THE OHIO STATE UNIVERSITY

PRIVACY AND CONFIDENTIALITY

1. Overview

Federal regulations require that research involving human subjects includes adequate provisions to protect the privacy interests of participants and to maintain the confidentiality of data. This policy describes requirements for protecting privacy and confidentiality in research involving human subjects, including the use of National Institutes of Health (NIH) Certificates of Confidentiality.

2. Definitions

Privacy: The state of being free from the observation, intrusion, or attention of others.

Confidentiality: In the context of human subjects research, the condition that results when data are maintained in a way that prevents inadvertent or inappropriate disclosure of participants' identifiable information.

3. General Information

A. It is important to note the distinction between "privacy" and "confidentiality" in human subjects research. In general, **privacy** concerns are about the *people* involved in the research, whereas **confidentiality** issues are those associated with the *data* obtained for research purposes.

B. Provisions for protecting privacy and/or confidentiality are relevant at all stages of research, including subject identification and recruitment, research participation, and analysis of individually identifiable data. For additional information on protecting participant privacy during recruitment see HRPP policy [Recruiting Methods, Recruitment Materials, and Participant Compensation].

4. Protecting Privacy Interests

A. Research involving human subjects must include adequate provisions to protect subjects' privacy interests. Respect for potential participants' right to privacy requires consideration of their interests in having control over the extent, timing, and circumstances of sharing themselves (physically, behaviorally, or intellectually) with others. For example, individuals might not want to participate in a study that involves their being seen entering a building that might stigmatize them, such as a substance abuse counseling center, or to provide personal information during an interview conducted in a crowded place (e.g., clinic waiting room).

B. What is considered to be "private" depends on the individual and may vary based on age, gender, ethnicity, socioeconomic class, education level, verbal skills, health, legal status, personality, and the individual's relationship with the investigator. For example, protecting the privacy interests of a young child might mean having a parent present at a session with an investigator, while protecting the privacy interests of a teenager might

mean having the parent absent. Knowledge of the characteristics of the potential participant population is important in considering research methods that respect privacy.

C. In the context of research, concerns about possible "invasions of privacy" are primarily associated with methods used to obtain information about participants, such as by review of personally identifiable records. When evaluating potential privacy concerns raised by the use of identifiable private records, the following factors should be considered:

- The original purpose of the records
- Sensitivity of the information involved (e.g., medical vs. attendance records)
- Potential risk of harm from unintended disclosure of the information
- Whether the research requires access to the identifiable private information.

D. In considering the sensitivity of identifiable private information, investigators and IRBs should evaluate whether disclosure of the information could be embarrassing or damaging to the participants' reputation, financial standing, employability or insurability, or place participants at risk of criminal or civil liability.

E. Access to and/or use of identifiable patient information from medical records or clinical databases for research purposes must comply with the requirements of the HIPAA Privacy and Security Rules and university policy [e.g., University Hospital Policy 09-11: Use of Patient Information by Hospitals and Medical Staff].

F. The proposed use of student education records in research must comply with the requirements of the Family Educational and Rights Privacy Act (FERPA).

G. Information collected by observation of individuals can also raise concerns about possible invasions of privacy, particularly when the individuals are unaware that they are being observed and/or the behaviors are observed in "quasi-public" places where individuals have a reasonable expectation of privacy (e.g., a physician's waiting room). To minimize potential risks, observations should be recorded whenever possible in a manner that does not allow participants to be identified, either directly or through identifiers linked to them. When identifiers are necessary for the research, adequate provisions for maintaining the confidentiality of the data are required.

5. Maintaining Confidentiality

A. Research involving human subjects must include adequate provisions to maintain the confidentiality of research data. Maintaining confidentiality requires safeguarding the information that an individual has disclosed in a relationship of trust and with the expectation that it will not be disclosed to others without permission, except in ways that are consistent with the original disclosure. Confidentiality in the context of human subjects research also refers to the investigator's agreement with participants, when applicable (i.e., through participants' informed consent), about how their identifiable private information will be handled, managed, and disseminated.

B. Provisions for maintaining the confidentiality of data are necessary for most research studies. However, in some types of research, such as in oral history or ethnographic

research, individuals may wish to be acknowledged for their research participation. In determining the extent to which confidentiality will be maintained, the nature of the information collected and expectations of potential research participants should be considered.

