IRB Standard Operating Procedures		
SOP#: 13 **Revision#:**	**Title: Confidentiality and Protection of Data**	**Effective Date:** **October 13, 2020**
Approved by:	**Institutional Review Board**	**Approval Date:** **October 13, 2020**

PURPOSE

The purpose of this Standard Operating Procedures (SOP) is to describe the systems and processes for managing data in the course of human subjects research activities at Northeastern Illinois University (University). Compliance with this SOP will ensure that all data collected during the research process is recorded, handled, and stored pursuant to best practices in such a way that maintains appropriate confidentiality and allows access and use as applicable. These best practices will need to adapt as technology evolves, so it is important that investigators keep current with the guidelines in the Federal Regulations, state and local laws, professional standards, and the University's rules and policies.

DEFINITIONS

Anonymous data - data that at no time has a code assigned that would permit the data to be traced back to an individual. This includes any information that was recorded or collected without any of the 18 identifiers included in the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Cloud storage services - a cloud-computing model in which data is stored on remote servers accessed from the internet, commonly referred to as the 'cloud'. Generally maintained, operated and managed by a cloud storage service provider on storage servers.

De-identified data - generally refers to data from which all PII and/or PHI (see definitions below) have been removed. The data has been made anonymous by stripping out any information that would allow someone to determine an individual's identity. The primary reason for "de-identifying" data is to protect the privacy or identity of the individuals associated with the data.

Encryption - a system of altering information using a code or mathematical algorithm to render it unintelligible to unauthorized readers.

External drive - device for storing electronic data. Includes jump drives, thumb drives and external hard drives.

Generalizable knowledge - information which has the potential to be expanded from the isolated circumstances in which it is acquired to a broader context.

Human subject - a living individual about whom an investigator (whether professional or student) conducting research: (i) obtains information or biospecimens through intervention or interaction with the individual, and uses, studies, or analyzes the information or biospecimens; or (ii) obtains, uses, studies, analyzes, or generates identifiable private information.

Informed consent - an agreement by an individual who is competent and of legal age to participate in research. Consent is typically obtained by written signature. For web-based research, consent can be obtained by requiring participants to respond to a survey question affirming their consent to participate.

Identifiable private information - private information for which the identity of the subject is or may readily be ascertained by the investigator or associated with the information.

Institutional Review Board (IRB) - a committee established in accord with and for the purposes expressed in the federal regulations for the protection of human research subjects.

Laptop - a portable computer that includes traditional laptops, netbooks, and other portable computing devices that generally have full range personal computer capacities.

Minimal risk - the probability and magnitude of harm or discomfort anticipated in the research are not greater in and of themselves than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests.

Personal computer (PC) - a stand-alone or networked desktop computer.

Personal identifying information (PII) - for the purposes of this SOP, this includes information that identify an individual, including any or all of the following: (1) names; (2) social security numbers; (3) birthdates; (4) addresses; (5) IP addresses; or (6) other data that could reasonably lead to discovering a personal identity.

Protected health information (PHI) - individually identifiable health information transmitted or maintained by a covered entity or its business associates in any form or medium (45 CFR 160.103). The definition exempts a small number of categories of individually identifiable health information, such as individually identifiable health information found in employment records held by a covered entity in its role as an employer.

Research - systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Server - a computer device with software that networks/links personal computers and databases or web applications.

Smartphone, tablet, PDA, and other mobile devices - portable computing devices that send and receive emails, text or phone messages, or other communications and that include data entry and data storage capacity.

Virtual Private Networks (VPNs) - the University allows access to selected drives and folders on University servers from remote locations using software provided by University Technology Services. With VPN access, investigators can connect to files from off-site computers. VPNs are password-protected for security purposes.

POLICY

Research practices involving human subjects routinely involve electronic data, utilized in a variety of ways. Some researchers still follow the traditional approach of collecting data in paper or hardcopy form. Accordingly, this SOP briefly covers the protection of data in paper or hardcopy form, but provides more extensive guidance for investigators to effectively protect electronic data during data collection, transmission, and storage.

