ALSTON & BIRD
The Atlantic Building
950 F Street, NW
Washington, DC 20004-1404
202-239-3300 | Fax: 202-239-3333

Direct Dial: 202-239-3720

August 18, 2023

CONFIDENTIAL
VIA OVERNIGHT DELIVERY

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

Re: Notice of Data Security Incident

To the New Hampshire Attorney General's Office:

We are writing on behalf of Mass General Hospital ("MGH") and Brigham & Women's Hospital ("BWH"), members of Mass General Brigham ("MGB"), to notify you of a data security incident. A breakdown of individuals impacted by this incident by entity is provided in Attachment A. A copy of the notifications being sent to approximately three (3) affected New Hampshire residents on August 18, 2023 by first class mail in accordance with notification requirements under the federal Health Information Portability and Accountability Act (HIPAA) and state law is provided in Attachment B.

On June 20, 2023, it was discovered that five (5) student visitors, previously invited by a BWH staff member to visit the hospital for specific educational purposes, accessed MGH's and BWH's electronic health record (EHR) system, without authorization, on June 14, 2023 and June 20, 2023. Upon learning of the potential unauthorized access, MGH and BWH immediately began an investigation to determine what personal information of patients may have been accessed. MGH and BWH learned that the student visitors were able to access MGH's and BWH's EHR through an employee's BWH laptop. The students are no longer BWH visitors and do not have access to MGH's and BWH's systems. MGH and BWH conducted a comprehensive review to determine what information was accessed and to whom the information was related. This review was completed on August 9, 2023. Based on MGH's and BWH's review, while there was evidence of access to certain patient information, there is no evidence that patients' information was printed or downloaded and, to date, MGH and BWH has no knowledge that any personal information has been used improperly.

MGH and BWH take data security very seriously and have taken necessary and appropriate steps to prioritize the continued protection of personal information. In response to this incident and as part of its ongoing effort to stay ahead of evolving threats, MGH and BWH continue to improve safeguards in place to protect their patients' information and promote training and education of their employees, including regarding educational visits.

If you have any questions regarding this incident or if you desire further information or assistance, please email me at .

Sincerely,

Kimberly Peretti

Enclosures

Mass General Brigham

Brigham and Women's Hospital
Founding Member, Mass General Brigham
Brigham and Women's Faulkner Hospital
Health Information Management
T 617 582 5201
F 617 983 4789

August 18, 2023

[name]
[address]

Notice of Data Breach

Dear [name]:

Brigham & Women's Hospital (BWH), a member of Mass General Brigham (MGB), is committed to protecting the privacy and security of our patients' health information. Regrettably, we are writing to inform you of an incident involving some of your information.

What Happened?
On June 20, 2023, it was discovered that five (5) student visitors, previously invited by a BWH staff member to visit the hospital for specific educational purposes, accessed our electronic health record (EHR) system, without authorization, on June 14, 2023 and June 20, 2023.

Upon learning of the potential unauthorized access, we immediately began an investigation. We learned the student visitors were able to access our EHR through an employee's BWH laptop. The students are no longer BWH visitors and do not have access to our systems.

What Information Was Involved?

What We are Doing.
We sincerely apologize and regret that this incident occurred. We want to assure you this matter was appropriately addressed. To help prevent something like this from happening again, we continue to improve safeguards in place to protect your information and promote training and education of our employees, including regarding educational visits.

BWH is offering you of free credit monitoring and other services through Experian's IdentityWorks℠ More information on these Experian services, including instructions on how to activate the credit monitoring, is enclosed with this letter. You have until November 30, 2023 to enroll in these services.

What You Can Do.
In addition to enrolling in complimentary credit monitoring, the enclosed Reference Guide includes additional information on general steps you can take to monitor and protect your personal information. BWH encourages you to carefully review credit reports and statements sent from health care providers as well as your insurance company to ensure that all account activity is valid. Any questionable charges should be promptly reported to the company with which you maintain the account.

For More Information.
BWH deeply regrets any concern that this incident may cause and wants to assure you that we take this matter seriously.

Sincerely,

Debra Torosian
Health Information Management Director and Privacy Officer
Brigham and Women's Hospital

REFERENCE GUIDE

Provide any updated personal information to your health care provider. Your health care provider's office will ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office will also ask you to confirm your date of birth, address, telephone, and other pertinent information so that we can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit helps us to avoid problems, and address them quickly should there be any discrepancies.

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.

Equifax Information Services	**Experian**	**TransUnion**
P.O. Box 105788 Atlanta, GA 30348 1-800-685-1111 www.equifax.com/ personal/credit-report-services/	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/help	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 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:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(202) 326-2222
https://www.consumer.ftc.gov/topics/privacy-identity-online-security

For Residents of Massachusetts

You have the right to obtain a police report with respect 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.

Experian IdentityWorks℠

To help you detect the possible misuse of your personal information, we are providing you with a complimentary 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℠ MEMBERSHIP Now in Three Easy Steps

1. Ensure that you **enroll by: [date]** (After this date, your code will not work and you will not be able to enroll)
2. **Visit** the Experian IdentityWorks website to enroll: **[URL]**
3. Provide your **activation code: [code]**

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

ADDITIONAL DETAILS REGARDING YOUR 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™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** 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.

