| CAMPBELL UNIVERSITY | **IRB SOP Investigator:** Privacy and Confidentiality | | |
|---|---|---|---|
| | NUMBER | APPROVED BY | EFFECTIVE DATE |
| | HSR-340 | Miranda van Tilburg, PhD<br>IRB Chair, IRB Office Campbell University | 12/02/2020 |

**Applies to** Campbell faculty, faculty advisors, students and staff conducting or overseeing human subjects research.

## Purpose

All research involving human research subjects or the use of information about human research subjects should be planned and conducted in a manner that protects the privacy interests of the research subjects and the confidentiality of any personal information about the research subject.

## Background

In its review of research proposals, the Campbell IRB will require that all reasonable measures be taken to protect the privacy of research subjects and the confidentiality of information relating to research subjects.

## Definitions

**Covered Entity:** is define as:

- A healthcare plan;
- A healthcare clearing house;
- A health care provider who transmits any health information in electronic form in connection with a transaction covered by the provisions of the Privacy Regulation.

**Confidentiality:** refers to the treatment that must be afforded to individually identifiable information about research subjects or potential research subjects. Confidential treatment of information in the context of research is required for all non-public information that has been disclosed by or about research subjects to researchers with the expectation that it will not be disclosed to others without permission.

**Privacy:** an individual's rights to be free from unauthorized or unreasonable intrusion into his/her private life and the right to control access to individually identifiable information about him/her. The term "privacy" concerns research subjects or potential research subjects as individuals.

**Protected Health Information (PHI):** Any individually identifiable health information, whether oral, written, electronic, transmitted, or maintained in any other form or medium that:

- Is created or received by a health care provider such as the Campbell University Health Center, a health plan, or a health care clearinghouse; and
- Relates to an individual's past, present, or future physical or mental health condition, health care treatment, or the past, present or future payment for health care services to the individual;
- That either identifies an individual (for example, name, social security number or medical record number) or can reasonably be used to find out the person's identity (address, telephone number, birth date, e-mail address, and names of relatives or employers).

**Identifiable Private Information:** means information about a living individual that is used for research purposes and includes information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information that has been provided for specific purposes by an individual and that the individual can reasonably expect will not be made public (e.g., a medical record). Under the OHRP regulations, identifiable private information must be individually identifiable (i.e., the identity of the research subject is or may readily be ascertained by the investigator or associated with the information) in order for the project to constitute research involving human subjects.

**Individually Identifiable Information (health care):** is a subset of health information, including demographic information collected from an individual, and:

- Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- 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
- That identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

**Personal Identifying Information (PII)) (FERPA):** includes but is not limited to a student's name and other direct personal identifiers, such as the student's social security or student number and at Campbell University this includes the student's email address. Directory information is not considered PII.

## Principal Investigator Responsibilities and Procedures

- The Principal Investigator (PI) is responsible for designing and conducting research studies that protect to the fullest extent possible both the privacy of the individuals who are potential or actual research subjects in research involving human subjects as well as the confidentiality of identifiable private information and individually identifiable health care information about such individuals.
- The PI is responsible for providing a detailed plan to the IRB regarding privacy and confidentiality. The plan should include, but is not limited to, the following:
    - Recruitment methods, identification processes, and approach plan of potential subjects for a research project
    - Data storage details (for data collected prior to recruitment, during recruitment, and after enrollment)
    - How a research subject's identifiable PHI or PII is being accessed?
    - Methods used to transmit and code or de-identify the research data
    - Length of research data storage
    - Timeline and manner of destruction of research data

- If obtaining the Social Security Numbers (SSN) of research subjects, the PI's plan for protecting privacy and confidentiality must also include the following information, at a minimum:
    - Justification for obtaining Social Security numbers
    - A statement in the Informed Consent document or other documents provided to research subjects explaining how SSN will be used such as in long-term follow-up for survival or for compensation
    - Whether Social Security numbers will be shared with parties outside of the institution
    - The method in which Social Security numbers will be stored
    - When and how Social Security numbers will be destroyed

The names of research subjects, Social Security numbers, and payments should be kept in a secure place separate from the research data, subject files, and source documents. A subject's Social Security number should not be used as an identifier on data collection forms.

