GUARDIANS OF THE DATA IN THE DIGITAL AGE

- Describe appropriate steps to ensure data security/ privacy/ confidentiality
- Identify potential vulnerabilities with data storage/ sharing
- Explore AI in research & data analysis

Speakers: **Ishwar Ramsingh,** Executive Director, Research Privacy – Data Broker
Joey Casanova, Data Broker Manager, Research Privacy – Data Broker
Timothy Smith, PhD, Director, IT-Research Informatics Governance & Security-UHCORP
Guest speaker: Carlos A. Canales, Manager, Business Process Analytics, CTSI

UNIVERSITY OF MIAMI
OFFICE of the VICE PROVOST for RESEARCH & SCHOLARSHIP

All presenters have indicated that they have no relevant financial relationships with ineligible companies.

CURATING CONNECTION
IRB Grand Rounds 2026

IRB Grand Rounds 2026 - Virtual Series

Time	Topic	SPEAKER
January 15, 2026, 10-11 am	State of our Union: Updates & Best Practices	ORA, RIC, EHS, IITSU, HSRO
February 19, 2026, 10-11 am	Guardians of the Data in the Digital Age	Data Brokers, AI
March 19, 2026, 10-11 am	**Key Ingredients to Running a Successful Clinical Trial (UM & JHS)**	**IITSU, JHS, CTD**
April 16, 2026, 10-11 am	Balancing Act: Biobanking, Big Data & Data Privacy	RI, OTT
May 21, 2026, 10-11 am	Beyond the Approval: Building a Culture of Compliance	RQA, DSAM, EC

GUARDIANS OF THE DATA IN THE DIGITAL AGE

Protecting Privacy, Confidentiality & Trust in Human Subjects Research

MIAMI

Ishwar Ramsingh, Executive Director, Research Privacy – Data Broker

Joey Casanova, Data Broker Manager, Research Privacy – Data Broker

Timothy Smith, PhD, Director, IT-Research Informatics Governance & Security-UHCORP

Why Data Protection Matters in Human Subjects Research

Human subjects data = **people, not just records**

Ethical foundations: **Respect for Persons, Beneficence, Justice**

Regulatory expectations: **IRB approval ≠ data security guarantee**

CURATING CONNECTION
IRB Grand Rounds 2026

What We Mean by Data Security, Privacy and Confidentiality

DATA SECURITY: SAFEGUARDS THAT PROTECT DATA FROM UNAUTHORIZED ACCESS

PRIVACY: INDIVIDUALS' CONTROL OVER THEIR PERSONAL INFORMATION

CONFIDENTIALITY: RESEARCHER OBLIGATION TO PROTECT IDENTIFIABLE DATA

Role of the Institutional Review Board

Reviews how identifiable and sensitive data will be **collected, stored, accessed, shared, retained, and destroyed**

Assesses whether **privacy and confidentiality protections are appropriate** to the level of risk

Requires that **all secondary uses of data** (including AI/ML analysis not described in the original protocol) receive IRB determination

Ensures consent language accurately reflects:

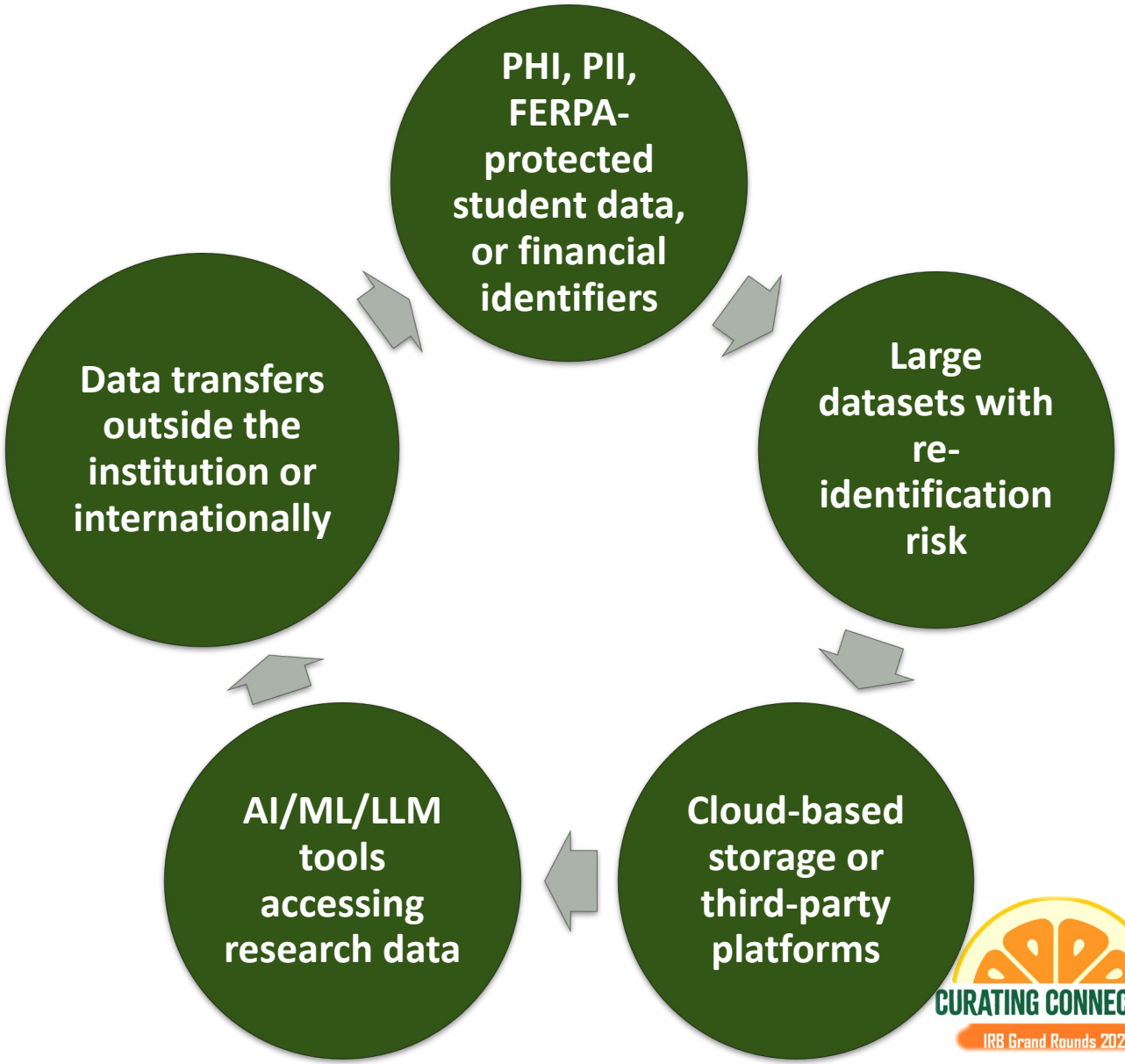
Data sharing plans

Use of third-party platforms

Potential future or AI-driven analyses

Role of the Data Security Ancillary Committee (DSAC)

The DSAC provides specialized oversight of information security risks associated with research involving sensitive or regulated data. DSAC review is typically required when studies involve:



DSAC Considerations

Storage location and encryption controls

Access management and authentication

Vendor security posture and contractual safeguards

Data minimization and segmentation strategies

Incident response and breach notification readiness

Types of Data in Human Subjects Research

- Direct identifiers (name, SSN, MRN)
- Indirect identifiers (dates, ZIP codes, rare diagnoses)
- Sensitive data: Health, genetic, biometric
- Behavioral, educational, financial
- Derived data (models, AI outputs)

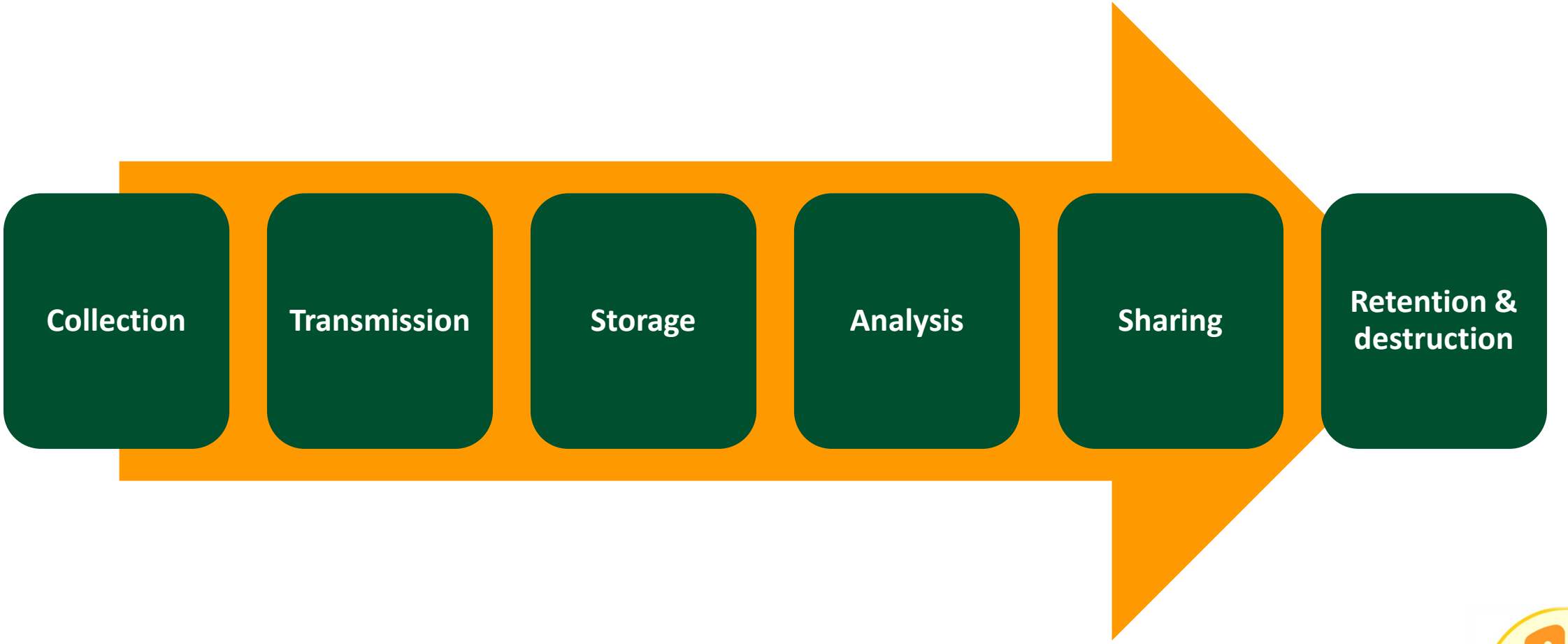
Data Classification Levels

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.

