

Identity Theft Prevention and Security Breach Notification Policy

Purpose:

Lahey Clinic is committed to protecting the privacy of the Personal Health Information (“PHI”) of our patients and the Personal Information (“PI”) of both our patients and our employees. This Information Security Policy (the “Policy”) guides this commitment as it achieves the following purposes:

1. To detect, prevent, and mitigate Identity Theft and other forms of fraud regarding the disclosure or use of the PI and/or PHI of any patient, employee, or any other individual related to Lahey Clinic business;
2. To provide a process and related guidance for investigating allegations of Identity Theft resulting from a breach of security, or from the unauthorized acquisition and/or use of an individual’s PI and/or PHI; and
3. To provide a process for appropriately notifying affected individuals and government agencies upon a breach of security or upon the unauthorized acquisition and/or use of an individual’s PI and/or PHI.

Applicable Law:

The Policy is best understood when we consider the laws that shape it. The following three laws and related guidance provide the foundations of this Policy:

1. The federal Red Flags Rule¹ requires Lahey Clinic to design and implement a written identity theft prevention program to prevent, detect, and mitigate identity theft in connection with certain accounts. Lahey Clinic is subject to the Red Flags Rule because the Rule considers hospitals to be the “creditors” of their patients.
2. The Massachusetts data breach law and implementing regulations² (the “MA data breach law”) require Lahey Clinic, as an entity that owns, licenses, stores, and/or maintains data that includes PI, to report certain breaches and unauthorized acquisition or use of such data to the individual and/or specified Massachusetts government officials.
3. The HITECH Act³ requires Lahey Clinic, as a covered entity under HIPAA, to notify individuals and the Department of Health and Human Services (“HHS”) in the case of a breach of unsecured PHI.

As detailed below, one or more of these laws may apply to a given situation.

Scope:

This Policy applies to all Lahey Clinic and Lahey Clinic Hospital employees, physicians, other clinicians, and anyone associated with Lahey Clinic Foundation, Inc., Lahey Clinic Hospital, Inc., or Lahey Clinic, Inc.

¹ 16 C.F.R. §§ 603.2(a) and 681.2.

² Mass. General Laws Ch. 93H § 3 and 201 CMR 17.002.

³ Health Information Technology for Economic and Clinical Health (Title XIII of the American Recovery and Reinvestment Act of 2009).

(collectively referred to herein as “Lahey Clinic”). This Policy should be read in conjunction with applicable HIPAA privacy and security policies and Lahey medical record policies.

Policy:

It is the policy of Lahey Clinic to:

1. Limit the amount of PI and PHI it collects to that reasonably necessary to accomplish the legitimate purpose for which the PI and PHI is collected;
2. Limit the time that it retains PI and PHI to that reasonably necessary to accomplish such the purpose for which the PI and PHI is collected consistent with applicable Lahey Clinic record and document retention policies;
3. Limit access to the PI and PHI to those Lahey Clinic Colleagues who are reasonably required to have such access in order to accomplish their job functions or to comply with state or federal retention requirements;
4. Follow procedures to detect and investigate Identity Theft or breaches of PI or PHI;
5. Investigate all reports of a breach of security or of an unauthorized acquisition and/or use of the PI or PHI of any patient, employee, or any other individual related to Lahey Clinic business; and
6. When applicable, notify the affected individuals and appropriate government agencies if an investigation determines the occurrence of a breach of security or an unauthorized acquisition and/or use of the PI or PHI.

Definitions:

See [Attachment A](#) for explanation of the defined terms used in this Policy and Procedure Document.

Procedure:

A. Red Flags and Identity Theft

(1) Identification of Red Flags and Identity Theft

Although not all Lahey Clinic employees typically deal with Covered Accounts, all Lahey Clinic employees, physicians, other clinicians should be familiar with how to identify Identity Theft. Generally, an individual may become aware of potential Identity Theft from the following sources:

1. Suspicious documents;
2. Suspicious PI or suspicious identifying information;
3. Suspicious or unusual use of Accounts; and/or
4. Alerts from patients, employees, victims of Identity Theft, law enforcement, or others.

All reports or allegations of Identity Theft shall be directed to the Corporate Compliance Officer. However, depending on the nature of the allegation, the following people should first be contacted:

1. Allegations pertaining to patient information shall be directed to the Privacy Officer who will also notify the Corporate Compliance Officer.
2. Allegations pertaining to information stored or maintained in computer systems shall be reported to the Security Officer who will notify the Corporate Compliance Officer.

For examples of more specific Red Flags and related prevention procedures and resolutions, please see [Attachment D](#).

(2) Detection of Red Flags and Identity Theft

Lahey Clinic employees, physicians, other clinicians must also make efforts to detect Red Flags and Identity Theft. Those efforts should include, at a minimum:

1. Require identification (such as by a driver's license or other government issued identification, insurance card);
2. Verify forms of identification if necessary;
3. Verify requests for change of billing address; and
4. Verify identification and authority before releasing identifying information.

