

November 12, 2025

[REDACTED]  
[REDACTED]  
[REDACTED]

Dear Mr. [REDACTED]:

I am writing on behalf of Mass General Brigham Home Care (MGBHC), a member of Mass General Brigham, to inform you of a recent issue concerning your protected health information.

On September 17, 2025, we discovered that an unauthorized third-party may have fraudulently gained access to your Mass General Brigham patient portal account. This account allowed access to your protected health information. Upon discovery, Mass General Brigham immediately deactivated this account and launched a thorough investigation. Our office also attempted to contact you by phone multiple times regarding this incident, most recently on October 17, 2025.

Our investigation revealed that the unauthorized access occurred on July 29, 2025. The third party viewed your information, including name, medical record number, date of birth, address, phone number, email, medications, lab results, medical conditions, and other treatment information, and downloaded a copy of your Massachusetts Driver's License. Importantly, this incident did **not** involve any access to your Social Security Number, financial account numbers, or credit card information.

As a Massachusetts 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.

MGBHC is committed to safeguarding your personal information and deeply regrets this incident. We have taken steps to prevent similar occurrences in the future, including deactivating your patient portal account and removing your driver's license from your electronic health record. We continue to strengthen our data protection measures and enhance workforce training and accountability.

If you wish to re-activate a patient portal account in the future, please contact our office directly. Additional protections have been placed on your account, and we will assist you in safely re-enrolling.

Mass General Brigham remains dedicated to providing the highest quality of care and service. If you

have any questions, please contact the Mass General Brigham Privacy Office at **855-726-1300** (Monday–Friday, 8:00 a.m.–4:00 p.m.) or email **privacyoffice@mgb.org**. When reaching out, please reference case number **PS INC-7503**.

Thank you.

Sincerely,

*Christine Griffin*

Christine M. Griffin  
MGB Privacy Manager

**Enclosures:    Steps you can take to protect your identity**

## **STEPS YOU CAN TAKE TO PROTECT YOUR PROTECTED HEALTH INFORMATION**

**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 statements sent to you from healthcare providers as well as from your insurance company to ensure that all of your account activity is valid. 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 to the provider or company with which you maintain the account.

**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.