BakerHostetler

Baker&Hostetler LLP

45 Rockefeller Plaza
New York, NY 10111

T 212.589.4200
F 212.589.4201
www.bakerlaw.com

Theodore J. Kobus III
direct dial: 212.271.1504
tkobus@bakerlaw.com

May 5, 2014

VIA OVERNIGHT DELIVERY

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

Re: Incident Notification

Dear Attorney General Foster:

On March 6, 2014, our client, UMass Memorial Medical Center (UMMMC), learned that a now former employee may have accessed patient information such as name, address, date of birth and Social Security number outside of the employee's normal job duties. The information may have been used to open commercial accounts, such as credit card and cell phone accounts. If any access to patient information occurred outside of normal job duties, it would have been during the former employee's tenure from May 6, 2002 to March 4, 2014. UMMMC is not aware of any misuse of any medical information. Upon discovering this incident, UMMMC immediately began an internal investigation. UMMMC continues to conduct its investigation and cooperate with law enforcement. The employee no longer works at UMMMC.

UMMMC believes that the former employee may have misused the information of up to four patients. Out of an abundance of caution, UMMMC is notifying approximately 2,400 additional patients whose information was accessed by the employee, although UMMMC has no indication of misuse of this information. UMMMC began sending notification letters to these potentially affected patients today, May 5, 2014. UMMMC is also notifying potentially affected patients through a public notice on its website and a press release in the event that there are patients in addition to those receiving the letter who were seen during the employee's tenure and are aware of the misuse of their information to open commercial accounts.

UMMMC is offering to eligible patients potentially affected by the incident one year of free credit monitoring and identity theft protection services through Experian. UMMMC is also providing call center support for those potentially affected. UMMMC will also further investigate any concerns raised by its patients of misuse of information to determine whether they are related to this incident.

UMMMC has had a privacy and information security program in place for several years, and is assuring its patients that UMMMC is committed to the security of patient information and taking this matter very seriously. To help prevent this type of situation from happening again, UMMMC is further strengthening its program, including identifying additional measures and enhancements to existing safeguards to protect patient information. UMMMC is also re-enforcing staff education regarding UMMMC policies and procedures to safeguard patient information.

UMMMC is notifying 50 New Hampshire residents in substantially the same form as the letter attached hereto, with mailing commencing on May 5, 2014.[1] As a covered entity under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), UMMMC is required to maintain procedures for responding to a breach of security, and notification to New Hampshire residents is being provided in compliance with these 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,

Theodore J. Kobus III

Enclosure

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

UMassMemorial Medical Center
Hahnemann /Memorial/ University Campuses
Worcester, MA

May 5, 2014

##A0745-LV1-0123456 T-0001 **********3-DIGIT 159
SAMPLE A SAMPLE
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

Dear Sample A Sample:

UMass Memorial Medical Center (UMMMC) is committed to protecting the privacy and confidentiality of patient information. Regrettably, we are writing to inform you of an incident potentially involving your information.

On March 6, 2014, UMMMC learned that an employee may have accessed patient information outside of the employee's normal job duties. The information may have been used to open commercial accounts such as credit card and cell phone accounts. We are not aware of the misuse of any medical information. Upon receiving this information, UMMMC immediately began an internal investigation. We continue to investigate and cooperate with law enforcement. Our investigation has determined that the employee had access to your information, including your name, date of birth, Social Security number, and address at some point between May 6, 2002 and March 4, 2014. The employee no longer works at UMMMC.

While we have no indication at this time that your information has been used improperly, to help you detect possible misuse of your information, we are offering you a free one-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and 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. **For more information on identity theft prevention and ProtectMyID Alert, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.**

We deeply regret this incident and any inconvenience it may cause you. UMMMC has had a privacy and information security program in place for several years, and we want to assure you that we are committed to the security of patient information and are taking this matter very seriously. To help prevent this type of situation from happening again, UMMMC is further strengthening its program, including identifying additional measures and enhancements to existing safeguards to protect patient information. UMMMC is also re-enforcing staff education regarding our policies and procedures to safeguard patient information.

0123456

If you have any questions, or you need further assistance, you may call our Incident Response Line at 877-218-3036, Monday through Friday from 9:00 a.m. to 7:00 p.m. Eastern Time (closed on U.S. observed holidays), and provide this ten digit reference number – 1124042814 – when prompted.

Sincerely,

Patrick Muldoon, FACHE
President
UMass Memorial Medical Center

A0745-LV1

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE **That You Enroll By: 8.10.14**
2. VISIT the **ProtectMyID Web Site to enroll: www.protectmyid.com/redeem**
3. PROVIDE **Your Activation Code: ABCDEFGHIJKL**

If you have questions or need an alternative to enrolling online, please call 877-371-7902 and provide incident #: PC83355.

Your complimentary one-year ProtectMyID membership includes:

- **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; 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.

Activate your membership today at www.protectmyid.com/redeem
or call 877-371-7902 to register with the activation code above.

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 877-371-7902.

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, directly from each of the three nationwide credit reporting agencies. To order your credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

Equifax	Experian	TransUnion
PO Box 740256	PO Box 9554	PO Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

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 in case you are asked to provide copies to creditors to correct your records. Please 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 obtain information from the sources above about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes.

* 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.

A0745-LV1