UNIVERSITY OF SOUTHERN MAINE
Office of Research Integrity & Outreach

Procedure #:	HRPP-048
AAHRPP:	Element II.3.D., Element II.3.E
Date Adopted:	9/15/2020
Last Updated:	5/27/2021
Prepared By:	Sheilan Hamasoor, Research Compliance Administrator
Reviewed By:	IRB Chair; IRB; ORIO
Procedure Title:	Privacy and Confidentiality

1.0 Objective

1.1. To describe the policies and procedures for privacy and confidentiality, including developing, reviewing, revising, and distributing standard operating procedures (SOP) for the University of Southern Maine (USM) Human Research Protection Program (HRPP).

2.0 General Description

2.1. The Institutional Review Board (IRB) will determine whether adequate safeguards and procedures are in place to protect the privacy of subjects and to maintain the confidentiality of their private information.

3.0 Definitions

3.1. **Privacy** is an individual's control over the extent, timing, and circumstances of sharing him or herself (physically, behaviorally, or intellectually) with others. In general, researchers must protect research participants' privacy throughout their participation in a study, including during recruitment and collection of private information. Private information must be stored securely and in a form that prevents, where possible, the identification of individuals by others.

3.2. **Confidentiality** is the treatment of private information disclosed in a trust relationship and with the expectation that it will not be divulged without permission to others in ways inconsistent with the understanding of the original disclosure.

3.2.1. Confidentiality is an agreement among parties made via the consent process. Researchers must not disclose private information unless participants have agreed in writing otherwise. Researchers, however, should not guarantee absolute/complete confidentiality and must inform participants of possible disclosures, such as mandatory reporting laws, that apply to a study. As with privacy, confidentiality requires researchers to keep private information secure, regardless of its form (e.g., verbal, paper-based, digital/electronic).

3.3. Private Information means individually private information, including:

3.3.1. Behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place;

3.3.2. Information that has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public.

3.4. **Sensitive Information** is that which, if disclosed, may reasonably pose a risk to the subject's psychological, social, medical, legal, or economic well-being or quality of life. Categories of sensitive information include (but are not limited to):

3.4.1. Sexual attitudes, preferences, or practices;

3.4.2. Use of alcohol, drugs, or other addictive substances or products;

3.4.3. Information pertaining to illegal conduct;

3.4.4. Information that, if released, might be damaging to an individual's financial standing, employability, or reputation within the community or might lead to social stigmatization or discrimination;

3.4.5. Health and medical information contained in a medical record, chart, or insurance file (This category may also require a Health Insurance Portability and Accountability Act (HIPAA) Privacy Board review); and

3.4.6. Information pertaining to an individual's psychological well-being or mental health (this category may also require a HIPAA Privacy Board review).

3.5. Protected Health Information (PHI) is individually identifiable health information that is transmitted or maintained in any form or medium by a HIPAA-covered entity, component, or business associate of a HIPAA-covered entity or component, including verbal, paper, or electronic.

3.6. Anonymity means that researchers are not collecting any identifiers (e.g., name, address, telephone number, Internet Protocol (IP) addresses) that allow information/records/ samples, either individually or when combined with other variables, to be linked to the individual from whom they were obtained.

3.7. Certificate of Confidentiality (CoC) protects 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.

4.0 Responsibility

4.1. It is the responsibility of the ORIO staff, Human Protections Administrator (HPA), and Institutional Review Board (IRB) to execute this Standard Operating Procedure (SOP).

5.0 Procedure

5.1. Privacy Interests

5.1.1. Researchers have a duty to respect the privacy of prospective subjects. The researcher allows the research subject to determine when, how, and to what extent information about them is communicated to others.

5.1.2. Researchers will protect an individual's right to privacy by obtaining voluntary and informed consent before collecting that individual's private information.

5.1.3. The Principal Investigator (PI) must make efforts to ensure that conditions in which research procedures are performed, or private information that is collected, occur in a manner which prevents private information from inadvertently being viewed or overheard by those without a research-based need-to-know. In addition, the PI must also ensure the private information collected is the minimum necessary to perform the research.

