

Data Compromise Notice Procedure Summary and Guide

Various federal and state laws require notification of the breach of security or compromise of personally identifiable data. No single federal law or regulation governs the security of all types of sensitive personal information. Under federal law certain industries are legally obligated to protect certain types of sensitive personal information. These obligations were created, in large part, when federal privacy legislation was enacted in the credit, financial services, health care, government, securities, and Internet sectors. Federal regulations were issued to require certain entities to implement information securities programs and provide breach notice to affected persons.

The summary below outlines the primary laws impacting the University of Massachusetts and the steps that must be taken if a legally “covered” data is compromised (i.e., intentionally or accidentally disclosed, accessed, or used),

A. Massachusetts General Law 93H (M.G.L. 93H)

Notice requirements are triggered under M.G.L. 93H when the University knows that:

- There has been breach of security including unauthorized acquisition or use (e.g., used for unauthorized reasons) of encrypted or unencrypted information that creates a substantial risk of identity theft or fraud OR
- Personal information, as defined in M.G.L. 93H and detailed below, of a resident of the Commonwealth has been acquired or used by an unauthorized person OR
- Personal information, as defined in M.G.L. 93H and detailed below, of a resident of the Commonwealth has been used for an unauthorized purposes.

There is no minimum number of impacted Residents so a breach of security or disclosure of information relating to a single resident may require notice under this law.

M.G.L. 93H defines personal information as an individual's first name or first initial, **and** last name in combination with one or more of the following data elements:

- Social Security Number,
- Driver's License Number
- State-Identification Card Number,
- Financial Account Number Or Credit Or Debit Card Number, **With Or Without Any Required Security Code, Access Code, Personally Identifiable Identification Number Or Password, That Would Permit Access To A Resident's Financial Account.**

The issues to consider related to M.G.L. 93H are:

1. Does the University own or license the data?
 - a. If yes, go to question 2.
 - b. If no, go to question 6.
2. Does the compromise impact Massachusetts residents?
 - a. If yes, go to question 3.
 - b. If no, determine if other laws (e.g., HIPAA, GLB, FERPA, other state breach notification laws, etc.) apply

3. Does the data fall into the defined PI data noted above.
 - a. If yes, go to question 5.
 - b. If no, go to question 4.

4. Is the information disclosed in security breach information that poses a substantial risk of identity theft or fraud against a Massachusetts resident? Several factors should be considered when determining the level of risk including but not limited to, whether the data was targeted by an attacker, the circumstances of the breach (e.g., random theft of a laptop out of a car versus theft out of a locked office), whether one or many data elements were compromised that if used in combination with other easily accessible information may increase the risk, etc.)
 - a. If yes, go to question 5.
 - b. If no, no action is needed.

5. Was the compromised data encrypted?
 - a. If yes, was the encryption key compromised? Maybe we need to change the order. First question is, was it encrypted, and was key comprised? Then second question, if key comprised, or if unencrypted, does it pose substantial risk? If no, no other action needed
 - b. If no, Notice must be given to: The Attorney General using University standard notice
 - The Director of Consumer Affairs and Business Regulation (required only for specific financially related data compromise)
 - Consumer reporting agencies (required only for specific financially related data compromise)
 - Affected individuals using University standard notice

6. Has the data owner/licensor specified a process to follow, either via a contract or other written document, when a compromise occurs?
 - a. If yes, follow that process.
 - b. If no, notify the data owner of the compromise.

B. Health Insurance portability and Accountability Act of 1996 (HIPAA)

Some University entities (e.g., health services, pharmacies, clinical studies, etc.) are subject to HIPAA and therefore, are impacted by HIPAA's Standards for Privacy (i.e., Privacy Rule) of Personally Identifiable Health Information (i.e., PHI - information relating to past, present or future physical or mental health or condition of an individual; provision of healthcare to an individual or payment for the provision of healthcare to an individual). The HIPAA Privacy Rule covers PHI whether it is on paper, in computers (i.e., electronic) or communicated orally.

Please note that student health records are classified as "education records" and are therefore, covered by the Family Educational Rights and Privacy Act (FERPA).

HIPAA defines PHI as including, but not limited to:

- Name
- Telephone/Fax Number,
- Email Address,
- Social Security Number,

- Driver's License Number,
- Name And Internet Address Or A
- Any Other Unique Identifying Number, Characteristic Or Code.

HIPAA contains no specific data compromise notice requirement other than for internal reporting. According to the Department of Health and Human Services, "This regulation does not specifically require any incident reporting to outside entities. External incident reporting is dependent upon business and legal considerations." Thus, while the HIPAA Security Rule does not require you be notified of a breach, other laws may require notice.

Within Massachusetts, the disclosure of confidential medical information is restricted by a statutory right of privacy as well as by statutes governing specific entities and medical conditions.

Regardless of the lack of external notice requirements of HIPAA, the compromise of personal patient/medical information may fall under M.G.L. 93H if the data compromised creates a substantial risk of identity theft or fraud against a Massachusetts resident.

The issues to consider for a security breach of patient/medical related personal data are:

1. Does the University own or license the data?
 - a. If yes, go to question 2.
 - b. If no, go to question 4.

2. Is the information disclosed in security breach information that poses a substantial risk of identity theft or fraud against a Massachusetts resident? Several factors should be considered when determining the level of risk including but not limited to, whether the data was targeted by an attacker, the circumstances of the breach (e.g., random theft of a laptop out of a car versus theft out of a locked office), whether one or many data elements were compromised that if used in combination with other easily accessible information may increase the risk, etc.)
 - a. If yes, go to question 3.
 - b. In no, no action needed.

3. Was the compromised data encrypted?
 - a. If yes, go to question 4.
 - b. If no, notify the affected individuals using University standard notice.

4. Was the encryption key compromised?
 - a. If yes, notify the affected individuals using University standard notice.
 - b. If no, no action needed

5. Has the data owner/licensor specified a process to follow, either via a contract or other written document, when a compromise occurs?
 - a. If yes, follow that process.
 - b. If no, notify the data owner of the compromise.

C. Family Educational Rights and Privacy Act (FERPA)

The University may disclose, without consent, "directory" information. The University has defined directory information as:

- Student's name;
- Major;
- Acknowledgment of a student's participation in officially recognized activities and sports;
- Weight and height of members of athletic teams;
- Date(s) of attendance;
- Degrees, certificates, awards received;
- The most recent previous educational agency or institution attended by the student; and
- Appointment as a Resident Assistant or Community Development Assistant.

For graduate students who are teaching credit courses, work department, office address, and employment category are also defined as directory information.

The University is required to give students a reasonable amount of time to request that the school not disclose directory information about them.

FERPA controls the disclosure of personally identifiable information (i.e., data directly related to student other than directory information) regardless of format (e.g., handwritten, audio, paper, electronic, etc.) to third parties. FERPA does NOT cover alumni records.

FERPA contains no specific data compromise notice requirement. Regardless of the lack of external notice requirements of FERPA, the compromise of personal student information may fall under M.G.L. 93H if the data compromised creates a substantial risk of identity theft or fraud against a Massachusetts resident.

The issues to consider for a security breach of student related data are:

1. Does the University own or license the data?
 - a. If yes, go to question 2.
 - b. If no, go to question 7.
2. Is the data defined as University directory information?
 - a. If yes, go to question 3.
 - b. If no, go to question 4.
3. Has the student requested that the University not disclose directory information about them?
 - a. If yes, go to question 4.
 - b. If no, no action needed.
 - c.
4. Is the information disclosed in security breach information that poses a substantial risk of identity theft or fraud against a Massachusetts resident? Several factors should be considered when determining the level of risk including but not limited to, whether the data was targeted by an attacker, the circumstances of the breach (e.g., random theft of a laptop out of a car versus theft out of a locked office), whether one

or many data elements were compromised that if used in combination with other easily accessible information may increase the risk, etc.)

