge requires such release in a lawsuit, if you tell us of your intent to harm yourself or others (including reporting behaviors consistent with child abuse). If a certificate of confidentiality (COC) is obtained for the study, remove the first example of the judge and lawsuit (since a COC protects against such release of information) and add boilerplate COC language (provided by NIH once the COC is granted)**

*For research activities, where confidentiality of subject identity is not proposed (e.g., where subjects will be quoted by name) this section should be very clear regarding where and how the quotes will be used. Subjects should also have the opportunity to review the text in which their quotes or identity appear, to ensure proper attribution.*

*If there will be payment to subjects, the following statement should be added:*

**By accepting payment for participating in this study, certain identifying information about you may be made available to professional auditors to satisfy audit and federal reporting requirements, but confidentiality will be preserved. Please note that if you earn \$600 or over in a calendar year as a research subject, you may have to pay taxes on these earnings.**

*If the study involves use of video/audiotaping of the subject, include a statement specifically addressing who has access to the tapes, how they are stored, for what purposes will the tapes be used, and what happens to the tapes once the study is ended (i.e., Are they erased after all the necessary information is collected from them? Are they kept for archival purposes?).*

**As a result of being in this study, identifiable health information about you will need to be used, generated, and or reported for the purpose(s) outlined in this consent form, and/or as required by law. Federal law protects your rights to privacy concerning this information. As such, there is certain specific information you need to know.**

**Individually identifiable health information (IIHI) under the federal privacy law is considered any information from your medical record, or obtained from this study, that can be linked to you, and that relates to your past, present, or future physical or mental health or condition. The following IIHI will need to be used, generated, or disclosed (reported) for the purpose of this study:**

- **Information from your medical record, including** (specify what health information you need from the subject's medical record)
- **Information obtained from this study, including** (specify what health information will be collected while the individual is a subject in this study, e.g., results of physical examinations, laboratory [blood, urine] tests, x-rays and other diagnostic medical procedures [be specific regarding tests - MRI, CT, etc.])
- *PI should add or delete as necessary.*

**Your IIHI will be shared with any person or agency when required by law, and by:**

- **the research team for this study**
- **the sponsor(s) of this study, 'Acme Drug Company'**
- **the Food and Drug Administration** (if applicable) if there is Food and Drug Administration (FDA) oversight (e.g., protocol involves use of drugs, biologics or devices), and/or if the research is sponsored (e.g., NIH, pharmaceutical company, oncology group)
- **your insurance company** (if third party payers are expected to pay for any procedure performed in the course of the research)
- **the Data Safety Monitoring Board** (if applicable) reviewing the safety of this study - name organization.
- **Stony Brook University's Committee on Research Involving Human Subjects, and/or applicable officials of SUNY-O, and/or the federal Office of Human Research Protections for the purpose of assessing compliance associated with the conduct of this study.**

*PI should add or delete as necessary (e.g., collaborating research sites, outside laboratories, cooperative study groups, CRO's, etc). Note that if an entity is not listed, that entity CANNOT legally access the subject's health information.*

**Use and disclosure of your health information will be necessary for an indefinite period of time.**

**You need to know that some of the individuals or groups referenced above are not obligated to protect the privacy of your IIHI. As an example, the sponsor, "Name of Sponsor", (if applicable: and 'Name of CRO, and the Data Safety Monitoring Committee) does not have the same obligation to protect your IIHI, and as such, the federal privacy laws no longer protect it from further disclosure.**

*If the grant/contract between the sponsor and the Research Foundation does address privacy issues, add such a statement here.*

*(if applicable): **Some IIHI that the investigators obtain about you will not be shared with you.** This includes (e.g., which study arm you are on, research blood test results etc...PI should add or delete as necessary). This information can be shared with you at the end of the study.*

**You have the right to revoke (withdraw) your authorization for the use or disclosure of your IIHI at any time in writing. If you revoke this authorization, you may no longer participate in this research activity. Revoking your authorization means that all access to, and collection of, your IIHI will be halted, unless the information concerns an adverse event (bad effect) you experienced related to the study. Your IIHI that was collected before you withdrew your authorization can continue to be used and reported.**

**When you sign the consent form at the end, it means that you have read this section and authorize the use and or disclosure of your individually identifiable health information in the manner explained above. Once available, to be distributed to the campus by April 14, 2003, and specifically for subjects who are patients of University Optometric Center, add **Your signature also means you have received a copy of SUNY-O's Notice of Privacy Practices.****

#### **Part V: Policy Violations**

SUNY-O faculty staff and students are obligated to report violations of this policy.

Such reports will be brought before IRB at a convened meeting. IRB will make a determination, in consultation with applicable University Officials, to assess whether additional information and/or further investigation is required. The affected departmental Chair and Dean will be copied on all correspondence between the committee and the involved parties. Where violations are apparent, the IRB chair, in consultation with applicable University Officials, may take immediate corrective action as deemed appropriate, prior to review by the full committee. In addition, other applicable University offices and/or external agencies (e.g., Office of Civil Rights) will be notified as required. **Note that health care providers who violate HIPAA may also be subject to significant criminal and civil penalties.**