James Madison University **Office of Research Integrity and Institutional Review Board** **Standard Operating Procedures**			
TITLE: Security of Research Data			
SOP # 4	**Revision #1**	**Effective Date: 11/8/19**	**Page 1 of 6**

OBJECTIVE

To describe policies and procedures for safeguarding research data.

GENERAL DESCRIPTION

Federal regulations require IRBs to determine the adequacy of provisions to protect the privacy of subjects and to maintain the confidentiality of their data. To meet this requirement, federal regulations require researchers to provide a plan to protect the confidentiality of research data [45 CFR 46.111(a)]. Safeguarding the confidentiality, integrity, and availability of research data is critically important to maintaining a successful research program. Good security ensures and builds research subject confidence that their personal information will be kept confidential, and also ensures that valuable research data is protected and accessible when needed. In addition, research is now a global enterprise, and investigators should understand the international laws or regulations that may apply when conducting research outside the United States.

The Principal Investigator (PI) is responsible for ensuring that research data is secure when it is collected, stored, transmitted, or shared. All members of the research team should receive appropriate training about securing and safeguarding research data. JMU Information Technology (IT) offers a wide range of services for all faculty, staff, and students. Investigators are encouraged to consult the Guidelines for Data Storage and Collaboration as well as consult with IT staff and Libraries & Educational Technologies to develop standard best practices.

This SOP applies to researchers and research team members who obtain, access or generate research data, in particular confidential information. The SOP also applies regardless of whether or not the research is funded and regardless of the source of funding for the research. Furthermore, this SOP applies to all research data regardless of the storage medium (e.g., disk drive, external drive, paper, etc.) and regardless of form (e.g., text, graphic, video, audio, etc.), physically housed at JMU or stored remotely under the management of JMU researchers.

DEFINITIONS

Anonymous data: Data that at no time can be connected back to the individual who provided it. No identifying information is collected from the individual, including direct identifiers such as name or address. Researchers should be aware that collection of indirect identifiers (i.e., information regarding other unique individual characteristics) might make it possible to identify an individual from a pool of subjects.

De-Identified: When any direct or indirect identifiers or codes linking the data to the individual subject's identify are destroyed.

Coded data: Identifying information (such as name) that would enable the investigator to readily ascertain the identity of the individual to whom the private information or specimens pertain has been replaced with a code (number, letter, symbol, or any combination) and a key to decipher the code exists, enabling linkage of the identifying information to the private information or specimens.

Protected Health Information (PHI): Any information transmitted or maintained in any form (i.e., by electronic means, on paper or through oral communication) that relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual or the past, present or future payment for health care and (a) identifies the individual or (b) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

Personally Identifiable Information (PII): Data that, on its own or with other information, may be used to identify, contact, or locate a single person, or to identify an individual in context.

Private information: 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 (for example, a medical record).

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

Identifiable biospecimen: is a biospecimen for which the identity of the subject is or may readily be ascertained by the investigator or associated with the biospecimen.

Sensitive Research Data: Data is considered sensitive when disclosure of identifying information could have adverse consequences for subjects or damage their financial standing, employability, insurability, or reputation.

Data Encryption: Encryption is the conversion of data into a form, through use of an algorithm, which cannot be easily understood by unauthorized people.

Secure Physical Location: A secure location is a place (e.g., room or file cabinet) for storing paper files, and other removable medium, computers, or equipment. Only the investigator and authorized research staff have access either through a physical or electronic key.

RESPONSIBILITY

Execution of SOP: IRB Chair, IRB Members, Office of Research Integrity (ORI); Principal Investigator (PI)/Study Personnel

PROCEDURES

What is the risk?

- Is the data identifiable, de-identified, coded, or anonymous?
- Is sensitive information being collected that could result in harm to participants?
- What is the risk of harm to the participant or others?

What are the protections against anticipated threats or hazards (during collection, transmission, storage)?

- Encryption of data on device to protect against loss/theft of device
- Use of secure data transmission channels to protect against data interception
- Strong passwords to protect against unauthorized access
- Store data behind a secure firewall whenever possible
- Ensure strong data security controls on all storage sites

What is the security and backup of data?

Data is the basis of research. If data is lost, recovery could be slow, costly, or impossible. Securing, storing, and backup of data should occur on a regular basis. Securing data will help prevent:

- Accidental or malicious damage/modification to data
- Theft of valuable data
- Breach of confidentiality agreements and privacy laws
- Premature release of data, which can void intellectual property claims
- Release before data have been checked for accuracy and authenticity

Keeping regular and reliable backups protects against the damage or loss due to hardware failure, software or media faults, viruses or hacking, power failure, or human errors.

