

10/7/2021

**CONFIDENTIAL**

Consumer Protection Bureau  
Office of the New Hampshire Attorney General  
33 Capitol Street  
Concord, NH 03301

RECEIVED

OCT 12 2021

CONSUMER PROTECTION

Re: Notice of Data Security Incident

To the Office of the Attorney General:

Brigham and Women's Hospital (BWH), a member of Mass General Brigham, is writing to notify you of a data security incident which may have involved the personal information of one resident in your state. A copy of the notification being sent to 1 New Hampshire resident via first-class mail on October 7, 2021 is attached to this letter.

On August 23, 2021, we learned that an approved user of clinical systems inappropriately accessed the electronic medical record of a BWH patient, without a job-related reason. An audit from January 1, 2019 to August 22, 2021 determined that multiple inappropriate accesses were made by this employee between June 3, 2020 and June 24, 2021.

We immediately began an investigation and determined that the information contained the patient's name, date of birth, address, phone number, medical record number, other demographics, insurance policy information, diagnosis, medications, medical/surgical/family history, recent appointments, clinical notes, and other clinical information was viewed.

Mass General Brigham has arranged to offer credit monitoring services for two years to the impacted New Hampshire resident whose personal information was involved.

If you have any questions, please call please contact the Brigham and Women's Privacy Office toll free at 833-294-2020 during the hours of 8:00am to 4:00pm Monday through Friday, or by email at [bwhcHIPAA@partners.org](mailto:bwhcHIPAA@partners.org). So we may better assist you, please reference incident case number: INC-871.


Sincerely,  
Tia Clayton  
HIPAA Privacy Specialist  
Brigham and Women's Hospital

Cc: James Contrino  
HIPAA Privacy Manager  
Brigham and Women's Hospital

Enclosure: Redacted Consumer Notification Letter



10/7/2021



*RE: Important Security Notification*  
*Please read this entire letter.*

Dear :

Brigham and Women's Hospital (BWH), a member of Mass General Brigham, is committed to protecting the security and confidentiality of our patients' information. Regrettably, we are writing to inform you of an incident involving some of that information and apologize for any concern this may cause.

On August 23, 2021, we learned that an approved user of clinical systems inappropriately accessed your electronic medical record without a job-related reason. An audit from January 1, 2019 to August 22, 2021 determined that multiple inappropriate accesses were made by this employee between June 3, 2020 and June 24, 2021. The information that may have been viewed contained your name, date of birth, address, phone number, medical record number, other demographics, insurance policy information, diagnosis, medications, medical/surgical/family history, recent appointments, clinical notes, and other clinical information. Please note that this incident **did not** involve access to any of your other financial information (e.g. social security number, credit account information, bank account information).

As a New Hampshire resident, you have the following rights:

- Right to obtain any police report filed regarding this incident.
- Right to file and obtain a copy of a police report if you are the victim of identity theft.
- Right to request that the credit bureaus place a security freeze on your file. Please refer to the enclosed information sheet for instructions on placing a security freeze on your credit report and additional steps you can take to further reduce any potential risk to you.

Additionally, we are offering you 24 months of free of credit monitoring and other services through Experian's IdentityWorks<sup>SM</sup>. More information on these Experian services, including instructions on how to activate the credit monitoring, is enclosed with this letter.

We sincerely regret any concern this may cause. BWH takes the privacy and security of our patients' information very seriously. We want to assure you that this matter was appropriately addressed with department leadership. To help prevent something like this from happening again, we continue to improve safeguards in place to protect your information (or to improve our business processes) and promote training and education of our employees.

If you have any questions, please call please contact the Brigham and Women's Privacy Office toll free at 833-294-2020 during the hours of 8:00 a.m. to 4:00 p.m. Monday through Friday, or by email at [bwhcHIPAA@partners.org](mailto:bwhcHIPAA@partners.org). So we may better assist you, please reference your incident case number: INC-871.