Please see [Attachment F](#) for department-specific procedures. *Note that in the event of suspected Identity Theft, Lahey Clinic physicians and other clinicians should report the matter to the applicable department manager for follow-up and response. The physicians' and clinicians' primary responsibility is the care and treatment of the patient. The manager shall be responsible for reporting to the Corporate Compliance Officer.

(3) Response to Red Flags and Identity Theft

The following steps may be taken to respond appropriately to Red Flags and instances of Identity Theft in order to prevent further Identity Theft and possibly reduce the harm caused by Identity Theft:

1. Monitoring an Account for evidence of Identity Theft;
2. Contacting the patient or Colleague;
3. Changing any passwords, security codes, or other security devices that permit access to an Account;
4. Reopening an Account with a new Account or medical record number,
5. Not opening a new Account;
6. Closing an existing Account;
7. Not attempting to collect on an Account or not referring an Account to a debt collector;
8. Notifying law enforcement; and/or
9. Determining that no response is warranted under the particular circumstance.

(4) Program Administration

Lahey Clinic Colleagues shall be trained in Red Flag identification and Identity Theft prevention in accordance with their duties. Lahey Clinic's program to identify Red Flags and prevent Identity Theft (the "Identity Theft Prevention Program") shall be updated periodically to reflect changes in risks of Identity Theft to patients, Colleagues, and others based on such factors as:

1. Lahey Clinic's experience with Identity Theft;
2. Changes in the methods of Identity Theft;
3. Changes in the methods to detect, prevent, and mitigate Identity Theft;
4. Changes in the types of Accounts that Lahey Clinic offers or maintains; and
5. Changes in Lahey Clinic's business arrangements.

B. Procedures Upon Breach of Security Under the MA Data Breach Law

(1) Internal Reports

All reports or allegations of a Breach of Security shall be directed to the Corporate Compliance Officer. However, depending on the nature of the allegation, the following people should first be contacted:

1. Allegations pertaining to patient information shall be directed to the Privacy Officer who will also notify the Corporate Compliance Officer.
2. Allegations pertaining to information stored or maintained in computer systems shall be reported to the Security Officer who will notify the Corporate Compliance Officer.

*Note that in the event of suspected Identity Theft, Lahey Clinic physicians and other clinicians should report the matter to the applicable department manager for follow-up and response. The physicians' and clinicians' primary responsibility is the care and treatment of the patient. The manager shall be responsible for reporting to the Corporate Compliance Officer.

Upon receipt of the report or allegation, the Corporate Compliance Officer will follow the procedures outlined in Attachment B.

(2) Reports by Lahey Clinic Service Providers

Any Lahey Clinic service provider shall provide notice of any suspected Breach of Security to Lahey Clinic and such notice shall include the following information:

1. A description of the breach;
2. The date or approximate date of such incident and the nature thereof; and
3. Any steps the service provider has taken or plans to take relating to the incident.

Such disclosure shall not be deemed to require the disclosure of confidential business information of trade secrets of the service provider. The service provider shall not be required to provide notice to an individual who may have been affected the Breach of Security or unauthorized acquisition or use of PI or PHI.

Upon receipt of the report or allegation from a service provider, the Corporate Compliance Officer will follow the procedures outlined in Attachment B.

C. Procedures Upon a Breach Under the HITECH Act

(1) Internal Reports

All reports or allegations of a Breach under the HITECH Act shall be directed to the Corporate Compliance Officer. However, depending on the nature of the allegation, the following people should first be contacted:

1. Allegations pertaining to patient information shall be directed to the Privacy Officer who will also notify the Corporate Compliance Officer.
2. Allegations pertaining to information stored or maintained in computer systems shall be reported to the Security Officer who will notify the Corporate Compliance Officer.

*Note that in the event of suspected Identity Theft, Lahey Clinic physicians and other clinicians should report the matter to the applicable department manager for follow-up and response. The physicians' and

clinicians' primary responsibility is the care and treatment of the patient. The manager shall be responsible for reporting to the Corporate Compliance Officer.

Upon receipt of the report or allegation, the Corporate Compliance Officer will follow the procedures outlined in Attachment C.

(2) Reports by Lahey Clinic Business Associates

Any Lahey Clinic business associate shall provide notice of any Breach under the HITECH Act to Lahey Clinic without unreasonable delay. Such notice shall identify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed as a result of the Breach.

Upon receipt of the report or allegation, the Corporate Compliance Officer will follow the procedures outlined in Attachment C.

Contact: Corporate Compliance Officer, Privacy Officer and Legal Services

References: Massachusetts General Laws, Chapter 93H. Security Breaches; 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth; Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 16 C.F.R. §§ 603.2(a) and 681.2; Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009.

