Subject: **Information Security**	Page **1**	Policy # Version: 1.1
Title: **Data Security Plans for Identifiable Information Used in Clinical Research**	Revision of:	Effective Date: **9/1/2014**
		Removal Date:

I. PURPOSE:

Protected health information and personally identifiable information which is entered, stored, transmitted, analyzed, and reported as part of approved clinical research studies are covered by this policy. This policy is primarily intended for clinical research and clinical research-related applicants.

The scope of this policy is not limited by the scope of Northwestern University's Institutional Review Board Policy but does embody all research seeking approval under expedited and full board reviews. http://irb.northwestern.edu/process/new-study/reviews.

Generally, this is a looking forward policy. It will apply to new research applications, re-applications and applications subject to renewal occurring subsequent to the effective date of this policy.

Federally sponsored research which mandates FISMA compliance and additional documentation requirements is not covered by this policy. The Federal or grant contract will outline the type of documentation which is required for FISMA compliance.

II. POLICY STATEMENT:

Clinical research studies collecting personal or health-related identifiable information must have a documented Data Security Plan. The Data Security Plan will be comprised of content defined by this policy and will also be consistent with requirements of the grant or research contract where applicable.

The Data Security Plan will be submitted through Northwestern University's Institutional Review Board (IRB) research application and workflow process. The applicant will attest to the adequacy of the submitted Data Security Plan through this same process. Data Security Plans are also subject to selective audits performed by internal or by external organizations.

Authoring Data Security Plans (Procedure)
The Principal Investigator will complete each of the seven sections of the Data Security Plan as defined below. The Data Security Plan will be documented and signed by the Principal Investigator and maintained in the official study files. For IRB approved studies, the documented Data Security Plan will also be uploaded to the Research Supplemental System which is part of the eIRB workflow. A separate Microsoft Word document will be available to complete the Data Security Plan in a standardized format.

Data Custodian – Who is the Data Custodian?
Compromises to data security can occur when there is no clearly defined responsibility and accountability for research data as it collected, processed, stored, analyzed and reported. The data custodian is responsible for developing and updating the Data Security Plan, overseeing compliance with the Data Security Plan and ensuring ongoing security of the data which is part of the research effort.
Ownership and responsibilities of research data are further defined in Northwestern University Policy, Research Data: Ownership, Retention and Access (http://www.research.northwestern.edu/policies/documents/research_data.pdf).

The primary data custodian will be the Principal Investigator. A secondary individual than can perform as a backup in the absence of the primary data custodian should be identified (e.g., co-primary investigator, research administrator).
1) Confirm the Data Custodian will be the Principle Investigator (or Co-Principle Investigators) as indicated on the protocol.
2) Identify, by name and role in the protocol, who will perform as a backup to the Data Custodian.

Data Sensitivity – What is the data sensitivity?
Information that is required to be protected by applicable law or statute (e.g., HIPAA, FERPA, or the Illinois Personal Information Protection Act), or which, if disclosed to the public could expose the University to legal or financial obligations is defined by Northwestern University Policy as legally/contractually restricted information
(http://www.it.northwestern.edu/policies/dataaccess.html**).**

1) Identify the highest level of sensitivity of data which will be collected/maintained during the research. Example categories of sensitivity include HIPAA PHI and/or non-PHI personally identifiable information (PII).
2) Indicate the approximate number of subject records anticipated.

Data Flow & Transmission – What are the sources of data, how will the data be collected and transmitted?
Securing of data must begin at its source and maintained as the data is shared and transmitted among locations and authorized personnel during the course of the study.

1) Describe the flow of data and how it will secured from its source (e.g., EMR system, web application, mobile device application, Internet survey tool, paper forms) to and/or through each processing location and technology platform (e.g., desktop and laptop computers, mobile devices, portable storage devices, Internet cloud services, FSM/NUCAT services, NUIT services).

Data Storage – Where will the data be stored?
Data must be stored in accordance with NUIT File Sharing Policy (http://www.it.northwestern.edu/file-sharing/overview.html) and Feinberg School of Medicine IT Storage Options (http://www.feinberg.northwestern.edu/it/services/storage-options.html).

1) Identify each storage location that will be utilized in the course of this research project.
2) Estimate the amount of storage required.

Data Access – Who will be allowed access to the data?
Access to data must be maintained in accordance with the NUIT Data Access Policy (http://www.it.northwestern.edu/policies/dataaccess.html), Feinberg Information Security & Access Policy (http://www.feinberg.northwestern.edu/policies/FSM-policy.html), and NU Human Subject Protection Program Policy Manual, page 44 (http://irb.northwestern.edu/sites/default/files/documents/northwesternhspppolicyv53.pdf)

1) Identify each individual and their research job role having access to data and confirm that access is consistent with those on the Authorized Personnel list of the IRB approved protocol (if applicable).

