MCW Office of Research
Standard Operating Procedure

PRIVACY AND CONFIDENTIALITY

Unit: Human Research Protections Program (HRPP), Office of Research

Applies to: Faculty and Staff involved in human research

PURPOSE:
It is the policy of Medical College of Wisconsin (MCW) that all research involving human research subjects or the use of information about human research subjects 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 subjects.

In its review of research proposals, the MCW Institutional Review Board (IRB) will require that reasonable measures be taken to protect the privacy of research subjects and the confidentiality of information relating to research subjects.

DEFINITIONS:
Covered Entity*:* MCW Corporate Policies (AD.HP.010) define a covered entity as:

- A health plan.
- A health care clearinghouse.
- 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 Medical College of Wisconsin, 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): MCW Corporate Policies (AD.HP.010) defines this as Information that 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.

Sensitive Information: means identifiable private information or individually identifiable health care information relating to an individual's private activities or practices. Examples include: sexual preferences or practices; history of treatment for use/abuse of alcohol or drugs; information relating to a person's mental health history or treatment for mental illness or disease; HIV status; financial information such as social security numbers or private health insurance; or criminal history or background.

HIPAA: means the federal law known as the Health Insurance Portability and Accountability Act that regulates, among other things, the disclosure of protected health information ("PHI") about patients treated by most health care providers and organizations in the United States ("Covered Entities"). In the context of human subject research, HIPAA establishes a federal standard for the manner in which the confidentiality of **PHI** will be maintained by Covered Entities and prescribes a process through which researchers can obtain **PHI** about patients who are sought by researchers to be research subjects or potential research subjects.

POLICY:

Investigator Responsibilities for the IRB Application

- The investigator is responsible for designing and conducting research projects that protect both the privacy of the individuals who are potential or actual research subjects as well as the confidentiality of identifiable private information and individually identifiable health care information about such individuals.
- The investigator 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 is being accessed
    - Methods used to transmit and code or de-identify the research data
    - Length of research data storage
    - Timeline for destruction of research data
- If obtaining the Social Security numbers of research subjects, the Investigator'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

- 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.

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

The investigator should be mindful when approaching research subjects, taking into consideration such elements as conducting the approach in a private room, time from diagnosis, and who to include in the approach if the subject is part of a vulnerable population. The investigator should stress the voluntary nature of participation and whenever possible, avoid the use of his/her own patients, clients, employees, and students. For additional information regarding privacy when interacting with potential research subjects, see *IRB SOP: Recruitment Methods and Compensation*.

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

- The Investigator should store project data in a manner consistent with project procedures and institutional requirements, such as password-protected computers, jump/USB drives, password-protected spreadsheets and/or databases with limited accessibility, locked filing cabinets, and/or locked offices.
- When proposing to collect sensitive information that, if disclosed, could have negative consequences for research subjects (in relation to their financial status, employability, insurability or reputation), the Investigator must have the appropriate safeguards and protection mechanisms in place to minimize the risk of disclosure.
    - **Certificates of Confidentiality (COC)**: COCs protect the privacy of research subjects by prohibiting disclosure of identifiable, sensitive research information to anyone not connected to the research except when the subject consents or in a few other specific situations. NIH funded researchers are automatically issued a COC through their award. Other Department of Health and Human Services (HHS) agencies issue COCs to researchers they fund. Researchers not funded by HHS can continue to apply to NIH or the FDA as appropriate to request a COC for HHS-mission relevant research. The use of a COC allows the investigator to withhold the names of research subjects from all persons not connected with the conduct of the research. Investigators, who have a COC, generally cannot be compelled to identify research subjects in any Federal, State, or local civil, criminal, administrative, or legislative proceedings.
    - **If a Certificate of Confidentiality (COC) is not available:** The Investigator should inform the research subject of the possibility of disclosure or a breach of confidentiality in the consent form. In addition, during 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.
- Investigators should be mindful when reporting on their research to ensure that all data reported in papers, abstracts, etc. do not include any identifiable information by which either the investigator may identify the subject or the subject may identify themselves.

