21961

Beth Israel Lahey Health
Primary Care

Please Read This Important Notice

July 29, 2021

Dear Patient,

We are writing to notify you of an incident that involved your information. On June 4, 2021, Beth Israel Lahey health Primary Care (BILHPC) learned of an incident that involved your personal and protected health information, including your name, address, date of birth, checking account number and medical record number.

BILHPC takes this incident and the protection of your information extremely seriously. We apologize for the inconvenience and deeply regret any concern this situation may have caused. BILHPC believes that it is important for you to be fully informed of any potential risk resulting from this incident.

We are attaching a brief guide to identity theft, which includes useful resources as well as information on filing a report with the police, requesting a security freeze from the credit reporting agencies, and tips on monitoring your accounts and information for indications of identity theft.

Additionally, we will provide complimentary credit monitoring services to you for eighteen months. If you are interested in making use of the complimentary credit monitoring services, please contact us by e-mail at BILHPCCompliance@bidmc.harvard.edu.

BILHPC is committed to maintaining the privacy of our patient's information and proactively takes precautions to maintain the integrity and security of that information. We continually test and modify systems, while aggressively enhancing practices to secure patient information. In this case, involved staff and/or vendors have completed re-education and revised their work processes to prevent a similar incident from occurring in the future.

If you wish to speak to someone at BILHPC about this notice, you may contact us directly at (617) 667-7259 or (617) 754-0541 between 9am and 5pm, Monday through Friday. If we are not available to take your call, please state in your message that you are calling about this letter and we will call you back as soon as possible.

Sincerely,
Lori A. Soares
Physician Practice Compliance Specialist
Ofc. of Integrity and Compliance
Beth Israel Lahey Health Primary Care
Tel. (617) 667-7259
Lsoares2@bilh.org

Beth Israel Lahey Health
Primary Care

## A Brief Guide to Identity Theft Resources

If you discover that someone has misused your personal information, there are several important steps you should take to protect yourself. A number of State and Federal authorities and consumer groups have prepared literature to explain resources available to you and you can learn more by visiting their websites or contacting them at:

**Federal Trade Commission**
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580
www.ftc.gov/idtheft
To Report Fraud:
1-(877) IDTHEFT (438-4338)
TTY: 1-866-653-4261

**Office of Attorney General Maura Healy**
One Ashburton Place
Boston, MA 02108-1518
www.mass.gov/ago
Tel.: (617) 727-2200
Consumer Hotline:
(617) 727-8400

**National Crime Prevention Council**
2001 Jefferson Davis Highway
Suite 901
Arlington, VA 22202
www.ncpc.org
Tel. (202) 466-6272

In addition, you can visit websites run by a number of government agencies and private companies to get helpful information and advice:

U.S. Department of Justice: www.usdoj.gov/criminal/fraud/websites/idtheft.html

U.S. Postal Inspection Service: https://postalinspectors.uspis.gov/

U.S. Secret Service: www.secretservice.gov/criminal.shtml

Federal Deposit Insurance Corporation: www.fdic.gov/consumers

Federal Reserve Bank of Boston: www.bos.frb.org/consumer/identity/index.htm

American Express: www.americanexpress.com/idtheftassistance/

Call for Action: http://www.callforaction.org/?cat=10

While these organizations can explain the tools available to you in detail, victims of identity theft are generally encouraged to do the following:

**Contact Your Banks & Credit Card Companies**: The first step in dealing with ongoing identity theft is to contact the financial institutions, banks and credit card companies that may be involved to notify them that someone has stolen your identity.

**Contact the Police**: If you find suspicious activity in your credit reports or you believe that your personal information has been misused, you have a right to obtain a police report. Call your local police department to file a police report. Remember to ask for a copy of the police report because creditors may request a copy of the police report before they remove errors or fraudulent transactions from your credit record.

**Contact a Credit Reporting Agency**: Three credit reporting agencies —Equifax, Experian and TransUnion — keep track of your credit report. When you know that someone has stolen your identity, you should call one of these agencies and report the fraud. You may contact the credit reporting agencies at the telephone numbers and addresses listed below:

**Equifax**
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com
To obtain your credit report: (800) 685-1111
To report fraud: (800) 525-6285

**Experian**
P.O. Box 9532
Allen, TX 75013
www.experian.com
To report fraud or obtain your credit report:
(888) EXPERIAN (397-3742)

**TransUnion**
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com
To obtain your credit report: (800) 916-8800
To report fraud: (800) 680-7289

**Place A Restriction On Your Credit Records**: Another way to protect yourself is to restrict access to your credit report. There are two kinds of restrictions. A "fraud alert" is a temporary restriction that requires potential creditors to take additional steps to confirm your identity when someone applies for credit and attempts to open an account in your name. A "security freeze" is a stronger option created by Massachusetts law that requires credit reporting agencies to contact you directly before releasing your credit report to a potential creditor.

