Tackling Technology & Data Trends

CURATING CONNECTION

SBS IRB Grand Rounds 2025

April 16, 2025

Joey Casanova, CIPT
Data Broker Manager

Vivienne Carrasco, MPH, CIP
Associate Director, Regulatory Oversight (HSRO)

Allan Gyorke
Deputy CIO

SBS IRB Grand Rounds 2025

2/12/2025 10-11am	**Building Blocks of Protocol Success**
3/12/2025 10-11 am	Carpe Diem: Dealing with & Planning for Tight Deadlines
4/16/2025 10-11am	Tackling Technology & Data Trends
5/7/2025 10-11am	Keeping the House in Order

Relevant Conflicts

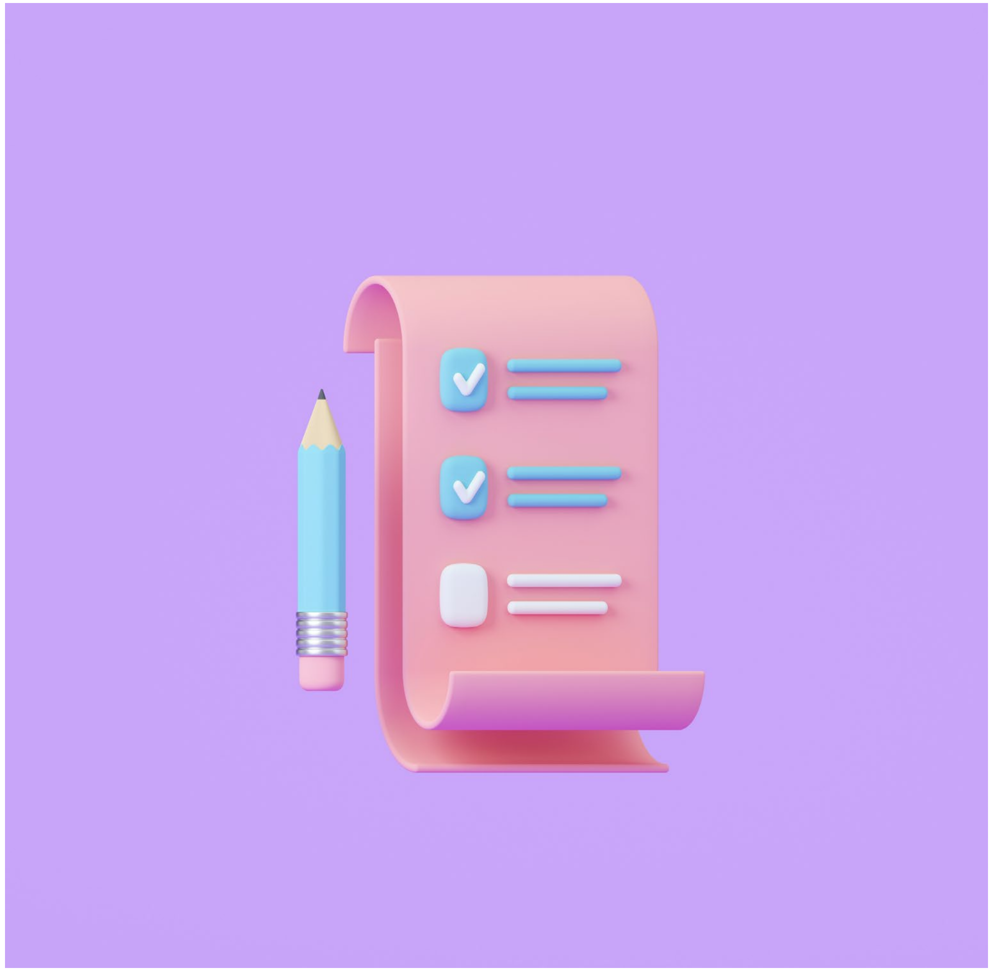
- I DO NOT have an actual or potential conflict of interest in relation to this program/presentation.

CURATING CONNECTION

SBS IRB Grand Rounds 2025

Objectives

- Describe appropriate steps to ensure data security/ privacy/ confidentiality
- Identify potential vulnerabilities with linking lists/data storage/ sharing
- Illuminate industry trends & best practices in social media and econsent especially in vulnerable communities
- Discuss AI in research & data analysis



Data Management and Compliance

Joey Casanova, CIPT

Data Broker Manager

I have no conflicts of interest related to the content of this presentation. I have no financial, personal or professional affiliations that could influence the material or conclusions presented.

