

DATA BROKER GROUP
STANDARD OPERATING PROCEDURE

Document Number:	SOP-HB-008-01	Effective Date:	4/12/23
Page No.	Page 1 of 8	Author:	J. Casanova
Title:	Data Security Ancillary Committee		

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

- 2.1 **Ancillary Committee:** Data Security Ancillary Committee. The Ancillary Committee is comprised of members of the Research Privacy, Data Broker Group, UM IT Security, UHealth IT Security, and the UHealth Privacy Office.
- 2.2 **Ancillary Committee Data Assessment Form:** The form to be completed by the PI (or PI designee) and submitted with the initial protocol submission, or as requested by HSRO. This form shall be used by the Ancillary Committee to conduct a preliminary security and privacy review of the electronic systems used in the research study.
- 2.3 **Data:** Data obtained during the conduct of human subject research
- 2.4 **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.
- 2.5 **IBISResearch:** University of Miami's Electronic Protocol Submission and Tracking system
- 2.6 **HIPAA Authorization Form B:** [Authorization to Use and Disclose Health Information for Research](#)
- 2.7 **HSRO:** Human Subject Research Office
- 2.8 **IRB:** Institutional Review Board
- 2.9 **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.

DATA BROKER GROUP
STANDARD OPERATING PROCEDURE

Document Number:	SOP-HB-008-01	Effective Date:	4/12/23
Page No.	Page 2 of 8	Author:	J. Casanova
Title:	Data Security Ancillary Committee		

- 2.10 **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.
- 2.11 **PI:** Principal Investigator
- 2.12 **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.
- 2.13 **Privacy and Security Review:** Ancillary Committee review of data management plans and review of Ancillary Committee Data Assessment forms, as necessary, 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.

DATA BROKER GROUP
STANDARD OPERATING PROCEDURE

Document Number:	SOP-HB-008-01	Effective Date:	4/12/23
Page No.	Page 3 of 8	Author:	J. Casanova
Title:	Data Security Ancillary Committee		

3. RESPONSIBILITY

3.1 PI/PI Designee

- Completes IBIS-Research New Study Application questions accurately, based on knowledge, information, and belief of the current and expected course of the study.
- Generates and submits the Ancillary Committee Data Assessment as required by the IBIS-Research New Study Application, answering questions accurately, based on knowledge, information, and belief of the current and expected course of the study.
- Adds Data Security Ancillary Committee to the set of required ancillary committees via the Manage Ancillary Reviews activity in IBIS-Research.
- Provides additional information to the HSRO and/or the Ancillary Committee, as requested.
- Addresses any required modifications or other changes based on deficiencies in data management plan, as directed by the ancillary committee and/or the HSRO and submits responses in IBIS-Research.
- Submits all required modifications promptly.

3.2 Ancillary Committee

- Receives notification from OVPRShelpdesk@miami.edu of necessary Privacy and Security Review.
- Hosts information regarding the Ancillary Committee and associated forms, including the Ancillary Committee Data Assessment, on website to act as a supplement to the HSRO site. Reviews the submitted Ancillary Committee Data 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.
- Conducts a review of privacy and security related study issues, as directed by the HSRO.
- Submits ancillary review on IBIS-Research promptly.
- Details reasons for not accepting proposed studies and provides recommended actions that will adequately protect subjects' privacy and security.
- Conducts a review of PI responses for any required study changes, as directed by the HSRO.
- Maintains a log of all reviews conducted by committee.

DATA BROKER GROUP
STANDARD OPERATING PROCEDURE

Document Number:	SOP-HB-008-01	Effective Date:	4/12/23
Page No.	Page 4 of 8	Author:	J. Casanova
Title:	Data Security Ancillary Committee		

3.3 HSRO

- Obtains information relating to storage of research data on computerized systems.
- Reviews Ancillary Committee’s submissions on IBIS-Research to determine if any deficiencies in data management plan must be addressed by PI.
- Requests required modifications to data management 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 issues for new protocols and modifications.