Origination Date: 2008

Reviewed/Revised: October 2010

Approved by: Corporate Compliance Committee
Audit/Compliance Committee of the Board Trustees

ATTACHMENT A

DEFINITIONS

A. General Definitions

“Colleagues” means all Lahey employees and temporary, per diem personnel, volunteers, students and others rendering paid or unpaid services to Lahey, including all Lahey agents.

B. Red Flags and Identity Theft Definitions

“Account” means a continuing relationship established by: (1) a patient with Lahey Clinic to obtain health care services in exchange for payment by the patient or a third party; or (2) a Colleague to provide services in exchange for payment by Lahey Clinic.

“Covered Account” means (1) any Account Lahey Clinic offers or maintains, primarily for personal (patient or employee) purposes, that involves multiple payments or transactions, including one or more deferred payments; and (2) any other Account Lahey Clinic identifies as having a reasonably foreseeable risk of Identity Theft. Lahey Clinic has identified the patient billing and payment plans and other types of deferred payment plans as Covered Accounts more specifically in Attachment E. Covered Accounts and Accounts are used interchangeably in this Policy.

“Identity Theft” means a fraud committed or attempted using the identifying information of another person without authority.

“Identifying information” means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any:

1. Name, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
2. Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
3. Unique electronic identification number, address, or routing code; or
4. Telecommunication identifying information or access device (as defined in 18 USC 1029(e)).

“Red Flag” means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft. Examples of Red Flags include: alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services; the presentation of suspicious documents; the presentation of suspicious personal identifying information such as a suspicious address changes; the unusual use of, or other suspicious activity related to an Account; and notice from patients, Colleagues, victims of Identity Theft, law enforcement authorities, or other persons regarding possible Identity Theft in connection with patient Accounts or Colleague Accounts.

C. Massachusetts Data Breach Law Definitions

“Affected individual” means a Lahey Clinic patient, employee, or any other individual whose PI is stored on Lahey Clinic’s computer systems and is the subject of a Breach of Security.

“Breach of Security” means the unauthorized acquisition or unauthorized use of Lahey Clinic data, whether encrypted or not, and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by Lahey Clinic or a party under contract with Lahey Clinic, that creates a substantial risk of Identity Theft or fraud against a Lahey Clinic patient, employee, or any other individual whose PI is stored on Lahey Clinic’s computer systems. A good faith but unauthorized acquisition, access, use or inadvertent disclosure of PI by Lahey Clinic, an employee of Lahey Clinic, or a Lahey Clinic business associate, within the scope of the employment or professional relationship, is not a Breach of Security unless the PI is used in an unauthorized manner or subject to further unauthorized disclosure, access, or use.

“Data” means any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

“Electronic” means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

“Encrypted” means the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

“Notice” means: written notice, electronic notice; or substitute notice if the cost of providing written notice will exceed \$250,000, or if the number of affected individuals to be notified exceeds 500,000 Massachusetts residents, or if Lahey Clinic does not have sufficient contact information to provide notice. In that case, substitute notice shall include electronic mail, posting a notice on Lahey Clinic’s website home page, and broadcast or publication in a medium that will provide notice throughout the Commonwealth. Any electronic mail notice must comply with the Electronic Signatures in Global and national Commerce (E-SIGN) Act, 15 U.S.C. §7001.

“Personal Information (PI)” means an individual’s first name and last name or first initial and last name in combination with the individual’s:

1. Social Security Number;
2. Driver’s license 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 an individual’s financial account.

Personal information does not include information that is lawfully obtained from publicly available information or from federal, state or local government records that are lawfully made available to the general public.

“Record(s)” means any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

“Service Provider” means any person that receives, stores, maintains, processes, or otherwise is permitted access to PI through its provision of services directly to Lahey Clinic.

D. HITECH Act Definitions

“Breach” means the acquisition, access, use, or disclosure of PHI in a manner not permitted under 45 C.F.R. Part 164, Subpart E (the “HIPAA Privacy Rule”) which compromises the security or privacy of the PHI.

“Breach” shall not include:

1. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of Lahey Clinic or its business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule; or
2. Any inadvertent disclosure by a person who is authorized to access PHI at Lahey Clinic or its business associate to another person authorized to access PHI at Lahey Clinic or its business associate, respectively, or Organized Health Care Arrangement in which Lahey Clinic participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule; or
3. A disclosure of PHI where Lahey Clinic or its business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

“Protected Health Information (PHI)” means individually identifiable health information transmitted or maintained in any form or medium including PHI that (i) is received by a business associate from Lahey Clinic as a covered entity, (ii) a business associate creates for its own purposes from individually identifiable health information that a business associate received from Lahey Clinic as a covered entity, or (iii) is created, received, transmitted or maintained by a business associate on behalf of Lahey Clinic as a covered entity. PHI excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g, records described at 20 U.S.C. § 1232g(a)(4)(B)(iv), and employment records held by Lahey Clinic, as a covered entity, in its role as employer. Undefined terms in this definition have the meaning set forth at 45 C.F.R. § 160.103.

ATTACHMENT B

PROCEDURE FOR BREACH OF SECURITY UNDER THE MA DATA BREACH LAW

A. Investigation of Alleged Breach of Security

1. The Corporate Compliance Officer, Legal Services Department, and the Privacy Officer and/or Security Officer, along with applicable departments shall develop a plan of investigation of any alleged Breach of Security. The scope of the investigation will depend on the department(s) and system(s) involved.
2. Such investigation shall include, as applicable:
 - a. Lahey Clinic computer system audits;
 - b. Contacting the IT individuals at the externally involved entities for relevant computer system information, including but not limited to Internet Protocol (IP) addresses; and/or
 - c. Review of the investigation with the Legal Services Department and the Corporate Compliance Officer and Privacy Officer as applicable. Other departments shall be included as applicable, including, but not limited to the Finance and Human Resources Departments.

B. Risk Assessment

In order to determine whether a Breach of Security has occurred, the Corporate Compliance Officer in consultation with the Legal Services Department must determine if there is a substantial risk of Identity Theft or fraud against a Massachusetts resident. If the Corporate Compliance Officer in consultation with the Legal Services Department determines that no such substantial risk exists, the incident does not constitute a Breach of Security and the below procedures in this Attachment B do not apply. However, if the alleged breach involved PHI, the Corporate Compliance Officer must follow the procedure set forth in Attachment C.

C. Provision of Notice

(1) Determination of Lahey Clinic's Relationship to the Data and Appropriate Notice

Following investigation and determination of a Breach of Security, the Corporate Compliance Officer shall then determine whether Lahey Clinic owns or licenses the data that includes the PI, or whether Lahey Clinic only maintains or stores the data.

1. If Lahey Clinic owns or licenses the data, the Corporate Compliance Officer shall provide notice of the Breach of Security to the Office of the Attorney General, the Director of Consumer Affairs, and the affected individual(s). The notice to the affected individuals shall contain the elements described below under, "Notice to Affected Individuals." The notice to the Attorney General and the Director of Consumer Affairs shall include, but not be limited to:

- a. The nature of the Breach of Security or unauthorized acquisition or use;
- b. The number of Massachusetts residents affected by the incident at the time of notification; and
- c. Any steps Lahey Clinic has taken or plans to take relating to the incident.

Upon such notification, the Director of Consumer Affairs shall provide Lahey Clinic with the names of consumer reporting agencies and applicable state agencies. Lahey Clinic shall then report the information listed directly above at (a)-(c) to the identified consumer reporting agencies and applicable state agencies.

2. If Lahey Clinic only maintains or stores the data, the Corporate Compliance Officer shall provide notice to the owner or licensor of the data and shall cooperate with the owner or licensor of such information, including but not limited to, informing the owner or licensor of the Breach of Security or unauthorized acquisition or use, the date or approximate date of such incident and the nature thereof, and any steps Lahey Clinic has taken or plans to take relating to the incident. Such cooperation shall not be deemed to require the disclosure of confidential business information or trade secrets, or to provide notice to a resident that may have been affected by the Breach of Security or unauthorized acquisition or use.

Lahey Clinic shall cooperate with law enforcement in its investigation of any Breach of Security or unauthorized acquisition or use, including the sharing of information relevant to the incident, provided that such disclosures do not require the disclosure of confidential business information or Lahey Clinic trade secrets.

(2) Notice to Affected Individuals

When appropriate, the affected individual (or next of kin if the affected person is deceased) shall be provided notice at the last-known address of the individual (or next of kin), by first-class mail (or by electronic mail if specified by the individual), as soon as practicable, but no later than 60 days after, Lahey Clinic or a Clinic Lahey business associate:

1. Knows or has reason to know of the Breach of Security; or
2. When Lahey knows or has reason to know that the PI of an affected individual was acquired or used by an unauthorized person or used for an unauthorized purpose.

The notice to the affected individuals shall include:

1. A brief description of the Breach of Security, unauthorized access or use;
2. The date or approximate date of the breach, if known;
3. The date Lahey Clinic discovered the breach;
4. Any steps Lahey Clinic has taken to investigate the breach, to mitigate losses and protect from further breaches;
5. The individual's right to obtain a police report;
6. Information on how the individual can request a security freeze and the necessary information to be provided when requesting a security freeze, as well as any fees required to be paid to any of the consumer reporting agencies; and
7. A telephone number at Lahey Clinic for additional information.

