University of Massachusetts
UMASS Medical School

Written Information Security Program (WISP)

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

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

The Written Information Security Program (WISP) is a set of comprehensive guidelines and policies designed to safeguard personal information maintained at the University of Massachusetts Medical School (UMMS) and to comply with applicable state and federal laws and regulations on the protection of personal information.

The WISP has been adopted in accordance with Chapter 93H of the Massachusetts General Laws and corresponding regulations setting forth Standards for the Protection of Personal Information of Residents of the Commonwealth (201 CMR §17) and other applicable laws, regulations, and contractual obligations.

Purpose

In accordance with federal and state laws and regulations, UMMS has developed and implemented comprehensive security policies that draw from HIPAA and HITECH standards and provide the framework by which employees are directed to securely manage data. Data is classified to allow for appropriate protection in its creation, storage, dissemination and destruction. The UMMS security program is standards based and draws from measurements and guidelines set by the HIPAA and NIST security standards for the storage and management of Protected Health Information (PHI).

UMMS is required to secure the confidentiality, availability, and integrity of our information technology infrastructure, to take measures to safeguard personal information and to provide notice about security breaches of protected information at the School to affected individuals and appropriate state agencies.

This document explains the elements of the Program, including the requirements for evaluating its electronic and physical methods of accessing, collecting, storing, using, transmitting and protecting personal information. The Program covers all forms of personal information, whether it is maintained on paper, digital, or other media.

The purposes of this document are to:

- Describe a comprehensive information security program designed to safeguard personal information under the stewardship of UMMS, in compliance with federal and state laws and regulations;
- Designate an individual to maintain and be responsible for the Program;
- Identify employee responsibilities in safeguarding data in accordance to its classification level;
- Describe how data security risks are identified;
- Define procedural, administrative, technical and physical safeguards for protecting Personal Information;
- Describe a third-party risk management process that ensures compliance with all applicable laws, regulations, and contractual obligations; and
- Identify processes to investigate potential security breaches or unauthorized use of Personal Information and report to appropriate agencies and individuals.

University of Massachusetts
UMASS Medical School

Written Information Security Program (WISP)

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

Scope

This WISP applies to all users including faculty, staff, students, employees, and any other individuals with access to UMMS data or systems.

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 UMMS computing, network and information systems and services.

Related Policy

- Information Security Policy
- Data Classification Policy
- Acceptable Use Policy
- Reporting Potential Breach and Security Incidents of Personally Identifiable Information
- Information Security Incident Response Team Policy

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; and
- The relevant documentation is maintained.

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 Standard includes the process to determine appropriate management actions and establish priorities for managing and implementing effective controls.

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.

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.

Computer System Safeguards

UMMS applies industry best practices to maintaining the confidentiality, availability, and integrity of information systems. UMMS maintains 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.

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.

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 in-scope Mass Reg data are required to attest to the appropriate level of protection and compliance to this WISP annually.

University of Massachusetts Medical School
UMASS

Written Information Security Program (WISP)

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

Employee Training

UMMS privacy and information security program 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) require 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.

Reporting Actual Breaches of Security

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 University, 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: 02/26/19

Approvals

Brian J Cohen

ACIO, Information Security

2/26/2019

Date

Revision log

Revision Date	Revision Description	Revised by
	Initial Release	

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.

Payment Credit Industry Data Security Standards (PCI DSS)
Personal credit card information is personal information and is covered by this Information Security Program. If a merchant agrees to accept credit cards as a form of payment, Payment Card Industry (PCI) Compliance is a requirement and is intended to help merchants protect their customers from fraudulent transactions.

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.

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), or "protected health information" (as defined in 45 CFR §160.103), or "personal data" (as defined in Mass. Gen. Laws c. 66A), "patient identifying information" as defined in 42 CFR Part 2 and any other individually identifiable information defined as confidential under state or federal law. All of the foregoing are considered "Personal Information" if not fully de-identified in accordance with 45 CFR §164.514.

Security Information - shall mean all materials pertaining to the manner in which an organization protects its information technology system and data; the disclosure of which could expose the system to external threats. Security Information includes, but is not limited to, diagrams, system schematic drawings, user account information, passwords, threat or vulnerability assessments and other measures to detect, document and counter threats.