

**Institutional Review Board (“IRB”)**

**Data Security Guidelines**

Federal regulations for human subjects research require Institutional Review Boards (“IRBs”) to determine that adequate provisions to protect the privacy of subjects and the confidentiality of data are in place and that researchers include adequate provisions for monitoring the data collected to ensure the safety of subjects in their research plan. This document will help investigators plan for the collection, transmission, and storage of research data in a secure manner consistent with Connecticut State Colleges and Universities (“CSCU”) policies and federal regulations.

The Principal Investigator (“PI”) is responsible for all aspects of research, including the collection, transmission, storage, backup, and security of data and ensuring those listed as key personnel are informed and trained on the procedures related to data security. Research team meetings should include documentation of training and discussion about the safeguards in place to protect research data. This is particularly important should a breach be suspected or actually occur or loss or theft of a device that stores identifiable data. These occurrences must be immediately communicated to the CT State IRB at [ctstate-irb@ct.edu](mailto:ctstate-irb@ct.edu) and the CSCU Information Security Program Office (“ISPO”) at [security@ct.edu](mailto:security@ct.edu).

The informed consent form must include information regarding any terms of service or end user agreement for technologies used in the research as well as information about whether a vendor has access to a participant’s contact list or other information on their device, ability to track location, and whether there is a possibility that any participant data will be used for marketing or other activities or sold to a third party.

**Definitions**

* **Anonymous Data:** These data do not include personally identifiable information (“PII”) including but not limited to date of birth and e-mail address.Internet Protocol (“IP”) addresses are considered by some international standards to be identifiable even though the address is linked to the computer and not specifically to the individual.
* **Confidential Data:** These data are regulated by federal or state laws including but not limited to the Family Educational Rights and Privacy Act (“FERPA”), the Health Insurance Portability and Accountability Act (“HIPAA”), or the Children’s Online Privacy Protection Act (“COPPA”), as amended.
* **De-Identified Data:** These data are stripped of all identifying information and there is no way the data could be linked back to an individual through a key or other coding method. Best practice when de-identifying data is to use the [safe harbor](https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#standard) method where all HIPAA identifiers are removed.
* **Coded Data:** These data are coded when a link or key to the code exists, such as a number, letter, symbol, pseudonym, or any combination, that is linked to an individual participant’s identifiers. The code should not include information related to an individual, such as initials or date of birth.
* **Identifiable Private Information:** This is private information for which the identity of the subject is or may readily be ascertained by the investigator or associated with the information.
* **Private Information:** This includes information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information that has been provided for specific purposes by an individual and that the individual can reasonably expect will not be made public (e.g., a medical record).
* **Protected Health Information (“PHI”)**: Individually identifiable health information, held or maintained by a covered entity or its business associates acting for the covered entity, that is transmitted or maintained in any form or medium. This includes identifiable demographic and other information relating to the past, present, or future physical or mental health or condition of an individual, or the provision or payment of health care to an individual that is created or received by a health care provider, health plan, employer, or health care clearinghouse. Note that genetic information is considered to be health information.
* **Sensitive Data:** These data include information related to alcohol or drug use, traumatic experiences, child/elder abuse, or illegal behavior, or where disclosure outside of the research study has the potential to place participants at risk of criminal or civil liability or be damaging to their financial standing, employability, educational advancement, or reputation.

**Transmission of Research Data**

Do not transmit identifiable datasets by e-mail due to the inherent risk of compromise. When e-mailing data that do not contain any personal identifiers, include “[encrypt]” in the subject line of an e-mail when sending from a CSCU email account. Compromised e-mails could place data at risk and result in loss of confidentiality for research participants. Identifiable data should be transmitted via a secure service or by using secure protocols such as a File Transfer Protocol Secure (“FTPS”).

**Online Data Collection Software**

For international research, investigators are cautioned that standards for handling data about people vary from country to country and that there are legal restrictions regarding the export of certain encryption software outside United States (“US”) boundaries. Similarly, data privacy regulations vary between states. Investigators are responsible for understanding the data privacy laws where data collection occurs for their research study and providing it to the IRB. To conduct surveys, investigators must use CSCU-approved and licensed applications.

**Data Storage and Disposal**

If a server is used for data storage, personal identifying information should be kept separate from the data. It is recommended that competent data destruction services be used to ensure that no data can be recovered from obsolete electronic media. Researchers must adhere to [CSCU IT policies](https://www.ct.edu/it/policy) and [CSCU data privacy guidelines](https://www.ct.edu/dataprivacy). As a reminder, federal regulations require human subjects records be retained for at least three (3) years after completion of the research study.