The notice to the affected individuals shall not include:

1. The nature of the breach or unauthorized acquisition or use; or

2. The number of Massachusetts residents affected by the breach or unauthorized access or use.

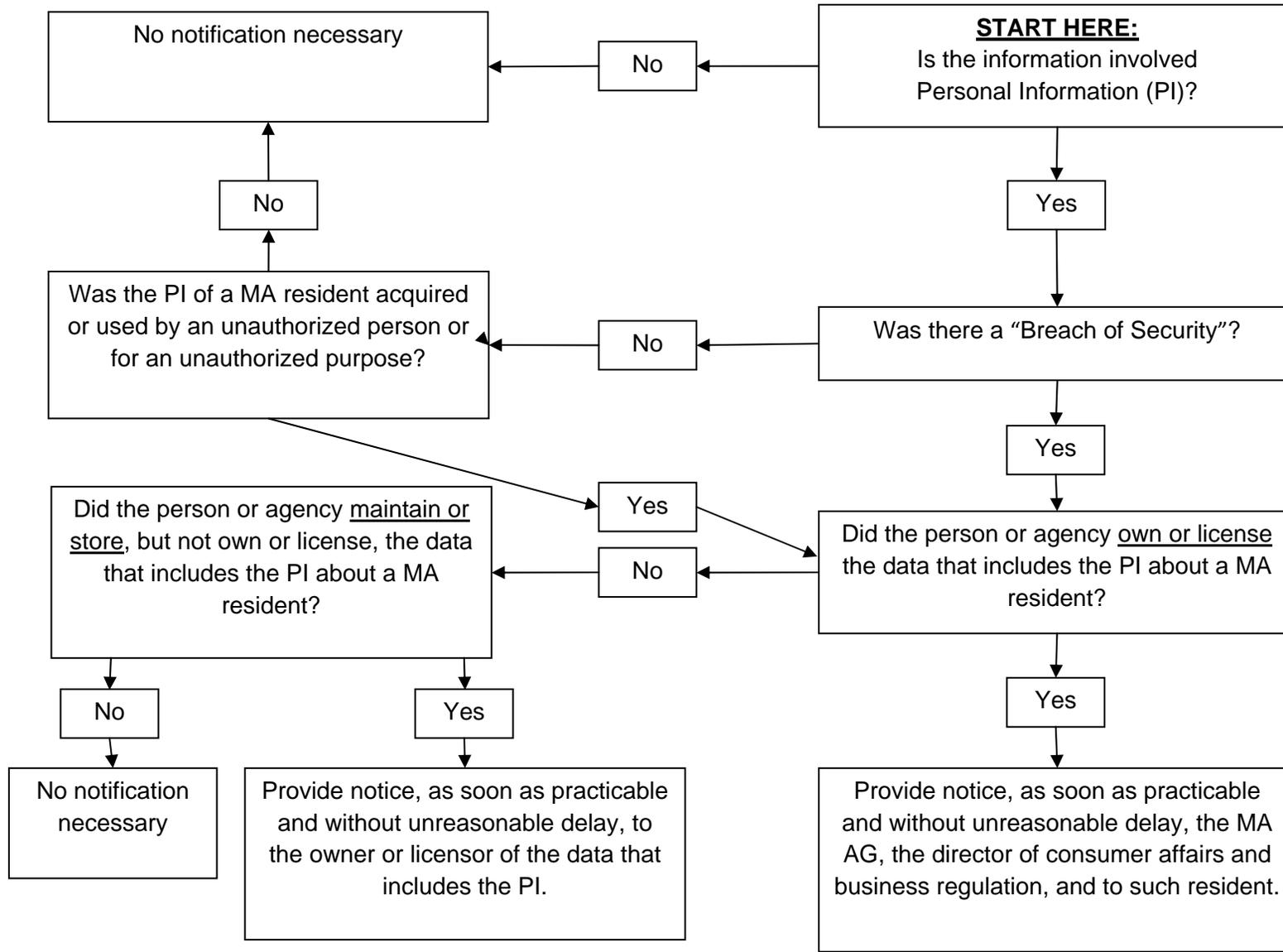
(3) Other Issues Regarding Notice

1. If the affected individual is not a Massachusetts resident, the Legal Services Department shall determine the notification requirements of the individual's state of residence and forward that information to the appropriate Colleagues.
2. Lahey shall delay notifying affected individuals upon notice by a law enforcement agency that providing such notice may impede a criminal investigation. Lahey Clinic shall then provide the notice as soon as the law enforcement agency determines and informs Lahey Clinic that notification no longer poses a risk of impeding a criminal investigation.

D. Reference Chart

Please see the "MA Data Breach Law Reference Chart" on the next page.

