Marcus Institute
for Aging Research
Hebrew SeniorLife

HARVARD MEDICAL SCHOOL
AFFILIATE

Data Encryption Policy

Institutional Policy

Title:	Data Encryption Policy
Responsible Officer:	Director, Research Informatics
Original Effective Date:	3/6/2014
Revised Date:	2/8/2019
Renewal Date:	On or before 2024
Approved By:	Kathryn Tasker

Table of Contents

1 Purpose

The research enterprise processes and stores many types of sensitive and private information that if lost or stolen could result in significant financial and criminal liability. The purpose of this policy is to clarify the technologies and environments where encryption technology must be employed to minimize the risk of data loss or a security breach.

2 Scope

This policy applies to all employees and contracted employees of Hebrew SeniorLife Marcus Institute for Aging Research (Marcus Institute).

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

It is the policy of this research institution to protect assets, such as mobile computers, portable data storage devices and communication devices, and to protect sensitive data (SD) that may reside in such devices from unauthorized access by employing encryption technologies.

5 Procedures

5.1 Use of Information Technology

All faculty and staff must comply with HSL corporate policy regarding Use of Information Technology (IT) Resources including password requirements, general security precautions, encryption software and disclosure of security issues. A copy of the policy is available on the HSL intranet.

5.2 Data Storage Devices

All "personal" data storage devices that are owned by, or contains data related to a project, must be encrypted. Examples of data storage devices are, but not limited to:

- Laptops
- Desktop Computers
- USB Flash Drives
- External Hard Drives
- Smartphones
- Personal Digital Assistant (PDA's)

Server-based storage devices (singleton hard drives, storage area networks, etc.) and systems physically located in the HSL data center are not subject to the encryption policy unless otherwise required by technical or project-specific requirements.

5.3 Encryption Administration

1. HSL IT will ensure that all portable data storage devices, purchased through IT, are encrypted as needed.
2. Data storage devices purchased or acquired through non-corporate channels must be encrypted according to the standards listed in Section 5.6. The HSL preferred office supply vendor offers pre-encrypted products that meet HSL's encryption standards.
3. Only encrypted devices may be used to access the HSL network, unless prior authorization is obtained from the Director of Research Informatics and IT Help Desk.

5.4 Data Transmission

Sensitive data must be encrypted if transmitted in any way over the Internet or a wide area network (email, Web download, etc.). Data transmissions must be conducted using a Secure Socket Layer (SSL) or an equivalent encryption protocol pre-approved by IT. See encryption standards for details.

Data may be transmitted unencrypted on the HSL private network, between devices on the HSL campus or between devices not connected to a public network (e.g. laptop to flash drive offsite).

5.5 File Encryption

In circumstances where whole-device encryption is not possible then individual data files (directories, databases, etc.) must be encrypted for transit and storage if containing sensitive data. Secure file encryption must meet minimum standards including algorithms and encryption key protocols.

5.6 Encryption Standards

All encryption technology must meet a minimal standard. This standard is provided below. Devices that employ technology that exceed the standard are permitted to be used. Devices or transmissions that fail to meet the standard may not be employed to store or transmit sensitive data.

1. Encryption algorithms (128-bit or higher)
    a. AES (128, 192, or 256 bit)
    b. RC6 (256 bit)
    c. Blowfish (128 or 448 bit)
    d. Triple DES (112 or 168 bit)
    e. RC4-128
    f. IDEA-128
    g. CAST-128
    h. RC5 (128 bit only)
    i. SAFER (128 bit)
2. Public key asymmetric encryption (e.g. SSL)
    a. RSA (minimum 1024 bit)
    b. ECC (minimum 384 bit)
3. Symmetric Key Generation (shared key)
    a. FIPS 186-2
    b. ANSI X9.31
    c. ANSI X9.62
    d. ANSI X9.82

5.7 Encryption Key Management

- All private keys, passwords or passcodes must be stored separately and not shared publically or in line of sight.
- A pre-approved certificate authority should be employed (HSL, Harvard, etc.) whenever encrypting and transmitting data over a public network. See HSL IT department for more information.

5.8 Policy Enforcement

Failure to encrypt a data storage device or otherwise subvert the encryption policy is grounds for administrative reprimand.

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 any time, without notice.

- HSL Policy - Use of Information Technology Resources
- HSL Policy - HIPPA

7 Reference Materials

NA

8 Appendix

8.1 Current Approved Technologies

The following technologies are preapproved for use in data encryption, storage and transmission. Technologies not listed below may be used only with approval by HSL IT.

Category	Products
File Transmission	• Accellion Secure File System (https://securefile.hsl.harvard.edu) • HSL-approved Web applications using HTTPS (SSL)
Device Encryption	• McAfee Enterprise Encryption
File Encryption	• Winzip (encryption-enabled, password-protected)
Email Encryption	• HSL Secure Email (https://securemail.hsl.harvard.edu/) • HSL Webmail (only for correspondence with BIDMC/Partners)

9 Document Properties

Title:	Data Encryption Policy
Author:	Jason Rightmyer
Version:	V1.1
File Name:	Data Encryption Policy.docx