**Privacy (Investigator Responsibilities when Interacting with Potential or Actual Research Subjects)**

- The Campbell IRB defines **privacy** as an individual's right to be free from unauthorized or unreasonable intrusion into his/her private life and the right to control access to individually identifiable information about him/her.
- PIs must describe their recruitment methods, identification processes and approach to potential subjects for a research project in their *IRB New Protocol Submission Form and Research Plan* at the time of initial submission. For more information regarding recruitment methods, see **Recruitment Methods and Compensation**. Investigators should be mindful with regard to these activities to ensure and protect a potential research subject's privacy. Examples include the following:
    - **Approach to Research Subjects:** The investigator should be mindful when approaching research subjects, taking into consideration such elements as conducting the approach in a private room if possible, time from diagnosis, and who to include in the approach if the subject is part of a vulnerable population.
    - **Minimizing the appearance of coercion:** The PI should stress the voluntary nature of participation and whenever possible, avoid the use of his/her own patients, clients, employees, and students. PIs should solicit research subjects through methods such as bulletin board notices, advertisements in newspapers, websites, and announcements in classes other than his/her own.

**Confidentiality (Principal Investigator Responsibilities when Handling the Data of Potential or Actual Research Subjects**

The Campbell IRB defines **confidentiality** as the activities or process used to store and share individually identifiable information that protects its unauthorized release.

PIs must describe their plans to store the research data, the methods used to code or de-identify data, the length of storage and when the data will be destroyed for a research project in their IRB initial submission. Examples include the following:

- **Identification of Research Subjects:** Research data should be at a minimum coded to ensure the confidentiality of subjects. PIs should also be mindful when reporting on their research and to ensure that all data reported in papers, abstracts, etc. does not include any identifiable information by which either the investigator may identify the subject or the subject may identify themselves. At the end of the project or at an earlier opportunity, it is recommended that the Investigator destroy the key code and effectively de-identify the data.
- **Storage of Research Data:** Project data should be stored in a manner consistent with project procedures such as password-protected computers, password-protected spreadsheets and/or databased with limited accessibility, locked filing cabinets, and /or locked offices. Data can be stored either on Campbell Owned computers on Campbell premises (not laptops) or on Egnyte. If storing in Egnyte, no one other than the investigative team, should have access to the folder with the data. The IRB offers Egnyte files, created and maintained by the IRB for the storage of research information as well.
- **Length of storage of research data:** The IRB requires original source documentation be maintained for 3 years following the completion of the research activities and to be readily accessible for review. Research materials containing HIPAA covered information must be maintained for 6 years following the completion of the research activities. For FDA regulated studies, Investigators review and follow the required length of storage as described in the protocol.

**Studies of illegal, sensitive, or socially or politically unacceptable activities**

For PIs and studies proposing to collect sensitive information as defined in this document, which if disclosed, could have negative consequences for research subjects in relation to their financial status, employability, insurability or reputation, it is vital to have the appropriate safeguards and protection mechanisms in place to minimize the risk of disclosure.

- **Certificates of Confidentiality (COC):** A Certificate of Confidentiality (CoC) is a tool for protecting certain information from forced or compelled disclosure, e.g., to oppose a subpoena. Effective Oct 1, 2017, NIH automatically issues CoCs to all research funded by NIH that is collecting or using identifiable, sensitive information. The new disclosure rules apply to everyone. For additional information, see the NIH website regarding Certificates of Confidentiality. Note that a Certificate of Confidentiality does not protect information as it relates to the North Carolina State mandate or the University policy to report child abuse and neglect.

  The National Institute of Justice requires a Privacy Certificate if you are working with prisoners. The NIJ Privacy Certificate guidelines can be found at: http://www.nij.gov/funding/humansubjects/pages/privacy-certificate-guidance.aspx.

The Privacy Certificate is not the same as a Certificate of Confidentiality and it is important to complete the application to comply with the confidentiality regulations found in 28 CFR Part 22.

If you have a Certificate of Confidentiality or a Privacy Certificate, the IRB will consider that information as part of its review.

- **If a Certificate of Confidentiality (COC) is not available:** The research subject should be informed of the possibility of disclosure or a breach of confidentiality in the consent form. In addition, some research, especially where illegal, sensitive, or socially or politically unacceptable activities are being researched, the protection of research subjects' rights may be enhanced by an assurance from the investigator that the written report will not be disseminated in any form until the research subjects have had an opportunity to read and modify the portions that relate to them. To the extent permissible under applicable law, such an assurance should be included in the consent form.

**Research Data Collection Tools (Records, Photographs, Questionnaires, Surveys, Videotapes, Audiotapes, Other Image Types)**

- A description of the tools to be utilized should be provided to the research subject. Research subjects should be informed (in a consent document) of their right to refuse to answer any questions and should be given an estimate of the length of time needed to complete the activity.

