



Data Classification

POLICY 07.01.03

Effective Date: 01/01/2015

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

Responsible Policy Administrator

Information Security Officer

Responsible Department

Information Technology

Contact 508-856-8643

Policy Statement

University of Massachusetts Medical School Data is information generated by or for, owned by, or otherwise in the possession of University of Massachusetts Medical School that is related to the School's activities. For purposes of these standards, data is information maintained in an electronic, digital or optical format. Data includes numbers, text, images and sounds, which are created, generated, sent, communicated, received by and/or stored on UMMS owned or contracted Information Technology Resources (ITR's). Data does not include hardware, platforms, software, applications or middleware.

This guideline defines four categories into which all University Data can be divided:

- Public
- Internal
- Confidential
- Highly Restricted Use

School Data that is classified as Public may be disclosed to any person regardless of their affiliation with the School. All other School Data is considered Sensitive Information and must be protected appropriately. This document provides definitions for and examples of each of the four categories. The Data Protection Requirements specifies the level of security protections that are required for each category of data. Some information could be classified differently at different times. For example, information that was once considered to be Confidential data may become Public data once it has been appropriately disclosed. Everyone with access to School Data should exercise good judgment in handling sensitive information and seek guidance from management as needed.

Reason for Policy

The purpose of this document is to identify the minimum standards that agencies must adopt for the appropriate classification of data and the ongoing management of that classification.

Entities Affected By This Policy

This policy affects all department heads, chairs, faculty, and staff responsible for ownership or oversight of UMMS data.

Related Documents

Additional Information

The following references were used in development of these standards:

ISO: International Standards Organization

FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems

NIST 800-60: Guide for Mapping Types of Information & Information Systems to Security Categories

IRS Pub 1075: Tax Information Security Guidelines for Federal, State and Local Agencies and Entities

Fair Information Practices Act: Mass. Gen. L. ch. 66A

Executive Order 504: Executive Order regarding security and confidentiality of personal information.

Public Records Division: Public records resources as provided by the Secretary of the Commonwealth

Massachusetts Identity Theft Law: Law relative to Security Freezes and Notification of Data Breaches

Family Educational Rights and Privacy Act (FERPA): The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records.

Information Security Risk Assessment Guidelines: Risk assessment methodology based on the Centers for Medicare and Medicaid Services (CMS) Information Security RA Methodology.

Mass. Gen. L. 93H: Commonwealth of Massachusetts Law that protects residents' personal information

FIPA: The Fair Information Practices Act

201CMR17: Standards for the protection of personal information of residents of the Commonwealth.

HIPAA: Health Insurance Portability and Accountability Act for protection and confidentiality handling of health information. HIPAA, HITECH, PHI and PII definitions are included on our website:
www.umassmed.edu/it/security/compliance

PCI: The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that ALL companies that process, store or transmit credit card information maintain a secure environment.

Scope

University of Massachusetts Medical School must adhere to the standards detailed in this document, except where such adherence would conflict with the Public Records Law or other laws, regulations or policies. Additional references that agencies may find useful as they classify their data are listed at the end of this document.

Responsibilities

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 interdepartmental agreements that may pertain to department acquisition, use or maintenance of data.

The roles defined below are representative of the types of functions involved in the process of data classification:

- **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. The Data Owner is also responsible for assigning individuals to the following roles.
- **Data Manager:** The Data Manager develops general procedures and guidelines for the management, security and access to data, as appropriate.
- **Data Steward:** The Data Steward has custodial responsibilities for managing the data for the day-to-day, operational-level functions on behalf of the Data Owner as established by the Data Manager.
- **Data User:** A Data User is any individual who is eligible and authorized to access and use the data.

Procedures

1. Classification Scheme

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

1.1 Public Information - Low Sensitivity

Definition: Data classified as having low sensitivity should be thought of as being for general use and is approved by UMMS as available for routine public disclosure and use. Public information refers to information the University does not have a legal, policy or contractual obligation to protect. Security at this level is the minimum required by UMMS to protect the integrity and availability of this data.

Examples: This may include, but is not limited to, data routinely distributed to the public regardless of whether UMMS has received a public records request, such as: annual reports, publicly accessible web pages, policies, marketing materials and press statements.

