# MCW IRB Committee Procedures

## PRIVACY AND CONFIDENTIALITY

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

Applies to: Institutional Review Board Committees

**PURPOSE:**
The MCW Institutional Review Board (IRB) must review, evaluate and require that all reasonable measures be taken to protect the privacy of research subjects and the confidentiality of information relating to research subjects prior to granting IRB approval.

The MCW IRB also serves as the privacy board for MCW, Froedtert Health (FH), Versiti and Children's Wisconsin (CW). The MCW IRB is charged with review of human subject research submissions to ensure protection of the research subjects and prospective research subjects privacy and confidentiality of the research data in accordance with federal regulations and that the requirements of the HIPAA Privacy Rule are met.

**DEFINITIONS:**
**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.

**Covered Entity:** *Per MCW Corporate SOP: HIPAA Privacy Definitions (AD.HP.010*) a covered entity is a health plan, or a health care clearinghouse, or 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.

**HIPAA:** the acronym for the federal law called the Health Insurance Portability and Accountability Act. This federal law 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.

**Private Information:** defined by the HHS Protection of Human Subjects Regulations as 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 HHS Protection of Human Subjects Regulations, 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 to obtain the information to constitute research involving human subjects unless the data are obtained through intervention or interaction with the individual.

**Individually Identifiable Information (health care):** *Per MCW Corporate SOP: HIPAA Privacy Definitions (AD.HP.010*), this is information that is a subset of health information, including demographic information collected from an individual, and:

1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
2. 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
    a. That identifies the individual; or
    b. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

**Privacy:** an individual's right to be free from unauthorized or unreasonable intrusion into their private life and the right to control access to individually identifiable information about themselves.

**Privacy Board:** defined by the Department of Health and Human Services as "A review body that may be established to act upon requests for a waiver or an alteration of the Authorization requirement under the Privacy Rule for uses and disclosures of PHI for a particular research project. A Privacy Board may waive or alter all or part of the Authorization requirements for a specified research project or protocol.

- A covered entity may use and disclose PHI, without an Authorization, or with an altered Authorization, if it receives the proper documentation of approval of such alteration or waiver from a Privacy Board."

**Protected Health Information (PHI):** *Per MCW Corporate SOP: HIPAA Privacy Definitions (AD.HP.010*) any individually identifiable health information that is:

1. Transmitted by electronic media
2. Maintained in electronic media;
3. Transmitted or maintained in any other form

Protected Health information excludes individually identifiable information that is in:

1. Education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended 20 U.S.C. 1232g
2. Records described at 20 U.S.C. 1232g(a)(4)(B)(iv)
3. Employment records held by a covered entity in its role as an employer, and
4. regarding a person who has been deceased for more than 50 years

**Sensitive Information:** means identifiable private information or individually identifiable health care information relating to an individual's private activities or practices which, if compromised, could cause harm to the individual. $RS.GN.080$Examples include personally identifiable medical information and is not limited to 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.

**PROCEDURE:**

**IRB Review Process**

1. The MCW IRB is responsible for assessing the degree to which a human subject research project has been designed to adequately address privacy and confidentiality issues.
2. Where necessary or appropriate, the IRB will require that Investigators modify the design of the research project or the recruitment process and enrollment procedures to satisfy any inadequacies identified by the IRB in relation to the protection of the privacy of research subjects and the confidentiality of identifiable private, sensitive or individually identifiable health care information of potential or actual research subjects.

3. The MCW IRB will consider issues of privacy and confidentiality when reviewing information in the eBridge SmartForm and supporting documentation. Necessary specific protections will depend on the nature of the research and the risks involved.
4. IRB members must evaluate whether the proposed plan for recruitment and consent, conduct and documentation of the research, and data storage includes adequate safeguards to protect the prospective and enrolled research participants privacy and confidentiality. Consideration should be given to the proposed plans for the following activities:
    a. **Recruitment/Consenting Process**, To approve research, the IRB must determine there are adequate provisions to protect the privacy interests of prospective and enrolled research participants. See *IRB Member SOP: Advertisements, Recruitment Methods, and Compensation*
    b. **Identification of Research Subjects:** Research data should be at a minimum coded to ensure the confidentiality of subjects and whenever possible store the code key separately from the research records. At the end of the project or an earlier opportunity, it is recommended that the Investigator destroy the key code and effectively de-identify the data.
    c. **Data Collection and the tools used for collecting data**, Research project is designed to limit the data collected to the minimum amount of data necessary to accomplish the research purpose.
    d. **Storage of research data** which includes but is not limited to password-protected computers, encrypted portable electronic devices, use of encryption codes for data, password-protected spreadsheets and/or databases with limited accessibility, locked filing cabinets, and/or locked offices. For federal funded research, teams should describe where research data will be stored such as a NIH data repository, level of identification and who may have access to the data. Electronic storage of data may be maintained in the following cloud-based storage options Box or OneDrive for MCW.
    e. **Transmission of research data** Adequate provisions should be in place when electronically transmitting identifiable or coded research data to another party outside of the MCW, FH, CW and/or Versiti firewall. Research data should only be transmitted when the security of the recipient's system is known and appropriate institutional agreements are in place such as Data Use Agreements. Considerations include use of a secure data transmission channel, and transmission of encrypted data. Examples include Secure Socket Layers (SSL), HTTPS or Secure File Transfer Protocol (SFTP), and Secure Zip,
    f. **Long term storage of research data:** The *MCW Corporate Policy: Ownership, Access and Integrity of Research Data (RS.GN.070)* states that records should be stored for a period of at least 10 years after the project has been completed. For Food and Drug Administration (FDA) regulated projects, Investigators should review and follow the required length of storage as described in the protocol.
5. Any changes in confidentiality protections must be reported to the IRB.
6. The assigned IRB reviewer will review the submission and complete the appropriate IRB reviewer checklist to determine if the submission meets the regulatory criteria for approval which includes ensuring privacy and confidentiality.