**MA Data Breach Law Reference Chart
(For Incidents Involving Personal Information)**



ATTACHMENT C

PROCEDURE FOR BREACH UNDER THE HITECH ACT

A. Investigation of Alleged Breach

1. The Corporate Compliance Officer, Legal Services Department, and the Privacy Officer and/or Security Officer, along with applicable departments shall develop a plan of investigation of any alleged Breach under the HITECH Act. The scope of the investigation will depend on the department(s) and system(s) involved.
2. Such investigation shall include, as applicable:
 - a. Lahey Clinic computer system audits;
 - b. Contacting the IT individuals at the externally involved entities for relevant computer system information, including but not limited to Internet Protocol (IP) addresses; and/or
 - c. Review of the investigation with the Legal Services Department and the Corporate Compliance Officer and Privacy Officer as applicable. Other departments shall be included as applicable, including, but not limited to the Finance and Human Resources Departments.

B. Risk Assessment

In order to determine whether a Breach has occurred, the Corporate Compliance Officer in consultation with the Legal Services Department must perform a risk assessment to determine if there is a significant risk of financial, reputational or other harm to the individual whose PHI was used or disclosed. The Corporate Compliance Officer in consultation with the Legal Services Department will consider a number of factors, including:

1. Who impermissibly disclosed or to whom the information was impermissibly disclosed (i.e. was the acquisition, access, use, or disclosure to a covered entity or business associate, or to a private individual or entity). There may less risk of harm to the individual if the recipient of the information is obligated by HIPAA and the HITECH Act;
2. The likelihood the information is accessible and usable by the unauthorized individual;
3. Whether Lahey Clinic has taken immediate steps to mitigate, including obtaining assurances from the recipient that the information will not be further used or disclosed, or that the information is destroyed or returned prior to it being improperly accessed;
4. The type and amount of PHI involved. The Corporate Compliance Officer in consultation with the Legal Services Department must examine the information that was acquired, accessed, used or disclosed, including whether the information involved the name of the individual and that services were received, the types of services received or where the services were received (i.e. at a specialized facility or department) and if the information increases the risk of identity theft (i.e. SSN, account number or mother's maiden name).

The Corporate Compliance Officer in consultation with the Legal Services Department should carefully conduct a fact intensive investigation that includes any type of health information that may cause reputational harm. The Corporate Compliance Officer will document the risk assessment in a memo that is kept on file with the Corporate Compliance Officer. If the Corporate Compliance Officer in consultation with the Legal Services Department determines that there is no significant risk of harm to the individual,

the below procedures in this Attachment C do not apply. However, if the alleged breach involved PI, the Corporate Compliance Officer must follow the procedure set forth in Attachment B.

C. Provision of Notice

If the Corporate Compliance Officer in consultation with the Legal Services Department determines that a Breach under the HITECH Act has occurred, and if that breach involves unsecured PHI, the Corporate Compliance Officer must coordinate the provision of notice as follows:

(1) Notice to Individuals

Notification must be provided to each individual whose unsecured PHI has been or is reasonably believed to have been, acquired, accessed, used or disclosed as a result of the breach without unreasonable delay and in no case later than 60 calendar days. If the breach requires the involvement of law enforcement, the notification may be delayed for a period of time as determined by a law enforcement official. The Corporate Compliance Officer must prepare a notification that includes (to the extent possible):

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
2. A description of the types of unsecured PHI that were involved in the breach (such as whether full name, SSN, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
3. Any steps individuals should take to protect themselves from potential harm resulting from the breach;
4. A brief description of what Lahey Clinic is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
5. Contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an email address, web site or postal address.

The Corporate Compliance Officer will be sensitive to only include general information (i.e. listing the types of information involved as opposed to listing the actual PHI that was involved in the breach) in the notification. Depending upon the nature of the breach and the information obtained during the investigation, the Corporate Compliance Officer may also include:

1. Recommendations that the individual contact applicable credit card companies and information about how to obtain credit monitoring services;
2. Information about the steps Lahey Clinic is taking to retrieve the breached information and improve security to prevent future breaches; and
3. Information about sanctions Lahey Clinic imposed on its workforce members involved in the breach.

To comply with other applicable laws, the Corporate Compliance Officer may also need to translate the notice into other languages and make the notice available in alternate formats, such as Braille, large print or audio.

The notice will be sent by first-class mail or, if Lahey Clinic does not have sufficient contact information for some or all of the affected individuals, by substitute notice (depending on the number of individuals for whom Lahey Clinic does not have sufficient contact information, through an alternate form of written

notice, by telephone or other means, or by a posting on www.lahey.org for 90 days or in major print or broadcast media in geographic areas where the affected individuals likely reside).

If Lahey determines the breach to have caused an urgent situation based on the possibility of imminent misuse of unsecured PHI, notice by telephone or other method is permitted in addition to any other method.

