University of Massachusetts
UMASS Medical School

Written Information Security Program (WISP)

Effective Date: 02/26/19
Last Reviewed Date: 01/19/2021

The following are responsible for the accuracy of the information contained in this document

Responsible Policy Administrator

Associate CIO, Information Security

Responsible Department

Information Technology

Program Statement

Pursuant to MGL 93H, all Massachusetts entities must have a Written Information Security Program (WISP). The Massachusetts data security regulations (201 C.M.R. 17.00) require every entity that owns or licenses "personal information" about Massachusetts residents to develop, implement, and maintain a WISP. The WISP must contain minimum administrative, technical, and physical safeguards to protect such "personal information".

Purpose

The purpose of the WISP is to:

(a) Ensure the security and confidentiality of Personal Information;

(b) Protect against any anticipated threats or hazards to the security or integrity of such information;

(c) Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

Definitions

Breach - the acquisition, access, use or disclosure of Personal Information in a manner not permitted under Subpart E of 45 CFR Part 164, M.G.L. c. 93H, or other applicable states' security breach statutes.

Data - information generated by or for, owned by, or otherwise in the possession of UMMS that is related to the school's activities.

Data Classification - UMMS Departments must classify their data into at least one of the four levels of classification. Each category denotes a unique level of sensitivity and has specific access and handling requirements.

Data Owner -The Data Owner has policy-level responsibility for establishing rules and use of data based on applied classification. UMMS Senior Level Management is ultimately the Data Owner and is responsible for assigning the classification, ensuring the protection and establishing appropriate use of the school's data. Individuals within UMMS may be delegated some portion of this responsibility on behalf of the Senior Leadership.

Personal Information - personal information (as defined in Mass. Gen. Laws c. 93H or other states' breach notification laws).

User – shall mean all faculty, staff, students, employees, contractors, vendors and any other individuals with access to UMMS data or systems.

University of Massachusetts
UMASS Medical School

Written Information Security Program (WISP)

Effective Date: 02/26/19
Last Reviewed Date: 01/19/2021

Scope

The data covered by this WISP includes any information stored, accessed or collected at UMMS or for UMMS operations, whether in paper, electronic or other form.

This WISP applies to all Users.

This WISP applies to UMMS computing, network and information systems and services.

Related Policies, Regulations and laws

Information Security Policy 07.01.11
Data Classification Policy 07.01.03
Acceptable Use Policy 07.01.01
Reporting Potential Breach and Security Incidents of Personally Identifiable Information 01.02.05
Information Security Incident Response Team Policy 07.01.04
The Massachusetts Data Privacy Laws and Regulations at M.G.L. c. 93H, c. 93I and 201 CMR 17.00
Financial Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act (the GLBA)) Safeguards rule and associated regulations
Family Education Rights and Privacy Act (FERPA) and associated regulations
Health Insurance Portability and Accountability Act (HIPAA) and associated regulations
European Union (EU) General Data Protection Regulation (GDPR)

Responsibilities

It is the responsibility of the Information Security Officer to ensure that:

- The Program is followed as described;
- The Program is annually reviewed and updated;
- The relevant documentation is maintained.

It is the responsibilities of all Users to ensure that:

- UMMS policies and standards are read and understood;
- In-scope WISP data is maintained in a secure manner according to UMMS policies and standards.

Components of WISP

1. Identification and Assessment of Risks to Medical School Information

UMMS has established the Information Security Risk Management Standard to outline the measures required to identify, assess and treat risks to the confidentiality, integrity, and availability of UMMS data and systems as well as identifying threats to UMMS assets. This Program includes the process to determine appropriate management actions and establish priorities for managing and implementing effective controls.

2. Safeguarding Data

Proper management of data requires departments to perform periodic reviews of data and assess their classifications and controls. The controls for classified data must be commensurate with the level of identified risk, regulatory requirements and contractual agreements.

Data Classification:

UMMS employs a comprehensive data classification schema that leverages four levels of classification. Each category denotes a unique level of sensitivity and has specific access and handling requirements.

Once data is assigned the appropriate classification level, departments must conduct a Risk Assessment to determine acceptable levels of risk and the appropriate level of security controls for information systems.

Examples of data include, but are not limited to:

- *Massachusetts Personal Information*
- *Sensitive Personal Information (SPI)*
- *Protected Health Information (PHI) under HIPAA*
- *Financial Customer Nonpublic Personal Information under the GLBA (Financial Customer GLBA Data)*
- *European Personal Data under the GDPR*
- *Personally Identifiable Information in Student Educational Records under FERPA*

Encryption:

UMMS requires all Users to apply UMMS approved encryption solutions to all sensitive UMMS data to preserve the confidentiality and integrity of, and control accessibility to, where this data is processed, stored or transmitted.

Access & Storage:

Access to UMMS systems and data is through authorized access controls, such as a unique account and credentials, to preserve the confidentiality and integrity of, and control accessibility to, UMMS data. All access to UMMS data is reviewed regularly to ensure access is appropriate.

