



MASSACHUSETTS
GENERAL HOSPITAL

Health Information Services

FND-860

55 Fruit Street

Boston, Massachusetts 02114-2621

Tel: 617.726.2465

Fax: 617.643.4041

June 30, 2017

Office of the Attorney General

33 Capitol Street

Concord, NH 03301

Attn: Attorney General Joseph Foster

RECEIVED
JUL 05 2017
CONSUMER PROTECTION

Re: Incident Notification

To whom it may concern:

Please allow the following to serve as notice of an information security incident involving information for one Massachusetts General Hospital ("MGH") patient.

On June 7, 2017, we learned that a patient's medical records were inadvertently released to an incorrect patient via hand-off error. The unintended recipient hand delivered the information back to MGH's Privacy Office on the same day in which it was reported.

We immediately began an investigation and determined that the released records contained the demographic information of one (1) patient, including the patient's name, date of birth, address, medical record number, and Medicare policy number.

MGH is notifying one (1) New Hampshire resident in substantially the same form as the letter attached hereto, with written notification being sent on June 30, 2017. This letter is written pursuant to N.H. Rev. Stat. Ann. § 359-C:20.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Erika M. Barber
MGH Privacy Manager

Enclosure



A Teaching Affiliate
of Harvard Medical School

A FOUNDING MEMBER OF
PARTNERS
HEALTHCARE



Health Information Services
FND-860
55 Fruit Street
Boston, Massachusetts 02114-2621
Tel: 617.726.2465
Fax: 617.643.4041

June 30, 2017

[PATIENT NAME]
[PATIENT ADDRESS]
[PATIENT ADDRESS]

Dear [PATIENT NAME]:

Massachusetts General Hospital (MGH) 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 your personal information.

On June 7, 2017, we learned that a patient picked up a packet of their medical records, but inadvertently the involved practice included some of your medical records in the packet as well. The involved medical records contained demographic information, such as name, date of birth, medical record number, address, and phone number. The records also contained clinical information such as progress notes with your diagnoses, blood work results, and medication lists. Additionally, one page listed your Medicare insurance policy number, which contains your social security number. The unintended recipient reported this incident to the MGH Privacy Office and returned the information to our office on the same day.

To date, we have no knowledge that any of your information has been used improperly and want to reassure you the other patient returned your information. But, as a precaution, you may want to review all "explanation of benefits" statements that your insurer sends you as well as any bills or statements you receive for medical care very carefully. If you notice any unauthorized charges or services, you should notify your insurer, the sender of the bill, the provider of the service, and file a police report immediately. As another precautionary measure, you may want to periodically request a listing of benefits paid in your name by your health insurer.

There are also additional steps you may take to further reduce any potential risk to you. These steps are described below.

First, we encourage you to review carefully your bank, credit card, and other account statements every month to ensure that all account activity is valid. If you notice any questionable charges, report them promptly in writing to your card or account issuer.

Second, we encourage you to 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, contact the relevant credit bureau promptly at the telephone number listed on the 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.

Third, 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. 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. The credit bureaus can be reached at:

Equifax
P.O. Box 740241
Atlanta, GA 30374
800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 6790
Fullerton, CA 92834
800-680-7289
www.transunion.com

Finally, you have the right to request that the credit bureaus place a security freeze on your file. A security freeze prohibits a credit bureau from releasing any information from your credit report without written authorization. Please be aware, however, that placing a security freeze on your credit report may delay or prevent the timely approval of any requests you make for new loans, credit, mortgages, or other services. To place a security freeze on your file, you must send a written request to each of the three credit bureaus at the addresses listed above. The credit bureaus may require that you provide proper identification and may charge you a reasonable fee. Further information about placing a security freeze is enclosed with this letter.

For more guidance on the steps you can take to protect against misuse of your information, you can also contact the Federal Trade Commission at 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.

We sincerely regret any concern this may cause. MGH takes the privacy and security of our patients' information very seriously. As a result of our investigation, appropriate action was taken with the workforce member who made the error. To help prevent something like this from happening again, we continue to enhance training and education.

If you have questions, please call the MGH Privacy Office toll-free at (877) 644-2003.

Sincerely,

Erika M. Barber
Privacy Manager





FURTHER INFORMATION ON SECURITY FREEZES

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies 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

TransUnion Security Freeze
Fraud Victim Assistance
P. O. Box 6790
Fullerton, CA 92834

When requesting a security freeze, you will need to provide the following information: (1) your full name; (2) your social security number; (3) your date of birth; (4) if you have moved in the past five years, the addresses where you have lived during that period; (5) proof of your current address, such as a current utility or telephone bill; and (6) a legible copy of your government-issued identification card, such as a state driver's license, state ID card, or military ID card. 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, the credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze. You will need to include payment by check, money order, or major credit card. Do not send cash through the mail.

The credit reporting agencies have three business days after receiving your request to place a security freeze on your credit report. The credit bureaus also must send written confirmation to you within five business days and provide you with a unique personal identification number (PIN) or password, or both, that you can use 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 to be available. The credit reporting agencies have three business days after receiving your request to lift the security freeze for those specific entities or individuals or for the specified period of time.

To remove the security freeze completely, 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 business days after receiving your request to remove the security freeze.