The Data Lifecycle: Where Risk Appears



CURATING CONNECTION
IRB Grand Rounds 2026

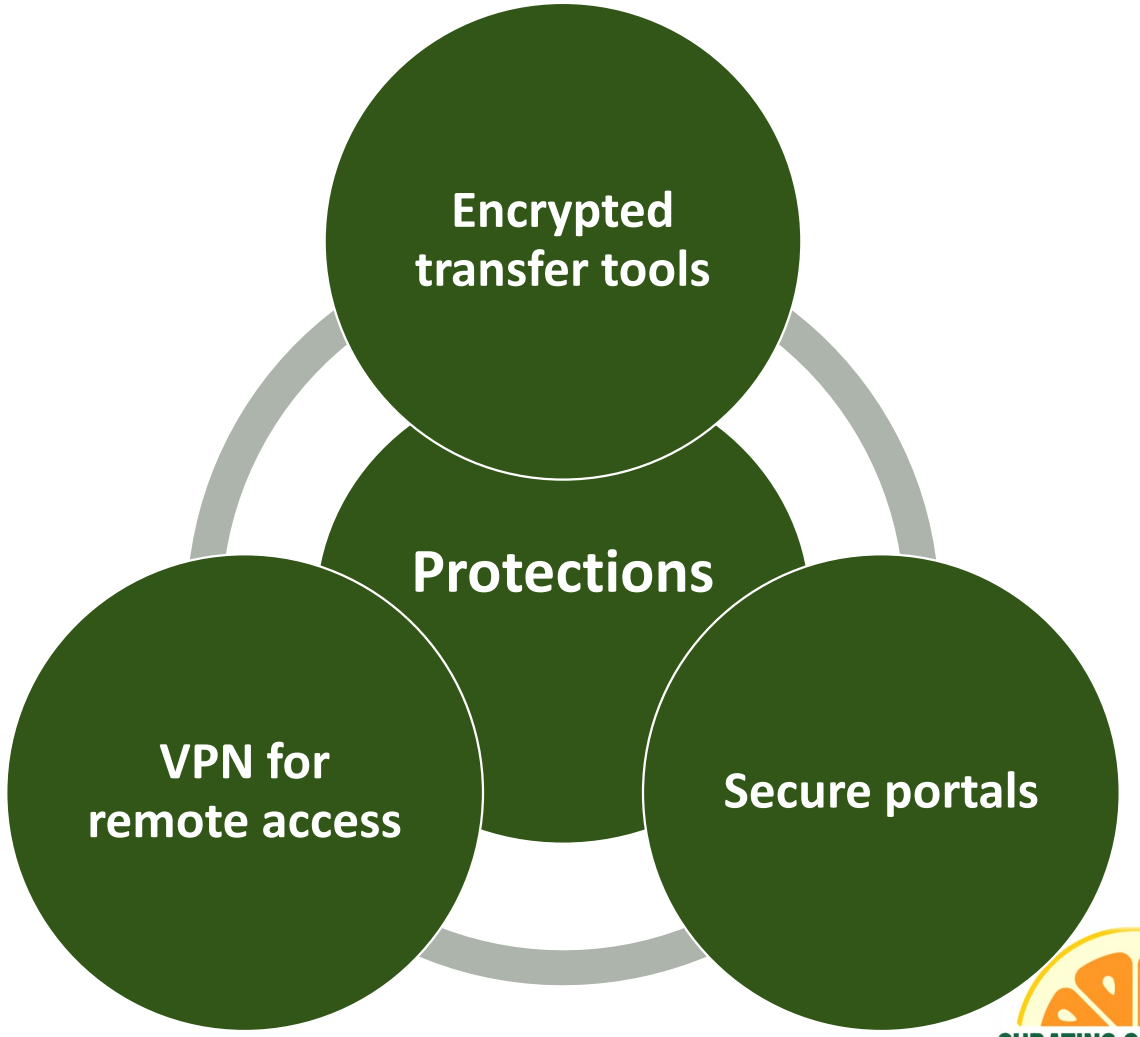
Common Threats to Research Data

Data Collection: Secure from the Start

Best practices

- Collect only what is necessary
- Use institution-approved tools (e.g., UM Box, UM REDCap)
- Avoid free consumer apps for sensitive data
- Separate identifiers from research data when possible

Transmission Risks and Protections



Secure Data Storage

Approved

- [ ] Institutional servers
- [ ] Encrypted, access-controlled cloud environments

