Home Health Foundation (HHF)
Home Health VNA (HH VNA)
Merrimack Valley Hospice (MVH)
York Hospital Hospice (YHH)
Circle Home Health
Hallmark Home Health

WRITTEN INFORMATION SECURITY PLAN (WISP)

Table of Contents

Comprehensive Written Information Security Program for 201 CMR 17.00

u. PHI, Accounting for Disclosures of #4003
v. Faxing PHI #4004
w. Medical Record – Scanning of Documentation #4006
x. PHI, Authorization for use or Disclosure of #4007
y. PHI, Client's Right of Access to/Release of M/R Information #4008
z. PHI, Minimum Necessary Use and Disclosure of #4009
aa. PHI, Notice of Privacy Practices #4010
bb. Use of Electronic Main (E-mail) in Communication of Restricted Information #4013
cc. Alternative Communication of PHI #4013
dd. Security, Safeguarding and Staff Access to M/R Information #4014
ee. Access to PHI in an Emergency Event #4015
ff. Confidential Paper Disposal #4016
gg. Destruction of Patient Records #4017
hh. Electronic Signature, Attestation and Authorship in Electronic Medical Record (EMR) #1009
ii. Vendor Confidentiality #1011
jj. Passwords for Information Systems #1034
kk. Information Security, Responsibility for #1052
ll. HHF Portal Policy/Procedure #1056
mm. HIPAA Privacy – Reporting of Data Breaches #1064
nn. Virtual Private Network (VPN) Remote Access #1065
oo. HHF Breach Tool

Comprehensive Written Information Security Program for 201 CMR 17.00

201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth is the regulation that implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own or license personal information (*PI*) about a resident of the Commonwealth of Massachusetts. As a part of the requirements of this regulation, Home Health Foundation and its subsidies is creating, implementing and training employees on this written information security program (*WISP*).

The information contained herein is a part of the Corporate Compliance Program at Home Health Foundation.

I. OBJECTIVE

HHF has developed this to create effective administrative, technical and physical safeguards for the protection of personal information for the residents of the Commonwealth of Massachusetts, as well as our employees, and to comply with our obligations under 201 CMR 17.00.

The WISP sets forth our procedure for evaluating and addressing our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information of residents of the Commonwealth of Massachusetts.

For purposes of this WISP, “personal information” is as defined in the regulations: a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident:

a. Social Security number;
b. Driver's license number or state-issued identification card number; or
c. 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; provided, however, that “personal information” shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

II. PURPOSE

The purpose of the WISP is to promote achievement of the following:

1. Ensure the security and confidentiality of personal information;
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information; and
3. Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

III. SCOPE

In formulating and implementing the WISP, HHF has addressed and incorporated the following protocols:

1. Identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information;
2. Assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;
3. Evaluated the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks;
4. Designed and implemented a WISP that puts safeguards in place to minimize those risks, consistent with the requirements of 201 CMR 17.00; and
5. Implemented regular monitoring of the effectiveness of those safeguards.

IV. RESPONSIBILITY FOR INFORMATION SECURITY – Security Manager

HHF has designated the V.P. of Quality, Compliance and Risk to implement, supervise, delegate authority and maintain the WISP. The V.P. of Quality, Compliance and Risk has delegated information security responsibility to the Director of Information Technology (Security) and to the Health Information and Compliance Coordinator (Health Information Privacy). These designated employees (the “Data Security Coordinators”) will be responsible for the following:

1. Implementation of the WISP including all provisions outlined in Section VI;
2. Daily operation protocols;
3. Training of all employees;
4. Regular testing of the WISP's safeguards;
5. Evaluating the ability of any of our third-party service providers to implement and maintain appropriate security measures for the personal information to which we have permitted them access, and requiring such third-party service providers by contract to implement and maintain appropriate security measures;
6. Reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing personal information;
7. Reviewing and revising any and all sections of this WISP as appropriate, as a result of an investigation of a data breach of personal information; and
8. Conducting training sessions for all managers, employees and independent contractors, including temporary and contract employees who have access to personal information on the elements of the WISP.

V. INTERNAL RISKS – MITIGATION/SAFEGUARDS

The following areas have been identified as reasonably foreseeable internal and external risks and have been assessed, considering the safeguards which are implemented as part of this WISP as noted:

1. **Personal information is used during the quoting of prospective accounts and the servicing and remarketing of existing clients' accounts.**
   - Some of this PI is found on paper records and files that are maintained at employees' desks for the period of time that the corresponding accounts are being worked.
   - Upon completion of the tasks and work corresponding to the paper records and files for these documents are then placed in a shred bin on the Agency floor until a third-party service provider, a shredding company, is called to come and dispose of these papers via shredding. A receipt and certificate of destruction is provided once the papers have been shredded.
   - PI is also found in an electronic format in the agency management system and in a separate document management system (that contains both client and employee information). All Agency employees have a unique used id and password for both systems that contain PI, and security permissions are set to restrict access to employee data to management only.