**Fraud Alert**: A fraud alert is a notice that the credit reporting agencies attach to your credit report that requires all potential creditors to use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name. A fraud alert lasts for 90 days and you can initiate an alert by calling one of the credit reporting agencies listed above (Equifax, Experian or TransUnion). You are likely to speak with an automated call attendant, so we recommend that you follow up with a written request. You only need to contact one of the three agencies to place an alert. The agency you call is required to contact the other two. As a result, all three agencies should send you a letter confirming the fraud alert and letting you know how to get a free copy of your credit report. If you do not receive a confirmation from one or more of the agencies, you should contact that company directly to place a fraud alert. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

**Security Freeze**: Placing a security freeze on your credit file will tell the credit reporting agencies to contact you before allowing anyone to access your credit report. This means that potential creditors will not be able to get access to your credit report — for example, to open new accounts or obtain loans — unless you temporarily lift the freeze. When you place a security freeze, the credit reporting agency that you contact will provide you with a personal identification number or password to use if you wish to release your credit information to a specific person or financial institution or when you remove the security freeze from the credit file. Please note that because a security freeze adds an additional layer of security, it may delay your ability to obtain credit while the security freeze is in effect.

*Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past two years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.

**Keep Your Eyes Open for Potential Identity Theft**: Even if you do not find any suspicious activity on initial credit reports, the FTC recommends that you check your credit reports periodically. Victim information sometimes is held for later use or shared among a group of identity thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

**Beth Israel Deaconess HealthCare**
**Written Information Security Program (WISP)**

**TITLE:** Written Information Security Program

**Objective**

The Beth Israel Deaconess HealthCare (BIDHC) Written Information Security Program (WISP) is a comprehensive set of guidelines and policies implemented in compliance with Massachusetts General Laws 201 CMR 17 "Standards for The Protection of Personal Information of Residents of the Commonwealth", as well as other federal and state regulations and standards. This plan is reviewed periodically and amended as necessary to protect personal information.

**Definitions**

I. Personal Information ("PI"), as defined by Massachusetts law (201 CMR 17.00), is the first name and last name or first initial and last name of a person in combination with any one or more of the following:

- Social Security number;
- Driver's license number or state-issued identification card number; or
- Financial account number (e.g. bank account) or credit or debit card number that would permit access to a person's financial account, with or without any required security code, access code, personal identification number, or password.

For the purposes of this Program, PI also includes passport number, alien registration number or other government-issued identification number.

II. Employees. Defined a workforce members including Providers, Contractors, Scribes, Students, Interns and Staff.

**Program**

**I. Administrative, Technical, and Physical Controls to Protect PI**

BIDHC maintains administrative, technical and physical controls to protect Personal Information (PI):

a. Administrative controls include, but are not limited to the corporate policies located in the BIDHC online policy manual. Access to institutional information is based on the need to know concept, where access to information is granted to those persons whose job duties and scope of employment create a need to know. Security practices are reviewed, modified and/or added based on business need, research, regulation, and evaluation of the threat landscape.

b. Technical controls include but are not limited to perimeter firewalls, intrusion prevention systems, interior firewalls, encryption, authentication and authorization systems, system logging, file backup, virtual private networks, and network monitoring solutions.

c. Physical controls include but are not limited to physical key card/key access control systems, locking mechanisms for areas and devices containing sensitive information and information processing assets, physical intrusion detection systems with central monitoring, monitoring and

recording systems, fire detection, reporting and suppression systems, and water leak detection systems.

## II. Designated Employees to Maintain Security Plan (201 CMR 17.03(a))

BIDHC maintains a comprehensive information security program. The administration of the program is a coordinated response between the Chief Information Officer, BILH Chief Information Security Officer, BIDHC Director of Compliance- Primary and Specialty Care.
The WISP is updated as needed and at least annually by the Chief Information Officer, BILH Chief Information Security Officer, BIDHC Director of Compliance- Primary and Specialty Care.