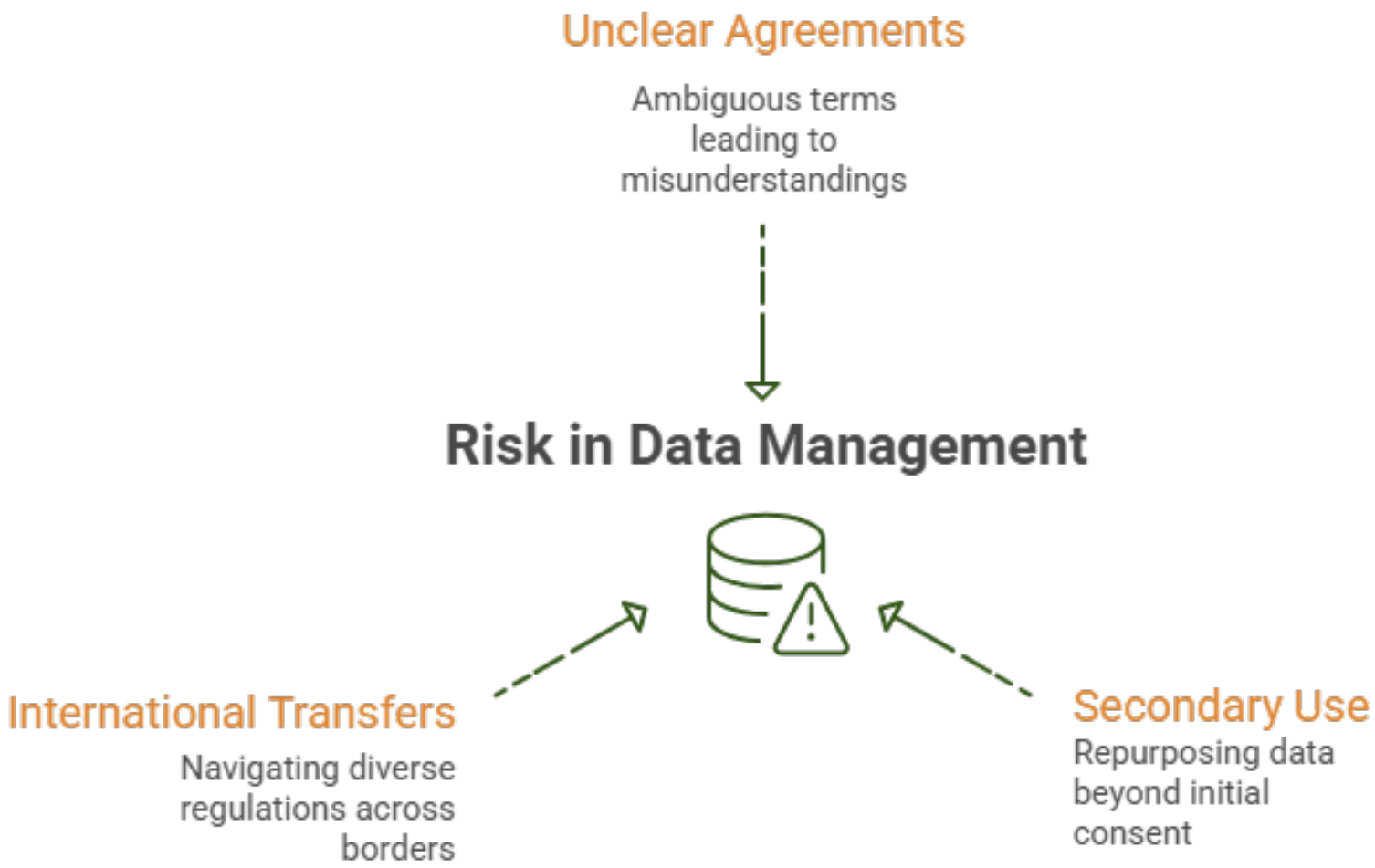
Avoid

- [ ] Personal Laptops without encryption
- [ ] USB Drives
- [ ] Shared folders without role-based access

CURATING CONNECTION
IRB Grand Rounds 2026

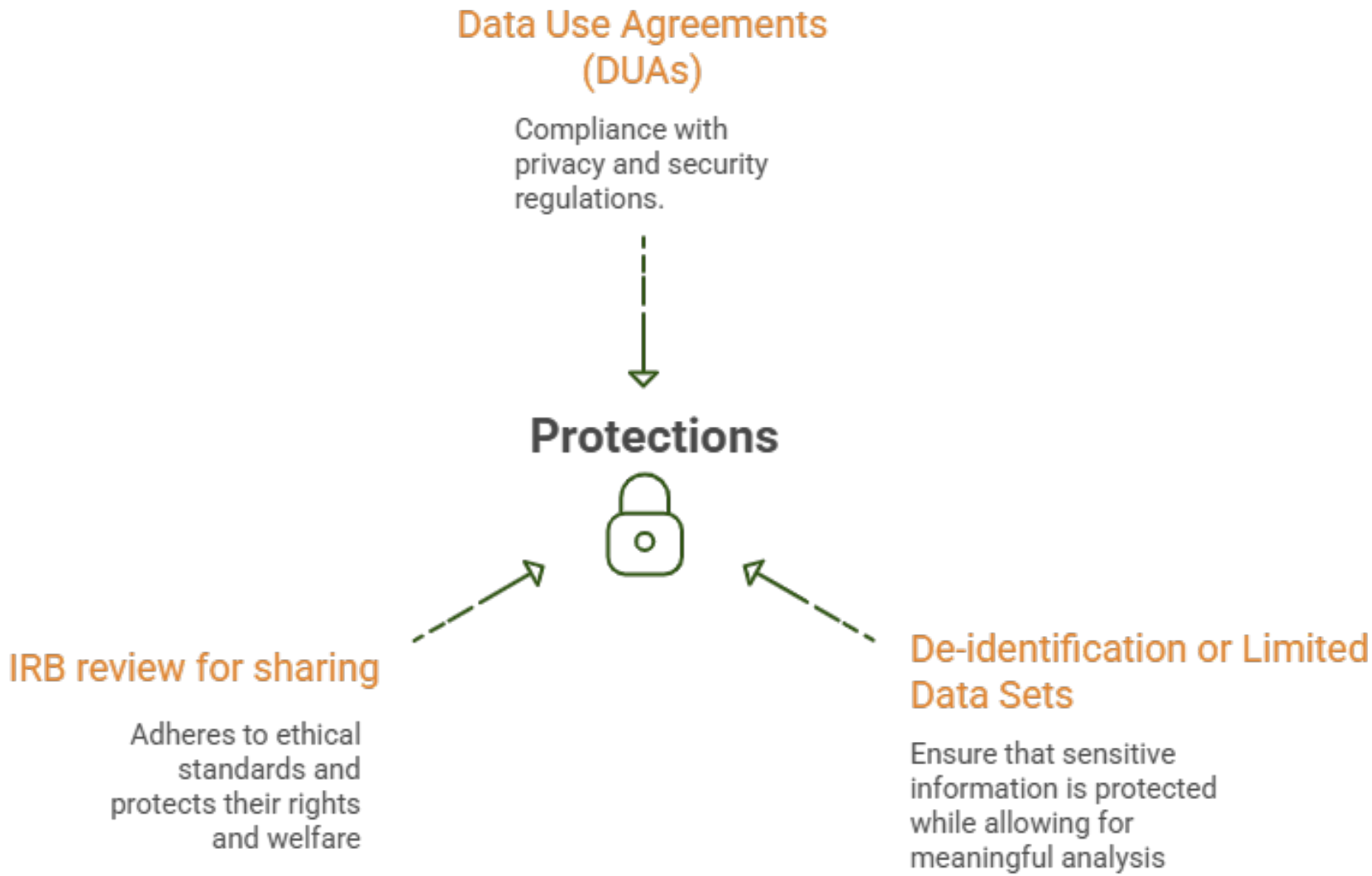
Access Controls and the Principle of Least Privilege

