

Baker Hostetler

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

July 11, 2012

Via Federal Express

Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Attn: Attorney General Michael A. Delaney

Re: Incident Notification

Dear Attorney General Delaney:

Memorial Healthcare System (MHS), our client, as part of an ongoing review of its patient information systems which commenced on April 27, 2012, discovered that employees of affiliated physicians' offices may have improperly accessed patient information through a web portal used by physicians who provide care and treatment at MHS. Specifically, patient names, dates of birth, and Social Security numbers may have been accessed during 2011 and 2012. Patient medical records were not changed or deleted. During MHS's investigation, MHS immediately contacted law enforcement and began a comprehensive review of its patient information systems to determine if other similar incidents may have occurred. The physicians have been advised that this incident occurred.

Law enforcement investigators asked MHS to withhold notification or public announcement of this incident until no earlier than July 11, 2012. Now that the law enforcement hold has been lifted, MHS notified affected individuals as quickly as possible. As such, any notification delay was reasonable and necessary at the request of law enforcement. See N.H. RSA 359-C:20(II).

MHS is notifying all potentially affected individuals and offering one year of free credit monitoring through Experian.

Law enforcement is still involved, and MHS continues to cooperate with their investigation. As a result of this incident, MHS has taken steps to help prevent such an incident from occurring in the future. MHS continues to refine its privacy policies, limit access by employees of affiliated physicians, reinforce with all staff and affiliated

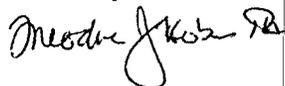
VIA FEDERAL EXPRESS

Attorney General Michael A. Delaney
July 11, 2012
Page 2

physicians' employees the importance of handling patient information carefully, and enhance its auditing controls by taking advantage of recent advances in technology.

There are approximately 29 New Hampshire residents potentially affected by this incident. Notification is being sent to those residents in substantially the form attached hereto.

Sincerely,

A handwritten signature in black ink, appearing to read "Theodore J. Kobus III". The signature is written in a cursive style with a large initial 'T' and 'K'.

Theodore J. Kobus III

Enclosure

Memorial Healthcare System

July 11, 2012

844871.01-0123456 T-
SAMPLE A SAMPLE
123 ANY ST
APT ABC
ANYTOWN, US 12345-6789



Dear Sample A Sample:

Memorial Healthcare System (MHS) is committed to maintaining the privacy and confidentiality of patient information at all times. We are writing now to inform you of an issue involving some of that information.

As part of an ongoing review of our patient information systems which commenced on April 27, 2012, we discovered that an employee of an affiliated physician's office may have improperly accessed your patient information through a web portal used by physicians who provide care and treatment at MHS. Specifically, your name, date of birth, and Social Security number **may** have been accessed during 2011 and 2012. However, your medical records were **not** changed or deleted. During our investigation, we immediately contacted law enforcement and began a comprehensive review of our patient information systems to determine if other similar incidents may have occurred. The physician has been advised that this incident occurred.

Law enforcement investigators asked that we withhold notification or public announcement of this incident until now. The law enforcement hold has been lifted, and we are notifying you as quickly as possible.

Because your information may have been improperly accessed, we are offering you a free, one-year membership in Experian's ProtectMyID™ Alert. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. For more information about ProtectMyID and instructions on how to activate your complimentary one-year membership, please see the page provided by Experian that is attached to this letter.

We want to assure you that we take this matter very seriously. Law enforcement is still involved, and we continue to cooperate with their investigation. We deeply regret that this incident has occurred, and we have taken steps to help prevent such an incident from occurring in the future. We continue to refine our privacy policies, limit access by employees of affiliated physicians, reinforce with all staff and affiliated physicians' employees the importance of handling patient information carefully, and enhance our auditing controls by taking advantage of recent advances in technology. If you have any questions, please call 1-855-770-0004 Monday through Friday from 8:00 A.M. to 5:00 P.M. (Eastern Time) and enter the reference code 6471071112 when prompted.

Sincerely,

Denise D. DiCesare
Privacy Officer
Memorial Healthcare System



Activate ProtectMyID Now in Three Easy Steps

1. ENSURE That You Enroll By: **October 30, 2012**
2. VISIT the **ProtectMyID Web Site: www.protectmyid.com/redeem** or call **877-371-7902** to enroll
3. PROVIDE Your Activation Code: **ABCDEFGHIJKL**

Once your ProtectMyID membership is activated, your credit report will be monitored daily for 50 leading indicators of identity theft. You'll receive timely Credit Alerts from ProtectMyID on any key changes in your credit report which could include new inquiries, new credit accounts, medical collections and changes to public records.

ProtectMyID provides you with powerful identity protection that will help detect, protect and resolve potential identity theft. In the case that identity theft is detected, ProtectMyID will assign a dedicated U.S.-based Identity Theft Resolution Agent who will walk you through the process of fraud resolution from start to finish for seamless service.

We realize 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.

Your complimentary 12-month ProtectMyID membership includes:

- ⇒ **Credit Report:** A free copy of your Experian credit report
- ⇒ **Daily 3 Bureau Credit Monitoring:** Alerts you of suspicious activity including new inquiries, newly opened accounts, delinquencies, or medical collections found on your Experian, Equifax and TransUnion credit reports.
- ⇒ **Identity Theft Resolution:** If you have been a victim of identity theft, you will be assigned a dedicated, U.S.-based Experian Identity Theft Resolution Agent who will walk you through the fraud resolution process, from start to finish.
- ⇒ **ExtendCARE:** Full access to the same personalized assistance from a highly-trained Fraud Resolution Agent even after your initial ProtectMyID membership expires.
- ⇒ **\$1 Million Identity Theft Insurance*:** As a ProtectMyID member, you are immediately covered by a \$1 Million insurance policy that can help you cover 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.

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