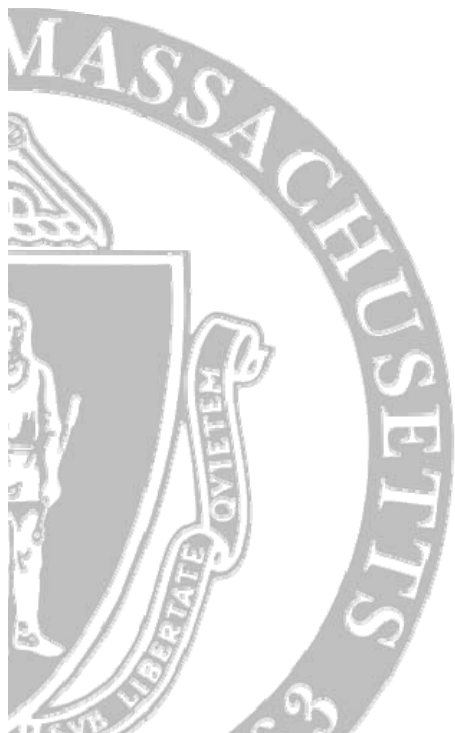


Handling Sensitive Data

New Massachusetts Legislation,
Compliance, and Handling

18 January 2008



Outline

- Introduction
- Law and Policy
 - Federal Law
 - State Law
 - University Policies
 - Data Classification
- Campus procedures
 - Department and OIT responsibilities
 - Data Inventory and Handling
 - Incident Response
- Questions

Introduction

- The State of Massachusetts has recently adopted a new data security law
 - Effective October 2007
 - Imposes a requirement to Notify in the case of a Security Breach of Personal Information.
- This resulted in the memo from John Dubach that was sent late December 2007
- The University needs to comply with these changes
 - Responsibilities of departments
 - Responsibilities of OIT

Sensitive Data Memo: December 2007

- To comply with the new state law and allow the University to take appropriate action in case of a security breach, the Office of Information Technologies (OIT) requests that each department takes four steps:
 - 1. Know what constitutes sensitive data**
 - 2. Keep what's necessary, purge what's not.**
 - 3. Identify the workstations/servers that contain sensitive data in your department.**
 - 4. Designate a 'data security' contact in your department.**

We will go through each, but lets take a step back

Scope and Context

- It is important to note the many different scopes and context for sensitive data:
 - Federal Legislation
 - FERPA, HIPAA
 - State Legislation
 - Mandatory notification of security breach (Ch. 93H)
 - University Policies
 - Data Classification and Handling
 - Industry Regulations
 - PCI-DSS

Sensitive Data: Federal Law

- Each statute imposes specific requirements
 - This is not intended as a comprehensive review of federal legislation
- FERPA (Education records)
 - students' academic, personal, and financial information as described in the most recent Academic Regulations Handbook
 - *There is much expertise here on this topic*
- HIPAA (Health information)
 - individually identifiable information related to a person's physical or mental health. This applies to any past, present, or future condition, treatment, or payment of health care service Protected Health Information (PHI)

Sensitive Data: State Law

- “An Act Relative to Security Freezes and Notification of Data Breaches”
 - Creates several new chapters of MGL.
- The law:
 - Defines Personal Information
 - Defines Breach of Security
 - Requires immediate Notification to those individuals whose Personal Information has been compromised as a result of a security breach.

Chapter 93H: Personal Information

- MGL Ch. 93H defines Personal Information as:
 - *an individual's name in combination with any of the following:*
 - *Social Security Number*
 - *Driver's License Number*
 - *State Identification Card Number*
 - *Financial account number, credit or debit card number*

Chapter 93H: Breach of Security

- MGL Ch. 93H defines a Breach of Security as:
 - *unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality or identity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth.*

Chapter 93H: Notice Obligation

- *From State ITD presentation by Linda Hamel*
- Notice obligation triggered when agency knows or should have known
 - Of breach of security -or-
 - that the sensitive data was acquired or used by an unauthorized person or for an unauthorized purpose
- Notice must be provided “as soon as practicable and without unreasonable delay”
- Notice requirements differ by agency’s handling of data
 - *Note: The details of notification are beyond scope here*

University Policy and Procedures

- In addition to Chapter 93H, the University has a set of policies that define data classifications, retention, disposition and management standards
- University Data and Computing Policies are at:
<http://www.massachusetts.edu/policy/datacomputingpolicies.html>
 - Data and Computing Standards
 - Records Management, Retention and Disposition Standards
 - Data/System Administrator Responsibilities and System Requirements

There are also some newer 'summary' documents available.

