Marcus Institute for Aging Research
Hebrew SeniorLife

HARVARD MEDICAL SCHOOL AFFILIATE

Sensitive Data Security Policy

Institutional Policy

Title:	Sensitive Data Security Policy
Responsible Officer:	Director, Research Informatics
Original Effective Date:	3/16/2014
Revised Date:	2/8/2019
Renewal Date:	On or before 2024
Approved By:	Kathryn Tasker

Table of Contents

1 Purpose

The purpose is to define the minimum technical and procedure standards required for all research projects in particular for projects with sensitive data (SD) or those under strict data use agreements (DUA).

2 Scope

This policy applies to all faculty and staff of Hebrew SeniorLife Marcus Institute for Aging Research (Marcus Institute) working with sensitive data obtained from public and private providers.

3 Definitions

Term: Sensitive Data

Any data which contains Social Security Numbers or other personal identification numbers, confidential personal or financial information, protected health information, student educational records, proprietary customer data or information that is otherwise deemed to be protected by HSL corporate policy, state, federal, or international laws, statutes, or regulations or explicitly identified in a contract.

4 Policy Statement

Minimum technical and procedural standards must be met by all faculty and staff on projects with sensitive data or on projects where requirements are governed by a DUA.

1) All physical materials must be stored securely
2) All electronic content must be stored in a secure location or device
    a. Data encryption must be employed on mobile devices or when in transit (see Data Encryption Policy for encryption requirements)
3) All projects must establish and follow staff access roles
    a. All projects must establish and follow access restriction procedures
4) All projects should author a Manual of Operations (MOO) or Data Management Manual that includes specific security details, staff roles and data handling procedures.

5 Procedures

Principal investigators are responsible for ensuring project-level compliance with these policies and procedures. The Director of Research Informatics in coordination with the IT Department may facilitate or directly assist in providing resources to ensure compliance with procedures.

5.1 Physical Data Security

Investigators are required to store all sensitive physical data in a locked storage cabinet or equivalent secure asset when not in use. Secure storage must be limited to study staff only with appropriate IRB approval.

- Projects should limit the physical transfer of sensitive data. Appropriate precautions should be taken to secure research data when in transit.
- Projects are encouraged to store physical data in a preapproved storage facility (see Sensitive Data Retention Policy)
    - If physical data is not stored in a preapproved facility then the principal investigator is required to document the physical security measures in place to ensure facility security and protection of storage assets therein.

5.2 Electronic Data Security

All employees are required to comply with all related HSL policies regarding HIPAA and the proper use of information technology. See related policies below.

Investigators are required to store all sensitive electronic data on the secure HSL corporate network or on infrastructure preapproved by the Director of Research Informatics or HSL Chief Information Officer.

- A list of preapproved network resources include
    - Research enterprise file servers (e.g. IFAR-NAS)
    - Application servers (e.g. REDCap, SharePoint, Accellion)
    - Database servers (e.g. MySQL, SQL Server)
- Sensitive data may not be stored on off-site servers or infrastructure without preapproval from the Director of Research Informatics or IT.
    - If sensitive data are stored off-site then the principal investigator is required to document the technical security details of the service including
        - Description of the security architecture of application or database system
        - Location and management of file servers
        - Description of the physical security of the off-site data center
- Servers and network resources should be accessible to approved staff only
    - Each project should maintain a dedicated network share located on corporate-approved file servers to ensure secure isolation of data and materials

- Investigators must follow institutional procedures to request employee access to network resources

- Sensitive data may only be stored temporarily on HSL office equipment (e.g. workstation, network scanner) for analysis or processing if the equipment is physically located within a locked office at a HSL facility.
    - Sensitive data may not be stored on non-HSL office equipment unless preapproved by the Director of Research Informatics or Chief Information Officer.

5.2.1 Mobile Devices

Investigators are discouraged from storing sensitive data on mobile devices including laptops, smart phones or tablet computers. However, if a project requires the use of these devices then all devices must comply with HSL corporate policy and the institution's Sensitive Data Encryption Policy.

