

DATA SECURITY & ARTIFICIAL INTELLIGENCE ANCILLARY COMMITTEE
STANDARD OPERATING PROCEDURE

Document Number:	SOP-DSAC-001-01	Effective Date:	06/01/2026
Page No.	Page 1 of 10	Author:	J. Casanova
Title:	Data Security & Artificial Intelligence Ancillary Committee		

1. PURPOSE

Define the process by which the Data Security & Artificial Intelligence Ancillary Committee (DSAC) reviews proposed human subject research studies conducted at, or involving the University of Miami, ensuring compliance with HIPAA, institutional policies, and applicable federal, state or international data security, privacy, artificial intelligence and related regulations and best practices.

2. SCOPE

- 2.1 New protocols submitted through IBIS-Research after the effective date of this SOP. Modifications will also be subject to this SOP upon request of the Human Subject Research Office (HSRO).
- 2.2 Use of non-University approved applications, storage, or third-party services (including wearables, mobile apps, and cloud services).
- 2.3 Transfer of identifiable data, PHI, PII, or Limited Data Sets (LDS) to third parties for research purposes.
- 2.4 Use of Artificial Intelligence (AI), Machine Learning (ML), and Large Language Models (LLMs). Responsibilities include:
 - Verifying that data used for training or inference is de-identified, minimized, appropriately consented or otherwise permitted.
 - Requiring risk mitigation strategies, including risk acceptance, for data leakage, model inversion, adversarial attacks.
 - Mandating secure storage and processing environments for AI/ML/LLM models and datasets.

3. DEFINITIONS

- 3.1 **Ancillary Committee** – As used in this SOP, the Data Security & Artificial Intelligence Ancillary Committee. The Ancillary Committee is comprised of members of Research Privacy/Data Brokers, Information Technology AI team and IT Security and UHealth Compliance/Privacy.
- 3.2 **Data** – Data obtained during the conduct of human subject research
- 3.3 **De-identified Data** - Information de-identified under 45 CFR §164.514(b) via Expert Determination or Safe Harbor removal of 18 identifiers. Please see references.
- 3.4 **IBISResearch** – University of Miami's electronic protocol submission and tracking system
- 3.5 **HIPAA Authorization Form B** - [Authorization to Use and Disclose Health Information for Research](#)

DATA SECURITY & ARTIFICIAL INTELLIGENCE ANCILLARY COMMITTEE
STANDARD OPERATING PROCEDURE

Document Number:	SOP-DSAC-001-01	Effective Date:	06/01/2026
Page No.	Page 2 of 10	Author:	J. Casanova
Title:	Data Security & Artificial Intelligence Ancillary Committee		

- 3.6 HSRO** – Human Subject Research Office, maintains IRB records on all human research at UM and JHS, as well as keeping a database to track all human research submissions at both institutions. Additionally, it provides support for Institutional Review Boards, assists with comprehensive stakeholder accreditation activities through educational and networking platforms, and offers support while maintaining records for Trial Registration and Result Reporting on clinicaltrials.gov.
- 3.7 IRB** – Institutional Review Board ensure adherence to all federal, state, local, and institutional regulations concerning the protection of human subjects in research. All human research conducted by UM faculty, staff, and students or employees of JHS must receive IRB review and approval prior to commencement.
- 3.8 Limited Data Set (LDS)** – PHI that excludes direct identifiers, permitted for certain uses and disclosures under a Data Use Agreement (DUA). Please see references below.
- 3.9 Protected Health Information (PHI)** – Individually identifiable health information held by a HIPAA Covered Entity, as defined under 45 CFR Part 164, Subpart C and E.
- 3.10 PI** – Principal Investigator is the researcher, usually a doctor or other medical professional, who leads the clinical research team and, along with the other members of the research team, regularly monitors study participants’ health to determine the study’s safety and effectiveness.
- 3.11 Personally Identifiable Information (PII)** - Information that can identify, contact, or locate an individual, either alone or in combination. Please see references below.
- 3.12 Privacy and Security Review** – DSAC review of data privacy plans and review of DSAC Data 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.
- 3.13 Sensitive Personal Data (SPD)** – Categories including biometric identifiers, human genomic data, precise geolocation, personal health data, personal financial data, and personal identifiers, as referenced in federal rulemaking.
- 3.14 DSAC Data Assessment** – The form the PI (or PI designee) 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.
- 3.15 Artificial Intelligence (AI)** - Development of computer systems that perform tasks requiring human intelligence—such as learning, problem-solving, decision-making, and perception.
- 3.16 Machine Learning (ML)** – A subset of AI that develops and uses computer systems that adapt and learn from data with the goal of improving accuracy.
- 3.17 Large Language Model (LLM)** – A form of AI that utilizes deep learning algorithms to create models pretrained on massive text datasets for the general purpose of analyzing and learning patterns and relationships among characters, words and phrases to perform text-based tasks