The views and opinions expressed in this presentation are solely those of the presenter and do not necessarily reflect the official policies or positions of the University of Miami. This presentation does not supersede any official guidelines or policies of the institution.

Your Role as a Researcher/Study Team

PI is always ultimately responsible for Data Management and Compliance

1

- Able to delegate responsibility to a proxy or other study team member
  - data mgmt primary
  - consider secondary as well

2

- Dual role of minding of administrative responsibilities and conducting the research

3

- How will data be stored, managed, analyzed, shared and preserved through the entire study lifecycle?

4

- Provides a reference framework for how to conduct research in line with best practices

5

- Practices aligned with career- and established research professionals (such as RCS personnel)

You may have to exercise some, many, or all of the following recommendations…

How are your acquiring your data?

Data generated by investigator or study:	
Experiment	A scientific procedure undertaken to make a discovery, test a hypothesis, or demonstrate a known fact
Observation	The action or process of observing something or someone carefully or in order to gain information
Simulations	The production of a computer model of something, especially for the purpose of study
Derived/ Compiled	Base data on a logical extension, modification, or collection of items

Data acquired from others:

- Does the data you need already exist?
  - Do you know how and where to find it?
- Is it already licensed by UM or need to be acquired?
  - Are appropriate funds available if needed?
- Does it require an appropriate agreement?

Guarantee efficient & accurate collection

Tools/applications for data collection at UM (e.g., surveys/chart reviews)

- REDCap (must be utilized when PHI is captured) or Qualtrics

Does the research study require additional support by UMIT/UHealth IT (e.g., implement new tech, etc)?

Clinical Data Requests (from UHealth/UChart)

- https://www.research.miami.edu/about/admin-areas/privacy/data-brokers/request-clinical-data/index.html
- Generally delivered by UHealth IT via UM Box
  - Study teams should copy these source files to their own UM Box or other approved UM-storage locations
  - Setup study-specific authorized cloud folder structure
  - Understand how permissions work & maintain access lists
- Initial release authorized to members of the study team in IBIS Research
  - PI/study team responsible for ensuring subsequent recipients of identifiable data are appropriately authorized

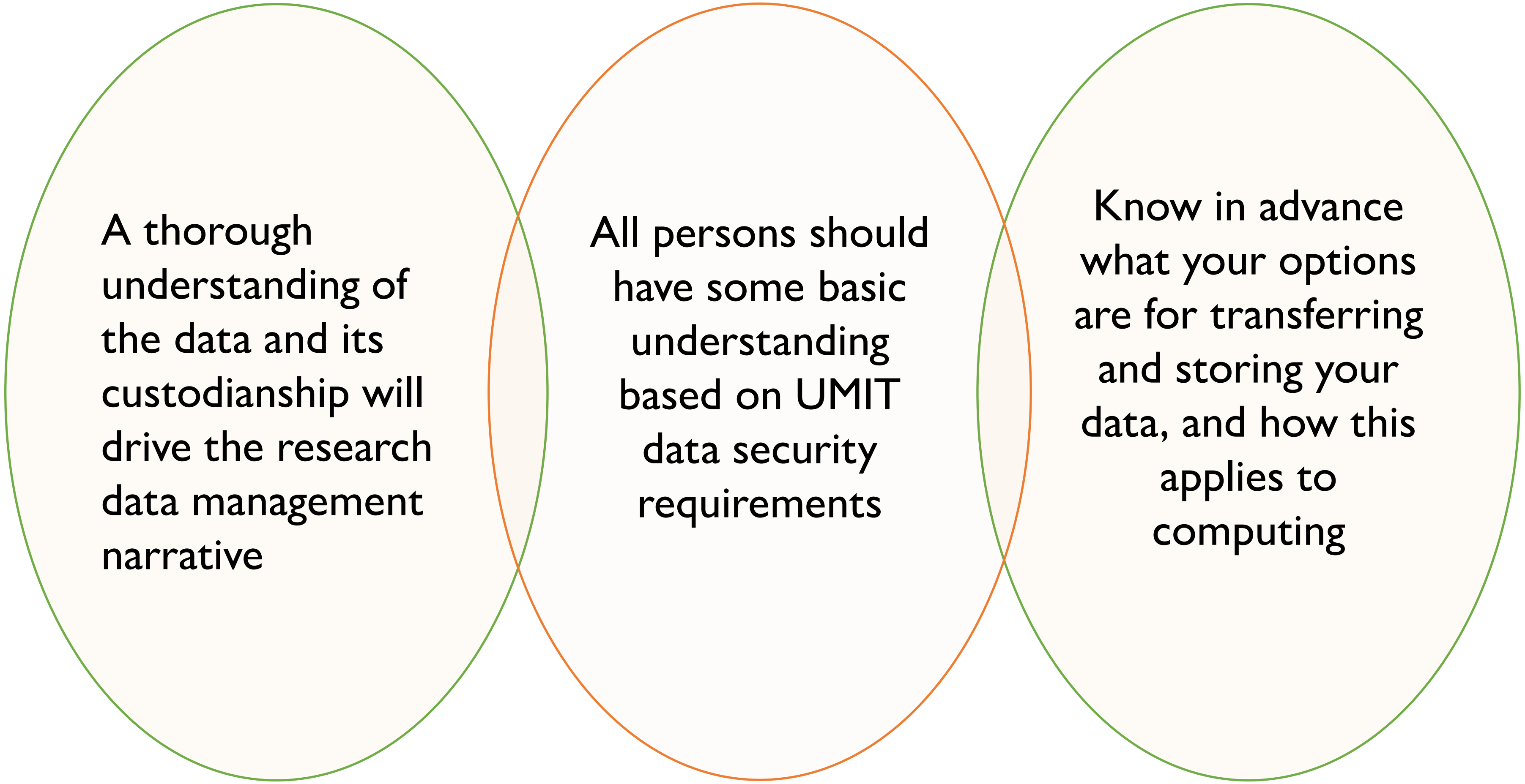
NIH Guidance Regarding Social Media Tools