1.2 Internal Use – Moderate Sensitivity

Definition: Data classified as having moderate sensitivity should be treated as internal, the release of which must be approved prior to dissemination outside UMMS. Its compromise may inconvenience the department, but is unlikely to result in a breach of confidentiality, loss of value or serious damage to integrity. This information is critical to the University's academic, research and business operations that require a higher degree of handling than public data. The department will define the level of protection required for this classification.

Examples: Data in this category is not routinely distributed outside UMMS. It may include, but is not limited to non-confidential data contained within: internal communications, minutes of meetings, system configuration/log files, campus infrastructure plans, and internal project reports.

1.3 Confidential - High Sensitivity

Definition: Data classified as having high sensitivity is considered confidential. Such data should not be copied or removed from UMMS operational control without authorized permission. High sensitivity data is subject to restricted distribution and must be protected at all times. Compromise of high sensitivity data could damage the mission, safety or integrity of UMMS, its staff or its constituents. It is mandatory to protect data at this level to the highest possible degree as is prudent or as required by law.

Examples: High Sensitivity data may include, but is not limited to, an individual's name in combination with Social Security Number, Credit Card numbers, Bank Account Numbers, HIPAA Protected Health Information, Research data that requires compliance with Export Administration Regulations (EAR), FERPA Educational Records, MA201, FACTA and Gramm-Leach-Bliley Act (GLB) students' or parents' financial records including names, addresses, phone numbers, bank and credit card numbers, credit histories, or Social Security Numbers as they relate to student financial aid information. In addition, personally identifiable, legally mandated, or sensitive data associated with: investigations, bids prior to award, personnel files, trade secrets, appraisals of real property, test questions and answers, constituent records, academic records, contracts during negotiation and risk or vulnerability assessments.

1.4 Highly Restricted Use - Extreme Sensitivity

Definition: Data classified as having extreme sensitivity is considered highly restricted use. Such data should not be copied or removed from UMMS operational control. Extreme sensitivity data is subject to the most restricted distribution and must be protected at all times based on regulatory compliance. Compromise of extreme sensitivity data could result in legal sanctions or required reporting to vendors.

Examples: High Sensitivity data may include, but is not limited to, social security numbers in association with protected health information, certain individually identifiable medical records and genetic information, specific contractual or customer obligations and research information classified as highly restricted use.

2. Required Considerations for Classification

The considerations listed below must be evaluated by UMMS departments when assigning classifications to their data.

2.1. Laws & Regulations

UMMS Departments are required to ensure that all laws, regulations, policies and standards to which their data is subject are met. Questions regarding laws, regulations, policies and standards that apply to specific agencies and departments should be directed to UMMS or department counsel.

2.2. Potential harm to the individuals to whom the data pertains

It is imperative to take into consideration any potential harm or adverse impact that the compromise of data may have on the parties to whom the data pertains. This consideration pertains to, but is not limited to patient data, personally identifiable information and medical information.

2.3. Risk of loss of confidentiality

Confidentiality has been defined as "ensuring that information is accessible only to those authorized to have access" and is one of the cornerstones of information security. Therefore, in appropriately assigning data with a classification level, departments must evaluate what the risk is for unauthorized access to classified data and what likely impact that loss would have.

2.4. UMMS Mission and Business Objectives

UMMS with unique missions and business objectives should take those needs into consideration when evaluating their data classifications. In some cases, UMMS may be obligated to share as much of their data as possible with the public or other outside agencies while others may be under the strictest constraints in ensuring that their data is protected against any exposure whatsoever. In either case, while it is incumbent on the department to ensure that those objectives are met, adequate controls need to be in place and in effect to address data integrity, security and availability.

2.5. Data Sharing Agreements and Contractual Requirements

Interagency Service Agreements (ISAs), Memoranda of Understanding (MOU's), grants, contracts and other written agreements between agencies and external entities may include agreements regarding data sharing and the use, disclosure and maintenance of data, as determined by the data classification of the Data Owner. The recipient UMMS or department's data classification must align with any such requirements.

Further, if an agreement states that the recipient department may further share the data, the subsequent recipients must adhere to the requirements of the original classification, unless the data has been de-identified or otherwise modified such that a different classification is required.

2.6. Intellectual Property

Departments must take into consideration any intellectual property rights owned by an entity other than the department while implementing and evaluating their data classification assignments.