Sincerely,  
Tia Clayton  
HIPAA Privacy Specialist  
Brigham and Women's Hospital

Cc: James Contrino  
HIPAA Privacy Manager  
Brigham and Women's Hospital

Enclosure: Steps you can take to protect your identity  
Details on Experian IdentityWorks<sup>SM</sup>, including steps to activate the credit monitoring

## STEPS YOU CAN TAKE TO PROTECT YOUR IDENTITY

**Security Freeze.** A security freeze prevents credit reporting bureaus from releasing information in your credit file. This can make it harder for identify thieves to open new accounts in your name. Please be aware, however, that placing a security freeze on your credit report may delay approval of any requests you make for new loans, credit, mortgages, or other services.

You have the right to request a security freeze for free. To place a security freeze on your file, you must contact each of the three national credit reporting bureaus. You can contact them by phone, online submission, or mail.

<b>Equifax Information Services</b> P.O. Box 105788 Atlanta, GA 30348 1-800-685-1111  www.equifax.com/ personal/credit-report-services/	<b>Experian</b> P.O. Box 9554 Allen, TX 75013 1-888-397-3742  www.experian.com/help	<b>TransUnion</b> P.O. Box 2000 Chester, PA 19016 1-888-909-8872  www.transunion.com/ credit-help
---	--	---

When requesting a security freeze, you will need to provide information to confirm your identity, such as your name, proof of your current address, your prior address if you've moved in the last five years, your date of birth, Social Security number, and other personal information.

A security freeze request made by phone or online will be effective within one hour. Requests by mail take up to three business days from when the bureau gets it to be effective. After requesting a freeze, you will be given a unique personal identification number (PIN) and/or a password. Keep this in a safe place as you will need it to temporarily lift or fully remove the security freeze.

The freeze will remain until you ask the credit bureau to temporarily lift or fully remove it. If the request is made online or by phone, a credit bureau must lift security freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request. There is no charge for placing, lifting, or removing a security freeze.

**Review Your Account Statements.** Carefully review your bank, credit card, and other account statements every month to ensure that your account activity is valid. Report any questionable charges promptly and in writing to the card or account issuer.

**Check Your Credit Report.** Check your credit report to ensure that all your information is correct. You can obtain a free credit report once per year by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com) or by calling 877-322-8228. If you notice any inaccuracies, report the dispute right away to the relevant credit reporting bureau. You can file a dispute on the relevant bureau's website or by contacting them at the number listed on your credit report. You can also report any suspicious activity to your local law enforcement, in which case you should request a copy of the police report and retain it for your records.

**Fraud Alert.** You have the right to request that the credit bureaus place a fraud alert on your file. A fraud alert tells creditors to contact you before opening any new accounts or increasing credit limits on your existing accounts. A fraud alert lasts for one year and is free of charge.

You need to contact only one of the three credit bureaus to place a fraud alert; the one you contact is required by law to contact the other two. For Fraud Alerts, use the credit bureau contact information, provided above in the Security Freeze section.

**Consult the Federal Trade Commission.** For more guidance on steps you can take to protect your information, you also can contact the Federal Trade Commission at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), or at 877-ID-THEFT (877-438-4338), or at the Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580.

## Experian IdentityWorks<sup>SM</sup>

To help you detect the possible misuse of your personal information, we are providing you with a complimentary 24 month membership in Experian's IdentityWorks credit monitoring product at no cost to you.

This product helps detect possible misuse of your personal information and provides you with superior identity protection services focused on immediate identification and resolution of identity theft.

### **Activate EXPERIAN IDENTITYWORKS<sup>SM</sup> MEMBERSHIP Now in Three Easy Steps**

1. Ensure that you **enroll by: September 8, 2022** (After this date, your code will not work and you will not be able to enroll)
2. **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
3. Provide your **activation code:** [REDACTED]

If you have questions or need an alternative to enrolling online, please contact Experian's customer care team at 877-890-9332 by **September 8, 2022** and provide engagement #: [REDACTED]

### **ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP**

The Experian IdentityWorks enrollment and services are provided at no cost to you.

A credit card is **not** required for enrollment in Experian IdentityWorks.

You have automatic and immediate access to fraud assistance through Experian. Contact Experian if you believe there was fraudulent use of your information. Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE<sup>TM</sup>:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance<sup>\*\*</sup>:** Provides coverage for certain costs and unauthorized electronic fund transfers.

For additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s), refer to [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration).

\* Offline members will be eligible to call for additional reports quarterly after enrolling

\*\* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions