**Data Security Plan Template**

Version: 1.4

Document Owner: Feinberg School of Medicine, Central IT

Effective Date: Coincides with eIRB7 Implementation

Last Update/Review Date: 21 April 2017

Review Cycle: Annual

**Policy Resource**

[Data Security Plans for Information Used in Clinical Research](http://www.feinberg.northwestern.edu/it/policies/information-security/data-security-plans.html)

[Data Security Plan Template (this document)](http://www.feinberg.northwestern.edu/it/policies/information-security/data-security-plans.html)

[Data Security Plan Examples](http://www.feinberg.northwestern.edu/it/policies/information-security/data-security-plans.html)

[Uploading Data Security Plans (step by step submission directions)](http://www.feinberg.northwestern.edu/it/policies/information-security/data-security-plans.html)

**Resource Assistance**

*Technology Questions*

Please address all questions and requests for IT resources (e.g., active storage, backup storage, archiving storage, granting/modifying access to data) to [FSMHELP@northwestern.edu](mailto:FSMHELP@northwestern.edu).

*Data Security Plan Questions*

Please address all questions, requests for clarification, suggestions for improvement and all other forms of assistance regarding Data Security Plans to [FSMIT-policy@northwestern.edu](mailto:FSMIT-policy@northwestern.edu).

**Use of the Data Security Plan Template**

The Data Security Plan is comprised of 12 questions consisting of either checklist selections or short answers.

The use of standardized clinical research services as provided by FSM NUCATS and/or FSM IT can further simplify the acquisition of resources (e.g., server and storage capacity) to accomplish research goals and objectives. In addition, the basic content of a Plan can be replicated across similar studies for a Principal Investigator or across a department.

A completed Plan is envisioned to be one to two pages in length. Please remove all non-applicable content from the completed template below before submitting as part of the IRB workflow.

**Data Security Plan**

**Study Number:** <insert study number>

**Study Name:** <insert study name>

**Data Custodian**

Additional Reference*:* [Research Data: Ownership, Retention and Access](http://www.research.northwestern.edu/policies/documents/research_data.pdf)

*1) Identify, by name and role/title in the protocol, who will be the Data Custodian. In most cases, this should be the Principal Investigator: <insert name and role/title>*

*2) Identify, by name and role/title in the protocol, who will be the backup to the primary Data Custodian: <insert name and role/title>*

**Data Sensitivity**

Additional Reference(s):

**\*** [NUIT Data Access Policy](http://www.it.northwestern.edu/policies/dataaccess.html)

**\*\*** [HIPAA Privacy Protected Health Information](http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#safeharborguidance)

**\*\*\*** [HIPAA Privacy Limited Data Sets (LDS)](http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/research.html)

***3) Identify the level(s) of data sensitivity that will be collected/maintained during the research. Example categories of sensitivity include HIPAA PHI and/or non-PHI personally identifiable information (PII) <select one or more options>:***

***\_\_\_\_\_Legally/Contractually Restricted (FERPA, Illinois Personal Information Protection Act) Information\****

***\_\_\_\_\_NU Internal Information (see NUIT Data Access Policy\*)***

***\_\_\_\_\_Protected Health Information (HIPAA defined\*\*)***

***\_\_\_\_\_LDS as a subset of Protected Health Information\*\*\****

***\_\_\_\_\_De-identified information\*\****

***\_\_\_\_\_Public Information\****

***\_\_\_\_\_Other <please explain>***

***4) Indicate the approximate number of research subjects anticipated <select one or more options>:***

***\_\_\_\_\_Less than 500 research subjects***

***\_\_\_\_\_500 or more research subjects***

***\_\_\_\_\_Other <please explain>***

**Data Flow & Transmission**

*5) Identify the services and platforms used for data collection and processing by selecting the options below:*