2. **All Agency employees have physical access to the few filing cabinets that are maintained at the Agency that contain PI. All Agency employees are deemed to have a true, business-related need, to have access to said information.**

3. **PI is also transmitted via email during the course of normal Agency operations. Most often this information is regarding start of care and is via (documents) attached to the emails. Internal email within our systems is encrypted.**

To guard against internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where

necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are employed:

1. We will only collect personal information of patients, customers or employees that is necessary to accomplish our legitimate business transactions or to comply with any and all federal, state or local regulations.
2. Access to records containing personal information shall be limited to those employees whose duties, relevant to their job description, have a legitimate need to access said records, and only for this legitimate job-related purpose.
3. Written and electronic records containing personal information shall be securely destroyed or deleted at the earliest opportunity consistent with business needs or legal retention requirements.
4. Our frequent business records associated retention and secure destruction periods are included in Destruction of PHI #7033.
5. A copy of the WISP/PHI Considerations is to be distributed to employees at new employee orientation. It shall be the employee's responsibility for acknowledging in writing, by signing the acknowledgement sheet, that he/she has received a copy of the WISP and will abide by its provisions. Employees are encouraged and invited to advise the WISP Data Security Coordinators of any activities or operations which appear to pose risks to the security of personal information. If the Data Security Coordinators is him or herself involved with these risks, employees are encouraged and invited to advise any other manager or supervisor or business owner.
6. All employment contracts, where applicable, will be amended to require all employees to comply with the provisions of the WISP and to prohibit any nonconforming use of personal data as defined by the WISP.
7. Terminated employees must return all records containing personal data, in any form, in their possession at the time of termination. This includes all data stored on any portable device and any device owned directly by the terminated employee
8. A terminated employee's physical and electronic access to records containing personal information shall be restricted at the time of termination. This shall include remote electronic access to personal records, voicemail, internet, and email access. All keys, keycards, access devices, badges, company IDs, business cards, and the like shall be surrendered at the time of termination.
9. Disciplinary action will be applicable to violations of the WISP, irrespective of whether personal data was actually accessed or used without authorization. All security measures including the WISP shall be reviewed at least annually to ensure that the policies contained in the WISP are adequate meet all applicable federal and state regulations.
10. Should operation practices change in a way that impacts the collection, storage, and/or transportation of records containing personal information the WISP will be reviewed to ensure that the policies contained in the WISP are adequate meet all applicable federal and state regulations.
11. The Data Security Coordinator(s) or designee shall be responsible for all review and modifications of the WISP and shall fully consult and apprise V.P. of Quality, Compliance and Risk of all reviews including any recommendations for improves security arising from the review.

12. The Executive Administrative Assistant to the CEO, or designee shall maintain a secured and confidential master list of all lock combinations, passwords, and keys. The list will identify which employees possess keys, keycards, or other access devices and that only approved employees have been provided access credentials.
13. The Data Security Coordinators or his/her designee shall ensure that access to personal information in restricted to approved and active user accounts.
14. Current employees' user ID's and passwords shall conform to accepted security standards. All passwords shall be changed at least every 90 days, more often as needed.
15. Employees are required to report suspicious or unauthorized use of personal information to a supervisor, Data Security Coordinators or V.P. Of Quality, Compliance and Risk.
16. Whenever there is an incident that requires notification pursuant to the Security Breach Notifications of Massachusetts General Law Chapter 93H: "Security Breaches", the V.P. of Quality, Compliance and Risk or designee shall conduct root cause and post-incident review of events and actions taken, if any, in order to determine how to alter security practices to better safeguard personal information.

VI. EXTERNAL RISKS – MITIGATION/SAFEGUARDS

To guard against external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are employed:

1. Firewall protection, operating system security patches, and all software products shall be reasonably up-to-date and installed on any computer that stores or processes personal information.
2. Personal information shall not be removed from the business premises in electronic or written form absent legitimate business need and use of reasonable security measures, as described in this policy.
3. All system security software including, anti-virus, anti-malware, and internet security shall be reasonably up-to-date and installed on any computer that stores or processes personal information.
4. There shall be secure user authentication protocols in place that:
    a. Control user ID and other identifiers;
    b. Assigns passwords in a manner that conforms to accepted security standards, or applies use of unique identifier technologies;
    c. Control passwords to ensure that password information is secure.

VII. DAILY OPERATION and RECORD KEEPING PROTOCOLS

This section of our WISP outlines our daily efforts to minimize security risks to any computer system that processes or stores personal information, ensures that physical files containing personal information are reasonable secured and develops daily employee practices designed to minimize access and security risks to personal information of our clients and/or customers and employees.

Daily Operation Protocols shall be reviewed and modified as deemed necessary. Any modifications to the Daily Operation Protocols shall be published in an updated version of the WISP.

Recordkeeping Protocols: We will only collect personal information of clients and customers and employees that is necessary to accomplish our legitimate business transactions or to comply with any and all federal and state and local laws.

The Daily Operation Protocols and the Recordkeeping Protocols are made up of the following features:

1. Any personal information stored shall be disposed of when no longer needed for business purposes or required by law for storage. Disposal methods must be consistent with those prescribed by the WISP.
2. Any paper files containing personal information of patients or employees shall be stored in a locked filing cabinet. The V.P. of each company will determine a limited list of employees who will maintain the keys to the secured data location and the Data Security Coordinators will be assigned keys to filing cabinets to only those individuals are allowed access to the paper files.
3. Individual files may be assigned to employees on an as-needed basis by the department supervisor.
4. All employees are prohibited from keeping unsecured paper files containing personal information in their work area when they are not present (e.g. lunch breaks).
5. At the end of the day, all files containing personal information are to be returned to the locked filing cabinet by all employees. Department heads, managers or coordinators are responsible for assuring adherence.
6. The Compliance Department or IT Department will conduct periodic, unannounced work space audits to assess for the existence of unsecured personal information.
7. Paper or electronically stored records containing personal information shall be disposed of in a manner that complies with M.G.L. c. 93I sec. 2 (See Attachment D: Standards for disposal of records containing personal information; disposal by third party; enforcement) and as follows:
    a. Paper documents containing personal information shall be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed;
    b. Electronic media and other non-paper media containing personal information shall be destroyed or erased so that personal information cannot practicably be read or reconstructed.
    c. Electronic records containing personal information shall not be stored or transported on any portable electronic device, sent or transmitted electronically to any portable device, or sent or transported electronically to any computer, portable or not, without being encrypted. The only exception shall be where there is no reasonable risk of unauthorized access to the personal information or it is technologically not feasible to encrypt the data as and where transmitted.
    d. If necessary for the functioning of individual departments, the department head, in consultation with the Data Security Coordinators or V.P. of Quality, Compliance

and Risk, may develop departmental rules that ensure reasonable restrictions upon access and handling of files containing personal information and must comply with all WISP standards. Departmental rules are to be published as an addendum to the WISP and be added to the Information Security Plan.

Access Control Protocols

HHF shall control access to personal information based upon employee role. We shall also apply the standard of minimum necessary and limit data sets to those required to successfully complete required job tasks. We shall employ the following:

1. All our computers shall restrict user access to those employees having an authorized and unique log-in ID assigned by the Information Technology Department.
2. All computers that have been inactive for 5 or more minutes shall require relog- in.
3. After 5 unsuccessful log-in attempts by any user ID, that user ID will be blocked from accessing any computer or file stored on any computer until access privileges are reestablished by the Data Security Coordinators or his/her designee.
4. Access to electronically stored records containing personal information shall be electronically limited to those employees having an authorized and unique login ID assigned by the Data Security Coordinators.
5. Where practical, all visitors who are expected to access areas other than the lobby space at all work locations or are granted access to office space containing personal information should be required to sign-in with a Photo ID at a designated reception area where they will be assigned a visitor's ID or guest badge. Visitors are required to wear said visitor ID in a plainly visible location on their body, unless escorted at all times.
6. Where practical, all visitors are restricted from areas where files containing personal information are stored. Alternatively, visitors must be escorted or accompanied by an approved employee in any area where files containing personal information are stored.
7. Cleaning personnel (or others on site after normal business hours and not also authorized to have access to personal information) are not to have access to areas where files containing personal information are stored.
8. All computers with an internet connection or any computer that stores or processes personal information must have a reasonably up-to-date version of software providing virus, anti-spyware and anti-malware protection installed and active at all times.
9. An inventory of all company computers and handhelds authorized for personal information storage is contained in HIPAA/HITECH Risk Assessment Year End 2018, which shall be made known only to the Data Security Coordinators and other managers on a "need to know" basis.