Data Sharing: When, Why, and How



CURATING CONNECTION
IRB Grand Rounds 2026

Data Sharing: When, Why, and How Cont.



De-identification is Not Bulletproof

- Small datasets increase re-identification risk
- Data linkage across sources
- AI can infer identities from patterns

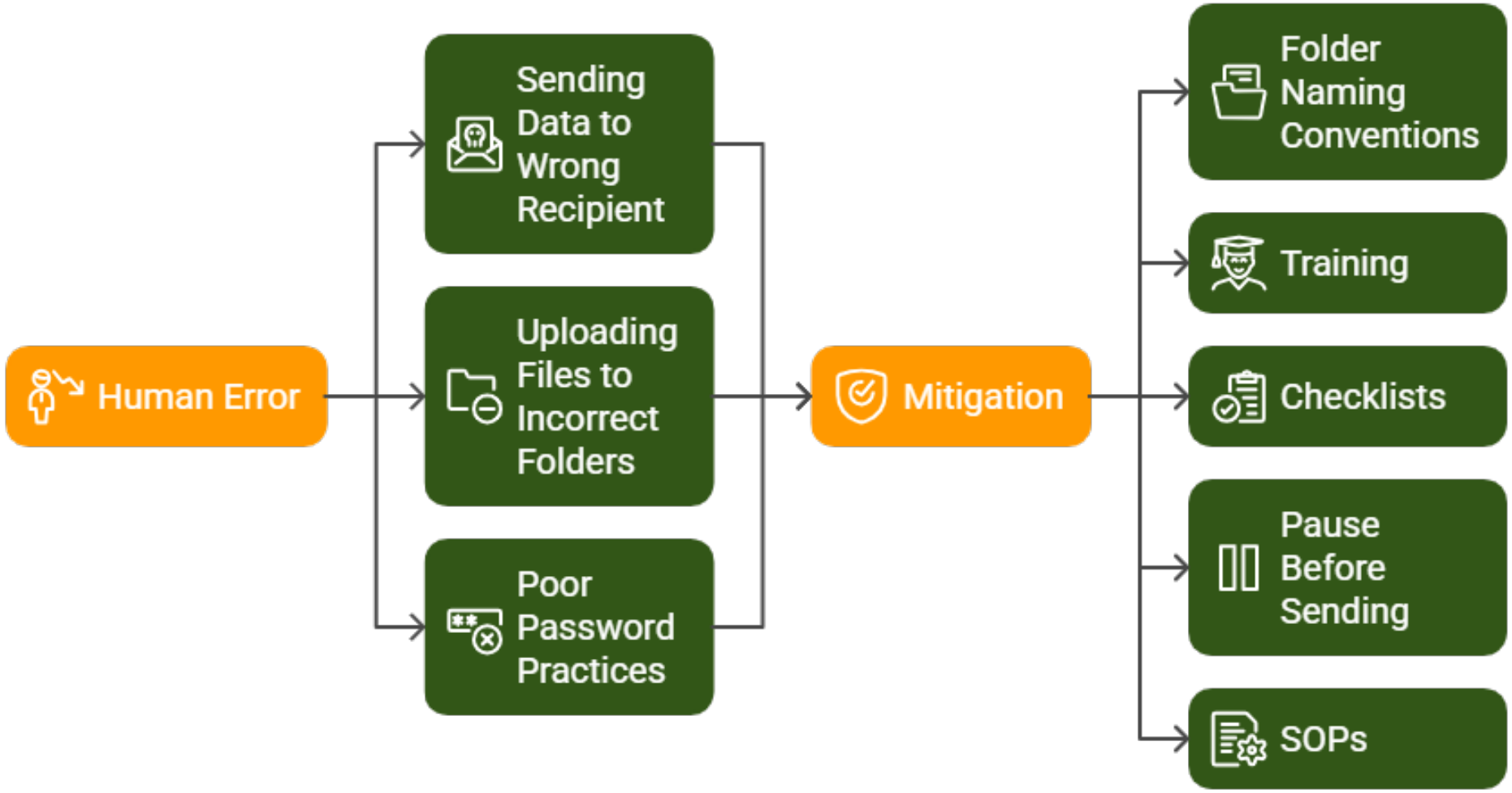
Retention and Secure Destruction

Follow IRB and sponsor retention requirements

Secure deletion (not just “delete”)

