IRB Standard Operating Procedures		
SOP#: 14 **Revision#:**	**NEIU Online Research/Online Consent**	**Effective Date:** **January 26, 2021**
Approved By:	**Institutional Review Board**	**Approval Date:** **January 26, 2021**

PURPOSE

This policy sets forth requirements and recommendations by which researchers can plan,develop, and implement computer and internet based survey research protocols that provide equivalent levels of protection of human participants to those found in more traditional research methodologies such as paper based surveys.

All studies, including those using computer and internet technologies, must:

- Ensure that the procedures fulfill the principles of voluntary participation and consent,
- Have appropriate safeguards to protect the privacy or confidentiality of information obtained from or about human participants,
- Adequately address possible risks to participants, including psychosocial stress and related risks.

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).

Belmont report - document that outlines the basic ethical principles in research involving human subjects.

Confidentiality - Prevention of disclosure, to other than authorized individuals, of a sponsor's proprietary information or of a subject's identity.

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

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.

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.

Internet data collection - Internet-based data collection methods that can range from the use of existing data and observations to interventions and survey/interview procedures.

IRB - an institutional review board established in accord with and for the purposes expressed in the federal regulations for the protection of human research subjects.

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.

Blog - A website used as a journal; can be personal or professional in nature.

Chatroom - An online location where individuals can come together to have text-based chat discussions that occur in real time.

Cloud computing - Distant storage or data management servers typically owned and operated by a third party.

Confidentiality - Pertains to the treatment of information that an individual has disclosed in a relationship of trust, and with the expectation that it will not be divulged without permission to others in ways that are inconsistent with the understanding of the original disclosure.

Cookie - A text file placed on a user's computer by a website or web server. Often used to keep track of individuals as they navigate a site, and more broadly, the web.

Encryption software - A piece of software that is used to obfuscate information to all of those who do not have the means to decrypt the information.

Internet Protocol (IP) address - A numeric address assigned to every computer that connects to a network, or more commonly, the Internet.

IRC - Internet Relay Chat, a protocol used for hosting and participating in chat rooms. Lurking: A behavior specific to online communities, wherein an individual remains silent,
observes, and does not participate in the community.

Online persona - An online character or avatar used by an individual.

Online survey - Any tool used to collect responses to survey questions via the Internet.

Privacy - Control over the extent, timing, and circumstances of sharing oneself (physically, behaviorally, or

intellectually) with others.

Publicly available - The general public can obtain the data.

Waiver of consent - A waiver of consent relieves a person or organization required to obtain consent form actually getting that consent. The PIs are required to follow appropriate procedures for requesting a waiver of consent.

POLICY

Internet data collection via email, list servs, apps, electronic bulletin boards, text messaging, virtual chats, and web surveys falls under the purview of the Institutional Review Board. Researchers must adhere to the same ethical principles protecting human subjects as mandated in more traditional research situations. These principles are: Respect for Persons, Beneficence, and Justice as are described in the Belmont Report. These ethical principles are reflected in procedures that seek and obtain informed consent, protect privacy of participants, maintain confidentiality of data, minimize risks and prevent coercion.

The IRB will review the use of internet-based research activities including subject recruitment and consent to ensure that:

- Risks such as violation of privacy, legal risks, and psychosocial stress are minimized
- Subjects' participation is voluntary
- Informed consent requirements are met
- Information obtained from or about human subjects is kept confidential

In general, the Internet is an insecure medium as data in transit may be vulnerable. The potential source of risk is harm resulting from a breach of confidentiality. This risk is heightened if the research involves data that places subjects at risk of criminal or civil liability or could damage their financial standing, employability, insurability, reputation or could be stigmatizing.

In general, email to inform and recruit participants is acceptable but should be avoided for the transmission of confidential data, unless encrypted. The IRB requires Investigators to follow the procedures outlined below to ensure the adequate protection of research participants and guarantee the validity of the data collected. These procedures will assist Investigators to plan and implement internet-based research studies while providing the same level of protection as human subjects involved in more traditional research studies.

