Subject: **Information Security**	Page **1**	Policy # Version: 1.0
Title: **Assessing the Probability of Public Disclosure of Protected Data**	Revision of: **8/11/2015**	Effective Date: **7/1/2014**
		Removal Date:

I. PURPOSE:

This policy and procedure defines the required method to assess a probability of unauthorized disclosure of protected University data resulting from all forms of device compromise and/or unauthorized data loss as a result of reported or discovered incident. The procedure complements existing Incident Response policies and procedures (see Related Policies and Procedures) and serves to define possible escalation paths based upon a technical assessment of the incident.

II. POLICY STATEMENT:

Protected data must be continually secured from unauthorized disclosure following all related organizational policy and procedure requirements (e.g., use of HIPAA Security grade storage) and using all approved technical capabilities (e.g., anti-malware detection, encryption, mobile device remote wipe).

Reporting Requirements
Northwestern University employees including faculty and staff, students, affiliates and other temporary workers are required to report actual or suspected loss of data through direct or indirect knowledge immediately to their supervisor and to the Northwestern University Feinberg School of Medicine, Chief Information Security Officer at FSMIT-policy at northwestern.edu.

This policy encompasses all forms of protected data as defined by Northwestern University Policy. Current Policy defines this as Internal Information and Legally/Contractually Restricted Information (e.g., HIPAA, FERPA, or the Illinois Personal Information Protection Act). It also encompasses all forms of data storage where University data is stored and transmitted to/from regardless of device type or location is included in the scope of this Policy. This scope includes but is not limited to desktop computers, laptop computers, portable computing devices, portable storage media, file and database storage servers, application servers, personally owned computing devices, Internet cloud services, commercial email and all forms of social media.

Northwestern University Feinberg School of Medicine prohibits storing protected data using personally owned computing devices, Internet cloud services, commercial email and all forms of social media sites without proper security controls and prior authorization. However, if protected data is stored using these services, unauthorized or otherwise, and a potential security incident occurs that involves these personal devices or services then this procedure applies.

Procedure
This procedure is enacted at the moment a device is suspected or known to be compromised through a reported or discovered incident. An incident report or discovery usually occurs prior to knowing the detailed circumstances of the incident and the type of data, if any, which exists on the device or is related to the incident report. Initial notification may occur through channels such as the user support call center, technical support staff and direct communication from internal or external sources, including the Internet.

This procedure manages the required method of assessing the probability that data was accessed, acquired or viewed by an unauthorized party and the escalation to a potentially reportable data breach status, if warranted. The assessment will follow the criteria set forth by Breach definition

exclusions (per 45 CFR §164.402) and will be applied to any form of protected data as defined by Northwestern University and as noted in the Scope statement of this Policy. The procedure is scenario-based with the outcome and next steps as defined in the Scenario Table below. Any scenario not listed here should be directed immediately to the Northwestern University Feinberg School of Medicine, Chief Information Security Officer at FSMIT-policy@northwestern.edu.

The outcome of executing this procedure will be an assessment of the probability that data was accessed, acquired or viewed by an unauthorized party. Outcomes as defined by this procedure will be either a probability of low or higher than low.

This procedure makes no attempt to determine if the probability is medium or high as any situation having a greater than low probability must be escalated and further investigated.

Scenario Table		*Risk Assessment Factors (probability level noted)*					*Next Steps Required (1) (2) (3) (4) (5) (6)*
		45 CFR §164.402 1(i)(ii)(iii)-Unintentional, inadvertent internal disclosure	*45 CFR §164.402 2(i)-Presence of PHI*	*45 CFR §164.402 2(ii)-Unauthorized Person Use of PHI*	*45 CFR §164.402 2(iii)-PHI Actually Acquired of Viewed*	*45 CFR §164.402 2(iv)-Risk Mitigation*	
Desktop computer, laptop computer (includes mapped resources)	Malware blocked or quarantined on desktop computer by end-point security software	Low	Unknown	Low	Low	Anti-malware security software	None
User opens support ticket reporting computer is running slow and/or with erratic or unusual behavior	Unknown circumstances	Unknown	Unknown	Unknown	Unknown	Unknown	(1) Device integrity, (3) Unauthorized access
Desktop computer, laptop computer (includes mapped resources)	Malware NOT blocked or quarantined. Device infected.	> Low (possibly)	To be determined	> Low (possibly)	> Low (possibly)	None	(2) Intent of malware
Desktop computer, laptop computer, portable storage media	Lost/Stolen, encrypted	Low	Unknown	Low	Low	Encryption security software	None
Desktop computer, laptop computer, portable	Lost/Stolen, unencrypted	> Low (possibly)	To be determined	> Low (possibly)	> Low (possibly)	Possibly password controls (bios, file level)	(4) Lost or Stolen Devices