*Recruitment Data Sources and Recruitment Methods <select one or more options>:*

*\_\_\_\_\_ Electronic Medical Records System (directly)*

*\_\_\_\_\_ Northwestern Medicine® Enterprise Data Warehouse (EDW)*

*\_\_\_\_\_ Physician referral*

*\_\_\_\_\_ NU IRB approved patient registry*

*\_\_\_\_\_ In-clinic solicitation*

*\_\_\_\_\_ Public solicitation (e.g., fliers, billboards)*

*\_\_\_\_\_ Direct email solicitation*

*\_\_\_\_\_ Other <please explain>*

*Input Sources and Input Platforms* ***<select one or more options>****:*

***\_\_\_\_\_Electronic Medical Records System (directly)***

***\_\_\_\_\_Northwestern Medicine*® *Enterprise Data Warehouse (EDW)***

***\_\_\_\_\_NU (or research academia/commercial partner) Client-server Application***

***\_\_\_\_\_NU (or research academia/commercial partner) Browser-based Application***

***\_\_\_\_\_NU (or research academia/commercial partner) Mobile Device Application***

***\_\_\_\_\_Public Cloud Application (e.g., Box.com, OneDrive, Google, Amazon, Qualtrics) <please specify>***

***\_\_\_\_\_Portable storage (e.g., external hard drives, flash drives, digital recorders)***

***\_\_\_\_\_ Encrypted?***

***\_\_\_\_\_Paper Forms (e.g., Case Report Forms, Paper Surveys)***

***\_\_\_\_\_Lab equipment, medical devices***

***\_\_\_\_\_Other <please explain>***

*Processing and Analysis Platforms/Services* ***<select one or more options>****:*

***\_\_\_\_\_FSM/NUCATS Services***

***\_\_\_\_\_NUIT Services (e.g., NUcloud, Quest)***

***\_\_\_\_\_Government-contract Services (e.g., NIH, NSF, DoD)***

***\_\_\_\_\_Public Cloud Services (e.g., Box.com, OneDrive, Google, Amazon, Qualtrics) <please specify>***

***\_\_\_\_\_Research Academia/Commercial Partner Services (includes sponsor-provided platforms)***

***\_\_\_\_\_FSM Department Desktops***

***\_\_\_\_\_FSM Department Laptops***

***\_\_\_\_\_FSM Department Smartphone Devices (includes tablets or smartwatches)***

***\_\_\_\_\_ Encrypted?***

***\_\_\_\_\_Portable storage (e.g., external hard drives, flash drives, digital recorders)***

***\_\_\_\_\_ Encrypted?***

***\_\_\_\_\_Personally-owned devices <please specify>***

***\_\_\_\_\_ Encrypted?***

***\_\_\_\_\_Lab equipment, medical devices***

***\_\_\_\_\_Other <please explain>***

*6) Describe the flow of research data from input, to processing and storage, including how data will be transferred between each processing location and technology platform: <insert description>*

**Data Storage**

Additional Reference(s):

[NUIT File Sharing Policy](http://www.it.northwestern.edu/file-sharing/overview.html)

[FSM IT Storage Options](http://www.feinberg.northwestern.edu/it/policies/file-storage.html)

*7) Identify each storage location that will be utilized in the course of this research project <select one or more options>:*

***\_\_\_\_\_FSM/NUCATS/NM Managed Storage (e.g., FSMFILES/departmental shared drive, REDCap)***

***\_\_\_\_\_NUIT Managed Storage (e.g., NUcloud, NU Sharepoint)***

***\_\_\_\_\_Public Cloud Storage (e.g., Box.com, OneDrive, Google, Amazon, Qualtrics)***

***\_\_\_\_\_Research Academia/Commercial Partner Storage (e.g., sponsor-provided storage)***

***\_\_\_\_\_FSM Department Desktops***

***\_\_\_\_\_FSM Department Laptops***

***\_\_\_\_\_FSM Department Smartphone Devices (includes tablets or smartwatches)***

***\_\_\_\_\_ Encrypted?***

***\_\_\_\_\_Portable storage (e.g., external hard drives, flash drives, digital recorders)***

***\_\_\_\_\_ Encrypted?***

***\_\_\_\_\_Personally-owned devices <please specify>***

***\_\_\_\_\_ Encrypted?***

***\_\_\_\_\_Lab equipment, medical devices***

***\_\_\_\_\_Other <please explain>***

*8) <Question Removed>*

**Data Access**

Additional Reference(s):

