WESTCLIFF UNIVERSITY
Educate. Inspire. Empower.

IRB Standard Operating Procedure

SOP 7	Data Security	Effective Date 1/1/2023

PURPOSE

When conducting human subjects research, one of the most common risks — regardless of the risk otherwise present in the study protocol — is that the confidentiality of data collected from the subjects will be breached.

The security of data is of concern not only during the conduct of research—but also after the study concludes. Data from closed studies must be appropriately secured and the investigators should have a clear data retention plan in mind even before starting the research.

Because the disclosure, loss, or theft of data potentially presents a risk both during and after a research study, the IRB is interested in determining if investigators have appropriate measures in place to protect the data that they collect.

DEFINITIONS

None

POLICY 7.1: Deidentification of Data

Section 164.514(a) of the HIPAA Privacy Rule provides the standard for de-identification of protected health information. Under this standard, health information is not individually identifiable if it does not identify an individual and if the covered entity has no reasonable basis to believe it can be used to identify an individual. Section 164.514(a) may be reviewed at:

- https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#standard

All studies must utilize at least the S*afe Harbor* method. However, *expert determination* may be utilized at the discretion of the IRB.

POLICY 7.2: Data Retention

In accordance with federal guidelines, the IRB requires that study data and consent forms must be maintained securely for, at minimum, three years after the completion of a study. Moreover,

- Following the minimum three-year retention period, individually identifiable information (including the password-protected *master key* [spreadsheet] and any combination of

indirect identifiers that could reasonably identify a subject) must be destroyed, if it has not been already. De-identified data may be retained indefinitely.

During the retention period, data, signed consent forms, and other documentation related to human subjects must be stored in the manner described in the IRB-approved protocol. Access must be limited to those identified in the approved protocol as having access to study data.

POLICY 7.3: IRB Recommended Practices

One of the easiest ways to help protect the confidentiality of data that you collect is through the use of coded identifiers.

- Assign each study participant a random unique identifier. Use this identifier to label all data collection instruments and sheets — do not record any individually identifiable information about the participant as part of the study data.
- Develop a password-protected master key enabling the organization of identifying information and data.
- Enter the contact or other identifiable information you collect into the master key.
- Record the coded study identifiers in the master key.
- Once the data are organized and analyzed, the master key (and participant contact information forms, if used) should be destroyed. If it is important to your study to keep the master key, please provide a detailed rationale to the IRB. In your proposal, detail how and when these keys will be destroyed.
- Data documents should have only the data and the study ID code; all other identifiers must be eliminated.

Transport of data should be limited to reduce the risk of loss or theft. Moreover:

- When it is not in transit, data should be stored in a secure location accessible only to the investigator.
- Data that are transported physically from a study site to an investigator's office or lab should be locked in a secure container. If possible, a personal vehicle (rather than public transit) should be used.
- Data must be transported separately (whether in separate electronic files or physical containers) from consent documentation or master keys. This ensures that if data is lost or stolen, there will be no associated identifiable information at risk of disclosure.
- Electronic data should be stored only on password-protected (and, if possible, encrypted) storage media or computers. Copies of electronic data files should be kept to an absolute minimum.
- Electronic data should not be sent over email; but, if necessary, it should only be sent if it is de-identified.

IRB Standard Operating Procedure

SOP 7	Data Security	Effective Date 1/1/2023

RESPONSIBILITIES

IRB Chair is charged with ensuring SOP 7.

The investigator is responsible for designing, implementing, and adhering to an IRB-approved data security plan.

REGULATIONS

§ 164.501

CONTACT INFORMATION

Please direct questions or concerns about this policy to:

Contact	Title/Role
	IO
Brett Gordon	IRB Chair

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 a suitable Institutional Official or IRB Member requests review or exception to this SOP.