4. PROCEDURE

4.1 Initial Assignment to DSAC

4.1.1 Completing the IBIS-Research New Study Application and adding Ancillary Committee Data Assessment

During the initial submission of study protocol, study teams will be asked to answer questions which describe the collection and storage of identifiable data. PIs will be required to upload the Ancillary Committee Data Assessment in the “Local Site Documents” section of the IBIS-Research New Study Application if the PI indicates the study collects and/or stores Data in non-UM approved storage solutions. The HSRO retains the ability to require DSAC review for any new protocol or modification.

4.2 Ancillary Committee Review

4.2.1 Notification

After PI adds the Data Security Ancillary Committee to the set of required ancillary reviewers via the “Manage Ancillary Reviews” activity in IBIS-Research, the system will automatically send a notification to all Ancillary Committee members via email.

DATA BROKER GROUP
STANDARD OPERATING PROCEDURE

Document Number:	SOP-HB-008-01	Effective Date:	4/12/23
Page No.	Page 5 of 8	Author:	J. Casanova
Title:	Data Security Ancillary Committee		

4.2.2 Conducting Privacy and Security Review

All Ancillary Committee members can individually assess information in the Ancillary Committee Data Assessment, as well any necessary and appropriate study documentation, including:

- Answers to IBIS-Research New Study Application 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.

Note: Studies that predate the existence of the Ancillary Committee and any modifications to those studies, will not undergo review unless requested by the HSRO or IRB Committee.

4.2.3 Submitting Recommendations

All Ancillary Committee members can individually review proposed studies and document their recommendations. The Ancillary Committee meets regularly to review and discuss proposed studies and recommendations. At least one representative from Research Privacy or the Data Broker Group (“Privacy Representative”) and one representative from UMIT Security or UHealth IT Security (“IT Security Representative”) shall be present during meetings.

The Privacy Representative, their designee, or other designated Ancillary Committee member assigned to approve recommendations shall document the ancillary review in IBIS-Research by executing the “Submit Ancillary Review” activity in IBIS-Research, therein accepting the proposed study on behalf of the committee.

If the study plan is not satisfactory due to privacy and security deficiencies in the PI’s data management plan(s), the Privacy Representative, or designee, shall not accept the proposed study and explain the modifications or clarifications required via the “Add Comment” activity in IBIS-Research.

The Ancillary Committee will aim to submit their study acceptance or request for further modifications within five (5) working days of receiving the Ancillary Committee Data Assessment. If additional time is needed, the need

DATA BROKER GROUP
STANDARD OPERATING PROCEDURE

Document Number:	SOP-HB-008-01	Effective Date:	4/12/23
Page No.	Page 6 of 8	Author:	J. Casanova
Title:	Data Security Ancillary Committee		

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 management plan(s), the HSRO shall review the ancillary review determinations and request a subsequent modification in IBIS-Research.

The PI shall make best efforts to promptly submit required modifications or responses in IBIS-Research, including any required attachments.

The PI and/or HSRO should notify the Ancillary Committee upon the PI's submission of required modifications in order to perform 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 Ancillary Committee Data Assessment if:

- 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 Ancillary Committee Data Assessment if the HSRO encounters any privacy and/or security related issues.

DATA BROKER GROUP
STANDARD OPERATING PROCEDURE

Document Number:	SOP-HB-008-01	Effective Date:	4/12/23
Page No.	Page 7 of 8	Author:	J. Casanova
Title:	Data Security Ancillary Committee		

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.

The PI shall make best efforts to promptly submit required modifications, attaching the Ancillary Committee Data Assessment, in IBIS-Research.

Upon receiving PI's modifications, including the Ancillary Committee Data 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

All Documents produced during the Privacy and Security Review, with the exception of personal notes, logs and emails, will be maintained on the IBIS-Research system in accordance with the HSRO/IRB's document retention policies.