DATA SECURITY & ARTIFICIAL INTELLIGENCE ANCILLARY COMMITTEE
STANDARD OPERATING PROCEDURE

Document Number:	SOP-DSAC-001-01	Effective Date:	06/01/2026
Page No.	Page 3 of 10	Author:	J. Casanova
Title:	Data Security & Artificial Intelligence Ancillary Committee		

4. RESPONSIBILITY

4.1 PI/PI Designee

- Accurately completes IBISResearch New Study Application, based on knowledge, information, and belief of the current and expected course of the study.
- Upload the DSAC Data Assessment, answering questions accurately, based on knowledge, information, and belief of the current and expected course of the study.
- Provides supplemental documentation upon request and addresses required modifications promptly.
- Avoid non-University-approved storage or applications, unless explicitly approved by the DSAC.

4.2 Ancillary Committee

- Receives system notification from IBISResearch of required reviews and assesses DSAC Data Assessments and study materials.
- are adequate to protect subject's privacy and security.
- Submits ancillary review on IBISResearch 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.

4.3 HSRO

- Verifies DSAC determinations and issues contingencies when data privacy/security deficiencies exist.
- Coordinates subsequent PI modifications and notifies DSAC upon resubmission for re-review.

DATA SECURITY & ARTIFICIAL INTELLIGENCE ANCILLARY COMMITTEE
STANDARD OPERATING PROCEDURE

Document Number:	SOP-DSAC-001-01	Effective Date:	06/01/2026
Page No.	Page 4 of 10	Author:	J. Casanova
Title:	Data Security & Artificial Intelligence Ancillary Committee		

5. PROCEDURE

5.1 System-Initiated Privacy and Security Review

- PI or designee completes SmartForm and uploads the DSAC Data Assessment when triggers are met:
 - The study uploads PII/PHI to a database or registry.
 - 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.
- IBISResearch generates DSAC notification.

5.2 DSAC Privacy and Security Review

- DSAC members shall review SmartForm responses, protocol, consent, DSAC Data Assessment, and related materials.
- All reviews of studies involving AI, ML, or LLM will incorporate considerations based on **§4.3 Considerations for Review of Studies Involving AI**.
- At any point during the Privacy and Security Review, the Ancillary Committee may request additional information from the PI/study team and/or the HSRO. These requests will be documented in IBISResearch.
- The Ancillary Committee meets regularly to review and discuss proposed studies and recommendations. At least one representative from Research Privacy/Data Broker, one representative from IT AI and IT Security shall be present during meetings. Decisions can be deferred until these stipulations are met, depending on need for specific expertise and protocol submissions.
 - If study plan is found to be satisfactory, a designee of the DSAC will submit ancillary review in IBISResearch, therein accepting the proposed study on behalf of the committee.

DATA SECURITY & ARTIFICIAL INTELLIGENCE ANCILLARY COMMITTEE
STANDARD OPERATING PROCEDURE

Document Number:	SOP-DSAC-001-01	Effective Date:	06/01/2026
Page No.	Page 5 of 10	Author:	J. Casanova
Title:	Data Security & Artificial Intelligence Ancillary Committee		

5.3 Considerations for Review of Studies Involving AI

- This checklist provides DSAC reviewers with a quick reference for evaluating human subject research studies involving Artificial Intelligence, machine learning, and large language models, aligned with NIST AI Risk Management Framework principles.
- **Data Management**
 - Confirm all data sets used for training/inference are de-identified, consented or otherwise permitted.
 - Verify compliance with HIPAA, institutional policies, and applicable federal and state regulations.
 - Communication for appropriate agreements prior to any external data sharing.
- **Risk Identification & Assessment**
 - Apply Risk Assessment Matrix for identifiability, sensitivity, external sharing, and storage.
 - Identify potential AI-specific risks: data leakage, model inversion, adversarial attacks.
 - Scan environment, including technical developments and regulatory framework impacting risk.
- **Security & Technical Controls**
 - Recommend secure storage and processing environments for models and datasets.
 - Recommend/review encryption, access controls, and audit logging for AI systems.
- **Ethical & Regulatory Alignment**
 - Ensure alignment with NIST AI RMF principles: Govern, Map, Measure, Manage.
 - Coordinate with IRB and HSRO for ethical considerations and participant rights, including consent/waivers.