C. Methods for keeping data confidential range from using routine precautions, such as substituting codes for participant identifiers and storing data in locked cabinets, to more elaborate procedures involving statistical methods (e.g., error inoculation), data encryption, or use of honest brokers. The method(s) selected depends on the nature of the information collected and potential risk to participants from a breach of confidentiality. Consideration should be given to requirements for data security and retention throughout and following completion of the study. Methods for handling and storing data (including the use of personal computers and portable storage devices) must comply with university policies. Restricted data, including protected health information, must be encrypted if stored or used on portable devices, if removed from a secure university location, or if electronically transmitted. For more information, see [Policy on Institutional Data] and [Research Data Policy].

D. Individuals are to be 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 researchers to offer strong assurances of confidentiality. Complete confidentiality should not be promised, however, unless personal identifiers have not been obtained or recorded.

E. Keeping the identities of participants confidential may be as important (or more important) than keeping the data obtained from/about them confidential, especially in studies where individuals are selected because of a sensitive, stigmatizing, or illegal characteristic (e.g., persons who have sought treatment in a drug abuse program, tested positive for HIV, or have engaged in underage alcohol use). Additional measures to safeguard confidentiality may be considered in such cases, such as a waiver of documentation of consent (i.e., to minimize the risk of breach of confidentiality from having a signed form linking the participant with the research). For more information on waiver of the requirement for documenting informed consent see HRPP policy [Documentation of the Informed Consent Process]. NIH Certificates of Confidentiality may also be used in certain situations to provide additional protections (see below).

6. NIH Certificates of Confidentiality

A. Certificates of Confidentiality are issued by NIH to protect the confidentiality of research data. These certificates are used to resist attempts to force disclosure (e.g., by subpoena) of sensitive information, allowing investigators and others who have access to research records to refuse to disclose the identifiable information of research participants in any civil, criminal, administrative, legislative, or other proceeding at the federal, state, or local level. Certificates of Confidentiality, however, do not eliminate the need for investigators and IRBs to assure that appropriate data security measures are in place to protect research participants' identifiable information.

B. Certificates of Confidentiality are not limited to federally funded research. They may be requested for any biomedical, behavioral, or other type of research involving sensitive information. NIH defines "sensitive" to mean that disclosure of the identifying information could have adverse consequences for participants or be damaging to their financial standing, employability, insurability, or reputation. Examples of sensitive information include, but are not limited to, information about the following:

- Genetics
- Psychological well-being of participants
- Participants' sexual attitudes, preferences, or practices
- Substance abuse or other illegal risk behaviors
- Litigation related to exposures under study (e.g., breast implants, environmental or occupational exposures).

C. Not all activities are eligible for a Certificate of Confidentiality. To be eligible, an activity must meet all of the following criteria:

- Defined as research involving human subjects
- Involves collection of personally identifiable information
- Has been reviewed and approved by an IRB
- Involves collection of information that if disclosed would significantly harm the participant.

D. Participants must be informed about the protections provided by a Certificate of Confidentiality and any exceptions to these protections. Informed consent documents should describe the protections and any limitations of a Certificate, including voluntary disclosures by research participants (e.g., to physicians), releases of information authorized in writing by participants (e.g., to insurers), and voluntary disclosures made by investigators (described below). For template language describing Certificates of Confidentiality, see Consent Template Language by Topic.

E. A Certificate of Confidentiality does not prevent an investigator from voluntarily disclosing sensitive information. For example, Certificates of Confidentiality cannot be used to protect research participants from disclosures of their sensitive information, such as evidence of child abuse, threats of violence to self or others, reasonable knowledge that a felony has been (or is being) committed, or reportable communicable diseases, by investigators who are subject to mandatory reporting requirements under Ohio law. An investigator's intention to report such (or other) information must be specified in the consent form.

F. For more information on Certificates of Confidentiality see the National Institutes of Health "Certificates of Confidentiality Kiosk."

7. Applicable Regulations/Guidance

21 CFR 56.111, 45 CFR 46.111, OHRP Institutional Review Board Guidebook: "Privacy and Confidentiality" (1993), The Ohio State University "Policy on Institutional Data" (08/15/14), The Ohio State University "Research Data Policy" (09/18/09), NIH Certificates of

Confidentiality Kiosk, University Hospital Policy 09-11: “Use of Patient Information by Hospitals and Medical Staff” (04/07/08)

8. History

Issued: 09/15/2008
Revised: 04/28/2009, 05/25/2012, 02/13/2013, 09/19/2016
Edited: 01/07/2010