This SOP applies to all studies involving individually identifiable participant data that include information of a personal or health nature. This can include even low to minimal risk studies so long as the information is personal or health related. Studies which may be excluded from this SOP include surveys which collect no

direct or indirect personal identifiers, or if identifiable, studies which are non-personal in nature, such as participation in hobbies, special or political interests, etc.

RESPONSIBILITIES

The following establishes data security responsibilities for investigators who collect, use, and store non-electronic data.

Data in Paper or Hardcopy Form

All data not received in an anonymised form must be collected with the permission of study participants, stored securely in a locked cabinet, locked away if unattended, and retained for only as long as has been requested and approved by the IRB. It should be clear in the protocol and informed consent form that personal data which can identify research participants will be kept separate from the study data in locked file cabinets. Access to this data will be restricted to members of the research team, unless authorised by the Principal Investigator.

The following establishes data security responsibilities for investigators who collect, use, and store electronic data:

Secure Servers/Desktop Computers

The recommended electronic devices for entering and storing human subjects data are secure servers or desktop computers that have encryption software for all PHI or other identifying data. The following conditions apply:

a. Operating systems are current with updates and security patches.
b. Server-based PHI or other identifiable human subjects' data should be secure by implementing firewall protection and the data itself is encrypted.
c. Non-networked computers can be used for storage of de-identified data without encryption, but requires password protection for the computer itself.
   Servers housing data are subject to the following standards:
   i. Account Control Plan where strong passwords/pass-phrases are used and enforced, accounts on the server are unique and those that are not needed are disabled or removed, and access to data is on a need to know basis.
   ii. Patching Plan where software patches are installed in a timely fashion and given a priority. This plan includes the operating system and any software applications installed on the server.
   iii. Access Control where all servers have network access controls enabled, capable of limiting network and Internet access to the server, the server is in a secured location with physical access limited only to those who have authorized access to the server, and when possible, the applications and services will operate in a non-administrative mode.
   iv. Malware Control in which Operating Systems are susceptible to malware and therefore must have protection installed, enabled, with anti-malware updates maintained.
   v. Logging where Operating System level and Application level events are logged and monitored to assist in troubleshooting and forensic investigations.
   vi. Backup Plan where a plan is in place for the backup/recovery of data, and data backups should be stored in a secure location separate from the original data.
d. Anonymous data or de-identified data that cannot be traced back to an individual using cue information in the data set matched to other data sources, can be stored on servers without encryption, but would still require authorized password access.

Laptops, Laptop Data Collection Devices, Smartphones, Tablets, PDAs, and Other Mobile Devices

Laptops may be approved to store data collection of human subject data under the following conditions:

Each user of the device maintains and safeguards a unique login and password.

a. All files containing PII or PHI are password protected.
b. Two factor authentication is used for storage or access of PHI.
c. If the device stores PHI or PII, the device hard drive is encrypted.
d. The device uses software that encrypts all PHI or PII.
e. The data are formatted such that PHI or other identifying data are in separate files or tables from any clinical or research information about the research subject.

In addition to the conditions above for laptops, the following conditions apply for all other mobile devices:

Operating systems of all devices must be kept current in order to ensure that critical security, anti-virus, and anti-malware programs are up-to-date. The following conditions apply:

a. When using mobile devices to collect research data, configure the mobile device to be secure by enabling auto-lock and requiring a password or passcode.
b. When using mobile devices to access research data sets, the device must use software that encrypts all personal health information or other personal identifying information and the data must be formatted such that PHI or other identifying data are in separate files or tables from any clinical or research information about the persons.
c. General best practices:
    i. Connect to secure Wi-Fi networks and disable both Wi-Fi and Bluetooth when not in use for safety purposes.
    ii. Regularly backup all devices.
    iii. Update mobile devices frequently. Select an automatic update option, if available.
    iv. Use appropriate sanitization and disposal procedures for mobile devices. Be sure to delete all information stored in a device prior to discarding, exchanging, or donating.