The level of security necessary is relative to the risk posed to the subject should personally identifiable information be inadvertently disclosed or released as a result of malfeasance. In an effort to ensure best practice, it is always desirable to have a high level of security rather than to risk operating at a minimal standard. The IRB has the authority to decide if the security plan to protect subjects' confidentiality or anonymity appears acceptable. For data that retains identifiers, the protocol must describe adequate administrative, physical, and technical safeguards. When a study involves greater than minimal risk, investigators are encouraged to consult with appropriate information technology and security experts such as their system administrators to develop appropriate data security plans. Specifically, investigators should:

- Collect the minimum identity data needed. Identifiers should only be collected if they serve a legitimate purpose in the context of the research.

- De-identify data as soon as possible after collection and/or separate data elements into a coded data set and an identity-only data set. Coded data and identity-only data should always be stored separately in a secure location. Not all research data sets can reasonably be de-identified (for example, in a video or audio recorded interview the subject may be readily identifiable). In this case, the original research data set must be considered personally identifiable and treated accordingly.
- Secure data encryption must be used if identifiable information is: (1) stored on a networked computer or device, either on campus or off-campus; (2) transmitted over a network; and/or (3) stored on a removable medium (e.g., laptop computer or a USB flash drive).
- Limit access to personally identifiable information. The opportunity for human error should be reduced through: a) limiting the number of people (both users and administrators) with access to the data and ensuring their expertise and trustworthiness; and/or b) using automatic (embedded) security measures (such as storing data on non-volatile medium only in secure data-encrypted form) that are professionally installed and administered. If this computer is connected to the campus network or to the public Internet, the professional administrator of the computer shall ensure that it complies with all minimum standards for network and data security listed below.
- When identifiable information is stored in personal or university-owned or - maintained computer, investigators are strongly encouraged to ensure that this computer be professionally administered and managed. If this is not possible, investigators should disclose such, and provide the IRB with a plan for how the sensitive data will otherwise be secured.

Roles and Responsibilities of Principal Investigator and Research Team in Safeguarding Research Data

Investigators are responsible for:

- Disclosing the nature of the confidential data they collect in their study protocol so that the IRB can assess the data security risk;
- Preparing data security plans and procedures in accordance with the appropriate security category requirements;
- Implementing and monitoring the data security plans and procedures over the course of the project.

In general, all members of the research team are responsible for correctly and sufficiently using research computers, databases, and records to ensure security and confidentiality of the data stored and transmitted using those resources.

PIs are responsible for ensuring research data remains secure when under the research team’s control by:

- Using appropriate safeguards to maintain the confidentiality, integrity, and availability of data that is collected, used, shared and/or stored for research purposes, including Protected Health Information (PHI);

- Establishing appropriate security oversight for a research project and identifying whether certain aspects should be delegated and to whom;

- Identifying all on-site and off-site research personnel who have or need access to research data in any form and ensuring they employ appropriate safeguards and follow all university policies regarding access to data;

- Ensuring all members of the research team in contact with the data understand their responsibilities and that access to this data is appropriately restricted;

- Ensuring that for human subject research, the IRB application appropriately explains the safeguards used to protect the data, including the Data Source (i.e., the types of records that are used to gather the data) and the Data Recording/Collection method; and

- Immediately reporting any suspected or known security breaches that compromise research data to ORI.

Security Plan

Each research project requires an appropriate security plan designed to safeguard the security of research data. This may be project specific, team specific, or lab or location specific.

This may be delegated to an appropriate person within a department, school, or division, but the PI is ultimately responsible for communicating needs and for ensuring an appropriate security organization plan exists.

The PI is responsible for identifying which security policies are applicable to their specific project and for oversight of the delegate. When the data security level has been established, researchers are responsible for creating and maintaining data documentation, implementing the security controls corresponding to the requirements of the data security level and developing and following a data security plan and procedures over the course of their projects.

REVISION HISTORY

Version No.	Brief Description of Changes	Created on Date
00	Creation of SOP	3/9/2016

01	Revision of SOP	11/8/2019

SIGNATURE HISTORY

Name and Title	Signature	Date

REFERENCES

45 CFR 46.111(a)
Guidelines for Data Storage and Collaboration