Third Party Service Provider Protocols

Any service provider or individual that receives, stores, maintains, processes, or otherwise is permitted access to any file containing personal information ("Third Party Service Provider") shall be required to meet the following standards as well as any and all standards of 201 CMR 17.00. (Examples include third parties who provide off-site backup storage copies of all our electronic data; paper record copying or storage service providers; contractors or vendors working with our customers and having authorized access to our records):

1. Any contract with a Third-Party Service Provider signed on or after March 1, 2010 shall require the Service Provider to implement security standards consistent with 201 CMR 17.00.
2. It shall be the responsibility of the V.P. of Quality, Compliance and Risk or designee to obtain reasonable confirmation that any Third-Party Service Provider is capable of meeting security standards consistent with 201 CMR 17.00.
3. Any existing contracts with Third Party Service shall be reviewed by the V.P. of Quality, Compliance and Risk or designee. These Service Providers shall meet the security standards consistent with 201 CMR 17.00 by March 1, 2012 or other Service Providers will be selected, when feasible to do so.
4. A list of currently known third party service providers is contained in Attachment B: Third Party Service Providers

VIII. Breach of PI Data Security Protocol

Should any employee know of a security breach at any of our facilities, or that any unencrypted personal information has been lost or stolen or accessed without authorization, or that encrypted personal information along with the access code or security key has been acquired by an unauthorized person or for an unauthorized purpose, the following protocol is to be followed:

1. Employees are to notify the V.P. of Quality, Compliance and Risk and/or Data Security Coordinators in the event of a known or suspected security breach or unauthorized use of personal information.
2. The V.P. of Quality, Compliance and Risk shall be responsible for drafting a security breach notification to be provided to the Massachusetts Office of Consumer Affairs and Business Regulation and the Massachusetts Attorney General's office. The security breach notification shall include the following (also see Appendix).:
    a. A detailed description of the nature and circumstances of the security breach or unauthorized acquisition or use of personal information;
    b. The number of Massachusetts residents affected at the time the notification is submitted;
    c. The steps already taken relative to the incident;
    d. Any steps intended to be taken relative to the incident subsequent to the filing of the notification; and
    e. Information regarding whether law enforcement officials are engaged in investing the incident
3. The notice to the Attorney General and the Director of Consumer Affairs and Business Regulation will also require to certify that credit monitoring services comply with Section 3A.
4. HHF shall provide notice as soon as practicable and without unreasonable delay (a) when it knows or has reason to know of a PI security breach, or (b) knows or has reason to know that PI was acquired or used by an unauthorized person or used for an unauthorized purpose (see Appendix).
5. The V.P. of Quality, Compliance and Risk shall be responsible for drafting a security breach notification to be provided to the Massachusetts Residents impacted. The security breach notification shall include the following (also see Appendix):
    a. the consumer's right to obtain a police report;

b. how a consumer requests a security freeze;
c. the necessary information to be provided when requesting the security freeze; and
d. that there shall be no charge for a security freeze; provided however, that the notification shall **not** include:
e. the nature of the breach or unauthorized acquisition or use; or
f. the number of Massachusetts residents affected by the security breach or the unauthorized access or use.

6. Per April 2019 Amendment, "A notice [to the Massachusetts Residents impacted] provided pursuant to this section shall not be delayed on grounds that the total number of residents affected is not yet ascertained. In such case, and where otherwise necessary to update or correct the information required, a person or agency shall provide additional notice as soon as practicable and without unreasonable delay upon learning such additional information."
7. Whenever there is a PI security breach or unauthorized use of PI, there shall be an immediate mandatory post-incident review of events and actions taken, if any, to determine whether any changes to HHF's security practices and the WISP are required to improve the security of PI for which HHF is responsible.

Appendix

Requirements for Security Breach Notifications under Chapter 93H

Pursuant to M.G.L. c. 93H, s. 3(b), if you own or license data that includes personal information of a Massachusetts resident, you are required to provide written notice **as soon as practicable and without unreasonable delay** to:

1. The Attorney General (AGO);
2. The Director of the Office of Consumer Affairs and Business Regulation (OCABR); and
3. The affected Massachusetts resident

When you know or have reason to know (a) of a breach of security; **or** (b) that personal information of a Massachusetts resident was acquired by or used by an unauthorized person or used for an unauthorized purpose.

Credit Monitoring Changes

Eighteen (18) months of credit monitoring services are now required per April 2019 Amendment.