Data Destruction:

Records containing Personal Information are destroyed once they are no longer needed for business purposes, unless state or federal regulations require maintaining these records for a prescribed period of time. Paper and electronic records containing Personal Information are destroyed in a manner that prevents recovery of the data.

3. Computer System Safeguards

UMMS applies industry best practices to maintaining the confidentiality, availability, and integrity of information systems by maintaining up-to-date firewall protection, operating system security patches, and malware protection. The most current security updates are applied regularly. UMMS performs regular Intrusion Detection monitoring and logging to prevent unauthorized access.

4. Password Requirements

Access to UMMS systems and data requires Users to authenticate with a unique User ID and password. Passwords must adhere to UMMS policy in their construction and change frequency. The sharing of an individual’s account and password is prohibited.

5. Third-Party Vendor Agreements Concerning Protection of Personal Information

Data Owners are responsible for confirming third-party service providers are maintaining appropriate security measures and data handling processes to protect UMMS data consistent with this Program.

All third parties with access to Data containing information of Massachusetts residents are required to attest to the appropriate level of protection and compliance to this WISP annually.

In all circumstances where UMMS provides data or access to data, third-parties must attest to compliance with this WISP.

6. Employee Training

Training serves to educate UMMS workforce in maintaining compliance within their particular UMMS business function or activity, whether it be under research grants or industry contracts’ privacy and security requirements, MGL Ch. 93H – Identity Fraud Statute, the Health Insurance Portability and Accountability Act (HIPAA), or other related federal and state laws and regulations regarding data privacy and information security.

The University of Massachusetts Medical School (UMMS) requires that employees are trained in the proper handling of sensitive data. All UMMS faculty, staff, contingent workers, contractors and students in its schools, departments, centers and business units are required to complete privacy and information security training.

7. Incident Reporting

Incidents that raise concerns about the privacy or security of Personal Information must be reported promptly upon discovery to the Information Security Officer. The Incident Response Team (IRT) shall investigate all reported security incidents and Breaches. Led by the UMMS’s Information Security Office, the IRT’s objective is to:

1. Coordinate and oversee the response to incidents in accordance with the requirements of state and federal laws and UMMS policy;
2. Minimize the potential negative impact to the UMMS, client and 3rd party as a result of such incidents;
3. Where appropriate, inform the affected client and 3rd party of action that is recommended or required on their behalf;
4. Restore services to a normalized and secure state of operation;
5. Provide clear and timely communication to all interested parties.

Enforcement

Any UMMS User violating any portion of UMMS' Information Security programs or policies may be denied access to UMMS systems or data. Additionally, the User may be subject to disciplinary action, up to and including dismissal from a school or termination of employment.

University of Massachusetts
UMASS Medical School

Written Information Security Program (WISP)

Effective Date: 02/26/19
Last Reviewed Date: 01/19/2021

Approvals

DocuSigned by:
Brian Coleman
232D95E3184B416...

1/20/2021

ACIO, Information Security

Date

Revision log

Revision Date	Revision Description	Revised by
02/26/2019	Initial Release	Brian Coleman

Related Rules and Compliance

In addition to Massachusetts regulations 201 CMR §17 (.pdf), handlers of data should also be aware of these other laws and regulations regarding personal information:

Massachusetts Data Breach Notification Law: Chapter 93H
This MA law requires that businesses and government agencies notify residents of data breaches in certain situations. Notification to the Attorney General, the Director of Consumer Affairs and Business Regulation and the affected resident is required if it "knows or has reason to know of a breach of security" or "knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose." These breaches include hard copy as well as electronic data.

The law defines "personal information" as a resident's first name and last name, or first initial and last name in combination with any one or more of the following:

1) Social Security number, 2) driver's license number or state-issued identification card number or 3) financial account number or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account.

Family Educational Rights and Privacy Act (FERPA)
Although student education records which include an individual's Social Security number, financial account number or other personal information are covered by this Information Security Program, all student records, regardless of whether they contain personal information, are also subject to the requirements of FERPA. The Family Educational Rights and Privacy Act (FERPA) is a federal law that protect the confidentiality of many student records. The law applies to all departments that receive funds under an applicable program of the U.S. Department of Education.

Health Insurance Portability and Accountability Act (HIPAA)
The federal Health Insurance Portability and Accountability Act (HIPAA) requires UMMS to maintain the confidentiality of electronic health information that can be linked to an individual patient (electronic Protected Health Information, or ePHI).

Gramm Leach Bliley Act (GLBA)
The GLBA requires “financial institutions” to adopt certain privacy safeguards. Insofar as “covered transactions” under GLBA include an individual's financial account number, this Information Security Program would also cover them.

FACTA "Red Flag Rules”

Section 114 of the Fair and Accurate Credit Transactions Act (FACTA), also known as the Red Flag Rules, requires that all organizations subject to the legislation must develop and implement a written "Identity Theft Prevention Program" to detect, prevent and mitigate identity theft in connection with the opening of certain new and existing accounts. In accordance with federal regulations, UMMS has adopted an Identity Theft Prevention Program. The safeguards referenced in the Identity Theft Prevention Program are the same as the minimum-security standards referenced in this Program.