Health Insurance Portability and Accountability Act (HIPAA)

- Investigators 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. Investigators must follow both MCW Corporate and Froedtert Hospital Corporate Policies and Procedures with regard to authorized access to PHI and medical records. Investigators must obtain IRB approval and/or approval from the Privacy Board to access this information. The MCW IRBs function as Privacy Boards for MCW and FH per 46 CFR 160 and 164. The IRB will include information in the IRB approval letter regarding the IRB's HIPAA determination for the project.
- Investigators should identify the type of records and PHI to be accessed, and used for the research project. This information should be described in the *Permission to Collect, Use and Share Health Information* section of the consent form.
- 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:** Investigators who wish to access medical records or charts without 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. Investigators 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 have 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 eBridge initial submission or eBridge amendment submission and upload the agreement.
    - **Decedents:** If the Investigator'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; then the Investigator should indicate this in the eBridge initial submission.
- If in the course of research, the Investigator determines there has been a potential violation of HIPAA (unauthorized access of PHI) or a data breach, Investigators must report those events promptly to the IRB and MCW Corporate Compliance Office as described in *MCW Guidance: Process for Reporting Potential HIPAA violations and/or Data Breach.*

Requirements of other Federal Agencies:

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 NIJ 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 conducted with the Bureau of Prisons:

- A non-employee of the Bureau may receive records in a form not individually identifiable when advance adequate written assurance that the record will be used solely as a statistical research or reporting record is provided to the agency.
- Except as noted in the consent statement to the subject, the researcher must not provide research information that identifies a subject to any person without that subject's prior written consent to release the information. For example, research information identifiable to a particular individual cannot be admitted as evidence or used for any purpose in any action, suit, or other judicial, administrative, or legislative proceeding without the written consent of the individual to whom the data pertain.
- Except for computerized data records maintained at an official Department of Justice site, records that contain non-disclosable information directly traceable to a specific person may not be stored in, or introduced into, an electronic retrieval system.
- If the researcher is conducting a project of special interest to the NIJ Office of Research and Evaluation (ORE) but the project is not a joint project involving ORE, the researcher may be asked to provide ORE with the computerized research data, not identifiable to individual subjects, accompanied by detailed documentation. These arrangements must be negotiated prior to the beginning of the data collection phase of the project.
- At least once a year, the Investigator shall provide the chief, Office of Research and Evaluation (BoP) with a report on the progress of the research .
- At least 12 working days before any report of findings is to be released, the researcher shall distribute one copy of the report to each of the following: the chairperson of the Bureau Research Review Board, the regional director, and the warden of each institution that provided data or assistance. The researcher shall include an abstract in the report of findings.
- In any publication of results, the researcher shall acknowledge the Bureau's participation in the research project.
- The researcher shall expressly disclaim approval or endorsement of the published material as an expression of the policies or views of the Bureau.
- Prior to submitting for publication the results of a research project conducted under this subpart, the researcher shall provide two copies of the material, for informational purposes only, to the Chief, Office of Research and Evaluation, Central Office, Bureau of Prisons.

- 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).

REFERENCES:
45 CFR Parts 160 and 164

SUPPORTING DOCUMENTS:
MCW Corporate Policy: HIPAA Privacy Definitions (AD.HP.010)
IRB SOP: Recruitment Methods and Compensation
MCW Guidance: Process for Reporting Potential HIPAA violations and/or Data Breach
MCW Informed Consent Templates

Effective Date:	06/15/2018
Version number:	4.0
Previous Version/date:	3.0, 07/24/2015
Responsible Office:	HRPP Office
Approval Date:	06/07/2018

Approved By
HRPP Authorized Official: David Clark, PhD, Director, HRPP
Human Research Protections Program (HRPP)
Office of Research
Medical College of Wisconsin