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.

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

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

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