storage media							
Printers, copiers, AV equipment, programmed logic controllers & other similar network attached devices.	Malware infected	> Low (possibly)	To be determined	> Low (possibly)	> Low (possibly)	None	(2) Intent of Malware
Application, Database, File, Print Server	Malware infected, unauthorized access	> Low (possibly)	To be determined	> Low (possibly)	> Low (possibly)	None	(2) Intent of Malware, (3) Unauthorized Access
Storage media (data center)	Malware infected	> Low (possibly)	To be determined	> Low (possibly)	> Low (possibly)	None	(2) Intent of malware
Storage media (data center)	Unauthorized access, file-level encryption	Low	Unknown	Low	Low	Encryption security software	None
Storage media (data center)	Unauthorized access, unencrypted	> Low (possibly)	To be determined	> Low (possibly)	> Low (possibly)	None	(3) Unauthorized access
Storage media (portable)	Malware infected	> Low (possibly)	To be determined	> Low (possibly)	> Low (possibly)	None	(2) Intent of malware
Storage media (portable)	Lost/Stolen, encrypted	Low	Unknown	Low	Low	Encryption security software	None
Storage media (portable)	Lost/Stolen, unencrypted	> Low (possibly)	To be determined	> Low (possibly)	> Low (possibly)	None	(4) Lost or stolen devices
Portable computing devices (iOS, Android)	Lost/Stolen, encrypted	Low	Unknown	Low	Low	Encryption security software	None
Portable computing devices (iOS, Android)	Lost/Stolen, unencrypted	> Low (possibly)	To be determined	> Low (possibly)	> Low (possibly)	None	(4) Lost or stolen devices
Personally owned devices with NU data	Lost/Stolen, encrypted	Low	Unknown	Low	Low	Encryption security software	None
Personally owned devices with NU data	Lost/Stolen, unencrypted	> Low (possibly)	To be determined	> Low (possibly)	> Low (possibly)	None	(4) Lost or stolen devices
Internet cloud services	Data theft/loss	> Low (possibly)	To be determined	> Low (possibly)	> Low (possibly)	None	(4) Data theft/loss
Commercial email	Data theft/loss	> Low (possibly)	To be determined	> Low (possibly)	> Low (possibly)	None	(4) Data theft/loss
Social media sites	Data theft/loss	> Low (possibly)	To be determined	> Low (possibly)	> Low (possibly)	None	(4) Data theft/loss
Compromise reported by affected party (e.g., via internet search engine)	Data theft/loss	> Low (possibly)	To be determined	> Low (possibly)	> Low (possibly)	None	(4) Affected Party Report
Public news story	Possible data theft/loss	> Low (possibly)	To be determined	> Low (possibly)	> Low (possibly)	None	(4) Affected Party Report
Circumstantial or anonymous report	Possible data theft/loss	> Low (possibly)	To be determined	> Low (possibly)	> Low (possibly)	None	(4) Affected Party Report

Next Steps

Requirements Resulting from Scenario Analysis Risk Assessment

The intent of these next steps is to assess the probability of data being accessed, acquired or viewed by an unauthorized party and to determine if there is a low or higher than low probability of an incident. Scenarios resulting in a probability higher than low may result in a potentially reportable situation and require further evaluation on a case-by-case basis.

Next step evaluations must be documented according to the Northwestern University Information Security Incident Response Protocol and in the end user support ticket.

(1)Device Integrity

Malware can contribute to a computer's degraded, erratic or unusual performance. The end user support technician must evaluate these situations for the presence of malware.

If it is determined the computer is infected with malware then the procedure for the scenario most relevant o to the discovery described in the Scenario Table above must be followed.

If it is determined no malware is present then further escalation of the incident is not warranted.

(2) Intent of Malware

Malware is typically designed for a multitude of malicious purposes such as infiltration of adware, internet usage tracking, botnet propagation, and other forms designed specifically to steal data at an individual and bulk/database level. The National Vulnerability Database (nvd.nist.gov) and The Cert Database (www.kb.cert.org) are authoritative sources for understanding the nature of specific vulnerabilities and their intent.

It is not unusual for a device to be infected with multiple forms of malware simultaneously. Each malware signature must be evaluated individually. If it is determined that any of the suspect malware is not intended to steal data than the probability rests at low and further escalation of the incident is not warranted. Consult your supervisor if there is any uncertainty resulting from this assessment.

If it determined that any of the suspect malware is specifically designed to steal data and data on the subject device contains protected data as defined by Northwestern University policy than the probability raises above low and the incident must be escalated according to the Northwestern University Information Security Incident Response Protocol.

