Subject: **Information Security**	Page **1 of 2**	Policy # **Version: 1.0**
Title: **Log Management Policy**	Revision of: **New policy**	Effective Date: **08/22/18**
		Removal Date:

I. PURPOSE

This policy and procedure establishes the requirements to record activity in information systems that contain or use electronic Personal Health Information (ePHI) or personally identifiable information (PII).

The purpose of recording activity is to enable the ability to evaluate data loss risk related to incidents, evaluate suspicious activity and conduct forensic analysis, troubleshoot information systems and meet HIPAA regulatory compliance requirements. Collection of log data may also enable the ability to analyze on going threats, forecast operational risks through correlation and implement preventative or remedial counter measures.

II. PERSONS AFFECTED:

All NU staff, faculty and students that implement or maintain information systems that support FSM research.

III. POLICY STATEMENT

Information systems that contain or use ePHI or PII will generate activity log records and utilize a log management tool to store and enable analysis of log records. A log management plan will be maintained according to the procedure.

The log management tool will be located on a separate technology resource from the source of the log records. Log management and analysis is a component of the overall FSM risk management plan.

Reporting will be developed to support analysis of log data within the stated purpose of this Policy.

Unauthorized modification or deletion and other falsification of activity log records is strictly prohibited.

Activity log records will be maintained, backed up and recoverable consistent with the retention period required for regulatory compliance.

Any exceptions to this Policy must be documented in writing and approved by the FSM IT Steering Committee.

IV. PROCEDURE STATEMENT

FSM IT Security will maintain a written operational log management plan and will include FSM use cases (e.g., phishing/compromised accounts, unauthorized data access, stolen/lost devices, data exposed to the public) and will identify log sources and log content required to analyze events defined in the use cases.

When additional use cases, reporting requirements or additional information systems are identified, the log management plan will be updated. The plan will be reviewed and updated at least annually. FSM IT Steering will be consulted when changes to the plan require non-trivial resources to implement.

V. ROLES AND RESPONSIBILITIES

FSM IT Security will oversee the log management policy and provide oversight, direction and reporting regarding compliance.

FSM IT Security will coordinate log collection with custodians/owners of information systems from which log data is necessary to collect. Examples of systems include email, data storage, networks, servers, endpoints, and business/research applications.

Custodian/owners of systems will oversee the implementation of audit trails through logging of system events as defined by FSM IT Security and as required to maintain regulatory compliance. Custodians/owners of information systems will ensure logging is enabled at all times.

VI. DEFINITIONS

Information Systems – Encompasses any component used in electronic processing of data. Examples include desktop computers, portable devices/computers, network devices, data storage devices, e-mail systems, database systems, office application systems such as Microsoft Office and business application systems such as clinical research participant tracking systems.

Custodians/Owners of Information Systems - The individual responsible and accountable for the overall development, implementation, integration, modification, securing and operation of technology-based systems and services.

VII. POLICY UPDATE SCHEDULE:

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

VIII. REVISION HISTORY:

08/22/18 – New policy effective.

IX. RELEVANT REFERENCES:

FSM Security Risk Management Policy:
http://www.feinberg.northwestern.edu/it/docs/Feinberg-IT-Security-Risk-Management-Policy-11_01_17.pdf