COLUMBIA | VAGELOS COLLEGE OF PHYSICIANS AND SURGEONS

Office of Medical Education Data Confidentiality Agreement

The Office of Medical Education (OME) and the Center for Education Research and Evaluation (CERE) at Columbia University aids in the conduct of Quality Improvement (QI) and research projects involving human subjects and student data. Protecting the confidentiality of all personal information collected or utilized from OME/CERE databases and other affiliate data sources during such projects is a paramount concern–critical to safeguard individual privacy and maintain trust.

As a Principal Investigator or investigator, you are required to adhere to the confidentiality protocols outlined below:

Data Protection and Access:

- The protection of data must take precedence over APPROVED research and quality improvement objectives.
- Data should be anonymized to the greatest extent theoretically possible. Access to identifiable information should be restricted to authorized personnel and only when necessary.
- Data that can directly identify an individual (e.g., names, contact information) must be stored separately from research data and protected by advanced security measures to prevent unauthorized access.
- **Reference:** Columbia University Data Classification Policy

Electronic and Network Security:

- All data must be stored on a CUIMC–approved OneDrive account protected by password and two-factor authentication. All electronic data must be stored on secure, encrypted servers with access controls that comply with university IT security policies and standards.
- Personal hard drives, flash drives, or other non-approved storage devices must not be used.
- Data transmission across networks should be encrypted, and remote access must be secured through virtual private networks (VPN) or other approved methods.
- Devices used to access or store sensitive data must have up-to-date anti-virus software and strong password protection, and adhere to CUIMC IT guidelines for acceptable data storage and usage.
- **Reference:** Acceptable Usage of Information Resources Policy

Responsibility and Compliance:

- You are required to maintain the confidentiality of all research/study data during and beyond the term of your project.
- Any breach of data security or confidentiality must be reported immediately to the principal investigator or the designated compliance officer.
- **Reference:** Information Security Risk Management Policy
- Sanitation and proper disposal of sensitive data must be outlined and completed within specific date stated within a protocol
- **Reference:** Sanitization and Disposal of Information Resources Policy

Artificial Intelligence (AI) Use Policy

In accordance with Columbia University's Generative AI Policy and the Guidelines for the Use of AI in Research with Sensitive Data (including RHI) (May 2025), the following rules apply to all research, education, and administrative activities involving confidential or sensitive information.

Approved Tools

- Only Columbia University–approved AI tools may be used for any research or educational activity involving sensitive or confidential data, including student information protected under FERPA and Research Health Information (RHI).

- Access to approved tools must occur **through Columbia University credentials** to ensure compliance with University privacy, data protection, and information security standards.
- Data should be de-identified whenever possible before input into approved AI systems, and only the minimum necessary data should be included.
- **Reference:** CUIMC Guidelines for the Use of AI in Education and Training with Sensitive Data

Prohibited Tools:

- **Publicly available versions of AI tools** (e.g., ChatGPT, Gemini, Copilot, Claude) **MUST NOT be used for handling or processing sensitive data.**
- No identifiable, confidential, or sensitive data—including research data, student information, or personal identifiers—may be input into or shared with any non-Columbia AI system that retains or uses user data to train models.
- AI tools must operate in HIPAA-compliant and CUIMC IT–approved environments where applicable.

Accountability and Prohibited Use:

- Any intended use of AI in research or QI must be documented in the research or QI study protocol or IRB submission, including the specific AI system and version used.
- Researchers remain fully responsible for the accuracy, validity, and ethical use of AI-generated content, including reviewing for potential bias, errors, or misleading information. Misuse or violation of this policy may result in disciplinary action under Columbia University's confidentiality, information security, and academic integrity standards
- https://www.vagelos.columbia.edu/departments-centers/ai-vp-s-initiative/resources
- **Reference:** AI Usage Policies and Resources

If a medical student is engaged in research projects with access to data from fellow students, students are required to adhere strictly to the confidentiality protocols outlined below in addition to the guidelines and policies above:

Responsibility and Compliance:

- Any breach of data security or confidentiality must be reported immediately to the principal investigator or the designated compliance officer.
- Failure to comply with these confidentiality measures may be Honor Code VP&S Standards of Professionalism violations, and/or may lead to disciplinary action, which can include termination of your role in the project and other academic penalties.

By signing this statement, you acknowledge your understanding of and commitment to these confidentiality obligations:

Faculty Signature: _____
Print Name: _____
Date: _____

Student Signature: _____
Print Name: _____
Date: _____