Columbia University IRB 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 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 pursuant to the terms of the Columbia University Data Classification Policy (the "Data Classification Policy") http://policylibrary.columbia.edu/data-classification-policy and therefore subject to the most stringent data security requirements.

II. Effective Date: The effective date of this Policy is November 15, 2013. This Policy replaces 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 Medical Center ("CUMC"), 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 an Clinical Health Act (HITECH), the U.S. Family Educational Rights and Privacy Act (FERPA), 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 (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 (PHI): any information processed, transmitted or stored by a Covered Entity (as defined in HIPAA) that relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual or the past, present or future payment for health care and (a) identifies the individual or (b) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. The University's Office of the General Counsel and Office of HIPAA Compliance are responsible for determining whether particular information maintained or disclosed by the University constitutes PHI.

Examples of Sensitive Data can be found in Appendix A hereto.

Any codes used to replace identifiable data must not be derived from any information relating to the individual and neither the master codes, nor the method to derive the codes, may be disclosed. Additionally, although the use of codes is highly recommended as a means of reducing risk, if a Principal Investigator (PI) or his/her research team has the ability to link coded data to identifiable information, the coded data will be considered to be identifiable. If the PI and his/her research team have no access to identifiable information, the coded data may be considered de-identified.

V. Policy

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 transferred. Any modification to the data security plan must be approved by the IRB. Protocol renewals must identify any changes in such 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 PI of any research study involving Sensitive Data to comply with all applicable University policies and guidelines, including all Information Security Policies (as defined in the Columbia University Information Security Charter (the "Charter") http://policylibrary.columbia.edu/information-security-charter**.** A list of the Information Security Policies is attached as Appendix B.

A. Data Storage

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

1. **Server Based Systems**

The data is stored on a System (as defined in the Charter) in compliance with the Columbia University Registration and Protection of Systems Policy (the "Systems Policy") http://policylibrary.columbia.edu/registration-and-protection-systems-policy. The specific server name and IP address and, if applicable and provided to the user, a copy of the CUMC IT System Certification Certificate should be included with the protocol.

2. **Endpoints**

The data is stored on an Endpoint (as defined in the Charter) in compliance with the Columbia University Registration and Protection of Endpoints Policy (the "Endpoints Policy") http://policylibrary.columbia.edu/registration-and-protection-endpoints-policy. The inclusion of a statement to such effect in a protocol will constitute a certification by the PI that each Endpoint to be used in the study will be so protected.

B. 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 http://policylibrary.columbia.edu/email-usage-policy-1**.**

C. 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 http://policylibrary.columbia.edu/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).

Appendix A

Examples of Sensitive Data

Examples of PII include, but are not limited to, any information concerning a natural person that can be used to identify such natural person, such as name, number, personal mark or other identifier, in combination with any one or more of the following:

- Social security number
- Driver's license number or non-driver identification card number
- Account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account
- Email address with password (in certain narrow instances)

Examples of PHI include, but are not limited to, any health information about an individual, in combination with any one or more of the following:

- Name
- Geographic subdivision smaller than a state
- Any element of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, or date of death
- Telephone number
- Fax number
- Electronic mail address
- Social security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/License number
- Vehicle identifier and serial number, including license plate number
- Device identifier and serial number
- Web Universal Resource Locator (URL)
- Internet Protocol (IP) address number
- Biometric identifier, including finger and voice print
- Full face photographic image and any comparable image
- Any other unique identifying number, characteristic, code or combination that allows identification of an individual.

Appendix B

Information Security Policies

Information Security Charter
http://policylibrary.columbia.edu/information-security-charter

Acceptable Usage of Information Resources Policy
http://policylibrary.columbia.edu/acceptable-usage-information-resources-policy

Data Classification Policy
http://policylibrary.columbia.edu/data-classification-policy

Registration and Protection of Systems Policy
http://policylibrary.columbia.edu/registration-and-protection-systems-policy

Registration and Protection of Endpoints Policy
http://policylibrary.columbia.edu/registration-and-protection-endpoints-policy

Information Resource Access Control and Log Management Policy
http://policylibrary.columbia.edu/information-resource-access-control-and-log-management-policy

Email Usage Policy
http://policylibrary.columbia.edu/email-usage-policy-1

Network Protection Policy
http://policylibrary.columbia.edu/network-protection-policy

Information Security Risk Management Policy
http://policylibrary.columbia.edu/information-security-risk-management-policy

Electronic Data Security Breach Reporting and Response Policy
http://policylibrary.columbia.edu/electronic-data-security-breach-reporting-and-response-policy

Sanitization and Disposal of Information Resources Policy
http://policylibrary.columbia.edu/sanitization-and-disposal-information-resources-policy

Business Continuity and Disaster Recovery Policy
http://policylibrary.columbia.edu/business-continuity-and-disaster-recovery-policy

Social Security Number (SSN) Usage Policy
http://policylibrary.columbia.edu/node_browser/social-security-number-ssn-usage-policy