Paper records: shredding or secure disposal

Human Error: The Biggest Vulnerability



Working with Vendors and Collaborators

Investigator Responsibilities

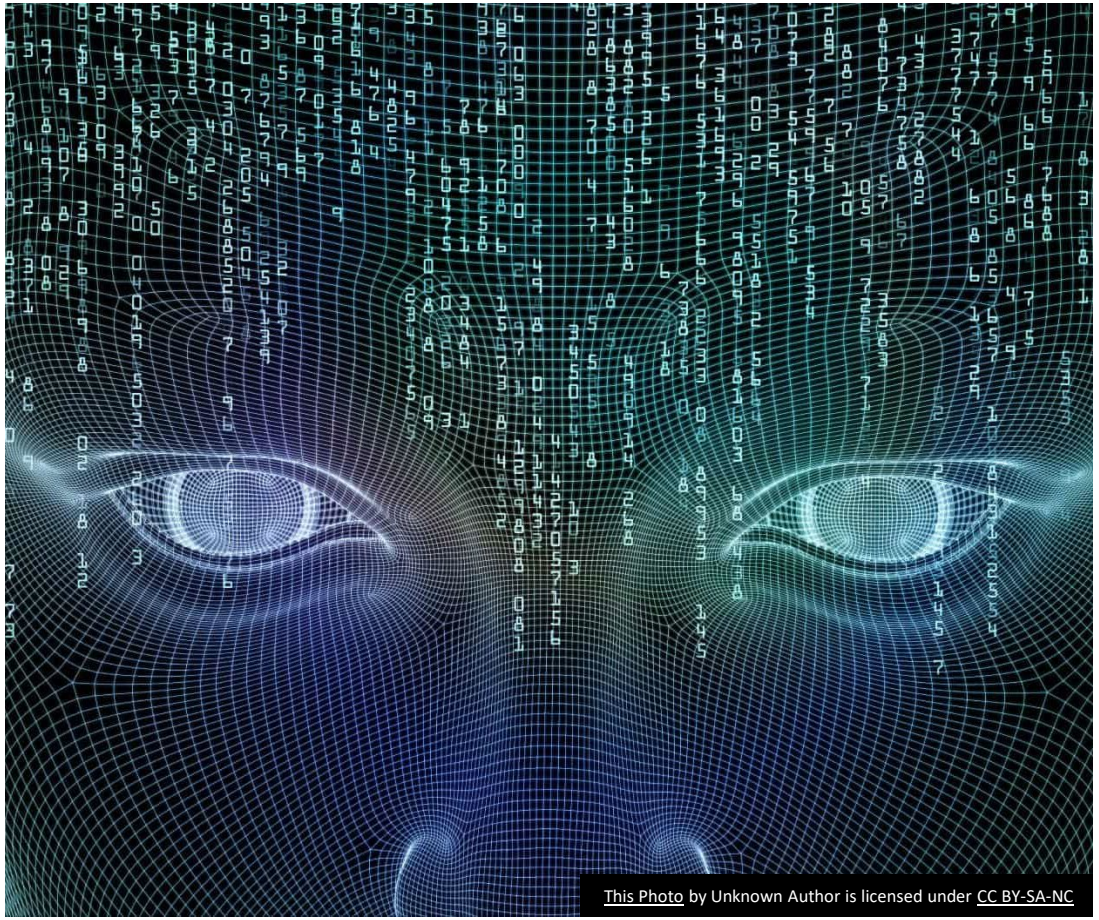
Principal Investigators are expected to:

- Use **institution-approved systems** for data collection and storage
- Ensure study personnel complete required privacy and security training
- Promptly report potential data incidents or near-misses
- Seek IRB/DSAC review before implementing new tools, vendors, or AI methods

Failure to comply may result in:

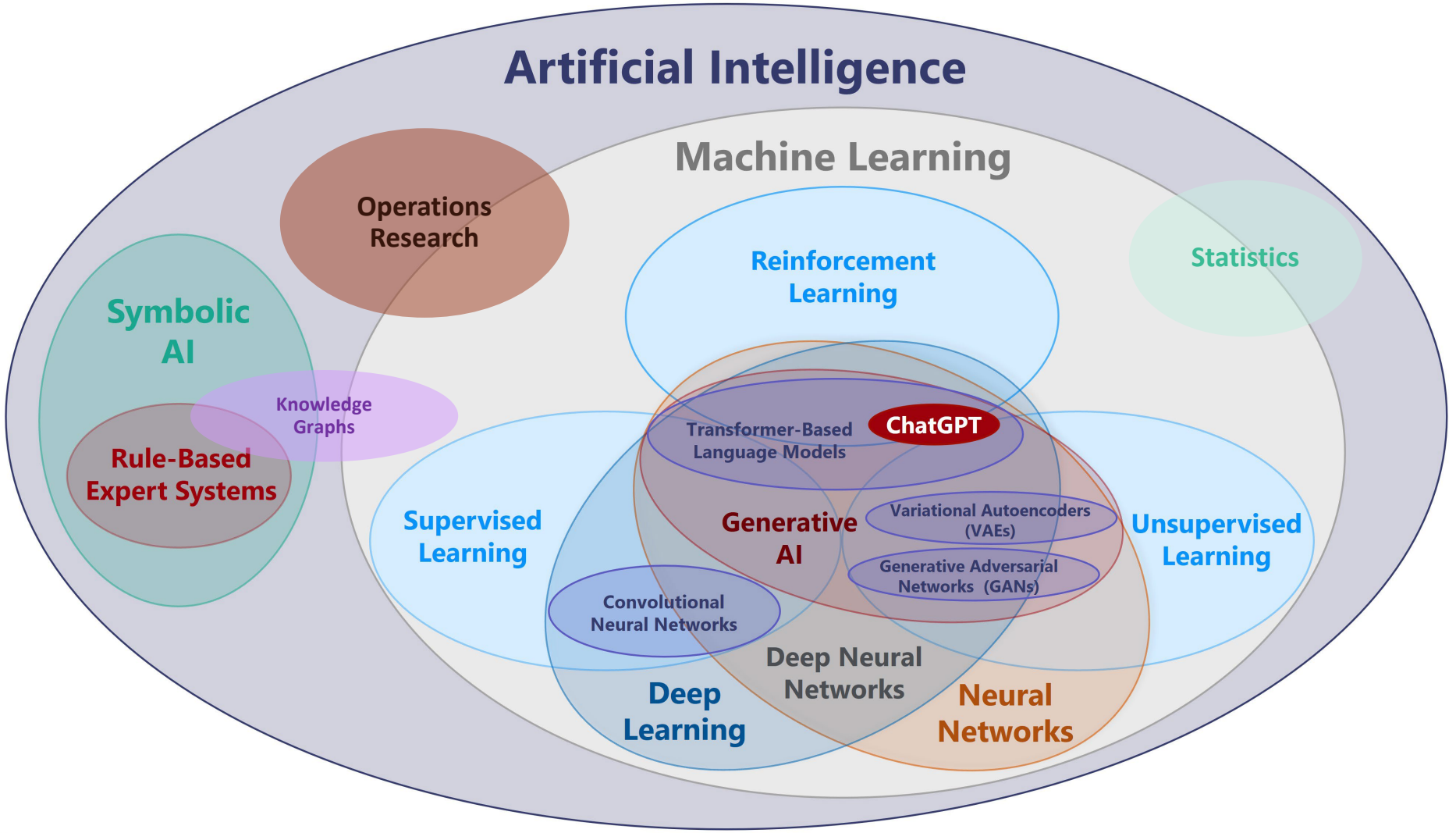
- Study suspension
- Mandatory corrective actions
- Reportability to sponsors or regulators

Artificial Intelligence in Research



- Uses in human subjects research:
  - Medical image analysis
  - Pattern detection
  - Predictive modeling and decision support
  - Natural language analysis (NLP)

What is Artificial Intelligence: AI is an umbrella term



Rev 3.0

Benefits of AI in Research

- Efficiency
- Scalability
- Discovery of hidden patterns
- Automation of repetitive tasks

AI-specific Risks to Human Subjects Data

Uploading sensitive data into public AI tools

Retention of prompts and data

Lack of transparency (“black box” models)

Bias amplification

AI and Informed Consent

Key questions:

- Was AI use disclosed?
- Is secondary use possible?
- Are outputs explainable?
- How AI use may affect participants?

Best Practices for Use of AI in Research

- Use institution-approved AI tools
- No PHI/PII in public AI platforms
- Document AI use in protocols
- Human oversight is mandatory

Acceptable Use Principles for AI in Human Subjects Research

AI tools may be used only when:

- Use is transparently described in the IRB protocol (or approved via amendment)
- Data are not uploaded into public or consumer AI platforms
- The tool has undergone institutional security and privacy review
- Human oversight is maintained over AI outputs

Prohibited practices include:

- Entering identifiable or sensitive data into non-approved AI tools
- Using AI outputs as the sole basis for decisions affecting participants
- Allowing data to be retained or reused for model training without authorization

Common Themes across Grant Funding Agencies

- **Data Sharing**: Most agencies require open access to AI-generated data, models, and code to support reproducibility.
- **Privacy Compliance**: AI research must follow IRB, HIPAA, and other privacy laws; sensitive data use is tightly controlled.
- **Ethical Use**: Agencies emphasize fairness, transparency, and bias mitigation in AI systems.
- **Security & Legal**: AI projects must comply with cybersecurity standards and export control laws.
- **Generative AI Restrictions**: Reviewers are banned from using generative AI; applicants must disclose its use.
- **Open Science Mandates**: Publications and software from AI research must be publicly accessible.
- **Agency-Specific Ethics**: Some agencies (DoD, NASA, DHS) have formal ethical AI frameworks guiding research.

Regulatory and Oversight Expectations

IRB responsibility extends to data handling

Privacy regulations (HIPAA, FERPA, GDPR where applicable)

Emerging AI governance frameworks (e.g., NIST AI RMF)

Building a Culture of Data Stewardship

- Data protection is a shared responsibility
- Encourage reporting of near-misses
- Normalize asking “Is this allowed?”

