Columbia University

Institutional Review Board Policy

Data Security Plans Involving the Use, Storage or Transmission of Electronic Research Data Constituting Sensitive Data

I. Background

Pursuant to regulations of the Department of Health and Human Services (**HHS**), including the National Institutes of Health (**NIH**) and the Food and Drug Administration (**FDA**), the Institutional Review Board (**IRB**) is charged with ensuring that each human subjects protocol includes provisions for protecting the privacy of subjects and maintaining the confidentiality of study data. This is particularly important when the study involves data constituting **Sensitive Data** (as defined in the Columbia University Data Classification Policy (the **Data Classification Policy)** and is therefore subject to the most stringent data security requirements.

Unless otherwise indicated, capitalized terms used in this Policy without definition are defined in the Columbia University Information Charter (the **Charter)**.

II. Effective Date: This Policy, originally dated as of November 15, 2013, was amended as of January 18, 2018 and October 10, 2022, and as so amended became effective as of October 10, 2022.

This Policy replaced the IRB Policy: Data Security Plans Involving the Use, Storage or Transmission of Electronic Research Data Constituting Protected Health Information or Personally Identifiable Information, dated February 1, 2013.

III. Scope

This Policy provides standards for IRB review and approval of data security plans involving the storage of electronic research data constituting Sensitive Data in human subjects research conducted at Columbia University, including Columbia University Irving Medical Center (**CUIMC**), or by Columbia University researchers. The intent of this Policy is to ensure that the protection of the privacy of research subjects and the confidentiality of identifiable research data is in accord with the requirements of HHS, NIH and FDA regulations and the Health Insurance Portability and Accountability Act (**HIPAA**).

IV. Sensitive Data

Pursuant to the Data Classification Policy, Sensitive Data is defined as follows:

"**Sensitive Data:** any information protected by federal, state and local laws and regulations or industry standards, such as HIPAA, the Health Information Technology for Economic and Clinical Health Act (HITECH), the New York State Information Security Breach and

Notification Act, similar state laws and the Payment Card Industry Data Security Standard (PCI-DSS).

For purposes of this Policy, Sensitive Data include, but are not limited to:

Personally Identifiable Information or PII: any information about an individual that (a) can be used to distinguish or trace an individual's identity, such as name, date and place of birth,. mother's maiden name or biometric records, (b) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization could result in harm to that individual and (c) is protected by federal, state or local laws and regulations or industry standards.

Protected Health Information or PHI: Individually Identifiable Health Information that is transmitted or maintained by the Columbia Health Care Component in electronic or any other form or medium, except (1) as provided in the definition of Protected Health Information in the HIPAA Privacy Rule (45 CFR 160.103) and (2) Research Health Information.

Research Health Information or RHI: Individually Identifiable Health Information that (1) is created or received in connection with research that does not involve a Covered Transaction or (2) although previously considered Protected Health Information, has been received in connection with research pursuant to a valid HIPAA Authorization or IRB waiver of HIPAA Authorization.

V. General

All IRB protocols must have a data security plan that specifies whether Sensitive Data will be obtained or created and if so, how it will be stored and transmitted. Any modification to the data security plan must be approved by the IRB. Protocol renewals must identify any changes in a data security plan and, at the time of renewal, the IRB will require that the plan be updated to meet new requirements. The data security plan must be acceptable to the IRB for a protocol or protocol renewal to be approved by the IRB.

It is the responsibility of the Principal Investigator **(PI)** of any research study involving Sensitive Data to comply with all applicable University policies and guidelines, including all Information Security Policies.

A code may be used to replace identifiable data in a dataset that would otherwise be considered to be Sensitive Data so long as the code is not derived from any information relating to the individual. Such data that are properly coded and stored separately from the key to the code may be stored or transmitted as de-identified data and would not be considered to be PII, PHI or RHI. However, if a PI or his/her research team has the ability to link the coded data to identifiable information, the coded data would be considered to be Sensitive Data and must be stored and transmitted as such in accordance with the Information Security Policies.

VI. Data Storage

The following methods of storing electronic research data containing Sensitive Data will be acceptable to the IRB:

A. Server Based Systems

The data is stored on a System (including a Columbia University multi-user System or a third party vendor System) that complies with the Columbia University Registration and Protection of Systems Policy (the **Systems Policy)** and meets the requirements set forth below:

1. PHI

All data constituting PHI (including Limited Data Sets (as defined in the Columbia University HIPAA and Research Policy), regardless of whether the data were generated in connection with research conducted by a CUIMC-based PI or a Morningside campus (**Morningside)**-based PI must be stored on a System listed as certified under the "1.2 CUMC Certified Systems List" tab in RSAM.

2. RHI or PII

All data constituting PHI or PII generated in connection with research conducted by a CUIMC-based PI must be stored on a System listed as certified under the "1.2 CUMC Certified Systems List" tab in RSAM.

All data constituting RHI or PII generated in connection with research conducted by a Morningside-based PI must be stored on a System registered under the "1.1 Search All Systems" tab or listed under the "1.2 CUMC Certified Systems List" tab in RSAM.

In each of the above cases, the RSAM ID must be included in the applicable IRB protocol.

B. Endpoints

The data is stored on an Endpoint that complies with the Columbia University Registration and Protection of Endpoints Policy (the **Endpoints Policy**).The inclusion of a statement to such effect in an IRB protocol will constitute a certification by the PI that each Endpoint to be used in the study will be so protected.

VII. Data Transmission

An acceptable data security plan must provide that all electronic transmissions of Sensitive Data over the internet (including by email), file transfers or other data transfer modalities, are made in compliance with the Systems Policy or the Endpoints Policy and the Columbia University Email Usage Policy.

VIII. Data Loss/Security Breach

Any loss of or breach of security relating to research data containing Sensitive Data must be reported (1) to the IRB in Rascal as an Unanticipated Problem Involving Risks to Subjects or

Others and (2) in compliance with the Columbia University Electronic Data Security Breach Reporting and Response Policy**.**

Examples of security breaches include: (1) lost or stolen desktops, laptops, USB drives, CD/DVD/Zip drives, etc. with stored data; (2) a compromised account that is used to look up data (e.g., unauthorized user has had access to the account); (3) a compromised work station or server that contains data; and (4) accidental disclosure or data to unauthorized recipients (e.g., sending data to an incorrect email address).