5.4 Timelines and Escalation

- DSAC will conduct its initial review within five (5) working days from receipt of a completed Data Assessment.
- If timelines cannot be met due to study complexity or pending clarifications, DSAC will notify IRB/HSRO and PI via comment in IBISResearch.

DATA SECURITY & ARTIFICIAL INTELLIGENCE ANCILLARY COMMITTEE
STANDARD OPERATING PROCEDURE

Document Number:	SOP-DSAC-001-01	Effective Date:	06/01/2026
Page No.	Page 6 of 10	Author:	J. Casanova
Title:	Data Security & Artificial Intelligence Ancillary Committee		

5.5 HSRO-Initiated Review (Compulsory/Discretionary)

- Compulsory triggers include requests to modify HIPAA Authorization language that affect data disclosures.
- Discretionary triggers include:
 - Emergent privacy/security/AI concerns in conduct of the study;
 - Sponsor request for the modification of the HIPAA Authorization Form B or HIPAA Addendum to the Informed Consent;
 - Discovery of vendor or data-sharing arrangements, including involving foreign entities;
 - Request for a partial or full waiver of the HIPAA Authorization Form B; or

6. DOCUMENTATION

- 6.1** All documents produced during the course of the Privacy and Security Review, with the exception of personal notes, logs and emails, will be maintained in IBISResearch in accordance with the IRB/HSRO retention policy.
- 6.2** Store electronic copies of working documents produced during the course of the AI, Privacy and Security Review on University-approved secure platforms with appropriate access controls (UM Box).
- 6.3** Documents and images containing PHI/PII may not be stored on personal devices or unapproved services.

DATA SECURITY & ARTIFICIAL INTELLIGENCE ANCILLARY COMMITTEE
STANDARD OPERATING PROCEDURE

Document Number: SOP-DSAC-001-01 Effective Date: 06/01/2026
Page No. Page 7 of 10 Author: J. Casanova
Title: Data Security & Artificial Intelligence Ancillary Committee

7. TEMPLATES / FORMS / TOOLS

7.1 Risk Assessment Matrix

- DSAC makes determinations based on the risk of the study based on the following factors:

Factor	Low	Moderate	High	Notes
Identifiability	De-identified data	LDS/ pseudonymized	Direct identifiers present	Apply HIPAA de-identification or DUA as applicable. Limit access.
Sensitivity	Non-sensitive PII	Health/financial data limited	PHI + sensitive categories (biometric/genomic/geolocation)	See EO 14117 categories
External Sharing	None	Domestic partners under agreements	Cross-border or foreign vendors	Assess DOF 28 CFR Part 202 applicability
Storage & Controls	Approved University systems	Approved cloud with encryption and other privacy/security controls	Non-approved insufficient or unclear controls	Require remediation or alternate solution, including contracting stipulations

DATA SECURITY & ARTIFICIAL INTELLIGENCE ANCILLARY COMMITTEE
STANDARD OPERATING PROCEDURE

Document Number: SOP-DSAC-001-01 Effective Date: 06/01/2026
Page No. Page 8 of 10 Author: J. Casanova
Title: Data Security & Artificial Intelligence Ancillary Committee

8. 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..
06/01/2026	J. Casanova	Comprehensive update: added oversight of AI, ML and LLM in research; added Scope; expanded Definitions; introduced Risk Assessment Matrix; clarified timelines and escalation; added Training and Audit; updated References.

9. RELATED DOCUMENTS AND REFERENCES

- [Ancillary Committee Data Assessment](#)
- [Authorization to Use and Disclose Health Information for Research \(Form B\)](#)
- HIPAA Security Rule – 45 CFR Part 164, Subpart C (Administrative, Physical, Technical Safeguards): <https://www.hhs.gov/hipaa/for-professionals/security/index.html>
- HIPAA Administrative Safeguards – 45 CFR §164.308 (eCFR): <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.308>
- HIPAA De-identification – 45 CFR §164.514 and OCR Guidance: <https://www.ecfr.gov/.../section-164.514>; https://www.hhs.gov/.../hhs_deid_guidance.pdf
- Limited Data Set FAQs (HHS OCR): <https://www.hhs.gov/hipaa/for-professionals/faq/limited-data-set/index.html>
- Personally Identifiable Information (PII) [see definition within FAQ section] - <https://www.research.miami.edu/about/units/2rise/privacy/>
- Executive Order 14117 & DOJ Final Rule – 28 CFR Part 202 (eCFR): <https://www.ecfr.gov/current/title-28/chapter-I/part-202>
- Federal Register Final Rule (DOJ) – 28 CFR Part 202 (Jan. 8, 2025): <https://www.govinfo.gov/content/pkg/FR-2025-01-08/pdf/2024-31486.pdf>

