Data Security Plans at Feinberg School of Medicine

IRB Brown Bag
April 20, 2016

Presented by
Marvina Roebuck
Senior Information Security Analyst
Northwestern University
Feinberg School of Medicine

David Gundrum
Senior Information Security Analyst
Northwestern University
Feinberg School of Medicine
Data Security Plans at Feinberg School of Medicine – Requirements

• Required for all studies collecting health information, in which the PI has a Feinberg appointment
  • Required at time of new submission or continuing review
  • Submitted through RSS section of eIRB+

• Consists of document with 13 checklist or short answer questions

• Describes what data is collected and maintained, and how it is handled

• Reviewed by Feinberg IT Security; independent of IRB approval process
Data Security Plans at Feinberg School of Medicine – Purpose

- Increases awareness of security requirements
- Helps Feinberg IT Security identify security concerns, risks, and compliance with policy
- Improve policy and regulatory compliance posture (e.g., where is your data?)
- Contributes toward an assurance of security and privacy to NM
Data Security Plans at Feinberg School of Medicine – Review Process

• All Data Security Plans subject to review and audit by the FSM IT Security team
  • > 1300 plans reviewed since September 1, 2015
  • > 300 audits initiated since September 1, 2015

• Plans are reviewed for completeness and compliance to FSM policies

• Initial determination made on review of each plan, to accept or flag for audit
  • Review status marked in our database
  • PI / Author not notified of plan acceptance unless plan was reviewed on request

• PI and plan’s author may be contacted via email with questions or concerns
  • PI/Author notified if their plans require clarification/auditing
Data Security Plans at Feinberg School of Medicine – Audit Process

- Plans that are not accepted on initial review are flagged for audit
- The audit is initiated via an email sent to the PI, plan’s author, and data custodian/s with questions and concerns
- An audit typically requires revision of the data security plan to incorporate clarifications or address concerns
- Revised plans are uploaded to the RSS and re-reviewed by the FSM IT Security team
- An audit is closed when the plan has been accepted
  - PI/Author will receive an email stating the plan has been accepted

“Audit” is often thought of as a dirty word. However audits exist to protect the organization and you, and we go out of our way to minimize the inconvenience to those involved.
Data Security Plans at Feinberg School of Medicine – Common Audit Reasons

- No plan submitted/Protocol submitted instead of Data Security Plan
- Policy violated
- Response to required question is missing/incomplete
- No backup plan provided
- Failure to <specify/explain> when requested to do so
- Risky or potentially risky practices noted
Data Security Plans at Feinberg School of Medicine – How to Avoid an Audit

• Answer all questions within the template
• Be clear and concise: avoid vague and lengthy responses
• Be specific:
  • Customized templates are OK, but they shouldn’t sacrifice specificity or accuracy. Plan still needs to say what is being done; not just how things are done when/if they are done.
  • When referencing systems, applications, or devices, include the location, owner, or name when relevant.
• Familiarize yourself with policies referenced in the template
• If you have a question contact the FSM IT Security team
Data Security Plan Template Explained
Data Security Plan Template Explained – Data Custodians

Data Custodian – Who is the Data Custodian?

1. Identify, by name and role/title in the protocol, who will perform as 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 perform as backup to the primary Data Custodian: <insert name and role/title>

- Responsible for ensuring safe and compliant data handling throughout the course of the study
- Backup Data Custodian preferred but not required
- Typically PI and Co-I

“As custodians of research data, Principal Investigators (PIs) and other researchers are stewards of research data. At the same time, no matter how such responsibilities are delegated, the flow of accountability runs from the PI being responsible to the institution for the stewardship of research data, just as the institution is ultimately responsible to the research sponsor.”

http://www.research.northwestern.edu/policies/documents/research_data.pdf
Data Security Plan Template Explained – Data Sensitivity

(3) Identify the level(s) of data sensitivity that will be collected/maintained during the research. <select one or more options>:

- Legally/Contractually Restricted (FERPA, Illinois Personal Information Protection Act) Information*
- NU Internal Information
- Protected Health Information (HIPAA defined**)
- LDS as a subset of Protected Health Information***
- De-identified Information
- Public Information
- Other <please explain>

- Even if all data is de-identified, a data security plan must be completed
- If your research data does not seem to fit into a predefined category, please select other and include a brief description of the data to be collected/maintained
- Links in template provide definitions
Data Security Plan Template Explained – Number of Subjects

(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>

• In the event of a breach, if records for 500 or more subjects are disclosed, notice must be published in local media outlets.

• HIPAA Breach Notification Rule:
  

• For multi-site studies, only indicate the number of participants for which your study team has access.