All use of records, photographs, videotapes, audiotapes, and other image types to be made or to be used for the research project must be described in the informed consent document for the research subject. The informed consent document should also describe the use of the materials and describe provisions for erasure or destruction if requested by the research subjects. If part of an image, video or audio will be used for educational or presentation purposes, this must be pre-approved by the IRB and included in the informed consent. Research participants should be provided the option to agree or not agree to this use. No photos/video/recording can be released that contains identifiable features (e.g. pictures of a patient's face or tattoos) or other description of unique traits that might make it possible for others to identify the research subject.

**Health Insurance Portability and Accountability Act (HIPAA)**

- PIs who plan to use or collect protected health information (PHI) for anything other than treatment, payment or healthcare operations may be required to obtain authorization from the research subject. PIs must follow appropriate covered identities policies and procedures with regards to authorized access to PHI and medical records. PIs must obtain IRB approval and/or approval from the IRB/Privacy Board of the appropriate covered entity to access this information.

- PIs should identify the type of records and PHI to be accessed and used for the research project. This information should be described in the Informed Consent document in the Permission to Collect, Use and Share Personal Health Information section.
- For some cases and types of data, a waiver of HIPAA authorization may be approved under HIPAA regulations by the IRB/Privacy Board or the IRB/Privacy Board may allow access via other HIPAA pathways. Examples include the following:
    - **Waiver of HIPAA authorization for recruitment/identification purposes:** PIs who wish to access medical records or charts with authorization from potential subjects to assist in the identification of potential research subjects must apply for a Waiver of HIPAA authorization for this research activity. PIs are required to keep a log of each medical record accessed for research purposes under this waiver and all other waivers of authorization.
    - **Limited Data Sets:** HIPAA regulations define what identifiers may be included with these types of data sets Limited Data Sets often are accessed or obtained by an Investigator once they completed a Limited Data Set Agreement with the holder of the data. If an Investigator is using a Limited Data Set for their research, they must identify it in the IRB initial submission or IRB amendment submission and upload the agreement.
    - **Decedents:** If the PI's research will involve the review of records of only deceased individuals, and no living subjects will be contacted or have their information accessed or utilized; the Investigator should indicate this in the IRB initial submission.
- If in the course of research, the PI determines there has been a potential violation of HIPAA (unauthorized access of PHI) or a data breach, PIs must report those events promptly to the IRB and other Institutional Officers, if applicable.

**Other Federal Agency Requirements**

Several Federal Agencies have additional requirements to ensure the protection of human subjects for projects being funded or conducted under their oversight.

- For National Institute of Justice (NIJ) funded research:
    - All projects are required to have a Privacy Certificate approved by the NIH Human Subjects Protection Officer.
    - All researchers and research staff are required to sign employee confidentiality statements, which are maintained by the responsible researcher.
    - The confidentiality statement on the consent form must state that confidentiality can only be broken if the subject reports immediate harm to subjects or others.
    - Under a privacy certificate, researchers and research staff do not have to report child abuse unless the subject signs another consent form to allow child abuse reporting.
    - A copy of all the data must be de-identified and sent to the National Archive of Criminal Justice Data, including copies of the informed consent document, data collection instruments, surveys or other relevant research materials.

- For research under U.S. Department of Education requirements, Investigators must work within the requirements set forth by the U.S. Department of Education, specifically the requirements of the Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendment (PPRA).

**Mandated reporting of child abuse**

All University employees (including all faculty, staff, and student employees) regardless of their position or assignment, by law (under the NC Law, NSGS 7B-301) have a duty to report suspected cases of child abuse and/or neglect. All students, volunteers, and third-party contractors who are engaged in research activities are required by University policy to report suspected cases of child abuse and/or neglect.

University employees are not mandated reporters in North Carolina of elderly abuse, neglect, or exploitation. However, it is possible that during the conduct of research you will encounter a circumstance in which an elderly participant in your research reports abuse, neglect, or exploitation. While there is no University policy that requires reporting, you may decide it is your ethical duty to make a report in good faith to the appropriate County Department of Social Services. By law, anyone making an elder abuse report in good faith has civil and criminal immunity from liability and professional disciplinary action.

**Conducting Research Using Genetic Information**

The Genetic Information Nondiscrimination Act of 2008 (GINA) prohibits discrimination in health coverage and employment based on genetic information. If you conduct research using genetic information, you are responsible for becoming familiar with the provisions of the law, both to implement measures to protect that information from inappropriate disclosures and to inform potential research participants about their rights under the law.

Recommended GINA language is available by contacting the IRB Office.

## References

45 CFR Parts 160 and 164
NSGS 7B-301
IRB New Protocol Submission Form
Research Plan Template
IRB Guidance: Research Plan