Harvard Pilgrim Health Care, Inc.
Harvard Pilgrim Health Care Institute, LLC
Office of Sponsored Programs

Policy and Procedure

TITLE: Privacy and Confidentiality of Research Subject Information

---

PURPOSE:

To describe the Institutional Review Board (IRB) policy and procedure for ensuring that adequate provisions are in place for protecting the privacy and confidentiality of research subjects.

PERSONS AFFECTED:

This policy & procedure (P/P) applies to all Harvard Pilgrim Health Care, Inc. (HPHC) and Harvard Pilgrim Health Care Institute, LLC (HPHCI) (collectively, HPHC/I) personnel engaged in research, teaching or research administration activities in support of the charitable and educational mission of HPHC.

POLICY:

Privacy and confidentiality refer to equally important, yet distinct aspects of research. Criterion for the approval of research include adequate provisions to:

- protect the privacy interests of subjects; and
- maintain the confidentiality of identifiable data.

IRB members should understand the differences between privacy and confidentiality, how to apply these criteria, and shall evaluate whether research submitted for review satisfies these criteria.

Privacy refers to persons and their interest in controlling the access of others to themselves. Based on their privacy interests, people may want to control:

- the time and place where they give information;
- the nature of the information they give; and
- the nature of the experiences that are given to them.

Confidentiality refers to the maintenance of the agreement between the investigator and subject on how the subject's identifiable private information will be handled, managed, and disseminated. IRB members shall be knowledgeable about strategies to maintain confidentiality of identifiable data, including controls on storage, handling, and sharing of data.

Confidentiality provisions include information obtained preparatory-to-research before the study or grant proposal is submitted, for example information collected from records to determine potential sample size, as well as the maintenance of the confidentiality of information after the study has ended when identifiable information is maintained.

When appropriate, the IRB should also know how certificates of confidentiality (CoC) can be used to maintain the confidentiality of identifiable data. In cases where identifiable, sensitive information (such as illegal behavior and alcohol or drug use) is collected, a CoC may be automatically issued by the United States Department of Health and Human Services (DHHS) for National Institutes of Health (NIH) funded research projects. A CoC provides protection against legally compelled disclosure of identifying information about subjects of biomedical, behavioral, clinical, and other research.

When appropriate, the IRB should also be aware of other methods to protect confidentiality, such as inter-file linkage, error inoculation, top coding, bracketing and data brokering.

In addition, the IRB shall confirm that confidentiality procedures are explained to subjects. A description of how confidentiality is maintained allows subjects to decide how much of their personal information they are willing to provide. For studies where consent is sought, the IRB shall determine whether investigators appropriately inform subjects of the available confidentiality protections and the limits to these protections.

DEFINITIONS:
For the purposes of this policy:

De-Identified Data: information that neither identifies nor provides a reasonable basis to identify an individual.

Identifiable, Sensitive Information: information about an individual that is gathered or used during the course of biomedical, behavioral, clinical, or other research, where:

- an individual is identified; or
- there is at least a very small risk, that some combination of the information, a request for the information, and other available data sources could be used to deduce the identity of an individual.

Identifiable, sensitive information includes but is not limited to name, address, social security or other identifying number, and fingerprints, voiceprints, photographs, genetic information, tissue samples, or data fields that when used in combination with other information may lead to identification of an individual.

Individually Identifiable Health Information: information that is a subset of health information, including demographic information collected from an individual, and:

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

Limited Data Set (LDS): PHI from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed. A LDS may be used and disclosed for research, health care operations, and public health purposes, provided the recipient enters into a data use agreement (DUA) promising specified safeguards for the PHI within the limited data set.

Private Information: Information about behavior that occurs in a context which an individual can reasonably assume that no observation or recording is taking place and information provided by an individual for specific purposes, which he or she can reasonably expect will not be made public (e.g. medical records). Private information must be individually identifiable (i.e., the identity of the subject is or may readily be ascertained by the investigator or associated with the information) for obtaining the information to constitute research involving human subjects.

Protected Health Information (PHI): individually identifiable health information that is transmitted by or maintained in electronic media or transmitted or maintained in any other form or medium including identifiable demographic and other information relating to the past, present, or future physical or mental health or condition of an individual, or the provision or payment of health care to an individual that is created or received by a health care provider, health plan, or health care clearinghouse.

Sensitive Information: private information that relates to sexual attitudes, preferences or practices; use of or treatment for alcohol, drugs, or other addictive products; illegal conduct that may present a risk of criminal or civil liability; certain health information, including psychological or mental health; genetic health information; or information which if released could reasonably cause stigmatization or discrimination, or result in damage to areas as financial well-being, insurability, employability, or reputation.

PROCEDURE:

1. The PI must include in the Initial Application and other submission documents the following information that the IRB shall consider in order to assess whether there are adequate provisions in place that protect privacy and confidentiality of research subject information:
   a. type and nature of data collected, including, but not limited to, sensitive information and PHI;
   b. when and where the data is collected;
   c. potential risk of harm from unintended disclosure of the information;
   d. original purpose of the collected data;

e. data authentication and authorization, including data encryption, firewalls, and password protection;
f. data storage and transmission;
g. data sources, access and disclosure;
h. data use agreements;
i. other provisions for protecting the privacy and confidentiality of subjects, such as use of limited data sets, substituting codes for identifiers, de-identification, *etc.*;
j. measures for protecting the physical security and software security of the data; and
k. description of a contingency plan for dealing with any unauthorized use or disclosure of subject information.