- Sensitive data may not be stored on personal (non-HSL) mobile devices

5.2.2 Data Transmission

Investigators are discouraged from routinely transmitting sensitive data over open networks (e.g. Internet, WAN, etc.). However, if a project requires transmitting sensitive data over an insecure network then the transmission must comply with the standards set in the Sensitive Data Encryption Policy.

5.2.3 Physical Security of Electronic Equipment

Investigators must provide physical security of electronic equipment storing sensitive data.

- Investigators and staff storing sensitive data on mobile devices, or devices in the field, must take appropriate precautions to physically secure these units. Investigators should document device handling procedures in the project MOO.
- All data center facilities (on-site or off-site) must comply or exceed the following requirements
    - Physical access to the facility is strictly prohibited to preapproved IT staff only
    - Facility is guarded by 24-7 security including card key (or equivalent) access, video surveillance and a dedicated security officer
    - Facility provides adequate temperature and fire suppression controls on server room
    - Access to server infrastructure by outside entities (e.g. vendors, site visitors, etc.) requires escort and administrative preapproval
    - Facility must monitor actively for data center network intrusions or security problems
    - Data center is protected from Internet intrusion with digital firewall measures
- HSL data centers comply with the above requirements.

5.3 Staff Training

All faculty and staff are required to take the online CITI Information Privacy and Security training modules to ensure proper training and understanding of all data security issues. Employees are required to be recertified every three years. The HSL IRB and the institute's Office Manager maintain records of training certifications.

5.4 Access Roles and Restrictions

Investigators are responsible for ensuring all project staff follows established HSL corporate policies regarding password security and granting access to project resources containing sensitive data.

5.4.1 Staff Roles

- All research projects are required to maintain IRB approval. IRB review includes assurances that individuals are qualified to access sensitive data.
- Investigators should maintain a list of staff, operational roles and access permissions
- All electronic systems (e.g. file share, REDCap project, etc.) should enforce these roles and access restrictions. Investigator should document where systems are not capable of enforcing these restrictions.

5.4.2 Access Restrictions

The following access restriction rules apply to all projects.

- All electronic storage containing sensitive data must be secured by at least a two-part security credential scheme (e.g. username and password).
    - Encrypted mobile devices must employ a password or security key maintained separately from physical access to the device. See Sensitive Data Encryption Policy for details.
- All staff accessing sensitive data must be given unique security credentials
    - Staff may never share security credentials
- Investigator is responsible for documenting and approving access changes
- Investigator is responsible for approving change requests to IT as the project roster or staff roles change
    - Changes to network resources (e.g. file share) must be completed by IT
    - Changes to application software (e.g. REDCap, SharePoint, Accellion) may be completed by project staff with appropriate privileges and training

5.5 Manual of Operations (MOO)

All investigators and managers are strongly encouraged to author a Manual of Operations, also often referred to as Standard Operating Procedures (SOP), for each project. The MOO provides basic documentation of the operations of the research project including data management activities. A full

description and rationale of a MOO is beyond the scope of this policy, but if employed should include the following information to ensure adequate documentation of data security.

- Study Overview
- Study Organization
    - Participating Centers (coordinating and study center(s), laboratories, etc.)
    - Administration and Governance
        - Committees, funding agencies, and data and safety monitoring board
    - Roles and Responsibilities
        - Matrix of responsibilities of investigators and study staff defined
        - Procedures for approving access or role changes
- Data Management Procedures
    - Overview of data flow
    - Data collection and handling (sending and receiving)
    - Data storage systems and resource locations (paper and electronic)
    - Standard technologies or applications (if pertinent)

6 Related Policies

The document author(s) have attempted to identify policies that may be applicable or related to this policy. This is not an exhaustive list. All HSL employees are expected to abide by all active policies of the organization at all times. As such, employees are encouraged to review any and all potentially applicable policies regardless of whether they are identified below. HSL reserves the right to modify, cancel, or enact new policies at anytime, without notice.

- HSL Policy: Computer Usage, Email and other Communication Services
- HSL Policy: HIPAA
- HSL Policy: Use of Information Technology Resources
- IFAR Policy: Sensitive Data Encryption Policy

7 Reference Materials

NA

8 Appendix

NA

9 Document Properties

Title:	Sensitive Data Security Policy
Author:	Jason Rightmyer
Version:	
File Name:	Sensitive Data Security Policy.docx