Depending on the risk level and the specific circumstances of the study, the IRB may elect to require researchers to provide an alternative means of collecting data. In addition, the IRB may elect to require additional protections, such as technical separation of identifiers, data, consent

forms and follow-up contact information, or a higher level of encryption.

RESPONSIBILITIES

Execution of SOP: Researchers, IRB

Informed Consent Process

Internet based surveys need to initially present an IRB approved consent form on which participants would either choose “I agree” or “I do not agree” buttons thus indicating their active choice of whether or not they consent to participate. Should participants not want to participate by choosing the “I do not agree” button, the researcher should immediately direct the participant to a next and final screen that thanks the participant for their consideration and ends the involvement in the study. Should the participants want to participate by choosing the “I agree” button and the data collected is anonymous, the researcher should immediately direct the participant to a next and separate screen from the consent form that will begin the data collection. For online studies with consent forms that require a participant to type their name, the consent form and data collection will be housed separately.

For surveys sent to and returned by participants via email, investigators should include an IRB approved consent form and inform participants that submitting the completed survey indicates their consent. Participants must be informed that, due to unintentional breaches of the data, this method of data collection cannot ensure anonymity.

For surveys sent to and returned by participants via email without a signature, investigators must include a consent document and inform participants that submitting the completed survey indicates their consent. This constitutes unsigned consent. In order to utilize this consent procedure, the investigator must request a waiver of documented consent.

Researchers conducting any form of web-based research convey that they will endeavor to provide confidentiality or anonymity but should be careful not to make guarantees of confidentiality or anonymity, as the security of online transmissions cannot be guaranteed.

Researchers should instruct subjects to close their browser window after participation and suggest that they clear their cache to protect their confidentiality, especially if the participant uses a shared computer.

After receiving consent from each participant in an online synchronous or asynchronous discussion board between two or more individuals, and when research includes observing a chat room that is

not open to the public, researchers must inform participants that observation is taking place, and that any information exchanged may be used for research purposes. Researchers remain vigilant to remove any unintended individual joining the established group after the researcher has gained consent.

Online consent may not be suitable for high risk studies where the research involves data that places participants at risk of criminal or civil liability, or could damage their financial standing, employability, insurability, reputation, or could be stigmatizing. Thus, researchers may be required to gather consent through direct contact with participants (i.e., not online).

NOTE: Research is subject to the Children's Online Privacy Protection Act. Therefore, researchers are prohibited from collecting personal information from a child without posting notices about how the information will be used and without getting verifiable, written parental permission. For minimal risk research, both assent forms from the child participant and consent forms from the parent or guardian must be secured before any data can be collected. If the research is more than minimal risk, the scope, child participation and potential risks of the study must be discussed virtually with the parent or guardian before assent and consent forms are secured and any data can be collected.

For research that excludes minor participants, in order to authenticate that the participant is not a minor posing as an adult, the IRB may ask the researcher to describe the procedures to be employed to authenticate that the participants are adults. Some options are using internet monitoring software or using adult check systems that can screen out minors.

Use of Internet for Subject Recruitment

The IRB must review and approve all materials to be posted on the Internet (e.g. through a website, a banner advertisement, or an email solicitation). Computer- and Internet-based procedures for advertising and recruiting potential study participants (e.g., internet advertising, e-mail solicitation, banner ads) must follow the IRB guidelines for recruitment that apply to any traditional media (e.g., newspapers and flyers). Investigators requesting to recruit through NEIU's mass email system must follow the appropriate NEIU policies and procedures for review and approval in addition to obtaining IRB approval for the recruitment procedure and message content.

