University of Massachusetts Lowell

Policy Title:	Institutional Review Board (IRB) Data Security Policy
Policy Number:	IT-5-113
Effective As Of:	October 1, 2016
Next Review Date:	October 1, 2017
Responsible Office:	Information Technology
Responsible Position:	Information Security Officer

I. POLICY STATEMENT

All Institutional Review Board ("IRB") protocols must have a data security plan that specifies whether Sensitive Data will be obtained or created and if so, how it will be stored and transferred. Any modification to the data security plan must be approved by the IRB. Protocol renewals must identify any changes in such data security plan and, at the time of renewal, the IRB will require that the plan be updated to meet new requirements. The data security plan must be acceptable to the IRB for a protocol or protocol renewal to be approved by the IRB.

II. PURPOSE

This Policy provides standards for IRB review and approval of data security plans involving the storage of electronic research data constituting sensitive data in human subjects research conducted at UMass Lowell, including UMass Lowell researchers and support staff.

Pursuant to regulations of the Department of Health and Human Services (DHHS), including the National Institutes of Health (NIH) and the Food and Drug Administration (FDA), the IRB is charged with ensuring that each human subjects protocol includes provisions for protecting the privacy of subjects and maintaining the confidentiality of study data. This is particularly important when the study involves data constituting Sensitive Data pursuant to the terms of the UMass Lowell Data Classification Policy (the "Data Classification Policy") and therefore subject to the most stringent data security requirements.

III. SCOPE

This policy applies to all IRB-related research and data security plans submitted for IRB review that may include Restrictive/Sensitive Data. This will ensure that the protection of the privacy of research subjects and the confidentiality of identifiable research data is in accord with the requirements of HHS, NIH and FDA regulations and the Health Insurance Portability and Accountability Act (HIPAA).

IV. DEFINITIONS

Sensitive/Restricted Data: any information protected by federal, state and local laws and regulations or industry standards, such as HIPAA, the Health Information Technology for Economic an Clinical Health Act (HITECH), the U.S. Family Educational Rights and Privacy Act (FERPA), M.G.L. c. 93H, and the Payment Card Industry Data Security Standard (PCI-DSS). For purposes of this Policy, Sensitive/Restrictive Data include, but are not limited to:

Personally Identifiable Information (PII): any information about an individual that (a) can be used to distinguish or trace an individual's identity, such as name, date and place of birth, mother's maiden name or biometric records (b) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization could result in harm to that individual and (c) is protected by federal, state or local laws and regulations or industry standards.

Protected Health Information (PHI): any information processed, transmitted or stored by a Covered Entity (as defined in HIPAA) 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. The University's Office of the General Counsel and Office of HIPAA Compliance are responsible for determining whether particular information maintained or disclosed by the University constitutes PHI.

V. PROCEDURES

A. Information Security Requirements

a. No data shall be removed from the UMass Lowell campus via any media, such as CD, DVD, USB storage cards, external hard drives, or any computing systems, such as laptops and mobile devices to further reduce risk of unauthorized access, uses, or disclosure of sensitive or confidential data.

b. It is the responsibility of the PI of any research study involving Restricted/Sensitive Data to comply with all applicable University policies and guidelines, including all Information Security Policies (as defined in the UMass Lowell Information Security Policy).

B. Data Storage

The following methods of storing electronic research data containing Restrictive/Sensitive Data will be acceptable to the IRB:

a. Server-based Systems: The data is stored on a System/server (as defined in the Information Security Policy) in compliance with the UMass Lowell Protection of Systems Standard. The specific server name and IP address and System Administrator is required at a minimum. Additionally, the server and associated storage must be located in a secure network segment, protected by the UMass

Lowell firewalls, and encrypted using industry standard encryption software. Access to the server and or storage from off campus can be accomplished by the campus VPN product, in accordance with the UMass Lowell VPN Policy.

b. The data is stored on an Endpoint (as defined in the Information Security Policy) in compliance with the UMass Lowell Registration and Protection of Endpoints Standard. The inclusion of a statement to such effect in a protocol will constitute a certification by the PI that each Endpoint to be used in the study will be so protected. Data located on each endpoint must be encrypted using industry standard encryption software.

c. Alternate methods for storing Restricted/Sensitive data not listed above must be reviewed and approved by the Office of Institutional Compliance and Information Security.

C. Data Transmission

a. An acceptable data security plan must provide that all electronic transmissions of Sensitive Data over the internet (including by email), file transfers or other data transfer modalities, are made in compliance with the Systems Standard or the Endpoints Standard and the UMass Lowell Email Policy. At a minimum, the data transmission must be made using secure protocols (https, SSL) between the sender and the recipient.

D. Data Loss/Security Breach

a. Any loss of or breach of security relating to research data containing Sensitive Data must be reported, (1) to the IRB as an Unanticipated Problem Involving Risks to Subjects or Others and (2) in compliance with the UMass Lowell Data Security Breach and Response Policy.

b. Examples of security breaches include: (1) lost or stolen desktops, laptops, USB drives, CD/DVD drives, etc. with stored data; (2) a compromised account that is used to look up data (e.g., unauthorized user has had access to the account); (3) a compromised work station or server that contains data; and (4) accidental disclosure or data to unauthorized recipients (e.g., sending data to an incorrect email address).

VI. RESPONSIBILTY

The Director of Institutional Compliance, in partnership with Information Technology is the responsible organization for implementing the provisions of this policy. The University's Chief Information Officer and the Information Security Officer are the designated point of contacts.

VII. ATTACHMENTS

None

VIII. RELATED POLICES, PRODEDURES AND ANNOUNCEMENTS

Acceptable Use Policy, IT-5-101
Data Classification Policy, IT-5-106 (reserved)
Email Usage Policy, IT-5-108 (reserved)
Information Security Policy, IT-5-111 (reserved)
Security Breach and Response Policy, IT-5-118 (reserved)

IX. APPROVAL AND EFFECTIVE DATE

On file with the Policy Office.