1. Implications of privacy in a new and less-controlled environment
2. How research and materials will be used.
3. Locked format for informational data
   - Study Title
   - Purpose of the study (in plain language)
   - protocol summary
   - basic eligibility criteria
   - study site location(s), and
   - how to contact the study site for further information
4. Privacy of the "contact for further information site"
5. Escalated the speed of interaction, allowing for greater opportunities for errors in protecting private information
6. Problems related to the portability and secure handling of information, including the encryption devices, encryption during transport, and reporting of unintended breaches
7. Complete strategy for use of the social media, protection of privacy, and informed consent explicitly described to the IRB
8. Invasive nature of joining groups (i.e., support groups, disease groups, advocacy groups, etc.) for the purpose of recruitment

https://www.nih.gov/health-information/nih-clinical-research-trials-you/guidance-regarding-social-media-tools

https://umhs-umhc.policystat.com/policy/16122383/latest

Data Security: An Important Planning Step!



A thorough understanding of the data and its custodianship will drive the research data management narrative

All persons should have some basic understanding based on UMIT data security requirements

Know in advance what your options are for transferring and storing your data, and how this applies to computing

https://www.research.miami.edu/about/admin-areas/privacy/data-brokers/data-handling-guidelines/index.html

Data Protection Regulation & Policies

- **HIPAA**
  - 18+ identifiers – alone or in combination datasets
  - Valid Authorization
- **Common Rule (Updated)**
  - U.S. Federal policies mandating the protection of Human Subjects
  - Informed Consent
- **FERPA**
  - Education information and special protections
- **GINA**
  - Protects individuals from discrimination based on their genetic information
- **GDPR** (General Data Protection Regulation in Europe)

Florida Data Protection Regulations

- **Florida Information Protection Act of 2014 (FIPA)**
  - Requires companies to obtain consent before collecting personal information
  - Prohibits selling personal information without consent
  - Regulates security breach notification requirements
- **Florida Digital Bill of Rights (2023)**
  - Defines residents' rights to access and correct personal data collected by companies
  - Requires opt-in for data sharing
  - Includes protections for children in online spaces
- **Florida Deceptive and Unfair Practices Act (FDUTPA)**
  - Provides protection against various privacy-related violations, including false advertising, deceptive practices and misrepresentation of products or services
- **Florida Security of Communications Act (FSCA)**
  - Prohibits unauthorized interception, use or disclosure of electronic communications without the consent of the parties involved
- **Protecting DNA Privacy Act**
  - Individuals own their genetic information
  - Requires express consent for collection, analysis, retention, sale etc.