Collecting data over the Internet can increase potential risks to confidentiality because of the frequent involvement of third party sites and the risk of third party interception when transmitting data across a network. For example, when using a third party website to administer surveys, the website might store collected data on backups or server logs beyond the timeframe of the research project. In addition, third party sites may have their own security measures that do not match those of the investigators'. Participants should be informed of

these potential risks in the informed consent document. For example:

i. “Although every reasonable effort has been taken, confidentiality during actual Internet communication procedures cannot be guaranteed.”

ii. “Your confidentiality will be kept to the degree permitted by the technology being used. No guarantees can be made regarding the interception of data sent via the Internet by any third parties” (Pennsylvania State University).

iii. “Data may exist on backups or server logs beyond the timeframe of this research project.”

IRB Requirements

The IRB must review all research activities involving the use of the Internet with the same considerations and standards for approval of research (45 CFR 46.111), for informed consent, and voluntary participation as all other research activities. The IRB must evaluate the appropriateness of the informed consent process. The IRB must take into consideration data collection and security. The IRB review must include a consideration for the delineation of boundaries (i.e., would the participant consider the access private or public space of the internet). The IRB must consider all additional requirements for the approval of research that involves a vulnerable population as all other studies recruiting those populations. As there is no standard for identifying distressed participants online, the IRB must take into consideration potential participant experiences (the sensitive nature of the research) that may be distressing when evaluating the risk/benefit ratio.

Data Collection/Storage:

Data collected from human subjects over computer networks should be transmitted in encrypted format. All databases storing identifiable information or data must be protected regardless of the source creating the data (e.g., encryption of the database, de- identifying the database). In general, personal identifiers such as Social Security Numbers, hospital or clinical patient numbers, or other information which might identify research subjects should be eliminated from research data or completely encrypted. Researchers might find it most practical to assign research subjects random or generated serial numbers; a map or table correlating these research IDs to personally identifying data could be maintained in a separate file or table which is stored more securely and only accessed as needed.

It is recommended that data backups be stored in a safe location; this could simply be locked storage in a private office, but a secure data room that is environmentally controlled and has limited access is desirable. It is recommended that either the researcher or the computer system administrator destroy unneeded copies or backups to ensure that no data can be recovered from obsolete electronic media.

If the data are stored on a server system, the researcher should determine not only what procedures are followed to back-up the data, but what provisions are in place to protect the backup media against inappropriate access and how long backups are maintained. Special provisions may need to be made so that confidential research data do not reside on backup media unknown to the researcher. Competent data destruction services should be used to ensure that no data can be recovered from obsolete electronic media. Researchers must have a written plan to dispose of old data on a consistent basis. This includes but is not limited to the overwriting or physical destruction of storage media e.g. hard drives, flash drives, tape cartridges, CD/DVD-ROM media before it is removed from the researcher's premises.

Researchers must provide a written schedule for when data will be removed from production and backup sites (Examples: upon termination of research, within 30 days of research termination, within one year of research termination, etc.). The IRB must approve the method and procedures for data collection and security.

NOTE: When posting a survey online, researchers will utilize third party distributors that have been approved by the IRB (e.g., Qualtrics, Survey Monkey, Zoomerang, etc.).

Survey Software Checklist

When using encryption software to handle sensitive information sent to and from websites, researchers should consider the following:

- Are there controls in place to prevent a respondent from accidentally entering survey data via the http protocol instead of the https protocol (i.e. Does the server display an error message or automatically reroute the respondent to an https page)?
- When accessing their data in the database via a username and password, researchers should ensure that survey data contained in the database(s) cannot be improperly accessed or information cannot be disclosed to parties other than authorized researchers.
- Are the servers that contain the research data located in a data center, with physical security controls and environmental controls?
    - Is there a finite time period in which a deleted dataset can still be retrieved?
    - What is that time period?
    - Is the respondent's IP address masked from the researcher? If collected, please explain what is done with the information.
    - Do other third parties have access to IP addresses?
    - Are there any circumstances where respondent identifiers and their survey responses would be released to third parties?

Regulations
45 CFR 46.102

Author Reference
NEIU IRB
George Mason Univers it y S OP “Classroom Projects”

University of South Alabama, IRB SOP 804
University of California, Berkeley

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.