| Subject:<br>**Information Security** | Page<br>**1** | Policy #<br>Version: 2.1 |
|---|---|---|
| Title:<br>**FSM General Information Security Policy** | Revision of:<br>Version 2.0, 4/15/2016 | Effective Date:<br>**9/22/2016**<br>Removal Date: |

## I. PURPOSE

The Feinberg School of Medicine (FSM) is committed to the highest standards of protecting electronic patient, research, and other sensitive information in accordance with our legal and ethical responsibilities. This information needs to be protected in all aspects of our research and other activities, including unauthorized disclosure, modification and destruction of data. Inappropriate disclosure of information can negatively impact our patients personally and professionally, the integrity of research information, and lead to an embarrassment to Northwestern University (NU), our research partners and affiliate clinical partners.

## II. POLICY STATEMENT

The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act are the minimum standard for handling any form of identifiable health information (e.g., PHI, PII). Where external collaborations require compliance with other information security policies and standards (e.g., National Institute of Standards and Technology-NIST, Federal Information Security Management Act-FISMA), those will apply as well.

## III. PROCEDURE STATEMENT

1. Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule must be followed when de-identification of data is required in an IRB approved research protocol.
2. All types of portable media must be encrypted and be verifiable as encrypted. Examples include but are not limited to laptop and tablet computers, USB and portable storage media, removable memory, backup media (e.g., tape, disk, cartridge), and smartphones. Desktop computers are also required to be encrypted.
3. Electronic transmission of data must be encrypted and the transmission path verifiable as encrypted. Examples include but are not limited to email, web application connections and file transfers.
4. Any actual or suspected data breach (including unauthorized access to or compromise of data, theft or removal of equipment, papers, storage media, etc.) must be reported immediately to: fsmhelp@northwestern.edu. Response to suspected or real incident will follow NU policy.
5. Electronic and physical access to information must be maintained consistent with an individual's job responsibility for administrative data and the approved IRB protocol for research data, if applicable. Access to data must be updated immediately upon leaving NU employment or changing job responsibilities.
6. Access to electronic information must require a complex password as defined by NU policy. This includes a PIN and/or password for smartphones. Passwords/PINs are not to be shared.
7. Device security features including configuration settings and software must not be disabled, removed or changed (e.g., disabling of encryption, removal of anti-malware software) from what is included in a standard device image as defined and provided by FSM IT.
8. Data is permitted to be stored on approved secure storage as defined by NU and FSM policy. Network attached storage (NAS) is not allowed. Similarly, cloud storage (e.g., Microsoft

OneDrive, Google Drive) and Box.com for any form of identifiable health information is not allowed.

9. Data backups must be performed regularly and stored on approved secure storage where data copies are sent to secure offsite storage (i.e., FSMFILES, CrashPlan). Offsite storage of data backups in secure media rated facilities is required. Offsite storage in personal locations (e.g., home) is not allowed.
10. The use of public email systems (e.g., Gmail) are not approved for any Feinberg purposes.
11. When Information Security training and awareness programs are presented, they are required to be completed.
12. Data security plans for research studies are required for those Principal Investigators with FSM appointments.
13. The use of commercial vendors for use in research must have a written agreement between NU and the vendor including written approval from the FSM Dean's office.
14. Personal devices (including smartphones, tablets and home computers) may have restricted capability to access or store FSM data but are still required to comply with NU and FSM policies.
15. Changes to the technology environment affecting information security will be recorded and approved in the FSM IT change management systems.
16. Logging will be enabled in the technology environment on networks, servers and applications to ensure traceability of access to identifiable health or other sensitive information.
17. This policy augments existing FSM and NU information security policies, procedures and guidelines. Where this FSM policy is more restrictive than NU policies, procedures and guidelines, then this FSM policy applies.
18. Exceptions to this policy require approval by the FSM Dean's Office. Exceptions may be revoked if the capabilities allowed through the exception are used inappropriately.
19. Audits and risk and vulnerability assessments will be performed to monitor compliance with this policy as directed by the FSM Dean's Office.
20. Unless otherwise contractually specified, all research, administrative and operational data and equipment are the property of NU.
21. Supervisors is responsible for ensuring that their employees and students are conducting all work consistent with NU and FSM policies.
22. Failure to comply with these policies will lead to sanctions, up to and including administrative suspension of NetID, loss of faculty appointment, department or unit financial penalties, or dismissal from NU.

## IV. PERSONS AFFECTED

All NU Feinberg School of Medicine faculty, staff, students, residents, and fellows.

## V. POLICY UPDATE SCHEDULE

No less than every five (5) years, but more frequent updates may be conducted as required.

## VI. REVISION HISTORY

04/15/2016 – Replaces existing policy.

09/22/2016 – Clarification of procedure statement #22.

## VII. RELEVANT REFERENCES

Health Insurance Portability and Accountability Act (HIPAA):
http://www.hhs.gov/hipaa/for-professionals/index.html

Health Information Technology for Economic and Clinical Health (HITECH)
http://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html

National Institute of Standards and Technology (NIST)
http://csrc.nist.gov/

Federal Information Security Management Act (FISMA)
http://csrc.nist.gov/groups/SMA/fisma/

Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule:
http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html

Feinberg Information Technology: http://www.feinberg.northwestern.edu/it/

Device Security Policy: http://www.feinberg.northwestern.edu/it/

NUIT Policies, Guidelines, and Practices: http://www.it.northwestern.edu/policies/

Incident Response Protocol: http://www.it.northwestern.edu/policies/incident.html

Secure IT at Northwestern: http://www.it.northwestern.edu/security/

NU Validate: Identity Management System (including passwords):
http://www.it.northwestern.edu/auth-svcs/nuvalidate.html

Service Provider Security Assessments
http://www.it.northwestern.edu/about/departments/itms/cpo/assessment.html

File Sharing at Northwestern:
http://www.it.northwestern.edu/file-sharing/overview.html

FSM Storage Options:
http://www.feinberg.northwestern.edu/it/services/storage-options.html