Data Classification Levels

UMIT Data Classification Policy

https://umiami.policystat.com/policy/token_access/0acc2dcc-0e0e-4599-bdb6-daab78c5ea1b/

Public	Sensitive	Private	Confidential (Restricted)
Available to anyone without any legal restrictions on access or use.	**Not approved for general or public distribution.**	**Considered proprietary and critical to the ongoing business continuity and operations of the University**	**University is under legal or contractual obligation to protect from disclosure, alteration or destruction.**
• Tuition and fees • Annual reports • Press statements • External facing website and social media, blogs, etc. • Employee names, titles, work phone numbers, work address, email addresses	• Accounting and financial information not otherwise classified as Confidential data (internal use only) • Prospective student/applicant information • Prospective employee/applicant information	• Salaries • Financial transactions which do not include confidential data • Educational records required for business and educational purposes • Information that is related to a student, faculty, employee	• Medical research technology • Controversial research topics • Financial information • Donor names and account numbers • PHI, patient data, health and medical records. • Intellectual property. • Information covered by non-disclosure agreements.

All Research Data falls in one of these two categories

Considerations for Non-Public Data

- Sensitive Data: human subjects, anything proprietary, or covered by DUA
- Deidentification may be tedious yet important step
  - *Highly recommend* that this be asked of data provider if possible
- Re-identification by grouping secondary data (or indirect identifiers) is very possible
  - Consider multiple approaches to permit data granularity and fidelity while preventing re-identification
  - E.g. if 1st three digits of ZIP codes + year of birth == 0.04% of individuals can be re-identified vs ZIP + birthday + sex == 87% (Sweeney et al.; 2000)
- Just as important to promote preservation and re-use of sensitive data
  - Get consent to retain and share data
  - Incorporate data-retention and -sharing clauses into study protocol and ICF
- Many evolving techniques to safeguard privacy yet promote reuse

Potential Vulnerabilities of data storage solutions

Insufficient Data Security Measures

- Weak encryption
- Poor access controls

Software Vulnerabilities

- Outdated software
- Unpatched vulnerabilities

Inadequate Backup Solutions

- Lack of redundancy
- Unsecured backups

Human error

- Misconfiguration
- Negligence

Cloud Storage Risks

- Shared infrastructure
- Data leakage

Physical Security

- Theft or damage
- Environmental hazards

Scalability Issues

- Limited scalability
- Cost constraints

Insider threats

- Malicious insiders
- Unintentional leaks

CURATING CONNECTION

SBS IRB Grand Rounds 2025

Data Security

- Security is more than where you store it
  - It's how you approach the care, handling, and movement of data
- Will vary depending on sensitive data level
- Is important to consider while on- and off-campus
  - Email at home?
  - Using your mobile phone or tablet
  - Even more important in our remote-work status
- May be determined by Data Safety plan.
- And these other helpful websites:
  - Remote Access Policy https://umiami.policystat.com/policy/token_access/50943793-1d90-4b81-87e8-30abd8fb3de6/
  - Protected Data Access and Confidentiality https://umiami.policystat.com/policy/token_access/9bf059a2-5075-4a69-b232-a08373c08351/

Coded Data and Linking Lists

Allows data to be traced back if necessary but keeps identities protected

1. Assign unique, randomly generated codes
2. Pseudonymization
   - Generalize specific details when possible (i.e. “teacher” vs. “high school math teacher”)
   - Aggregate demographic information (e.g. age ranges – “20-30”)
   - Perturbation
     - Random Noise
     - Masking Sensitive Data
     - Data Shuffling
3. Consider where the code-to-identifier list is stored
4. Regularly assess reidentification risk

Research Data Retention

- How long do I need to keep research records?
  - Federally funded:
    - min. 3 years
  - FDA-regulated:
    - min. 2 years after marketing application is approved
    - Min. 2 years after study discontinued and FDA notified product approval will not be sought
  - HIPAA-regulated:
    - Min. 6 years after completion of research
  - Contractual & Study specific obligations may vary
- Long term storage
  - If keeping locally, follow security protocols (for example, a locked cabinet for paper records; secure/restricted network space which is routinely backed up)
  - https://umhs-umhc.policystat.com/policy/12620532/latest