## III. Internal and External Risk Assessment (201 CMR 17.03(b))

In order to assess any risks of access to personal information, as part of the IT Analysis Inventory, BIDHC has evaluated where that information may be present. BIDHC may keep information or other sensitive information securely in our filing cabinets and off-site servers. Our internal computers are protected behind a firewall.
BIDHC continuously evaluates reasonably foreseeable internal risks to all forms of PI. These evaluations are performed in the normal course of business. Recommendations arising from these efforts are returned to the appropriate department or practice for consideration and implementation.
BIDHC employees may from time to time need access to personal information. In order to insure that none of this information is vulnerable to a breach, we have implemented the following policies:

- Computer Hardware Policy
- Access and Password Policy
- ADM-17 Records Management Policy
- ADM-31 BIDHC Practices – Phone Downtime
- BILHPC Remote Work Policy
- Clinical and Medical Students Policy
- Safeguarding and Protecting Protected Health Information (PHI) and Personal Information (PI)
- ADM-4 Hotline and Reporting Policy
- Inspection, Access to or Copying of Medical Information Policy- Protected Health Information (PHI) and Personal Information (PI)
- Electronic Communications and Information Policy
- Corrective Action Policy
- Compliance Training and Education Policy
- ADM-28 External audit requests

### a. Employee Training (201 CMR 17.03(b)(i))

All employees are responsible for maintaining the privacy and integrity of personal information. Any paper record containing personal information about any patients, employees or third party must be kept behind lock and key when not in use. Any digital file containing personal information is saved on off-site servers that unique access IDs and password, or they are saved on local encrypted

hard drives. No personal information is to be disclosed without first fully authenticating the receiving party.
Paper records containing personal information are securely shredded. An outside shredding service is used (Vendor Shred-It). Similar appropriate electronic methods are used for disposing of electronic media as per the ADM-17 Records Management Policy
Human Resources trains all new employees on this policy, and there are also periodic reviews for existing employees as part of the annual Keep Information Private Program (KIP) and Annual Compliance Training.

b. Employee Compliance (201 CMR 17.03(b)(ii))

Any employee who discloses personal information or fails to comply with these policies will face immediate disciplinary action including the possibility of termination.

c. Detecting and Preventing Security System Failures (201 CMR 17.03(b)(iii))

BIDHC provides regular network security audits in which all server and computer system logs are evaluated for any possible electronic security breach. Audits are performed by Beth Israel Deaconess Medical Center (BIDMC) and business associate Versatile Health on behalf of BIDHC. Additionally, all employees are trained to watch for any possible physical security breach, such as unauthorized personnel accessing file cabinets or computer systems. Failures are reported to appropriate staff via event messages sent via email. Prevention of system failures is accomplished by implementation of failover systems, rigorous attention to maintaining all security systems with current operating system and application patches and fixes, and regular maintenance.

IV. Keeping, Accessing and Transporting Personal Information (201 CMR 17.03(c))

BIDHC takes all possible measures to ensure that employees are trained to keep all paper and electronic records containing personal information securely on-premises at all times. When there is a need to bring records containing personal information off-site, only the minimum information necessary will be brought; electronic records will be password-protected and encrypted, paper records will be kept behind lock and key. Records brought off-site should be returned to the BIDHC premises securely as soon as possible.
Under no circumstances are documents, electronic devices, or digital media to be left unattended in an employee's car, home, or in any other potentially insecure location.

V. Disciplinary Measures (201 CMR 17.03(d))

Any employee who willfully discloses personal information or fails to comply with these policies will face immediate disciplinary action including the possibility of termination.

VI. Prevention of Terminated Employees from Accessing Information (201 CMR 17.03(e))

Any terminated employees' computer access passwords will be disabled by means of notification from Human Resources or third party sponsors. In urgent situations where access must be

immediately terminated, a supervisor notifies the IS help desk service. Physical access to any documents or resources containing personal information will also be immediately discontinued by collection of keys and/or other access tokens used to access physical spaces. In certain cases, incremental situation specific safeguarding actions may be taken.

VII. Third-Party Service Providers (201 CMR 17.03(f))

Access to personal information by third-party service providers will be kept to a bare minimum. Any third party service provider who does require access to information will be fully vetted. A random post-access audit is performed to ensure compliance. BIDHC contracts with a third party service provider requires that the service provider protect and maintain PI consistent with Massachusetts data security regulations, including the existence of a Written Information Security Program (WISP).