5.2. Confidentiality

5.2.1. Research projects vary substantially in the sensitivity of the information involved, the possibility of identifying particular individuals, and the magnitude and probability of harms that may result from the identification of research subjects. Researchers have a duty to respect the confidentiality of private information collected during research.

5.2.2. The researcher has a duty to protect research subjects from harm through the unauthorized release of private information.

5.2.3. The PI will provide the information regarding the confidentiality of private information at the time of initial review through the completion of the application, any necessary HIPAA forms, research protocol, and/or other submitted, applicable materials. The IRB will review all information received from the PI and determine whether or not confidentiality of research subject private information is sufficiently protected.

5.2.4. In reviewing confidentiality protections, the IRB shall consider the nature, probability, and magnitude of harms that would be likely to result from disclosure of private information outside the research. It shall evaluate the effectiveness of proposed de-identification techniques, coding systems, encryption methods,

storage facilities, access limitations, and other relevant factors in determining the adequacy of confidentiality protections.

5.3. Certificate of Confidentiality (CoC)

5.3.1. A CoC is only issued for research projects that are:

5.3.1.1. Collecting subject names or other identifying characteristics, on a sensitive research topic;
5.3.1.2. Approved by an IRB operating under a Federal-wide assurance (FWA) issued by the United States Department of Health and Human Services (HHS) Office of Human Research Protections (OHRP) or with the approval of the Federal Drug Administration (FDA);
5.3.1.3. On a topic that is within the HHS health related research mission found: https://www.nih.gov/about-nih/what-we-do/mission-goals;
5.3.1.4. Storing private information in the United States;
5.3.1.5. Allowable under federal regulations; or
5.3.1.6. When federal funding is not required but issuance is at the discretion of the issuing agency.

5.3.2. Private information may only be disclosed when:

5.3.2.1. Required by Federal, State, or local laws;
5.3.2.2. Necessary for the medical treatment of the individual to whom the information, document, or biospecimen pertains and made with the consent of such individual;
5.3.2.3. Made with the consent of the individual to whom the information, document, or biospecimens pertains; or
5.3.2.4. Made for the purposes of other scientific research that is in compliance with applicable Federal regulations governing the protection of human subjects in research.

5.3.3. To remain compliant, it is the PI's responsibility to ensure that:

5.3.1.1. All funding is accurately described in the eProtocol application;
5.3.1.2. All consent and assent forms are up to date with the appropriate CoC; and
5.3.1.3. A new CoC is obtained should funding end and is not renewed via a No Cost Extension or a new reward.

5.3.4. Informed Consent Process: When an investigator obtains a CoC, the subjects must be told about protections afforded by the CoC and any expectations to those protections. In addition, researchers may not represent the CoC as an endorsement of the research project by HHS or use it in a coercive manner when recruiting subjects.

5.3.5. Significant Changes: If a significant change in the research project is proposed after a CoC is issued, the PI must inform the Certificate Coordinator of the Institute issuing the Certificate by submitting an amended application for a CoC (in the same form and manner as the original application for a Certificate). Significant changes include:

5.3.5.1. Major changes in the scope or direction of the research protocol;
5.3.5.2. Changes in personnel having major responsibilities in the project; or
5.3.5.3. Changes in the drugs to be administered (if any) and the persons who will administer them.

5.3.6. If the PI obtained a CoC prior to the policy change (October 1, 2017) and subsequently obtains National Institutes of Health (NIH) funding, CoC coverage is based on the date allowing for the most time. As of April 15, 2020, the NIH no longer accepts amendments or extensions to CoCs. A new CoC must be obtained.

5.3.6.1. All research that was started or ongoing on or after December 13, 2016 and is within the scope of the policy is automatically issued a Certificate.

5.4. The Principal Investigator will agree in writing to maintain confidentiality through eProtocol, a federal-wide assurance agreement, reliance agreement, or contract.

6.0 References

6.1. 45 CFR 46.111(a)(7);

6.2. 21 CFR 56.111(a)(7);

6.3. 38 CFR 16.111(a)(7);

6.4. 10 CFR 745;

6.5. 28 CFR 22;

6.6. 49 CFR 512.11-13, 15;

6.7. 45 CFR Part 164