University Policy: Data Classification

- University data classifications must be adhered to. The data classifications determine how the data will be secured, managed, retained, and disposed of.
- Dissemination of University data to external sources is dictated by relevant regulations
- There are (3) defined classes of data:
 - Unclassified
 - Operational Use Only
 - Confidential

University Policy: Data Classification

- **Unclassified**
 - data that does not fall into any of the other data classifications noted below. This data may be made generally available without specific data custodian approval.
- **Operational Use Only**
 - data whose loss, corruption or unauthorized disclosure would not necessarily result in any business, financial or legal loss BUT which the University had determined is critical to its business and requires a higher degree of handling than unclassified data. Access to Operational Use Only data is available to data custodian approved users only.
- **Confidential**
 - data whose loss, corruption or unauthorized disclosure would be a violation of federal or state laws/regulations or University contracts (i.e., protected data); personally identifiable data; data that involves issues of personal privacy; or data whose loss, corruption or unauthorized disclosure may impair the academic, research or business functions of the University, or result in any business, financial, or legal loss.

Retention Management and Disposition of Data

- University data will be secured, managed, handled and disposed of based on the data classification.
- University of Massachusetts departments should not use, store, or display Social Security Numbers (i.e., SSNs) unless required by law.
- Collect, distribute, and retain only the minimal amount of personal and protected data that is related to their business needs.
- Collect and retain only that personal and protected data which is essential to the performance of assigned tasks.
- Delete personal and protected information when there is no longer a business need for its retention.

Sensitive Data: Compliance

- Going back to the original memo:
 - 1. Know what constitutes sensitive data**
 - 2. Keep what's necessary, purge what's not.**
 - 3. Identify the workstations/servers that contain sensitive data in your department.**
 - 4. Designate a 'data security' contact in your department.**

So what does it all mean?

- Sensitive data includes both Personal Information (*per Ch. 93H*) and Confidential Data (*per University policies*)
- As a campus, we need to be aware of where we have sensitive data in the case of security breaches
 - And security breaches will occur, despite our best efforts.
- We need to implement and improve security controls for sensitive data
 - Though we are doing a good job, there is much to be done

So what does it all mean?

- Having an accurate inventory of classified data will prepare us as a campus for responding to security incidents
- Having an accurate inventory of workstations and servers that hold this data will allow us to determine how to respond to a security breach
- Having a data security contact will permit us to communicate effectively during an incident
- Reporting incidents as they occur will also allow us to ensure we are in compliance

Responsibilities: Departments

- Ongoing processes
 - ***Designate a data security contact***
 - Know where sensitive data is located
 - Regularly updating contact and data inventory (at least annually)
 - Implement appropriate retention and disposal processes
- Notify OIT of security breaches
 - abuse@umass.edu
 - data-security@oit.umass.edu

Responsibilities: OIT

- Respond to security breaches
 - Triage to determine the scope of the incident
 - Possibly including forensic analysis
 - Working with legal counsel
- Issue Notifications to impacted parties
 - If necessary
- Provide support to departments to assist in compliance
 - We may need some guidance on how best to do this
- Awareness and Education

What remains unclear...

- Is the combination of First and Last Name along with SPIRE id constitute Personal Information (PI) under the statute?
 - We are not sure at this point if this qualifies under the statute
- Does the above combination constitute confidential data under University Policy?
 - Student number and employee number are classified as as confidential data (Personally Identifiable Information)
 - The University may choose to notify of a data breach even if there is no statutory requirement to do so.

Questions

- We would be happy to take any questions now or help to clarify any of this material.
- Please make sure that you have a designated data security contact for your department
- *Please complete the data security checklist*
- You can always feel free to contact us at:
 - data-security@oit.umass.edu

Relevant Links

- Data Security Compliance at UMass Amherst
 - <http://www.oit.umass.edu/security/compliance/index.html>
- OIT Policies
 - <http://www.oit.umass.edu/policies/index.html>
- University Data and Computing Policies
 - <http://www.massachusetts.edu/policy/datacomputingpolicies.html>
- Massachusetts Identity Theft Law
 - <http://www.mass.gov/legis/laws/mgl/gl-93h-toc.htm>