(2) Notice to the Secretary of HHS

The Corporate Compliance Officer must provide notice to the Secretary of the United States Department of Health & Human Services (the “Secretary”) concurrently with the notification sent to the affected individuals (for any breach involving 500 or more individuals) or within 60 days after the end of each calendar year (for breaches involving less than 500 individuals). In the latter case, the Corporate Compliance Officer will maintain a log and other documentation of each breach to ensure that the scope and extent of the information provided to the Secretary is in compliance with HITECH. The content of the notice will be the same as described above.

(3) Notification to the Media

The Corporate Compliance Officer may also be required to notify a prominent media outlet for any breach that involves more than 500 residents of any one state or jurisdiction. The notification will contain the same information as described above and will be made concurrently with the notification sent to the affected individuals. The Corporate Compliance Officer, depending on the circumstances of the breach, will determine what constitutes a prominent media outlet.

(4) Notification by Business Associates

The Corporate Compliance Officer will work with business associates of Lahey Clinic to ensure that business associates report any Breaches of unsecured PHI promptly to Lahey Clinic.

The Corporate Compliance Officer will be responsible for documenting that all notifications required under the HITECH Act were made in a memo to be kept on file with the Corporate Compliance Officer.

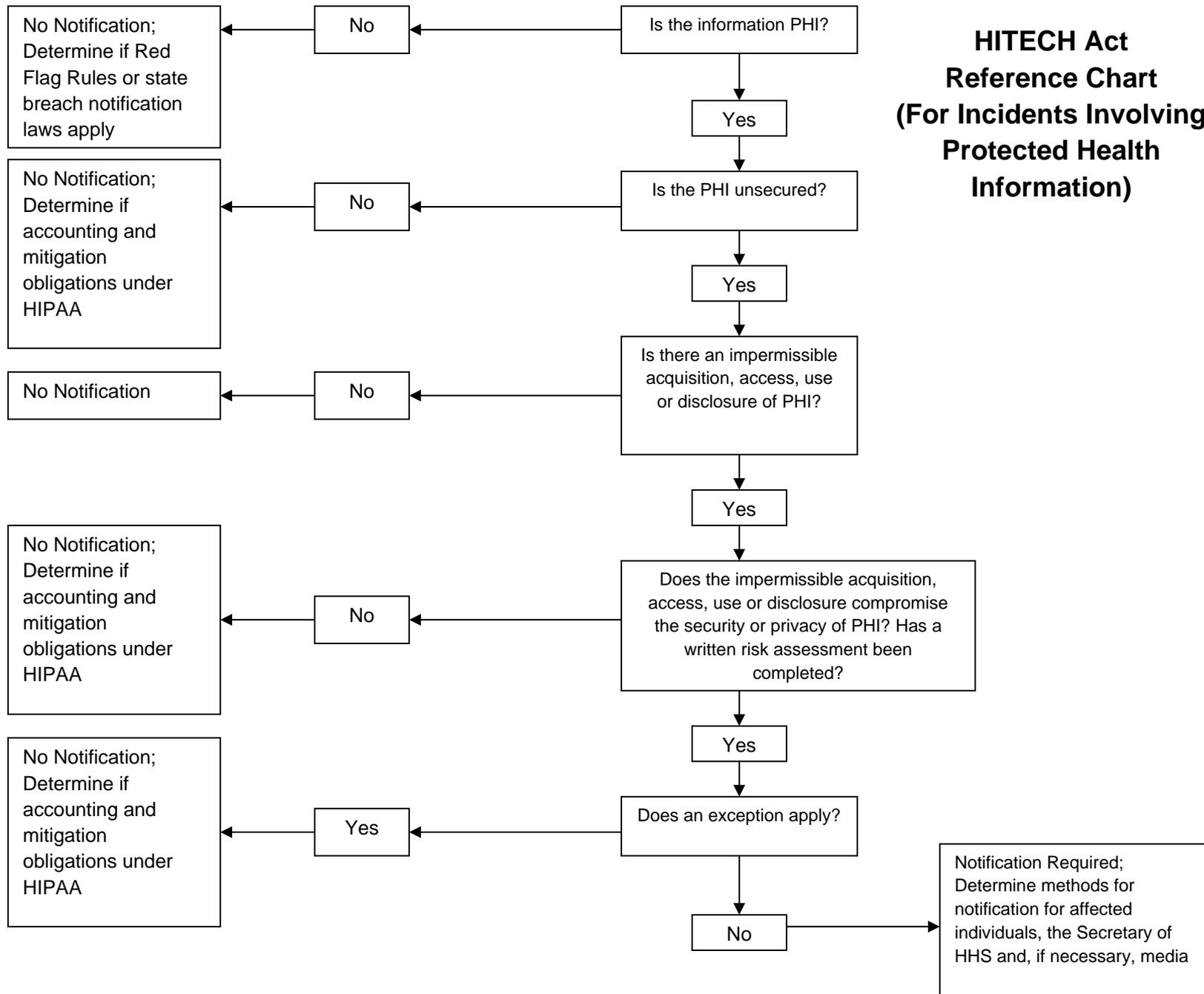
D. Reference Chart

Please see the “HITECH Act Reference Chart” on the next page.