Additional Considerations

- **Who will access the data?**
  - External collaborators based outside of the US → may need vetting with **UM Export Control**
- **What technologies will be utilized in the project?**
  - MS Copilot is the University's approved AI solution
  - Use of ChatGPT is not permitted for use with any patient data
  - All AI-based projects must be vetted through **UM AI Governance Committee**
- **Where will the data be held?**
  - Internal vs External
  - Considerations if External:
    - Data transmission method
    - Where will data be hosted? (outside of US → vet with **UM Export Control**)
    - Must vet with **UHealth IT Cybersecurity**

Data Sharing

Limitations in de-identifying data

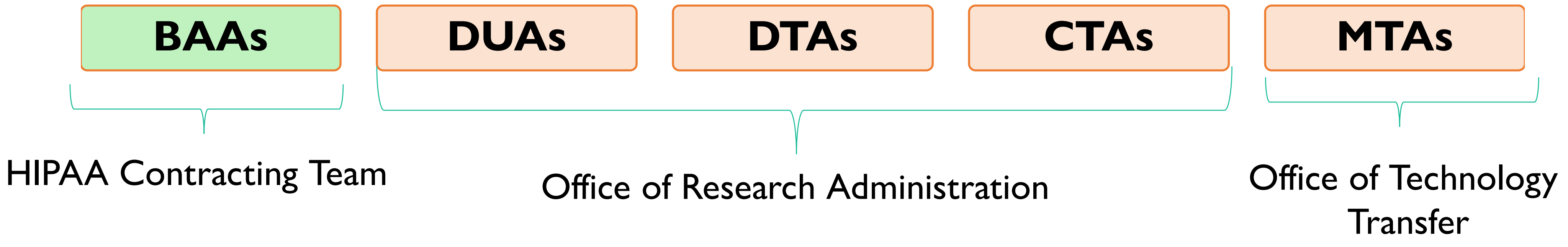
Many AI projects request unstructured data (e.g., notes/reports) and images

Software/tools can be used to assist in censoring PHI

However, none can provide 100% assurance that all PHI is removed

Therefore, study teams are responsible to **manually** review/certify all such data are de-identified to be considered as such

Agreements



BAAs

DUAs

DTAs

CTAs

MTAs

HIPAA Contracting Team

Office of Research Administration

Office of Technology Transfer

- Govern access to and treatment of data:
  1. May be required by an outside organization to your organization for use in your organization's research, or
  2. Provided by your organization to an outside organization for use in its research
- Important in the context of <u>protecting</u> ownership/privacy of UM research data
- Agreements module in IBIS-Research

In Summary…

- Think carefully about data collection, including security & legal documents
- There are many options for storage, security, and analysis – choose thoughtfully & wisely
- Data dissemination and preservation are important considerations throughout all phases of your work
- Please reach out to the Human Subject Research Office (hsro@miami.edu), the Data Security Ancillary Committee (dsac@miami.edu), the Data Broker Team (databroker@miami.edu) and/or UMIT Cybersecurity (help@miami.edu / help@med.miami.edu) with your questions. And please reach out sooner.

We wish you success in your research

Electronic consent (e-consent)

Vivienne Carrasco, MPH, CIP
Associate Director, Regulatory Oversight (HSRO)

e (Electronic)- Consent vs Remote Consent: Digital Systems compared to physical location!

In-Person Consent: a method of obtaining informed consent using an electronic system instead of a paper consent form.

For example, DocuSign, an iPad/tablet that displays the consent form in REDCap, discussing the consent form in person and then the participant agreeing to participate by tapping the appropriate button in REDCap.

Remote Consent: obtaining informed consent form where the study team and participant are not in the same physical location during the consent process.

*This can be achieved through various methods like phone calls, video conferencing, or online platforms, with the aim of ensuring the participant understands the study and agrees to participate. .

Considerations:

*Not all e-consent systems contain the ability to document legally effective signatures.

UM-Supported system REDcap ✓

Participants:

- Age
- e literacy and comprehension
- Physical limitations
- Participant verification

System

- Data Security and Privacy
- Part 11 (FDA studies)
- Version control
- Study Impact
- SOP: example- new information?

Technology limitation:

- Internet connectivity/stable Wi-Fi
- Smartphone/computer access
- Phone service usage
- Software use

E-Consent in Vulnerable Communities

- *When implementing e-consent in vulnerable populations, key considerations include* ***ensuring accessibility (perhaps remote consent is an alternative?)****, understanding, and voluntariness of the process. This involves providing clear and understandable information, offering alternative formats like paper consents for those uncomfortable with technology, and ensuring the process is flexible and accommodating to individual needs.*
- Belmont Principle and approval criteria listed in Sections 111
    - Respect for Persons
        - Improve Understanding (Videos, FAQs, Comprehension Checks)
        - Screen reader compatibility and adjustable fonts (accessible to individuals with disabilities)
        - Protect Privacy (Robust Data Security Measures, Clear Privacy Policies)
    - Beneficence
        - Identify and reduce the risks considering the vulnerable communities
    - Justice
        - Consideration of the potential impact of the research on vulnerable populations
        - Are alternative formats appropriate?

