BakerHostetler

January 30, 2015

VIA OVERNIGHT MAIL

Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Attn.: Attorney General Joseph Foster

Re: Incident Notification

Dear Attorney General Foster:

On April 9, 2014, our client, UMass Memorial Medical Group (UMMMG), learned that information related to some of its patients may have been accessed inappropriately and potentially for fraudulent purposes. UMMMG immediately began an investigation and reported the incident to law enforcement. Thereafter, law enforcement required that UMMMG withhold notification to its patients while they conducted their investigation. On January 28, 2015, UMMMG was given permission by law enforcement to notify and it began notifying potentially affected patients on January 30, 2015.

Upon further investigation of the incident, UMMMG identified an employee who may have accessed billing records outside of normal job duties from January 7, 2014 to May 7, 2014. That employee no longer works with UMMMG. Also, in August 2014, law enforcement advised UMMMG that they found copies of some patient billing documents in possession of an unauthorized person related to the April incident. The precise information potentially accessed by the former employee varies with regard to different patients, but it may have included patients' names, addresses, dates of birth, medical record numbers, and Social Security numbers. The information also may have included credit or debit card numbers used for payments to UMMMG, phone number(s), email addresses and guarantors' names, if any. UMMMG continues to work with law enforcement in its investigation.

This incident did not affect all UMMMG patients. UMMMG is notifying the potentially affected patients and offering to eligible patients one year of free credit monitoring services. UMMMG is also providing call center support for those potentially affected.

UMMMG deeply regrets this incident and any inconvenience it may cause its patients. To help prevent this type of situation from happening again, UMMMG is further strengthening its

privacy and information security program, including identifying additional measures and enhancements to existing safeguards to protect patient information. UMMMG is also re-enforcing staff education regarding its policies and procedures to safeguard patient information.

UMMMG is notifying approximately 76 New Hampshire residents in substantially the same form as the attached letter.[1] As a covered entity under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), UMMMG is required to maintain procedures for responding to a breach of security, and notification to New Hampshire residents is being provided in compliance with those procedures. *See* N.H. Rev. Stat. Ann. § 359-C:20(V); *see also* 45 C.F.R. §§ 160.103 and 164.400 et seq.

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

Sincerely,

[1] As UMMMG does not conduct business in New Hampshire, this report is not, and does not constitute, a waiver of personal jurisdiction.

UMassMemorial
Medical Group
A Member of UMass Memorial Health Care

January 30, 2015

##A7524-L03-0123456 P- 0001 T- 00000007 **********3-DIGIT 123
SAMPLE A SAMPLE
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

Dear Sample A Sample:

UMass Memorial Medical Group (UMMMG) is committed to protecting the privacy and confidentiality of our patients' information. Regrettably, we are writing to inform you of an incident involving that information.

On April 9, 2014, UMMMG learned that information related to some of our patients may have been accessed inappropriately and potentially for fraudulent purposes. We immediately began an investigation and reported the incident to law enforcement. Thereafter, law enforcement required that we withhold notification to potentially affected individuals and any public announcement of this incident while they conducted their investigation. On January 28, 2015, we were given permission by law enforcement to notify and we are notifying you as quickly as possible.

Upon further investigation of the incident, we identified an employee who may have accessed billing records outside of normal job duties from January 7, 2014 to May 7, 2014. That employee no longer works with UMMMG. In August, law enforcement advised us that they found copies of patient billing documents in possession of an unauthorized person that included your name, address, date of birth, medical record number, Social Security number, and a credit or debit card number used for payments to UMMMG. The billing documents also may have included your phone number(s), email address and guarantor's name, if any. To date, we have no evidence that your medical records were accessed and your care at UMMMG will not be affected. We continue to work with law enforcement in their investigation.

We want to assure you that we are committed to the security of patient information and are taking this matter very seriously. If you see a fraudulent charge on your credit or debit card, please immediately contact the financial institution that issued your card. Additionally, to help you detect other possible misuse of your information, we are offering a complimentary one-year membership in Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and the resolution of identity theft. ProtectMyID Alert is completely free to you for one year and enrolling in this program will not hurt your credit score. Unfortunately, due to privacy laws, we are not able to enroll you directly. **For more information on ProtectMyID Alert and instructions on how to activate your complimentary one-year membership, please see the instructions included in this letter.**

0123456

(OVER PLEASE)

We deeply regret this incident and any inconvenience it may cause you. To help prevent this type of situation from happening again, UMMMG is further strengthening its privacy and information security program, including identifying additional measures and enhancements to existing safeguards to protect patient information. UMMMG is also re-enforcing staff education regarding our policies and procedures to safeguard patient information.

If you have any questions, or you need further assistance, you may call our Incident Response Line at [redacted], Monday through Friday from 9:00 a.m. to 7:00 p.m. Eastern Time (closed on U.S. observed holidays). Please be prepared to provide the following ten digit reference number when calling: [redacted]

Sincerely,

Stephen P. Tosi

Stephen Tosi, MD
President, UMass Memorial Medical Group

[redacted]

A7524-L03

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE **That You Enroll By: May 15, 2015** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll: www.protectmyid.com/redeem**
3. PROVIDE **Your Activation Code: A99999999999**

If you have questions or need an alternative to enrolling online, please call 877-288-8057 and provide engagement #: [redacted]

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; and contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

Even if you choose not to enroll in this program, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank and other financial statements for any unauthorized activity. You may also obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide consumer reporting companies. You should review your credit reports and have any information relating to fraudulent transactions deleted. To order your annual free credit report please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide consumer reporting companies is as follows:

Equifax	Experian	TransUnion
PO Box 740241	PO Box 9554	PO Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

0123456

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact your local law enforcement authorities and file a police report. Obtain a copy of the police report, which can be helpful in case you are asked to provide copies to creditors to correct your records. Please also inform the UMass Memorial Privacy Line at 508-334-5551. You should also immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/idtheft
1-877-438-4338

You can also obtain information from the sources above about steps an individual can take to avoid identity theft.

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of 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.