✔ **Good response:** _X_ 500 or more research subjects

✗ **Inadequate response:** _X_ 500-200 or more research subjects
Data Security Plan Template Explained – Input and Processing

(5) Describe the flow of data and how it will be secured from its source to and/or through each processing location and technology platform:

**Input Sources and Input Platforms** = Explain what that means

- 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 Internet Web application (e.g. Saas Services) <specify vendor/services>
- Paper Forms (Case Report Forms)
- Other <please explain>

**Processing and Analysis Platforms/Services** = Explain what that means

- FSM/NUCATS Services
- NUIT Services (e.g. Nucloud, Quest)
- Government-contract Services “(e.g. NIH, MSF, DoD)
- Public Internet Services (e.g., Saas Services)
- Research Academia/Commercial Partner Services
- FSM Department Servers, Desktops, Laptops
- Mobile/Portable Devices
- Other <please explain>

• **Input**: Where data *comes from* and what data is *entered into*

• **Processing**: What is used to analyze or manipulate data once collected

**EXAMPLE**

- Insufficient response:
  
  _X_ Other: Patient interviews

- Better response:

  _X_ Other: Patient interviews - digital recorder and departmental desktop computer
Data Security Plan Template Explained – Data Flow

(6) Describe the flow of research data from input, to processing and storage: <insert description>

- Provide a comprehensive narrative
- **How** is data transferred between systems or parties (connect the dots)?
- A good response will clarify and tie all the other responses together to give a complete picture of study data

**X** Inadequate response: Data will be stored on password protected computers.

**✓ Better response:**

The EDW will provide a report with potential participants that meet inclusion criteria. Once participants have been consented, they will be interviewed at the Department of General Medicine or via phone, and their responses will be recorded using a digital audio recorder. Recordings will then be manually transcribed using an FSM desktop computer in the Department of General Medicine, and the recordings will be deleted after transcription. Transcripts will be stored on FSMFiles.
Data Storage – Where will the data be stored?

(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 (includes FSMFILES)
- NUIT Managed Storage (e.g., NUcloud, NU Sharepoint)
- Public Internet Storage
- Research Academia/Commercial Partner Storage
- FSM Department Servers, Desktops, Laptops
- Mobile/Portable Devices
- Other <please explain>

(8) Estimate the amount of total file storage required: <insert estimated storage requirements>

- Question 8: Optional at this time
Data Security Plan Template Explained – Data Access

(9) 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) <select one or more options>:

— Access is maintained consistent with those on the approved study’s Authorized Personnel list.
— Additional personnel access is required:
  <List additional personnel access and their role in the study>
— <Please explain other circumstances if necessary>

• Authorized Personnel list = Study Team in eIRB+

X Inadequate response:
_X_ Additional personnel access is required: Additional departmental personnel may be granted access on an as-needed basis.

✓ Better response:
_X_ Additional personnel access is required: Sponsor’s monitors/representatives may be granted access to study data as needed.
Data Security Plan Template Explained – Backup & Recovery

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 (includes FSMFILES)
- NUIT Managed Storage (e.g., NUcloud, NU Sharepoint)
- Public Internet Storage
- Research Academia/Commercial Partner Storage
- FSM Department Servers, Desktops, Laptops
- Mobile/Portable Devices
- Offsite Location <please specify>
- Other <please explain>

- **For non-reproducible data**, backups that rotate offsite are **required**
  - Centrally managed storage or backup solutions will fulfill this requirement (e.g. FSMFiles, QUEST, REDCap)
Data Security Plan Template Explained – Backup & Recovery

11) If using FSM/NUCATS/NM Managed Storage then backup and recovery services 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>:

- If data is not stored on centrally-managed storage as indicated in the previous question, this question must be answered.
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: <specify the retention period>

13) Archive data will be stored:
   - FSM/NUCATS/NM Managed Storage (includes FSMFILES)
   - NUIT Managed Storage (e.g., NUcloud, NU Sharepoint)
   - Public Internet Storage
   - Research Academia/Commercial Partner Storage
   - FSM Department Servers, Desktops, Laptops
   - Mobile/Portable Devices
   - Offsite Location <please specify>
   - Other <please explain>

- Sponsored research data must be retained for at least 3 years after study completion unless otherwise specified, per NU policy.

✔️ Good question 12 response:

Data will be maintained on FSMFILES for 7 years as required by study sponsor, after which time all data will be destroyed. Paper records will be stored by Reebie Records Storage for the same duration.
Data Security Plans at Feinberg School of Medicine – Contact and Resources

FSM IT Security (General Questions):

FSMIT-policy@northwestern.edu

Marvina Roebuck:

mroebuck@northwestern.edu
312-503-5735

David Gundrum:

d-gundrum@northwestern.edu
312-503-3869

Data Security Plans on FSM IT Security Website:

http://www.feinberg.northwestern.edu/it/policies/information-security/data-security-plans.html
Questions?