E. Procedures When Breaches of PI and PHI Would Result in Dual Notice to Affected Individuals

In cases where a breach of security involves both PI and PHI, notice to affected individuals may be required by both MA data breach law and the HITECH Act. In these cases, Lahey Clinic need not send the same individuals two separate notices. Instead, Lahey Clinic should follow the notice procedures set forth by the HITECH Act, and described in this [Attachment C](#). Lahey Clinic will then notify the Massachusetts Office of the Attorney General and the Office of Consumer Affairs and Business Regulation of the breach as soon as practicable and without unreasonable delay. Such notice should consist of, but not be limited to, any steps Lahey Clinic has taken or plans to take relating to the breach pursuant to the HITECH Act and applicable regulations and guidance.

**HITECH Act
Reference Chart
(For Incidents Involving
Protected Health
Information)**



ATTACHMENT D

RED FLAG IDENTIFICATION AND IDENTITY THEFT PREVENTION PROCEDURES

IDENTITY THEFT RED FLAG	PREVENTION/MITIGATION PROCEDURE	POSSIBLE RESOLUTION OF RED FLAG
Documents provided for identification appear to have been altered or forged.	Stop the admissions/billing process and require patient to provide additional satisfactory information to verify identity.	Additional documentation must be provided to resolve discrepancy and continue admissions/billing process.
Personal identifying information provided by the patient is not consistent with other personal identifying information provided by the patient. For example, there is a lack of correlation between the Social Security Number (SSN) range and date of birth.	Stop the admissions/billing process and require patient to provide additional satisfactory information to verify identity.	Additional documentation must be provided to resolve discrepancy and continue admissions/billing process.
The SSN provided is the same as that submitted by other persons opening an Account or other patients.	Stop the admissions/billing process and require patient to provide additional satisfactory information to verify identity.	Additional documentation must be provided to resolve discrepancy and continue admissions/billing process.
Patient has an insurance number but never produces an insurance card or other physical documentation of insurance.	Stop the admissions/billing process and require patient to provide additional satisfactory information to verify identity.	<p>Additional documentation must be provided to resolve discrepancy and continue admissions/billing process. Contact insurance company as necessary.</p> <p>If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.</p>
Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient (e.g., inconsistent blood type).	Investigate complaint, interview individuals as appropriate, review previous files for potential inaccurate records. Items to consider include: blood type, age, race, and other physical descriptions may be evidence of medical identity theft.	<p>Depending on the inconsistency and review of previous file, either delay/do not open a new Covered Account, or terminate services.</p> <p>If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.</p>
<p>Complaint/inquiry from an individual based on receipt of:</p> <ul style="list-style-type: none"> • a bill for another individual 	Investigate complaint, interview individuals as	Terminate treatment/credit until identity has been accurately resolved; refuse to continue attempting to collect

<ul style="list-style-type: none"> • a bill for a product or service that the patient denies receiving • a bill from a health care provider that the patient never patronized • a notice of insurance benefits (or Explanation of Benefits) for health services never received. 	<p>appropriate.</p>	<p>on the Account until identity has been resolved.</p> <p>Notify law enforcement as appropriate.</p> <p>If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.</p>
<p>Mail sent to the patient is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the patient's Covered Account.</p>	<p>Skip-tracing procedures are used to find the patient's current mailing address.</p>	<p>Patient is found and contact information is updated.</p>
<p>Hospital is notified by a patient, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent Account for a person engaged in identity theft.</p>	<p>Investigation to determine if billing was made fraudulently.</p>	<p>Additional documentation must be provided to resolve discrepancy and continue admissions/billing process. Contact insurance company as necessary.</p> <p>Notify law enforcement as appropriate.</p> <p>If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.</p>
<p>Personal identifying information provided by the patient is associated with known fraudulent activity as indicated by internal or third-party sources used by the Hospital. For example:</p> <ul style="list-style-type: none"> • The address on an application is the same as the address provided on a fraudulent application; or • The phone number on an application is the same as the number provided on a fraudulent application. 	<p>Investigate complaint, interview individuals as appropriate</p>	<p>Terminate treatment/credit until identity has been accurately resolved; refuse to continue attempting to collect on the Account until identity has been resolved.</p> <p>Notify law enforcement as appropriate.</p> <p>If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.</p>

ATTACHMENT E

LAHEY CLINIC COVERED ACCOUNTS

COVERED ACCOUNT	DESCRIPTION

ATTACHMENT F

DEPARTMENT SPECIFIC POLICIES