[NUIT Data Access Policy](http://www.it.northwestern.edu/policies/dataaccess.html)

[FSM Information Security & Access Policy](http://www.feinberg.northwestern.edu/it/policies/information-security/FSM-policy-security.html)

[Identifying the Study Team](https://irb.northwestern.edu/process/new-study/requirements#Study%20Team%20Members)

*9) Identify each individual and their research job role having access to data and confirm that access is consistent with those on the Study Team/Authorized Personnel List of the IRB approved protocol (if applicable) <select one or more options>:*

***\_\_\_\_\_Access is maintained consistent with those on the approved study’s Study Team / Authorized Personnel list.***

***\_\_\_\_\_Additional personnel access is required:***

***<List additional personnel access and their role in the study>***

***\_\_\_\_\_<Please explain other circumstances if necessary>***

**Data Backup & Recovery –** Research data must be recoverable in the event of equipment malfunction, physical facilities impairment, theft or natural disaster.

Additional Reference(s):

[FSM General Information Security Policy (see Section III Item 9)](http://www.feinberg.northwestern.edu/it/docs/General-Security-Policy-41516-V1.pdf)

*10) 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. Where are backups being stored <select one or more options>:*

***\_\_\_\_\_FSM/NUCATS/NM Managed Storage (e.g., FSMFILES, REDCap, CrashPlan)***

***\_\_\_\_\_NUIT Managed Storage (e.g., NUcloud, NU Sharepoint)***

***\_\_\_\_\_Public Cloud Storage (e.g., Box.com, OneDrive, Google, Amazon, Qualtrics)***

***\_\_\_\_\_Research Academia/Commercial Partner Storage (includes sponsor-provided storage)***

***\_\_\_\_\_FSM Department Desktops***

***\_\_\_\_\_FSM Department Laptops***

***\_\_\_\_\_Portable storage (e.g., external hard drives, flash drives, digital recorders)***

***\_\_\_\_\_ Encrypted?***

***\_\_\_\_\_Personally-owned Devices <please specify>***

***\_\_\_\_\_Offsite Location <please specify>***

***\_\_\_\_\_Lab equipment, medical devices***

***\_\_\_\_\_Other <please explain>***

*11) If FSM/NUCATS/NM Managed Storage is selected above, then backup and recovery services are already included; otherwise describe the frequency at which backups are taken and the schedule of sending backups to an offsite storage location: <please describe the data backup plan>*

**Data Retention (Archiving) –** Once a research project is completed research data must be stored and secured for the length of time required by the grant, the contract or Northwestern University Policy.

Additional Reference(s):

[University policies for data retention are Retention of University Records (see Appendix A)](http://policies.northwestern.edu/docs/Retention_of_University_Records_030410.pdf)

[Research Data: Ownership, Retention and Access](http://www.research.northwestern.edu/policies/documents/research_data.pdf)

*12) 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 the length of retention at the long term storage location: <specify the retention period>*

*13) Archive data will be stored <select one or more options>:*

***\_\_\_\_\_FSM/NUCATS/NM Managed Storage (e.g., FSMFILES)***

***\_\_\_\_\_NUIT Managed Storage (e.g., NUcloud, NU Sharepoint)***

***\_\_\_\_\_Public Cloud Storage (e.g., Box.com, OneDrive, Google, Amazon, Qualtrics)***

***\_\_\_\_\_Research Academia/Commercial Partner Storage (includes sponsor-provided storage)***

***\_\_\_\_\_FSM Department Desktops***

***\_\_\_\_\_FSM Department Laptops***

***\_\_\_\_\_Portable storage (e.g., external hard drives, flash drives, digital recorders)***

***\_\_\_\_\_ Encrypted?***

***\_\_\_\_\_Personally-owned Devices <please specify>***

***\_\_\_\_\_Offsite Location <please specify>***

***\_\_\_\_\_Lab equipment, medical devices***

***\_\_\_\_\_Other <please explain>***