* 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.

Mass General Brigham

Brigham and Women's Hospital
Founding Member, Mass General Brigham
Brigham and Women's Faulkner Hospital
Health Information Management
T 617 582 5201
F 617 983 4789

August 18, 2023

Notice of Data Breach

Dear [name]:

Brigham & Women's Hospital (BWH), a member of Mass General Brigham (MGB), is committed to protecting the privacy and security of our patients' health information. Regrettably, we are writing to inform you of an incident involving some of your information.

What Happened?
On June 20, 2023, it was discovered that five (5) student visitors, previously invited by a BWH staff member to visit the hospital for specific educational purposes, accessed our electronic health record (EHR) system, without authorization, on June 14, 2023 and June 20, 2023.

Upon learning of the potential unauthorized access, we immediately began an investigation. We learned the student visitors were able to access our EHR through an employee's BWH laptop. The students are no longer BWH visitors and do not have access to our systems.

What We are Doing.
We sincerely apologize and regret that this incident occurred. We want to assure you this matter was appropriately addressed. To help prevent something like this from happening again, we continue to improve safeguards in place to protect your information and promote training and education of our employees, including regarding educational visits.

What You Can Do.
This incident did not involve access to your Social Security Number, health insurance information, financial account numbers, or credit card numbers. We are enclosing with this letter a list of various steps that you can take to protect your personal and health information.

For More Information.
BWH deeply regrets any concern that this incident may cause and wants to assure you that we take this matter seriously.

If you have any questions about the incident, please contact the Brigham and Women's Privacy Office toll free at during the hours of 8:00 a.m. to 4:00 p.m. Eastern Time Monday through Friday or by email at . We will make every effort to address any questions you may have.

Sincerely,

Debra Torosian
Health Information Management Director and Privacy Officer
Brigham & Women's Hospital

REFERENCE GUIDE

Review Your Account Statements. Carefully review statements sent to you from health care providers as well as from your insurance company to ensure that all of your account activity is valid. Report any questionable charges promptly to the provider or company with which you maintain the account.

Provide any updated personal information to your health care provider. Your health care provider's office will ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office will also ask you to confirm your date of birth, address, telephone, and other pertinent information so that we can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit helps us to avoid problems, and address them quickly should there be any discrepancies.

For Residents of Massachusetts

You have the right to obtain a police report with respect 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.

Consult the Federal Trade Commission. For more guidance on general steps you can take to protect your information, you also can contact the Federal Trade Commission:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(202) 326-2222
https://www.consumer.ftc.gov/topics/privacy-identity-online-security

Massachusetts General Hospital
Founding Member, Mass General Brigham

Health Information Management

55 Fruit Street, Austen 8-860
Boston, MA 02114
T 617 726 1098
F 617 643 4041
massgeneral.org

August 18, 2023

Notice of Data Breach

Dear [name]:

Massachusetts General Hospital (MGH), a member of Mass General Brigham (MGB), is committed to protecting the privacy and security of our patients' health information. Regrettably, we are writing to inform you of an incident involving some of your information.

What Happened?
On June 20, 2023, it was discovered that five (5) student visitors, previously invited by a staff member from one of our affiliated MGB hospitals, namely Brigham and Women's Hospital (BWH) to visit the hospital for specific educational purposes, accessed our electronic health record (EHR) system, without authorization, on June 14, 2023 and June 20, 2023.

Upon learning of the potential unauthorized access, we immediately began an investigation. We learned the student visitors were able to access our EHR through an employee's BWH laptop. The students are no longer BWH visitors and do not have access to our systems.

What We are Doing.
We sincerely apologize and regret that this incident occurred. We want to assure you this matter was appropriately addressed. To help prevent something like this from happening again, we continue to improve safeguards in place to protect your information and promote training and education of our employees, including regarding educational visits.

What You Can Do.
This incident did not involve access to your Social Security Number, health insurance information, financial account numbers, or credit card numbers. We are enclosing with this letter a list of various steps that you can take to protect your personal and health information.

For More Information.
MGH deeply regrets any concern that this incident may cause and wants to assure you that we take this matter seriously.

If you have any questions about the incident, please contact the MGH Privacy Office toll free at 877-644-2003during the hours of 8:00 a.m. to 4:00 p.m. Eastern Time Monday through Friday or by email at MGHPrivacyOffice@partners.org. We will make every effort to address any questions you may have.

Sincerely,

Mallory Getman
Privacy Manager
Massachusetts General Hospital

REFERENCE GUIDE

Review Your Account Statements. Carefully review statements sent to you from health care providers as well as from your insurance company to ensure that all of your account activity is valid. Report any questionable charges promptly to the provider or company with which you maintain the account.

Provide any updated personal information to your health care provider. Your health care provider's office will ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office will also ask you to confirm your date of birth, address, telephone, and other pertinent information so that we can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit helps us to avoid problems, and address them quickly should there be any discrepancies.

For Residents of Massachusetts

You have the right to obtain a police report with respect 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.

Consult the Federal Trade Commission. For more guidance on general steps you can take to protect your information, you also can contact the Federal Trade Commission:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(202) 326-2222
https://www.consumer.ftc.gov/topics/privacy-identity-online-security