DATA SECURITY ANCILLARY COMMITTEE
STANDARD OPERATING PROCEDURE

Effective Date: 03/15/19

1. PURPOSE

The purpose of this document is to define the process by which the Data Security Ancillary Committee will review University of Miami data privacy plans for human subject research studies. These reviews are intended to assess the privacy and security of data maintained within computerized systems used in the conduct of human subject research.

2. DEFINITIONS

- **Ancillary Committee** – Data Security Ancillary Committee. The Ancillary Committee is comprised of members of the Office of Privacy and Data Security ("Privacy Office") and IT Security.
- **Data** – Data obtained during the conduct of human subject research
- **De-identified Data -** Information that has been de-identified in accordance with the requirements for de-identification of Protected Health Information under 45 CFR §164.514(b). Please see here for more information.
- **eProst** – University of Miami's Electronic Protocol Submission and Tracking system
- **HIPAA Authorization Form B** - Authorization to Use and Disclose Health Information for Research
- **HSRO** – Human Subject Research Office
- **IRB** – Institutional Review Board
- **Limited Data Set (LDS)-** Protected Health Information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: Names; Postal address information, other than town or city, State, and zip code; Telephone numbers; Fax numbers; Electronic mail addresses; Social Security numbers; Medical record numbers; Health-plan beneficiary numbers; Account numbers; Certificate and license numbers; Vehicle identifiers and serial numbers, including license plate numbers; Device identifiers and serial numbers; Web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers; Biometric identifies including fingerprints and voice prints; and full-face photographic images and any comparable image. Please see here for more information.
- **Protected Health Information (PHI) -** The following individually identifiable data elements, when combined with health information about that individual: Names; All geographic subdivisions smaller than a State; All elements of dates (except year) for dates directly related to an individual including birth date, admission date, discharge date, date of death; Telephone numbers; Fax numbers; Electronic mail addresses; Social Security numbers; Medical record numbers; Health-plan beneficiary numbers; Account numbers; Certificate and license numbers; Vehicle identifiers and serial numbers, including license plate numbers; Device identifiers and serial numbers; Web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers; Biometric identifies including fingerprints and voice prints; Full-face photographic images and any comparable image; and any other unique identifying number, characteristic, code, or combination that allows identification of an individual.
- **PI** – Principal Investigator

- **Personally Identifiable Information (PII)** - any information that can be used to identify, contact, or locate an individual, either alone or combined with other easily accessible sources, including but not limited to, a user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account or an individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual: (i) a social security number; (ii) a driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity; (iii) a financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account (iv) any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or (v) an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.. Please see here for more information.
- **Privacy and Security Review** – Ancillary Committee review of data privacy plans and review of Research Data Security Assessment forms, as necessary, in order to assess the privacy and security of data maintained within computerized systems used in the conduct of human subject research at the University of Miami.
- **Research Data Security Assessment** – The form the PI must complete and submit with initial protocol submission, or as requested by the HSRO, which shall be used by the Ancillary Committee to conduct a preliminary security assessment of the electronic systems used in the research study.

3. RESPONSIBILITY

3.1 PI/PI Designee

- Answers eProst SmartForm questions accurately, based on knowledge, information, and belief of the current and expected course of the study.
- Generates and submits the Research Data Security Assessment as required by the eProst SmartForm, answering questions accurately, based on knowledge, information, and belief of the current and expected course of the study.
- Provides additional information to the HSRO and/or the Ancillary Committee, as requested.
- Addresses any required modifications based on deficiencies in data privacy plan, as directed by the ancillary committee and/or the HSRO, and submits changes in eProst.
- Submits all required modifications promptly.

3.2 Ancillary Committee

- Receives notification from the eProst system of necessary Privacy and Security Review.
- Hosts information regarding the Ancillary Committee and associated forms, including the Research Data Security Assessment, on website. Reviews the submitted Research Data Security Assessment form and other study documentation to assess if computerized systems used to collect and store Data are adequate to protect subject's privacy and security.

- Submits ancillary review on eProst promptly.
- Details reasons for not accepting proposed studies and provides recommended action that will adequately protect subject's privacy and security.
- Conducts a review of PI responses for any required study changes, as directed by the HSRO.
- Conducts a review of privacy and security related study issues, as directed by the HSRO.

3.3 HSRO

- Obtains information relating to storage of research Data on computerized systems.
- Reviews Ancillary Committee's submissions on eProst to determine if any deficiencies in data privacy plan must be addressed by PI.
- Requests required modifications to data privacy plans.
- Reviews modifications to verify that required modifications were completed.
- Requests Privacy and Security Review, as necessary or required, when presented with a potential privacy and security issue.