Best Practices Checklist

- ✅ Minimize data collection
- ✅ Use approved tools only
- ✅ Encrypt and control access
- ✅ Train staff regularly
- ✅ Review sharing agreements
- ✅ Document AI use
- ✅ Plan for secure destruction

What To Do If Something Goes Wrong

- Do not panic or conceal
- Report immediately to:
  - IRB
  - Privacy Office*
  - IT Security
- Early reporting limits harm

CURATING CONNECTION
IRB Grand Rounds 2026

Key Takeaways

- Human Subjects data requires heightened care
- Most risks are preventable
- AI increases power – and responsibility
- Trust is the foundation of research

CURATING CONNECTION
IRB Grand Rounds 2026

Resources and Contacts

Data Security Ancillary Committee dsac@miami.edu	UMIT Help Desk help@miami.edu
Human Subject Research Office hsro@miami.edu	Artificial Intelligence Use ai@miami.edu
Data Brokers databroker@miami.edu	Information Security infosec@miami.edu
Questions about UM REDCap redcapadmin@med.miami.edu	Suspected Phishing phish@miami.edu
Questions about UChart ucharthd@med.miami.edu	UHealth Privacy Office privacy@miami.edu
Export Control exportcontrol@med.miami.edu	Disclosures and Scholarly Activities dsam@miami.edu

CURATING CONNECTION
IRB Grand Rounds 2026

EVERYONE is a

CURATING CONNECTION

IRB Grand Rounds 2026

ResearchPass

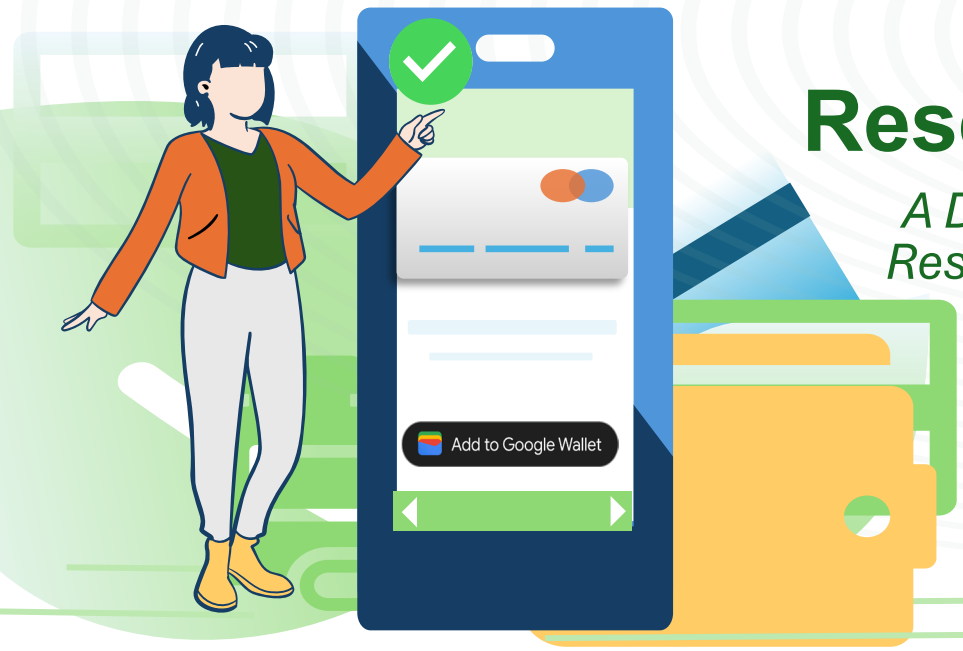
A Digital Study ID for Research Participants

Guest Speaker
Carlos A. Canales
Manager, Business Process Analytics

CTSI MIAMI CLINICAL & TRANSLATIONAL SCIENCE INSTITUTE

UNIVERSITY OF MIAMI
OFFICE of the VICE PROVOST
for RESEARCH & SCHOLARSHIP

CURATING CONNECTION
IRB Grand Rounds 2026



CTSI MIAMI CLINICAL & TRANSLATIONAL SCIENCE INSTITUTE

ResearchPass

A Digital Study ID for Research Participants

ResearchPass give participants instant access to study details and contacts that are easy to share with outside providers.

What is ResearchPass?

BASIC INFO

Built into REDCap, ResearchPass automatically creates a digital study ID that participants can save to Apple Wallet or Google Wallet.

HOW DOES IT WORK?

Add the ResearchPass External Module to your REDCap project with Admin assistance. With a few required fields, study titles, PI details, and contact information are automatically displayed on the digital study ID..

WHICH PLATFORMS ARE SUPPORTED?

Google Wallet Pass | Apple Wallet still in development

WHERE RESEARCHPASS FITS

ResearchPass can be used across a wide range of research settings where participants need quick access to study information.

RESEARCH STUDIES

STUDY TYPES

ResearchPass can be used across many types of research studies, especially those that include clinic visits, follow-up activities, or ongoing participation over time.

WHO TO CONTACT

STUDY TEAM

ResearchPass displays the study team's contact information, so participants know who to reach with questions about their study, appointments, or next steps. Outside care teams can also contact studies with any questions/concerns.

Upcoming IRB Grand Round

March 19, 2026 (10-11 AM)

Key Ingredients to Running a Successful Clinical Trial (UM & JHS)

- 1. Describe existing resources for protocol development
- 2. Identify nuances for JHS studies
- 3. Highlight best practices & requisite training

Speakers: IITSU, JHS, CTD

Registration:

Please use your Miami email address when submitting your request.

UNIVERSITY OF MIAMI
OFFICE of the VICE PROVOST
for RESEARCH & SCHOLARSHIP

CURATING CONNECTION
IRB Grand Rounds 2026

Continuing Medical Education (CME)

Below please find the claim credit link for session scheduled for 2.19.2026:
https://miami.cloud-cme.com/cme/ClaimCredit?P=850&eventid=18748

CURATING CONNECTION
IRB Grand Rounds 2026

2026 IRB Grand Rounds - Continuing Nursing Education (CNE) Credit Registration Form

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.

CURATING CONNECTION
IRB Grand Rounds 2026

Thank you!

For additional information about today's presentation,

Please contact curatingconnection@miami.edu and reference

"IRB Grand Round 2026".