DATA SECURITY & ARTIFICIAL INTELLIGENCE ANCILLARY COMMITTEE
STANDARD OPERATING PROCEDURE

Document Number:	SOP-DSAC-001-01	Effective Date:	06/01/2026
Page No.	Page 9 of 10	Author:	J. Casanova
Title:	Data Security & Artificial Intelligence Ancillary Committee		

- CISA Security Requirements for Restricted Transactions (Jan. 3, 2025): <https://www.cisa.gov/resources-tools/resources/EO-14117-security-requirements>
- NIST SP 800-53 (Latest Release 5.2.0 overview): <https://csrc.nist.gov/News/2025/nist-releases-revision-to-sp-800-53-controls>
- NIST SP 800-171 Rev. 3 (May 2024): <https://csrc.nist.gov/pubs/sp/800/171/r3/final>
- NIST AI Risk Management Framework (AI RMF): <https://www.nist.gov/itl/ai-risk-management-framework>
- DHHS AI Strategy - [Artificial Intelligence \(AI\) Strategy v3](#)
- [IRB Considerations for use of AI in Human Subjects Research](#)

DATA SECURITY & ARTIFICIAL INTELLIGENCE ANCILLARY COMMITTEE
STANDARD OPERATING PROCEDURE

Document Number: SOP-DSAC-001-01 Effective Date: 06/01/2026
Page No. Page 10 of 10 Author: J. Casanova
Title: Data Security & Artificial Intelligence Ancillary Committee

10. SIGNATURES

Prepared by: *Jose Casanova* Date: 06/01/2026
 Joey Casanova, BBA, CIPT
 Data Broker Manager

Approved by: *Terry Butcher* Date: 06/02/2026
 Terry Moore Butcher, MBA, CIPP/US, CIPT
 Manager, IT Security

Approved by: *Ishwar Ramsingh* Date: 06/03/2026
 Ishwar Ramsingh, MBA, CISSP, CISM, CISA, CIPP/E, CIPM, CIPT, CHC, CHRC
 Executive Director – Research Privacy

Approved by: *T. Smith* Date: 6/2/26
 Timothy Smith, PhD, CISSP, PMP
 Director, Research Informatics Governance & Security












SOP-DSAC-001-01_rev 2026

Final Audit Report

2026-06-03

Created:	2026-06-01
By:	Jose Casanova (JCasanova@med.miami.edu)
Status:	Signed
Transaction ID:	CBJCHBCAABAAvv8zlp6iDH8WTYZudijywPWav_uVO3E_

"SOP-DSAC-001-01_rev 2026" History

-  Document created by Jose Casanova (JCasanova@med.miami.edu)
2026-06-01 - 7:21:00 PM GMT- IP address: 129.171.6.113
-  Document emailed to Terry Butcher (tmbutcher@miami.edu) for signature
2026-06-01 - 7:21:45 PM GMT
-  Email viewed by Terry Butcher (tmbutcher@miami.edu)
2026-06-02 - 3:10:58 PM GMT- IP address: 73.245.133.32
-  Document e-signed by Terry Butcher (tmbutcher@miami.edu)
Signature Date: 2026-06-02 - 3:54:35 PM GMT - Time Source: server- IP address: 73.245.133.32 - Signature Appearance Selected: IMAGE
-  Document emailed to Timothy Smith (txs908@med.miami.edu) for signature
2026-06-02 - 3:54:37 PM GMT
-  Email viewed by Timothy Smith (txs908@med.miami.edu)
2026-06-02 - 5:05:14 PM GMT- IP address: 104.47.58.126
-  Document e-signed by Timothy Smith (txs908@med.miami.edu)
Signature Date: 2026-06-02 - 5:05:44 PM GMT - Time Source: server- IP address: 129.171.6.208 - Signature Appearance Selected: IMAGE
-  Document emailed to Ishwar Ramsingh (iramsingh@med.miami.edu) for signature
2026-06-02 - 5:05:46 PM GMT
-  Email viewed by Ishwar Ramsingh (iramsingh@med.miami.edu)
2026-06-03 - 3:27:58 PM GMT- IP address: 104.47.55.126
-  Document e-signed by Ishwar Ramsingh (iramsingh@med.miami.edu)
Signature Date: 2026-06-03 - 3:28:26 PM GMT - Time Source: server- IP address: 129.171.6.116 - Signature Appearance Selected: IMAGE
-  Agreement completed.
2026-06-03 - 3:28:26 PM GMT