VIII. Limiting Information Collected (201 CMR 17.03(g))

BIDHC is committed to collecting only the minimum of personal information necessary to accomplish business purposes or to comply with state or federal regulations. Information no longer needed for business purposes, is disposed of securely as per our ADM-17 Records Management Policy.

IX. Identifying Where Personal Information is Stored (201 CMR 17.03(h))

We have identified the locations where personal information is stored on our network. Personal information is stored in the following: Filing cabinets, off-site servers, and encrypted devices.

X. Physical Access Restrictions (201 CMR 17.03(i))

BIDHC offices and computer network are kept locked – third-parties are not allowed physical access to records. Paper files that are not currently in use are kept locked in filing cabinets. In addition, electronic records are kept in databases and on off-site servers which are behind multiple layers of electronic safeguards.

XI. Monitoring and Upgrading Information Safeguards (201 CMR 17.03(j))

BIDMC Information Security (IS) and business associate Versatile Health continually monitor and annually assess all of our information safeguards to determine when upgrades may be necessary. Issues escalated to Chief Information Officer. Emergent issues may be sent to all users via email.

XII. Annual Review (201 CMR 17.03(k))

The WISP is updated as needed and at least annually by the Chief Information Officer, BILH Chief Information Security Officer, BIDHC Director of Compliance- Primary and Specialty Care.

XIII. Documenting and Reviewing Breaches (201 CMR 17.03(l))

BIDHC relies on the BIDMC computer security incident response protocol and observes the FTC mandated "Red Flags" protocol. As the computer security incident protocol is executed, BIDMC documents actions taken and performs a post incident review to improve security where technically, operationally and financially feasible.

XIV. Computer System Requirements (201 CMR 17.04)

To combat external risk and security of our network and all date, we have implemented the following:

a. Secure user authentication protocols:
(201 CMR 17.04(1)(i, ii, iii, iv, v))

- Unique 16-18 character passphrase is required for all user accounts; all employees receive their own user accounts.
- For active directory authenticated resources, access is blocked for 30 minutes after 6 successive failed authentication attempts. Adaptive Authentication is in place for SSL VPN access.
- Any terminated employees' computer access passwords are disabled as noted in section VI

b. Secure access control measures: (201 CMR 17.04(2)(i, ii))

- Only Employees that need access the personal information are given access to proper folders
- Each person has a unique password to the computer network. These passwords are not assigned by any vendor.

c. Encryption on Public Networks
(201 CMR 17.04(3))

We do not transmit unencrypted Personal Information across public networks under any circumstances.

d. Reasonable monitoring (201 CMR 17.04(4))

Audits are performed by Beth Israel Deaconess Medical Center (BIDMC) and business associate Versatile Health on behalf of BIDHC. Issues escalated to Chief Information Officer. Emergent issues may be sent to all users via email.

e. Portable or Removable Devices
(201 CMR 17.04(5))

Any portable or removable device owned by BIDHC is encrypted prior to distribution to employees.

f. Security Updates and Patches: (201 CMR 17.04(6))

BIDHC uses perimeter access control lists, firewalls and intrusion prevention systems. Where technically permitted BIDHC owned and managed devices are "patched" automatically. In cases where the application of a patch may disrupt operations, patches may be applied manually.

g. Antivirus and Updates(201 CMR 17.04(7))

- All BIDHC owned and managed computers are automatically enrolled in a centralized update service for antivirus/malware protection. Virus definition updates are installed on a regular basis.

h. Education and training of employees on the proper use of the computer security system and the importance of personal information security. (201 CMR 17.04(8))

- All employees are responsible for maintaining the privacy and integrity of personal information. All employees have been trained that any paper record containing personal information about any client or third party must be kept behind lock and key when not in use. Human Resources trains all new employees on this policy, and there are also periodic reviews for existing employees as part of the annual Keep Information Private Program (KIP) and Annual Compliance Training.

**Owner:** Don Pare, Chief Information Officer

**Reviewed/Approved by:** Alex Barker, Chief Operating Officer- Regional South, BILHPC

**Regulatory Reference:** Massachusetts Regulations 201 CMR 17.00

**Reviewed/Updated:** 8/4/2021

**Next Review Date: 8/4/2022**