Recommendations for e-Consent

Pros:

- eConsent in IRB (Institutional Review Board) can:
  - Provide improved participant understanding of informed consent
  - Increase convenience and accessibility
  - Streamline workflows
  - Enhanced data capture and verification.
  - Increased regulatory Compliance
  - Reduce paperwork and improve efficiency in the research process

Cons:

- Ensuring proper documentation, verifying identity
- Guaranteeing comprehension of the consent process by participants
- Ensuring that the electronic signature is legally valid and attributable to the individual (Redcap)
- Ensuring the consent process is accessible to all participants, regardless of their digital literacy or ability to access technology.
- Assent of Minors

CURATING CONNECTION
SBS IRB Grand Rounds 2025

Key Questions About the Use of AI as Part of an IRB Review

ALLAN GYORKE

DEPUTY CIO

Typical AI Questions:

Processing Data:

- Are you processing sensitive data?
- Are you using a UM-managed AI system or an external AI system?
- Is the data transmitted and stored securely?
- Who has access to the data?
- Has the company agreed not to use the data for other purposes?
- Is the data being used to train AI models?

Generating Content:

- Are you using an AI system to generate content like images or scripts?

Participant-Bot Interaction:

- Are the participants aware that they are interacting with a bot?

Are you processing sensitive data?

No – Public Data

Example: I am analyzing Twitter streams for content related to local elections.

Example: I am analyzing drafts of legislation proposed by state governments related to infrastructure funding.

Yes – Sensitive Data

Example: I am using AI to analyze student journals and recommend mental health practices.

Example: I am analyzing private communication between a legal team and client.

Are you using a UM-managed AI system or an external AI system?

UM – Managed

- The system leverages the university's Copilot licenses
- The system I am using is run by IDSC on University servers

External

- I have my own license for ChatGPT that I will be using for this study.
- I am using Fireflies to record and transcribe subject interviews

Is the data transmitted and stored securely?

- “Encrypted in Transit” means that the data is securely sent from its origin to the AI system.

- “Encrypted at Rest” means that when the data is stored, it is encrypted so it can’t be easily read.

Who has access to the data?

- Ideally, no one aside from the researchers. Some AI companies will access data for quality assurance or leverage third-party companies.

Has the company agreed not to use the data for other purposes?

- One company said that they could and would leverage any content submitted to their system for marketing and commercial purposes. Read the fine print.

Is the data being used to train AI models?

- Hopefully not. You don't want your sensitive information showing up as output for other people. This violates confidentiality and anonymity.

Are you using an AI system to generate content like images or scripts?

- This is generally okay, but it depends on the case. The biggest concern is cultural bias and potentially disclosure to research participants about the origin of the content.

Are the participants aware that they are interacting with a bot?

- This should be disclosed to participants so they are not being deceived. Some participants may bond with AI characters and act according to their instructions. Others may change their behavior if they see the AI character as an expert.

What next?

Collect answers to these questions

Include links to data use agreements and privacy statements

For now: contact me (a.gyorke@miami.edu) for review if your study involves using AI with sensitive data

IRB Grand Rounds - Continuing Nursing Education (CNE) Evaluation and Registration

UNIVERSITY OF MIAMI
SCHOOL of NURSING
& HEALTH STUDIES

SHARE.
SIMULATION HOSPITAL ADVANCING RESEARCH & EDUCATION

ACCREDITED
PROVIDER
AMERICAN NURSES
CREDENTIALING CENTER

Nursing Continuing Professional Development (NCPD)

The University of Miami School of Nursing and Health Studies is accredited as a provider of nursing continuing professional development by the American Nurses Credentialing Center's Commission on Accreditation.

Thank you!/ Questions?

5/7/25 SBS IRB Grand Rounds

Keeping the House in Order

For additional information please contact curatingconnection@miami.edu and reference IRB Grand Rounds.

CURATING CONNECTION

SBS IRB Grand Rounds 2025