- a. If yes, go to question 5.
 - b. In no, no action needed.
5. Was the compromised data encrypted?
 - a. If yes, go to question 7.
 - b. If no, notify the affected individuals using University standard notice.
 6. Was the encryption key compromised?
 - a. If yes, notify the affected individuals using University standard notice.
 - b. If no, no action needed
 7. Has the data owner/licensor specified a process to follow, either via a contract or other written document, when a compromise occurs?
 - a. If yes, follow that process.
 - b. If no, notify the data owner of the compromise.

D. Graham-Leach-Bliley Act (GLBA)

GLBA requires that the University ensure the security and confidentiality of “customer” records (i.e., personally identifiable information) such as names, addresses, phone numbers, bank and credit card account numbers, income and credit histories, and Social Security numbers.

GLBA contains no specific data compromise notice requirement however some of this data is included in M.G.L. 93H (i.e., names plus bank and credit card account numbers and Social Security Numbers) so notice requirements of this law take effect in the event of a data breach. Follow section A of this document.

Regardless of the lack of external notice requirements of GLBA, the compromise of personal customer information other than PII may fall under M.G.L. 93H if the data compromised creates a substantial risk of identity theft or fraud against a Massachusetts resident. Note: In most cases this would be related to the compromise of financial aid information so students would be the impacted customers.

The issues to consider for a security breach of customer data are:

1. Does the University own or license the data?
 - a. If yes, go to question 2.
 - b. If no, go to question 5.
2. Is the information disclosed in security breach information that poses a substantial risk of identity theft or fraud against a Massachusetts resident? Several factors should be considered when determining the level of risk including but not limited to, whether the data was targeted by an attacker, the circumstances of the breach (e.g., random theft of a laptop out of a car versus theft out of a locked office), whether one or many data elements were compromised that if used in combination with other easily accessible information may increase the risk, etc.)
 - a. If yes, go to question 3.
 - b. In no, no action needed.

3. Was the compromised data encrypted?
 - a. If yes, go to question 4.
 - b. If no, notify the affected individuals using University standard notice.
4. Was the encryption key compromised?
 - a. If yes, notify the affected individuals using University standard notice.
 - b. If no, no action needed
5. Has the data owner/licensor specified a process to follow, either via a contract or other written document, when a compromise occurs?
 - a. If yes, follow that process.
 - b. If no, notify the data owner of the compromise.

E. Other Confidential Information Compromises Requiring Notice

As previously noted, regardless of the lack of external notice requirements for specific types of data (e.g., mother's maiden name, birth date, employee identification number, etc.) the compromise of personal information may fall under M.G.L. 93H if the data compromised creates a substantial risk of identity theft or fraud against a Massachusetts resident.

The issues to consider for a security breach of the other data types are:

1. Does the University own or license the data?
 - a. If yes, go to question 2.
 - b. If no, go to question 5.
2. Does the data disclosure create a substantial risk of identity theft or fraud against a Massachusetts resident?
 - a. If yes, go to question 3.
 - b. In no, no action needed.
3. Was the compromised data encrypted?
 - a. If yes, go to question 4.
 - b. If no, notify the affected individuals using University standard notice.
4. Was the encryption key compromised?
 - a. If yes, notify the affected individuals using University standard notice.
 - b. If no, no action needed
5. Has the data owner/licensor specified a process to follow, either via a contract or other written document, when a compromise occurs?
 - a. If yes, follow that process.
 - b. If no, notify data owner of compromise.
 - c.

Lastly, this Procedure is not intended to impose any further data security breach/compromise notice requirements other than those dictated in M.G.L. 93H however, there may be incidents involving PII or protected data for which Campuses determine external notification is prudent. This is especially true if multiple data elements are compromised which, when taken as a whole present a significant risk of safety, identity theft or fraud to impacted individuals. The need for such notices will be determined by the Campuses, in coordination with University legal counsel, and as authorized by the Campus CIO.