Data Backup & Recovery – How will data be recovered in the event of equipment mal-function, physical facilities impairment or natural disaster?
Irrecoverable loss of data may jeopardize continuation of research studies, potential promising research results, ongoing loss of grant revenue and reputation with grant and contracting sponsors.

1) Describe the backup and recovery plan for data that is not reproducible from other sources and related research computer programming that may have been customized for this research data collection.

Data Retention (Archiving) – Once a research project is completed where will research data be stored and secured for the length of time required by the grant, the contract or Northwestern University Policy?
When a research project is concluded, data may be left unmanaged initially and then possibly forgotten over a longer period of time. If the device is repurposed in a less secure environment without removing prior protected health information and personally identifiable information the risks of unauthorized disclosure increases.

Once a research project is completed data must be stored and secured for the length of time required by the grant, the contract or Northwestern University Policy.
University policies for data retention are Retention of University Records http://policies.northwestern.edu/docs/Retention_of_University_Records_030410.pdf and Research Data: Ownership, Retention and Access http://www.research.northwestern.edu/policies/documents/research_data.pdf).

1) Describe the data retention (archiving) plan including when the data will be removed from the active study storage location to the long term data retention location and
2) Indicate the length of retention and the long term storage location.

Exceptions
Exceptions to this Policy may be considered given appropriate research and business justification. Requests which will unduly raise the risk of inadvertently exposing protected health information and personably identifiable information will be respectively declined. Please send requests to FSMIT-policy@northwestern.edu.

Compliance and Enforcement
Research applicants must ensure compliance with underlying Feinberg School of Medicine Policies & Procedures, overarching Northwestern University Policies & Procedures, and human subject protection regulations which includes: Protection of Human Subjects (45 CFR 46, 21 CFR 50); Institutional Review Boards (21 CFR 56); HIPAA Privacy (45 CFR 160, 45 CFR 164 Subparts A and E); HIPAA Security (45 CFR 160, 45 CFR 164 Subparts A and C); HITECH Act of 2009; The Family Educational Rights and Privacy Act of 1974 (FERPA); and relevant application State and local regulations.
Failure to comply with these policies will lead to sanctions, up to and including administrative suspension of activities, loss of faculty appointment, department or unit financial penalties, or dismissal from the University.

III. PERSONS AFFECTED:

All FSM faculty, staff, students and trainees engaging in clinical research.

IV. DEFINITIONS:

eIRB (electronic Institutional Review Board system) Portal for electronic submission of research proposals to the IRB

HIPAA: Health Insurance and Portability and Accountability Act of 1996 and the privacy regulations under that Act

Institutional Review Board (IRB): A federally mandated body that reviews and approves research in accordance with federal regulations including, but not limited to DHHS regulations at 45 CFR 46 and its subparts, as well as FDA requirements at 21 CFR 50 and 21 CFR 56. When research involving products regulated by the FDA is funded, supported or conducted by FDA and/or DHHS, both the DHHS and FDA regulations apply. The IRBs have a central role in ensuring that human subject research is planned and conducted in an ethical manner, and in compliance with federal and state regulations.

Principal Investigator (PI): The individual with primary responsibility for the design and conduct of a research project. The PI is also responsible for ensuring that all individuals who work under the supervision of the PI and participate in the conduct of the research have adequate education in order to discharge their duties in a manner that is consistent with the federal regulations for protection of human subjects as well as with this policy and with the specific requirements of the NU IRB.

Protected Health Information (PHI): Any patient or individually identifiable health information.

Research: As defined by the Department of Health and Human Services (DHHS), a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. DHHS regulations further define a human subject as a living individual about whom an investigator (whether professional or student) conducting research obtains either: (a) data through intervention or interaction with the individual or (b) identifiable private information.

Sponsor: For the purposes of this policy, a sponsor is limited to a person or entity that provides funding to cover the expenses to conduct the research study. A study sponsor is usually the entity that developed the drug or device being used in a clinical investigation, but could also be any person or entity that serves as funding source for the research study. Therefore a sponsor can be external to Northwestern (e.g. drug or device company, an NIH Institute...etc) or internal to Northwestern (such as an NU Department, NMF grant…etc).

V. POLICY UPDATE SCHEDULE:

Policy review to occur no less than annually.

VI. RELEVANT REFERENCES:

Technology Resources
Please address all questions and requests for IT resources required (e.g., storage and storage estimates, backup storage, archiving storage, granting access to data) of the Data Security Plan to FSMHELP@northwestern.edu.

Data Security Plan Questions
Please address all questions, request for clarification and all other forms of assistance regarding Data Security Plans to FSMIT-policy@northwestern.edu.

Data Security Plan Template (http://www.feinberg.northwestern.edu/it/standards-policies/index.html)

Example Data Security Plans
Using Central IT FSM Resources (http://www.feinberg.northwestern.edu/it/standards-policies/index.html)

Using Customized and/or External Resources (http://www.feinberg.northwestern.edu/it/standards-policies/index.html)