SOP 1002: PRIVACY & CONFIDENTIALITY

1. POLICY

In accordance with federal law and regulations, the IRB shall determine that where appropriate, adequate provisions are in place to protect the privacy of participants and maintain the confidentiality of data when reviewing human subjects research. There must be an adequate plan in place to preserve the participant’s right to choose how and when his or her private information will be used, withheld, and or disclosed. Potential risks of a breach to privacy and confidentiality must be disclosed. The IRB may determine additional methods as needed to minimize risks to participants.

Specific Policies

1.1 Protecting Privacy

The IRB may only approve research that does not unreasonably invade the privacy of research participants. Privacy is a person’s right to control the extent, timing, and circumstances of sharing access to oneself (physically, behaviorally, or intellectually) and to their information with others.

1.1.1 Human participant research must be designed to gather only the minimum necessary information to accomplish the intended purpose of the use, disclosure, or request without the participants’ knowledge or consent in any phase of the research, including recruitment and screening.

1.2 Maintaining Confidentiality

The IRB will approve research that adequately protects the confidentiality of research data commensurate with risks associated with disclosure, legal obligations, and the confidentiality commitment made to research participants.

Confidentiality pertains to non-disclosure of personal information that an individual has disclosed in a relationship of trust with the expectation that it will not be divulged to others without permission in ways that are inconsistent with the understanding of the original disclosure.

1.2.1. Methods for keeping information 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) or data encryption. The method(s) selected are determined by the nature of the information collected and potential risk to participants from a breach of confidentiality.

1.3 NIH Certificate of Confidentiality

Some research projects may require that the investigator obtain a Certificate of Confidentiality to protect the privacy and confidentiality of research participants. Investigators generally may not be compelled to release data covered by a Certificate of Confidentiality in any federal, state, or local civil, criminal, administrative, legislative, or other proceedings.

OHRP does not issue Certificates of Confidentiality. The NIH and other federal agencies issue these to protect identifiable information from forced or compelled disclosures. See https://humansubjects.nih.gov/coc/index for Info from NIH about CoC.
Other federal agencies may evaluate IRB research projects for Certificates of Confidentiality using different criteria.

1.3.1 Restrictions on Disclosure:

a. When research is covered by a Certificate of Confidentiality, investigators may not disclose or provide, in any Federal, State, or local civil, criminal, administrative, legislative, or other proceeding:
   - the name of research participant
   - any information, document, or biospecimen that contains identifiable, sensitive information about the research participant and that was created or compiled for purposes of the research,

In addition to the above restrictions, investigators may not disclose or provide this information to any other person not connected with the research.

b. Exceptions to the above restrictions include when:
   - Required by Federal, State, or local laws (e.g., as required by the Federal Food, Drug, and Cosmetic Act, or state laws requiring the reporting of communicable diseases to State and local health departments), excluding instances of disclosure in any Federal, State, or local civil, criminal, administrative, legislative, or other proceeding.
   - Necessary for the medical treatment of the individual to whom the information, document, or biospecimen pertains and made with the consent of such individual;
   - Made with the consent of the individual to whom the information, document, or biospecimen pertains; or
   - Made for the purposes of other scientific research that is in compliance with applicable Federal regulations governing the protection of human subjects in research.

1.3.2 Federally-Funded Research: Effective October 1, 2017, all research that commenced or was ongoing on or after December 13, 2016, that collects or uses identifiable sensitive information is automatically issued a CoC for applicable NIH awards as part of the award terms and conditions.

“Identifiable sensitive information” is information about an individual that is gathered or used during the course of biomedical, behavioral, clinical, or other research where the following may occur:
   - An individual is identified; or
   - For which there is at least a very small risk that some combination of the information, a request for the information, and other available data sources could be used to deduce the identity of an individual.

The IRB website provides additional information on how Investigators can obtain a Certificate of Confidentiality. In the IRB submission, the investigator will indicate that a Certificate of Confidentiality is needed. The IRB will hold the official approval letter but will issue a contingent approval letter for the research project in order for the investigator to...
obtain the Certificate of Confidentiality. However, no research activities can begin until the Certificate of Confidentiality is received by the IRB. At that time, the IRB will release the research project approval letter and stamped consent documents to the investigator.

If a CoC is automatically issued, such as for an NIH-funded study, the IRB will not require a separate CoC document. However, the consent form must include the appropriate CoC language, located in the consent template.

Non-Federally-Funded Research: The IRB may determine that investigators obtain a Certificate of Confidentiality if the research will collect or use information that is of a sensitive nature and protection is necessary to perform the research. Research that collects information related to the following types of information may be considered sensitive:

- Information related to sexual attitudes, preferences, or practices
- Information related to the use of alcohol, drugs, or other addictive substances
- Information pertaining to illegal conduct
- Information that if released, could reasonably be damaging to an individual’s financial standing, employability, or reputation in the community
- Information that would normally be recorded in the patient’s medical record, but disclosure could reasonably lead to social stigmatization or discrimination
- Information pertaining to psychological well-being or mental health
- Genetic information

1.3.3 Sharing Identifiable, Sensitive Information with Other Researchers and Organizations: Investigators conducting research covered by a Certificate of Confidentiality, regardless of the funding source, must ensure that if identifiable, sensitive information is provided to other investigators or organizations, the other investigator or organization must comply with applicable requirements of the Certificate.