(3)Unauthorized Access

Unauthorized access is usually associated with an individual gaining access through hacking techniques or device misconfiguration for the sole purpose of stealing data.

If data on the subject device does not contain protected data as defined by Northwestern University policy then the probability rests at low and further escalation of the incident is not warranted.

If data on the subject device contains protected data as defined by Northwestern University policy than the probability raises above low and the incident must be escalated according to the Northwestern University Information Security Incident Response Protocol.

(4)Lost or Stolen Devices

Data on lost or stolen devices without encryption is considered to be accessible and viewable by an unauthorized party.

Data backups of the device, if available, must be restored to determine if protected data exists on the subject device. If data backups do not exist, then the user of the subject device must be interviewed and required to submit an inventory of the data they recall being on the device.

If data on the subject device does not contain protected data as defined by Northwestern University policy then the probability rests at low and further escalation of the incident is not warranted.

If data on the subject device contains protected data as defined by Northwestern University policy than the probability raises above low and the incident must be escalated according to the Northwestern University Information Security Incident Response Protocol.

(5)Data Theft/Loss

The user of the subject service must be interviewed and required to submit an inventory of the data they recall being disclosed.

If data on the subject service does not contain protected data as defined by Northwestern University policy then the probability rests at low and further escalation of the incident is not warranted.

If data on the subject service contains protected data as defined by Northwestern University policy than the probability raises above low and the incident must be escalated according to the Northwestern University Information Security Incident Response Protocol.

(6)Affected Party Report

Verification of the report should be corroborated with internal NU departments. It the report can be reasonably corroborated then an investigation must be performed to locate the source of loss. If the source of loss can be determined then the incident should be evaluated according to the Scenario Table and Next Steps Required as noted above.

Technical Analysis

Additional technical analysis may be required to assess the possibility of actual data theft. These activities may become part of assessment, which varies by case-by-case, when the probability of data being accessed, acquired or viewed by an unauthorized party raises above a low probability.

1. Review of the device configuration such as open ports and services and accessibility of administrative capabilities by the end user.
2. Published CVE data and revisions and date of reported incident.
3. Malware delivery mechanism and date stamps on malware components.
4. Analysis of device and mapped drive log/audit records looking for access dates and other unusual activity correlated to the dates discovered above.
5. Analysis of application access and log/audit records looking for access dates and other unusual activity correlated to the dates discovered above and related to the user ID of the device compromised.

6. Read/access date stamps on individual data files similarly correlated.
7. Analysis of net flow data for outbound (primarily) data volumes.
8. Determination of destination IP addresses and their association with data theft malware.
9. Anti-malware management console records associated with the device.
10. Internet use history, downloads and temporary files.
11. Comparative analysis of compromised device state and uncompromised device state if available from backup or mirrored image.
12. Examination of the device by an expert technology forensics firm.

Compliance and Enforcement
Northwestern University employees including faculty and staff, students and other temporary workers are expected to report actual or suspected loss of University data on a timely basis.

Failure to comply with these policies will lead to sanctions, up to and including administrative suspension of activities, loss of faculty appointment, department or unit financial penalties, or dismissal from the University.

III. PERSONS AFFECTED:

All FSM faculty, staff, students and trainees.

IV. DEFINITIONS:

Protected Data
Any data subject to regulatory or contractual requirements or restrictions.

Incident
Generally defined as any known or highly suspected circumstance where Protected Data has been subject to an actual or possible unauthorized access or acquisition, beyond the University's sphere of control.

Malware (malicious software)
Malware is any software-based technique used to gain unauthorized control of a computing device. Typically malware is used to disrupt the functioning of computing device, gather sensitive information, or gain access to private computer systems without the user knowing.

Breach (per 45 CFR §164.402)
The acquisition, access use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

Unsecured protected health information (per 45 CFR §164.402)
(2) Protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.

Breach definition exclusions (per 45 CFR §164.402), Unintentional, inadvertent internal disclosure
(1)(i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.
(1)(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected

health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.
(1)(iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Breach definition exclusions (per 45 CFR §164.402): 2(i) Presence of PHI; 2(ii)-Unauthorized Person Use of PHI; 2(iii)-PHI Actually Acquired of Viewed; 2(iv)-Risk Mitigation
(2) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors: (i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
(ii) The unauthorized person who used the protected health information or to whom the disclosure was made; (iii) whether the protected health information was actually acquired or viewed; and (iv) The extent to which the risk to the protected health information has been mitigated.

V. POLICY UPDATE SCHEDULE:

Policy review to occur no less than annually.