Subject: **Information Security**	Page **1 of 5**	Policy # Version: 1.0
Title: **Risk Management**	Revision of: New Policy	Effective Date: **11/1/17**
		Removal Date:

I. PURPOSE

This policy formally establishes the information security risk management program and oversight for the Northwestern University (NU) Feinberg School of Medicine (FSM). The scope of this policy includes regular determination of prioritization and implementation of safeguards or transfer or acceptance of risk. The outcome of risk management is to ensure FSM as part of NU is operating with an acceptable and agreed to level of risk.

II. PERSONS AFFECTED

NU Feinberg School of Medicine Dean's Office Administration, NU and FSM IT leadership, NU and FSM compliance and NU Risk Management.

III. POLICY STATEMENT

Information security risk management covers all of FSM information resources, whether managed or hosted internally or externally. The risk management process will include risk categorization, risk analysis, risk remediation and risk monitoring.

Items for discussion within the risk management process will be derived from a number of sources, including but not limited to, external security technology alerts and notifications, evolution of technology, changes in federal and state regulations, changes in environmental factors and items submitted from those listed in Persons Affected.

Documentation of potential risks and assessment of those risks will be compiled and maintained in a Risk Registry as defined by the Procedure.

University and FSM IT leadership will convene regularly as the FSM IT Steering Committee to determine the disposition of potential risks as defined by the Procedure. The charge of the Feinberg Information Technology Steering Committee (FSM IT Steering Committee) for this policy is defined in Appendix A.

IV. PROCEDURE STATEMENT

Risk Categorization

Information resources are categorized based on the sensitivity of data, impact from loss of data availability, and potential risk exposure from technical vulnerabilities and lack of user knowledge of policy and accepted data handling practices.

Security controls to minimize threats and manage risks are based upon the following security control framework:

HIPAA Privacy Rule, Security Rule, HITECH
Combined Regulation Text of All Rules (HHS HIPAA)

National Institute for Standards and Technology (NIST)
NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments
NIST SP 800-53r4 Security and Privacy Controls

NIT HIPAA/ISO and ISO 27001/2 Information Security Guidance

Risk Analysis

The risk analysis process may consider:

- Ongoing identification and prioritization of threats and vulnerabilities in the technical environment and the impact on data protection.
- Technical upgrade/changes to the environment.
- Emerging threats resulting from the evolution of technology.
- Federal and state regulatory impact.
- Compensating controls implemented via policy and/or technology.
- New policy requirements from external collaborators.
- Learned risks from security incidents.

Risk determination will consider the above factors and apply the likelihood of occurrence and potential impact as defined in NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments. Risks expressed as High, Medium and Low, defined as follows:

- High: There is strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
- Medium: Corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
- Low: Corrective actions may still be required but the organizations decides to accept the risk.

Risk Remediation

Risk remediation will be derived the risk analysis and consider the following options:

- Risk elimination, mitigation or reduction
- Risk avoidance
- Risk acceptance
- Risk transference

Risk Monitoring

Risk monitoring processes may include:

- Routine general risk assessments at least yearly.
- Daily monitoring of external security technology alerts and notifications.
- Vulnerability and penetration testing.
- Assessment of impact from technology changes and upgrades.
- Evaluation of new/revised application systems.
- Data security plan reviews and audits.
- Changes of federal and state laws and regulations, industry standards and University policies.

Risk Registry

The risk registry will be updated monthly by the FSM CISO with new potential risks and updates on remediation efforts.

The FSM IT Steering Committee will review and approve the presented risk analysis, risk prioritization and desired remediation plans, no less than quarterly. The Committee may also indicate revisions to the content and format of the Registry.

V. POLICY UPDATE SCHEDULE:

Policy review to occur one year after initial implementation and every three years thereafter.

VI. REVISION HISTORY:

11/1/17 – New policy effective.

VII. RELEVANT REFERENCES:

NU Data Access Policy
http://www.it.northwestern.edu/policies/dataaccess.html

Combined Regulation Text of All Rules (HHS HIPAA)
https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html

NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

NIST SP 800-53 Rev. 4 Security and Privacy Controls
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

NIT HIPAA/ISO, ISO 27001/2 Information Security Guidance
http://www.it.northwestern.edu/policies/HIPAA-guidance.html

VIII. APPENDIX A: FSM IT Steering Committee Charge

Charge: The FSM IT Steering Committee will:

- Advise the Feinberg Dean on priorities, policies and procedures concerning the School's Information Technology (IT) and Information Security program
- Recommend for approval policies and procedures pertaining to the school's IT and Information Security programs
- Provide periodic review of IT and Information Security policies and procedures, consistent with University and Feinberg guidelines
- Oversee Feinberg's IT risk management process
  - Maintain Feinberg's risk registry
  - Identify mitigation strategies to protect data, information, and intellectual property
  - Design, implement and monitor Feinberg's IT risk management action plan
  - Perform continual risk assessments
  - Review and implement appropriate risk responses and remediation plans
  - Serve as a formal input into Northwestern University's enterprise risk management process
- Review requests for exceptions to standards, or deviations from policy or standard procedures
- Review IT and Information Security metrics; recommend improvements or modifications, as appropriate
- Charter subcommittees or working groups as required

Membership: The FSM IT Steering Committee will include:

- Feinberg Representatives:
  - Chief Information Officer (CIO)
  - Deputy CIO
  - Chief Information Security Officer (CISO)
  - Vice Dean for Scientific Affairs and Graduate Education
  - Senior Executive Director for Administration
  - Director, Center for Data Science and Informatics
- Northwestern University Representatives
  - CIO
  - CISO

The Committee shall identify one of its members to serve as Chair.

Term: To ensure continuity of operations, individuals will serve as long as they are in the positions above. Membership composition will be reviewed annually to ensure appropriate representation.

Quorum: One-half of total membership plus one.