1.3.4 Required Disclosure Under Oklahoma Law: Even though a Certificate of Confidentiality has been issued by a federal agency, Oklahoma law requires disclosure of certain information, such as child abuse or intent to harm self or others. In these situations, the consent documents must notify research participants of the investigator’s legal reporting obligations.

1.3.5 VA Research Requirements for Notes in the Medical Record: 

a. For studies that do not involve a medical intervention, no annotation may be made in the medical record.

b. For studies involving a medical intervention, a progress note in the medical record should be made indicating the following:
   - the individual has enrolled in a research study,
   - any details that will or may impact clinical care, and
   - the name and contact information of the Principal Investigator.

1.4 Web-Based Survey, Data Collection, and Data Storage Tools
Investigators may use a variety of web-based programs to administer surveys and collect and store research data. Collecting data using web-based programs can increase potential risks to confidentiality. To aid in minimizing such risks, investigators should use University IT-approved programs or submit the programs to IT for a risk assessment and work with the appropriate University office to enter into a contract with the vendor that includes sufficient protection of the research data before using any web-based software for data collection.

1.4.1 REDCap is the recommended software for survey administration, data collection, and data storage. REDCap satisfies all data security requirements for the University, state law, and regulatory requirements such as HIPAA and FERPA.

1.4.2 SurveyMonkey and Qualtrics may only be used if the survey or other tools will collect and store de-identified or anonymous information. Personally Identifiable Information (PII) and Protected Health Information (PHI) cannot be stored or transmitted in either program.

Refer to SOP 502L: Internet/Social Media-Based Research for more information regarding technology-assisted survey administration and data security.

Investigators should also contact their respective campus' IT Office for additional information regarding the process to use web-based programs in human research, including risk assessments and obtaining agreements with vendors.

1.5 Other University Requirements That Impact Human Research

1.5.1 Portable Computing Device Encryption Policy: The University requires encryption of portable computing devices that are used for University business. This applies to all University personnel, including affiliates and volunteers, who use portable computing devices, regardless of ownership. Portable devices include laptops, tablets, flash drives, and smartphones.

The privacy protections in this policy apply to all investigators engaged in human participant research at the University and all device types listed above that are used to collect data for research purposes. Refer to the Senior Vice President and Provost's Encryption memo and to University IT Security Policy for more information.

1.5.2 Information Security Risk Assessment Policy: In accordance with this University IT Security Policy, investigators' technology, software, devices, and the like that are acquired for or used in University research must undergo a product review or risk assessment through IT Security.

Refer to the IT Security website and policy for more information regarding this process.

1.5.3 Investigators must comply with the University’s HIPAA policies (including those of the HRPP) when applicable to their research. Refer also to SOP 1001: Health Insurance Portability and Accountability Act (HIPAA Privacy Rule).

2. SCOPE

This SOP applies to all human research that involves the access to or creation, acquisition, disclosure, or maintenance of identifiable participant information.

3. RESPONSIBILITY
3.1 The IRB is responsible for reviewing all human subjects research protocols to ensure that adequate protections for privacy and confidentiality are in place, according to applicable federal law and regulations, applicable local and state requirements, and applicable policies.

3.2 Investigators are responsible for including adequate provisions to protect the privacy of participants and confidentiality of participant information and research data. These provisions must be described in the IRB application and research protocol.

3.3 Investigators are responsible for ensuring they comply with all HRPP, IT, and other University policies related to securing and protecting the privacy and confidentiality of individuals enrolled or included in human subjects research.

4. APPLICABLE REGULATIONS AND GUIDELINES

45 CFR 46.111
21 CFR 56.111
Health Insurance Portability and Accountability Act (HIPAA)
Family Educational Rights and Privacy Act (FERPA)
10 O.S. § 7103

5. REFERENCES TO OTHER APPLICABLE SOPS

This SOP affects all other HRPP/IRB SOPs.

6. ATTACHMENTS

None

7. PROCESS OVERVIEW

7.1 The IRB Chair or IRB Designee or the convened IRB will review human subjects research applications and determine whether adequate provisions are in place to protect the privacy of participants and the confidentiality of their information, according to applicable federal law and regulations, applicable local and state requirements, and applicable policies.

7.2 The IRB may require verification of information submitted by an investigator or the IRB may require additional provisions to minimize potential risks to participants. The IRB will document such requests in the IRB’s electronic information system.

7.3 The IRB Administrator contacts the investigator to request verification or additional provisions if indicated during IRB review.

7.4 The QI Coordinator will verify compliance with this policy during random and for-cause evaluation procedures as described in SOP 901: Quality Improvement Program.

APPROVED BY: ___________________________ DATE: 01/06/2020

NEXT ESTABLISHED REVIEW DATE: AUGUST 2020