**Research related activities that require additional considerations for privacy and confidentiality**

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

1. When reviewing projects proposing to collect sensitive information as defined in this procedure that if disclosed could have negative consequences for research subjects in relation to their financial status, employability, insurability or reputation, it is vital for IRB reviewers to determine if the appropriate safeguards and protection mechanisms in place to minimize the risk of disclosure.

a. **Certificates of Confidentiality (COC)**: NIH funded researchers are automatically issued a COC through their award for research that is collecting or using identifiable, sensitive information. 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 the research. The use of a COC allows the investigator to withhold the names of research subjects from all persons not connected with the performance 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.
b. **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.

**Use of Social Security Numbers (SSN)**
**Collection and use of Social Security Numbers for the human subject research may be required in two situations: individual stipend payments or long term survival data such as the SSN Death Index.**

1. In accordance with *MCW Corporate Policy: Business Purchases, Payments and Reimbursements* (BF.PA.010) and *Office of Research SOP: Subject Payments for Research Participation*, a research subject's Social Security Number may be required based on the payment type and total amount of compensation.
    a. Social Security numbers should be obtained from all research subjects who may receive monetary compensation for participation in a research project.
    b. The consent form should include a statement that the MCW Finance Department requires this information.
    c. 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.
2. If obtaining research subjects' Social Security numbers is an essential part of the project design, the Investigator must provide the following information to the IRB
    a. Justification for obtaining Social Security numbers
    b. 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
    c. Whether Social Security numbers will be shared with parties outside of the institution
    d. The method in which Social Security numbers will be stored
    e. When and how Social Security numbers will be destroyed
    f. The Social Security number should not be used as an identifier on data collection forms.

**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.

1. For National Institute of Justice (NIJ) funded research:
    a. All projects are required to have a Privacy Certificate approved by the NIJ Human Subjects Protection Officer.
    b. All researchers and research staff are required to sign employee confidentiality statements, which are maintained by the responsible researcher.
    c. 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.

d. 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.

2. For research conducted with the Bureau of Prisons:
   a. 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.
   b. 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.
   c. 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.
   d. If the researcher is conducting a project of special interest to the 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.
3. For Department of Energy (DOE) funded research:
   a. IRB review to ensure that research protocols submitted to IRB for review comply with the DOE requirements for protecting personally identifiable information. http://science.energy.gov/ber/human-subjects/regulations-and-requirements/doe-special-requirements/#ProitectionofData

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

1. The MCW IRB Committees serve as the research privacy board for MCW, FH, CW and Versiti Investigators who plan to use or collect PHI for anything other than treatment, payment or healthcare operations may be required to obtain authorization from the research subject. Investigators must follow the MCW Corporate Policies, Froedtert Hospital Corporate Policies, Versiti Corporate Policies, Children's Wisconsin Corporate Policies and MCW HRPP procedures about authorized access to PHI and medical records and must obtain review and approval for their use.
2. IRB reviewers should evaluate the type of records and PHI to be accessed and used for the research project as described in the initial eBridge submission. This information should be described in the project's proposed informed consent form, if applicable.
   a. The *MCW Informed Consent* Templates include authorization language in the Permission to Collect, Use and Share Health Information section.
3. 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:
   a. Waiver of HIPAA authorization for recruitment/identification purposes;
   b. Limited Data Sets;
   c. Decedents
4. The IRB will include information in the IRB approval letter indicating if the IRB has approved a waiver of HIPAA authorization, and/or an approved consent form and HIPAA authorization form for use in the project.

**REFERENCES:**

20 U.S.C. 1232g
20 U.S.C. 1232g(a)(4)(B)(iv)

**SUPPORTING DOCUMENTS:**

*MCW Corporate Policy: HIPAA Privacy Definitions (AD.HP.010)*
*MCW Corporate Policy: Business Purchases, Payments and Reimbursements (BF.PA.010)*
*MCW Corporate Policy: External Sharing and Privacy of Research Data (RS.GN.080)*
*MCW Corporate Policy: Ownership, Access and Integrity of Research Data (RS.GN.070)*
*MCW Corporate Policy: Research Involving Human Subjects and/or their Private Identifiable Information (RS.HS.010)*
*Office of Research SOP: Subject Payments for Research Participation*
*IRB Member SOP: Advertisements, Recruitment Methods and Compensation*
MCW Informed Consent Templates

---

| | |
|---|---|
| Effective Date: | 07/01/2023 |
| Version number: | 4.0 |
| Previous Version/date: | 3.0; 04/28/2023 |
| Responsible Office: | HRPP Office |
| Approval Date: | 05/30/2023 |

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