3. Risk Assessment

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. **Risk Assessments must at a minimum include:**

- 3.1. Appropriate documentation including what is being identified, system purpose and description and system security level based on data classification levels.
- 3.2. System risk determination including identification of threats and vulnerabilities, description of risks, identification of existing controls, determination of likelihood of occurrence, determination of severity of impact and determination of risk levels.
- 3.3. Safeguard determination including recommended controls and safeguards, determination of residual likelihood of occurrence, determination of residual severity of impact and determination of residual risk level.
- 3.4. Data Owner acceptance and sign-off.

4. Security Controls

The Risk Assessment will recommend safeguards or security controls and describe the expected level of risk that would remain if these controls were put in place. Following are minimum security controls that must be considered based on the four data classification levels. Departments may assign more stringent requirements based on the results of their risk assessment. Departments that receive data from other agencies must adhere to any security controls agreed to by the originating department and the receiving department.

- 4.1.1. **Security Controls for Extreme Sensitivity Data:** Highly Restricted Use data must be protected using the strictest level of controls for the following categories: access control, audit and accountability, awareness and training, contingency planning, incident response, media protection, network, personnel security, physical and environmental protection, risk assessment, system and communications protection and vendor controls.
- 4.1.2. **Security Controls for High Sensitivity Data:** Confidential data must be protected using rigorous level of controls for the following categories: access control, audit and accountability, awareness and training, contingency planning, incident response, media protection, network, personnel security, physical and environmental protection, risk assessment, system and communications protection and vendor controls.
- 4.1.3. **Security Controls for Medium Sensitivity Data:** Internal use data must be protected using the moderate level of controls for the following categories: access control, audit and accountability, awareness and training, contingency planning, incident response, media protection, network, personnel security, physical and environmental protection, risk assessment, system and communications protection and vendor controls.
- 4.1.4. **Security Controls for Low Sensitivity Data:** Public data may be protected using low level of controls for the following categories: access control, audit and accountability, awareness and training, contingency planning, incident response, media protection, network, personnel security, physical and environmental protection, risk assessment, system and communications protection and vendor controls.

Departments must include the following in their ongoing monitoring, evaluation and data management:

- 4.2. Assigned data classification levels should be reviewed and evaluated on a periodic basis to insure that the classification remains valid. Best practices indicate that classifications should be reviewed annually. However, it is ultimately the responsibility of the Data Owner to identify the appropriate review cycles.
- 4.3. Documentation of ongoing efforts must be maintained indicating the scope, date and results to show compliance with this standard.
- 4.4. Departments are obligated to observe classification and security controls assigned to data obtained under written agreement from other departments or external sources throughout the data's lifecycle.
- 4.5. Except as required under the Public Records Law, data must only be accessed on a need to know, need to perform or need to protect basis.
- 4.6. Data must only be accessed by systems or persons with the appropriate security level. Access must be revisited whenever persons change roles within the department.
- 4.7. Access to Extreme Sensitivity data must be audited and logged.
- 4.8. Data must keep its classification level across different media.
- 4.9. Data must keep its classification level across changes in business process (i.e. if it's sensitive on paper, it's still sensitive when the business process goes online).
- 4.10. Departments must consider chain of custody issues with classified data and the personnel responsible for the handling, accessing, maintaining or creating data.

Definitions

HIPAA - The Office for Civil Rights enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; the HIPAA Breach Notification Rule, which requires covered entities and business associates to provide notification following a breach of unsecured protected health information; and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety.

FERPA - The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

Export Administration Regulations (EAR) - The Export Administration Act of 1979 authorized the President to regulate exports of civilian goods and technologies (equipment, materials, software, and technology, including data and know-how) that have military applications (dual-use items).

FACTA - The Fair and Accurate Credit Transactions Act of 2003 is a United States federal law as an amendment to the Fair Credit Reporting Act. The act contains provisions to help reduce identity theft, such as the ability for individuals to place alerts on their credit histories if identity theft is suspected, or if deploying overseas in the military, thereby making fraudulent applications for credit more difficult. Further, it requires secure disposal of consumer information.



Data Classification

Effective Date: 1/1/2015

Gramm-Leach-Bliley Act (GLB) - also known as the Financial Services Modernization Act of 1999, GLB compliance is mandatory; whether a financial institution discloses nonpublic information or not, there must be a policy in place to protect the information from foreseeable threats in security and data integrity.

Forms/Instructions

In support of this policy, specific procedures and guidelines are provided. These items can be found on the Information Security website.

Appendices

None

Approvals


Responsible Policy Administrator

1/22/15
Date


Vice Chancellor for Administration & Finance

1.21.15
Date