4. PROCEDURE

4.1 eProst System Initiated Privacy and Security Review

4.1.1 Submission of eProst SmartForm and Research Data Security Assessment

- During the initial submission of study protocol, submitters will be asked to answer questions which assess the storage, transfer, sensitivity and controls of Data. PIs will be required to upload the Research Data Security Assessment in the "Local Site Documents" section of the eProst SmartForm if the PI indicates any of the following:
    - The study uses a database or registry containing personally identifiable information.
    - The study involves the sharing of PHI, PII, LDS or other identifiable Data outside of the University of Miami and such Data is not being shared pursuant to a legally appropriate agreement.
    - The study uses an application (app) or tool such as a tablet, watch or other wearable that collects and transmits PII.
    - The study stores Data in non-UM approved storage solutions**.**

  Note: PIs will not be able to submit their study protocol through the eProst SmartForm without first submitting the Research Data Security Assessment.

4.2 Ancillary Committee Privacy and Security Review

4.2.1 Notification

- After PI submits the Research Data Security Assessment on eProst, the system will automatically send a notification to all Ancillary Committee members via email.

4.2.2 Conducting Privacy and Security Review

- All Ancillary Committee members shall individually assess information in the Research Data Security Assessment, as well any necessary and appropriate study documentation, including:
    - Answers to eProst SmartForm questions;
    - protocols and informed consent forms; and
    - other study-related materials and/or documentation.
- At any point during the Privacy and Security Review, the Ancillary Committee may request additional information from the PI and/or the HSRO.

4.2.3 Submitting Recommendations

- All Ancillary Committee members shall individually report their recommendations to the representative Privacy Office ("Privacy Representative") and IT Security ("IT Representative") Ancillary Committee member assigned to approve recommendations.
- If both the Privacy Representative and IT Representative agree with the Ancillary Committee's overall recommendations, the Privacy Representative shall submit the ancillary review on eProst.
    - If there is any disagreement on the initial recommendations, both Representatives shall meet with the Ancillary Committee members of their respective department and conduct another Privacy and Security Review. If necessary, all Ancillary Committee members shall meet, either by telephone or in person, to determine the appropriate recommendations to be submitted.
- If study plan is found to be satisfactory, the Privacy Representative shall accept the proposed study on behalf of the committee and leave a comment stating "Ancillary review complete, data plan approved.."
- If the study plan is not satisfactory due to privacy and security deficiencies in the PI's data privacy plan(s), the Privacy Representative shall not accept the proposed study and leave a detailed comment explaining the modifications required.

- The Ancillary Committee will aim to submit their study acceptance or request for further modifications within five (5) working days of receiving the Research Data Security Assessment. If additional time is needed, the need for an extension of time will be discussed with appropriate personnel in the HSRO and/or the PI.

4.3 HSRO Review of Ancillary Review Determinations

4.3.1 Study Acceptance

- If study plan is accepted, the HSRO shall follow established procedures until study moves into an approved state.

4.3.2 Data Plan Not Satisfactory

- If the Ancillary Committee identifies and communicates privacy and security deficiencies in the data privacy plan(s), the HSRO shall review the ancillary review determinations and request a subsequent modification in the eProst system.
- After the HSRO requests further modifications, by executing the pending contingency activity, the PI will receive a system generated eProst reminder that action is pending.
- The PI shall make best efforts to promptly submit required modifications, attaching all supporting documentation in eProst.
- Upon receiving notification of PI's submission of required modifications, the eProst system shall automatically notify the Ancillary Committee of the need for a subsequent Privacy and Security Review.
- Ancillary Committee will again conduct a Privacy and Security Review in accordance with section 4.2.

4.4 HSRO Initiated Privacy and Security Review

4.4.1 Compulsory Privacy and Security Review

- The HSRO must require changes to the study and request the PI to complete the Research Data Security Assessment if:
    - the HSRO receives a sponsor request for the modification of the HIPAA Authorization Form B standard Form B; or
    - the HSRO receives a request for the transfer of data outside of the United States.

4.4.2 Discretionary Privacy and Security Review

- The HSRO may require changes to the study and request for PI to complete the Research Data Security Assessment if:
    - the HSRO receives a request for a partial or full waiver of the HIPAA Authorization Form B;
    - the HSRO receives a request for an exception for studies involving "cold calling"; or
    - the HSRO encounters any privacy and/or security related issues.

4.4.3 Initiating Privacy and Security Review

- After requesting changes under 4.4.2 above, the HSRO will add the Ancillary Committee to the list of required ancillary reviews via the Manage Ancillary Reviews activity.
- After requesting modifications, the PI will receive a system generated eProst reminder that action is pending.
- The PI shall make best efforts to promptly submit required modifications, attaching the Research Data Security Assessment, in eProst.
- Upon receiving PI's modifications, including the Research Data Security Assessment, HSRO shall promptly notify the Ancillary Committee of the need for a Privacy and Security Review.
- Ancillary Committee will conduct a Privacy and Security Review in accordance with section 4.2.

5. DOCUMENTATION

5.1 Maintenance of Documents

5.1.1 All documents produced during the course of the Privacy and Security Review will be maintained on the eProst system in accordance with the HSRO/IRB's document retention policies.

5.1.2 Any electronic copies of documents produced during the course of the Privacy and Security Review will be maintained in a shared Box drive folder.

6. RELATED DOCUMENTS

- Research Data Security Assessment
- Authorization to Use and Disclose Health Information for Research (Form B)

7. REVISION HISTORY

Effective Date	Revision Date	Author	Description of Changes