BakerHostetler

Baker&Hostetler LLP

[redacted]

November 26, 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 September 29, 2014, our client, Highlands-Cashiers Hospital ("HCH"), learned that a data security screening of its computer systems had revealed a potential exposure that was inadvertently caused by a third party information technology vendor, TruBridge, the wholly owned subsidiary of Computer Programs and Systems, Inc. ("CPSI"), with whom HCH contracts for specialized computer services. The data security screening revealed that servers containing some patient, employee, and volunteer information were inadvertently left accessible via the Internet by TruBridge between May 2012 and September 2014. Potentially accessible patient information included names, addresses, dates of birth, treatment information, diagnoses, health insurance information, and Social Security numbers. Potentially accessible employee and volunteer information included names, dates of birth, Social Security numbers, and, for some employees, bank account and routing numbers. Forensic computer investigators hired by HCH found no evidence, based upon their investigation, that this information was accessed through the Internet or used in any way at all. Upon learning of the potential exposure, HCH took immediate steps to have TruBridge secure the servers to protect the affected information and to make sure it was no longer accessible via the Internet.

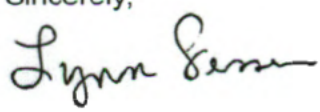
As a precaution, HCH is notifying affected individuals and offering eligible individuals a complimentary one-year membership in credit monitoring and identity theft protection services from Experian. HCH has also established a dedicated call center to assist individuals with any questions they may have.

TruBridge has secured the servers and HCH has added additional security. HCH is also reinforcing with its vendors the importance of handling HCH information securely to help prevent something like this from happening again in the future.

HCH is notifying five (5) New Hampshire residents in substantially the same form as the letter attached hereto, with notification commencing November 26, 2014.[1] As a covered entity under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), HCH 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.[2] *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,



Lynn Sessions

Enclosure

---

[1] This report is not, and does not constitute, a waiver of personal jurisdiction.

[2] HCH is notifying all five (5) affected New Hampshire residents pursuant to its obligations as a HIPAA covered entity. *See* 45 C.F.R. §§ 160.103 and 164.400 et seq.

HIGHLANDS-CASHIERS HOSPITAL

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<First Name>><<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>,<<State>><<Zip>>

<<Date>>

Dear <<First Name>> <<Last Name>>:

Highlands-Cashiers Hospital ("HCH") is committed to protecting the security and confidentiality of our patients' information. While we currently have no knowledge that your patient information has been accessed through the internet or used in any way at all, we felt it important to inform you that a data security screening of our computer systems uncovered a potential exposure that was inadvertently caused by a third party information technology vendor, TruBridge, the wholly owned subsidiary of Computer Programs and Systems, Inc. ("CPSI"), with whom we contract for specialized computer services.

On September 29, 2014, a data security screening revealed that servers containing patient information were inadvertently left accessible by TruBridge between May 2012 and September 2014, and created the potential for your name, address, date of birth, treatment information, diagnosis, health insurance information and social security number to be accessed via the internet. Forensic computer investigators hired by us found no evidence based upon their investigation that this information was accessed through the internet or used in any way at all. We also want to assure you that we took immediate steps to have TruBridge secure the servers to protect your information and to make sure it is no longer accessible via the internet. Additionally, we are re-enforcing with our vendors the importance of handling patient information securely.

Recognizing how important the privacy of your information is to you, and as an added precaution, we are offering you a complimentary one-year membership in Experian's® ProtectMyID® Alert. This product helps detect the possible misuse of your personal information and provides you with superior identity protection services focused on immediate identification and resolution of identity theft. ProtectMyID Alert is completely free to you 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 identity theft prevention and ProtectMyID Alert, including instructions on how to enroll and activate your complimentary one-year membership, please see the additional information attached with this letter.** We also recommend that you regularly review the explanation of benefits statement that you receive from your health insurer. If you identify services listed on your explanation of benefits that you did not receive, please immediately contact your insurer.

Again, we deeply regret any inconvenience this may cause you. We take our responsibility to protect your information very seriously and want to reassure you that safeguarding your confidential information remains a priority for us. If you have any further questions or concerns, please call 1-888-227-1416, Monday through Friday between 9:00 a.m. and 9:00 p.m. Eastern Time.

Sincerely,

Craig James
President, Highlands-Cashiers Hospital
Attachment: Experian® ProtectMyID Instructions

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE **That You Enroll By: 2/27/2015** (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: <<code>>**

If you have questions or need an alternative to enrolling online, please call 877-288-8057 and provide engagement #: **PC90419.**

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP:

This service is free and 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; 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 take advantage of this free credit monitoring service, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit report and 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 credit reporting companies. 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 credit reporting companies 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 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
1-877-438-4338

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also 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.

* 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.