2. The IRB shall evaluate the methods used to protect subjects' privacy by considering the potential subject population (i.e., vulnerable groups, language barriers, customs, cultural differences, *etc.).* When reviewing privacy concerns, the IRB shall also consider the sensitivity of identifiable information by evaluating whether disclosure of the information could have negative consequences to the subjects or damaging to the subject's reputation, financial standing, employability or insurability, or place subjects at risk of criminal or civil liability.

3. The IRB shall confirm that the investigators will obtain and release only the minimum necessary data to achieve research goals and that they have explained in their submission materials how/why the data they aim to collect or release meets the minimum necessary requirements.

4. Other considerations when evaluating privacy interests of subjects include:
   a. study titles - it is often best if the title of the study does not reveal sensitive information about subjects;
   b. email - subjects' employee email may not be secure and some personal accounts may be accessed by anyone in the family or household; and
   c. phone calls to subjects' homes - it may be appropriate to use script for calls so that no information is revealed about the caller or the subject to anyone other than the subject.

In some cases, it may be appropriate to remind subjects to prevent possible violations of their privacy in their homes by, for example, closing browsers after completing an online survey on a sensitive topic.

5. The IRB's intent is to ensure that subjects are informed about the extent to which confidentiality of their data will be maintained during all phases of the study, including who will have access to the data, what security measures will be used, and where data will be stored. Extensive security procedures may be needed in some studies, either to give individuals the confidence they need to participate and answer questions honestly, or to enable investigators to offer strong assurances of confidentiality. Complete confidentiality should not be promised, however, unless personal identifiers have not been obtained or recorded. Please see the *Policy and Procedure on Informed Consent.*

6. The IRB should be aware of the existence of other mechanisms to collect and maintain confidentiality of data, including:

a. coded information - code information by replacing identifying information of the individual with a number, letter, symbol, or some combination;
b. de-linked or anonymized data - data, originally collected with identifiers, which subsequently have been removed, are considered de-linked or anonymized; and
c. anonymous data - data originally collected without any identifiers where the data were never associated or linked to an individual. Wherever possible, confidentiality is best maintained by anonymous data collection.

7. *Use and Disclosure of Protected Health Information for Research*

Use or disclosure of PHI for research purposes is permitted if one of the following applies:

a. written authorization has been obtained from the research subject;
b. the IRB, which serves as the Research Privacy Board for HPHC, grants a waiver of authorization;
c. where HPHC/I is using or disclosing only data contained in a LDS and HPHC has entered into a DUA;
d. where HPHC/I is using or disclosing only de-identified data;
e. where the use involves an internal review of data preparatory-to-research (this use does not require IRB approval); or
f. where the research involves only decedents' information.

8. *Certificate of Confidentiality*

As per the 2017 NIH Certificates of Confidentiality Policy, all ongoing or new research funded by NIH as of December 13, 2016 that collects or uses identifiable, sensitive information is automatically issued a CoC. Compliance requirements are outlined in the NIH Grants Policy Statement, which is a term and condition of all NIH awards.
This includes research that:

a. meets the definition of human subjects research, including exempt research in which subjects can be identified;
b. is collecting or using human biospecimens that are identifiable or that have a risk of being identifiable;
c. involves the generation of individual level human genomic data; and
d. involves any other information that might identify a person.

This policy applies to NIH funded:

a. grants;
b. cooperative agreements;
c. R&D contracts;
d. other transaction awards; and
e. NIH's own intramural research.

Investigators with a CoC may only disclose identifiable, sensitive information in the following circumstances:

a. if required by other federal, state, or local laws, such as for reporting of communicable diseases;
b. if the subject consents; or

c. for the purposes of scientific research that is compliant with human subjects regulations.

In addition, investigators must ensure that anyone who is conducting research as a sub-awardee or who receives a copy of identifiable, sensitive information protected by the policy understands they are they are also subject to the disclosure restrictions, even if they are not funded directly by NIH.

9. For non-federally funded research, the NIH will continue to consider requests for CoCs for specific projects in accordance with the current NIH policy for issuing CoCs.

10. The investigator must identify the potential for compelled disclosure in the initial application and inform research subjects of the protections and limits to protections provided by the CoC, in studies which informed consent is sought. The CoC does not govern the voluntary disclosure of identifying characteristics of subjects by the investigator but only protects subjects from compelled disclosure. Investigators, therefore, are not prevented from the voluntary disclosure of matters such as child abuse or a subject's threatened harm to self or others. If an investigator intends to make such voluntary disclosures, however, the consent form shall clearly indicate this possibility to subjects. Please see the *Policy and Procedure on Informed Consent*.

REVISION HISTORY:

Department: OSP - Research Integrity & Compliance	**Title**: Privacy and Confidentiality of Research Subject Information
Effective Date: 01/21/19	**Owner:** Senior Compliance Manager, IRB
Replaces P/P Dated: IRB SOP (02/17)	
Related Documents: Initial Application; Initial Application - Data Health Information-Only Studies; Reviewer Sheet - Initial Review	
References: 45 CFR 46.102; 45 CFR 160.103; 45 CFR 46.111(a)(7); 21 CFR 50.3; 21 CFR 56.111(a)(7); OHRP IRB Guidebook 1993; Certificate of Confidentiality Policy (2017); AAHRPP Elements II.3.D. and II.3.E; AAHRPP Tip Sheets 1, 4, 5, & 20	