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

6. REFERENCES

7. RELATED DOCUMENTS

- [Ancillary Committee Data Assessment](#)
- [Authorization to Use and Disclose Health Information for Research](#) (Form B)

8. TEMPLATES / FORMS / TOOLS

N/A

DATA BROKER GROUP
STANDARD OPERATING PROCEDURE

Document Number:	SOP-HB-008-01	Effective Date:	4/12/23
Page No.	Page 8 of 8	Author:	J. Casanova
Title:	Data Security Ancillary Committee		


9. REVISION HISTORY

Effective Date	Author	Description of Changes
10/1/2019	Office of Privacy & Data Security	Changes made to reflect ancillary form name change, address procedures for committee review, as well as handling study modifications and submitting recommendations.
4/12/2023	J. Casanova	Revise Formatting to match Data Broker SOPs. Update all references to “eProst” to reflect name change to “IBIS-Research” and update procedures to be consistent with revised workflow therein. Move UHealth Privacy Office to optional role. Add Research Privacy as part of the process.

9. SIGNATURES

Prepared by: 
Joey Casanova, BBA, CIPT, CHRC, CIP
Data Broker Manager
Date: 4/12/2023

QA by: 
Winston Galiz
Data Broker Manager
Date: 4/12/2023

Approved by: 
Ishwar Ramsingh, MBA, CISSP, CISM, CISA, CIPP/E, CIPM, CIPT, CHC
Data Broker Director
Date: 4/12/2023

Approved by: 
[Hilary Cox \(Apr 12, 2023 14:07 EDT\)](#)
Hilary Cox, JD, CIPP/US
Executive Director, University & Research Privacy
Date: 4/12/2023












SOP - DSAC rev 04.12.23 - final

Final Audit Report

2023-04-12

Created:	2023-04-12
By:	Jose Casanova (JCasanova@med.miami.edu)
Status:	Signed
Transaction ID:	CBJCHBCAABAAj9lieao1Q7WqsDeT7gmA1FkdJqE8VThu

"SOP - DSAC rev 04.12.23 - final" History

-  Document created by Jose Casanova (JCasanova@med.miami.edu)
2023-04-12 - 2:22:05 PM GMT- IP address: 129.171.150.146
-  Document emailed to Ishwar Ramsingh (iramsingh@med.miami.edu) for signature
2023-04-12 - 2:22:49 PM GMT
-  Email viewed by Ishwar Ramsingh (iramsingh@med.miami.edu)
2023-04-12 - 2:23:22 PM GMT- IP address: 129.171.249.138
-  Document e-signed by Ishwar Ramsingh (iramsingh@med.miami.edu)
Signature Date: 2023-04-12 - 2:25:06 PM GMT - Time Source: server- IP address: 129.171.249.138
-  Document emailed to Winston Galiz (wxg44@miami.edu) for signature
2023-04-12 - 2:25:07 PM GMT
-  Email viewed by Winston Galiz (wxg44@miami.edu)
2023-04-12 - 6:02:32 PM GMT- IP address: 104.47.55.126
-  Document e-signed by Winston Galiz (wxg44@miami.edu)
Signature Date: 2023-04-12 - 6:03:23 PM GMT - Time Source: server- IP address: 129.171.249.147
-  Document emailed to Hilary Cox (hxc823@miami.edu) for signature
2023-04-12 - 6:03:24 PM GMT
-  Email viewed by Hilary Cox (hxc823@miami.edu)
2023-04-12 - 6:07:14 PM GMT- IP address: 73.46.156.203
-  Document e-signed by Hilary Cox (hxc823@miami.edu)
Signature Date: 2023-04-12 - 6:07:59 PM GMT - Time Source: server- IP address: 73.46.156.203
-  Agreement completed.
2023-04-12 - 6:07:59 PM GMT

Names and email addresses are entered into the Acrobat Sign service by Acrobat Sign users and are unverified unless otherwise noted.