External Drives

External drives may only be used under the following conditions:

a. For storing and analyzing de-identified data on human subjects.
b. Must be stored/transported in a secure location.
c. Must be password protected.
d. Must have files that have software to automatically encrypt all PHI or other identifying information or the entire external drive is encrypted.
e. The data must be formatted to ensure that PHI or other identifying data are in separate files or tables from any clinical or research information about the research subjects.

Web-based Data Entry/Surveys

Web-based data entry and surveys are subject to the following conditions:

a. Research data collected through online portals and/or survey tools should use secure web server (https) protocols and the server should encrypt any PHI or other identifiers upon submission.
b. The server used to store collected survey data must have a firewall implemented, managed, and monitored.
c. If the survey data is stored by a third-party vendor (i.e., cloud storage), the service must be approved by the University's Chief Information Officer (CIO) or Acting CIO.
d. Web-based anonymous or de-identified data need not be encrypted.

CDs and DVDs

PHI, PII, or other identifying data should not be stored on CDs or DVDs unless the entire CD or DVD is encrypted. However, de-identified human subject data may be stored on CDs or DVDs in open format.

Email

PHI or PII or other identifying data should **not** be contained in email communications unless the attachments are encrypted files where the password is sent in a separate communication.

Encryption

Before using an encryption program, an investigator should evaluate if it is absolutely necessary to store confidential or private data on a computer or mobile computing device (e.g., flash drive). If it is critical to store private data, an investigator must take steps to encrypt the data to help prevent unauthorized disclosure of private data. At this time, the University does not endorse or support any type of software-based encryption application.

Following are important guidelines regarding the use of encryption:

a. Consult with appropriate technical support staff.
b. Be sure you fully understand the encryption product (i.e., how to configure the software, where to store the keys and what is encrypted).
c. Use strong passwords. All encrypted data can be permanently lost if you forget the encryption password. If you decide to save this password, any decryption keys should be safely secured.
d. Download the encryption software from a reputable company (beware of spyware, etc.).
e. Do not decrypt a file and store it in a temporary file someplace.
f. Consider setting up a secure folder or disk partition on your computer for storing private data.

Web-based Surveys

Individual proprietary survey programs incorporate investigators' own measures, but store data on their own servers outside of the University. Investigators need to have a clear understanding about the protections that are afforded by the independent proprietary provider. Investigators should obtain information about the tools' security and privacy protections, including learning whether user IP addresses are captured and saved during completion of the surveys.

Qualtrics, an online survey platform, is available for use by University faculty, staff, and students at no charge. Investigators should be aware that other survey platforms may involve individual software licensing agreements which are subject to review and approval by the University's Chief Information Officer (CIO) or Acting CIO.

Warning: Data is most vulnerable during the time the survey program is open and being used by the research participant. This is the point at which hacking could discover the identity or other personal information. This

is not unique to web-based research, but includes any period when a user is online. Investigators need to be assured that when any PHI or PII are being collected in web-based tools, once the data are transmitted, they are encrypted.

Informed consent forms should be utilized. These forms should clarify the protections that are available to the web-using participant and should describe the specific web-based data security being used. If proprietary vendors are being used to collect the data, and if breach of confidentiality could put respondents at risk due to the nature of the survey questions, the consent forms should explicitly describe this possibility.

Regulations
45 CFR 46.102

Author Reference
NEIU IRB
George Mason University, SOP "Classroom Projects"
North Dakota State University, Confidentiality and Data Security Guidelines for Electronic Research Data

Contact Information
Please direct questions or concerns about this policy to:

Contact	**Phone**	**E-Mail**
IRB Office	773-442-4675	irb@neiu.edu
Dean of the College of Graduate Studies and Research	773-442-6012	gradstudies@neiu.edu

Disclaimer
The University reserves the right to modify or amend sections of this IRB SOP at any time at its sole discretion. This IRB SOP remains in effect until such time as the Responsible Officer calls for review. Requests for exception to any portion of this policy, but not to the policy statement, must be presented in writing to the Responsible Officer.