Notice to the AGO and OCABR

The notice to the Attorney General and the Director of Consumer Affairs and Business Regulation shall include, but not be limited to:

1. the nature of the breach of security or the unauthorized acquisition or use;
2. the number of Massachusetts residents affected by such incident at the time of notification; the name and address of the person or agency that experienced the breach of security;
3. the name and title of the person or agency reporting the breach of security, and their relationship to the person or agency that experienced the breach of security;
4. the type of person or agency reporting the breach of security;
5. the person responsible for the breach of security, if known;

6. the type of personal information compromised, including but not limited to, social security number, driver's license number, financial account number, credit or debit card number or other data;
7. whether the person or agency maintains a written information security program; and
8. any steps the person or agency has taken or plans to take relating to the incident, including updating the WISP.

The notice to the Attorney General and the Director of Consumer Affairs and Business Regulation will also require that they certify that credit monitoring services comply with Section 3A.

See Attorney General Template below.

Notice to Affected Massachusetts Residents

A person or agency that has experienced a breach of security or the unauthorized acquisition or use of personal information of Massachusetts residents must also provide notice to those affected Massachusetts residents. This notice shall include, but not be limited to:

1) the consumer's right to obtain a police report;
2) how a consumer requests a security freeze;
3) the necessary information to be provided when requesting the security freeze; and
4) that there shall be no charge for a security freeze; provided however, that the notification shall **not** include:

a) the nature of the breach or unauthorized acquisition or use; or
b) the number of Massachusetts residents affected by the security breach or the unauthorized access or use.

Per April 2019 Amendment, "A notice provided pursuant to this section shall not be delayed on grounds that the total number of residents affected is not yet ascertained. In such case, and where otherwise necessary to update or correct the information required, a person or agency shall provide additional notice as soon as practicable and without unreasonable delay upon learning such additional information."

ATTORNEY GENERAL NOTIFICATION TEMPLATE LETTER

Attorney General Maura Healey
Office of the Attorney General
One Ashburton Place, 20th Floor
Boston, MA 02108

Dear Attorney General Healey:

Pursuant to M.G.L., c. 93H, we are writing to notify you of a (a breach of security/an unauthorized access to use of personal information) involving (number) Massachusetts resident (s).

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OF ACCESS
(Incident description)

NUMBER OF MASSACHUSETTS RESIDENTS AFFECTED
(This paragraph should specify the number of affected individuals residing in Massachusetts whose personal information was the subject of the incident. This paragraph should also indicate that these Massachusetts residents have received or will shortly receive notice pursuant to M.G.L. c. 93H, s. 3(b) and should specify the manner in which Massachusetts residents have or will receive such notice. Also include a copy of the notice to affected Massachusetts residents in your notification to the Attorney General).

STEPS TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT
(outline the steps taken or plan to take relating to the incident including without limitation, what was discovered during the incident, reported the incident to law enforcement; evidence of personal information has been used for fraudulent purposes; whether credit monitoring was offered to consumers; and what measures you have taken to ensure that similar incidents do not occur in the future.)

OTHER NOTIFICATION AND CONTACT INFORAMTION
(Indicate whether we provided similar notification to the Director of Consumer Affairs and Business Regulation. Include the name and contact information for the person whom the Office of the Attorney General may contact if there are any additional questions)

TEMPLATE LETTER TO AFFECTED MASSACHUSETTS RESIDENTS

Date

Consumer Name
Address
City, MA

Dear _____:

We are writing to notify you that a [breach of security/unauthorized acquisition or use] of your personal information occurred on [date(s)].

YOUR NOTICE MUST INCLUDE THE FOLLOWING INFORMATION:

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;

8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

[**NOTE: Although not required by M.G.L. c. 93H, you should also consider providing the affected Massachusetts residents with additional information to protect themselves against identity theft or other fraud including, but not limited to: the placement of fraud alerts on their credit file; the need to review their credit reports for unexplained activity; and the need to review credit card or other financial accounts for any suspicious and/or unauthorized activity. Many companies provide affected Massachusetts residents with free credit monitoring services. If you are providing credit monitoring services for affected Massachusetts residents, you should provide them with information concerning how they may enroll for such credit monitoring services as well as any telephone numbers or websites that you have set up to answer any questions they may have concerning the incident. Please note that any additional advice provided to affected Massachusetts residents may vary on a case-by-case basis and these information suggestions are not a complete list of all the information that you may want to provide affected Massachusetts residents to better protect themselves against identity theft or fraud].**

If you should have any further questions, please contact [provide contact information].

Sincerely,