BakerHostetler

STATE OF NH
DEPT OF JUSTICE
2017 MAR 27 AM 9:43

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Paulette M. Thomas
direct dial: 513.929.3483
pmthomas@bakerlaw.com

March 24, 2017

VIA OVERNIGHT MAIL

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol St.
Concord, NH 03301

Re: Incident Notification

Dear Attorney General Foster:

We are writing on behalf of our client, Washington University School of Medicine ("WUSM"). On January 24, 2017, WUSM learned that a phishing email was sent to employees of WUSM who had previously responded to an email on December 2, 2016, believing it to be a legitimate request. WUSM immediately secured the email accounts and began an investigation. The investigation could not rule out that an unauthorized third party may have gained access to some employees' email accounts. WUSH conducted a thorough review of the employees' email accounts and confirmed that some of the emails contained personal information of patients and employees, which may have included patients' names, dates of birth, medical records numbers, diagnosis and treatment information, and clinical information and employees' names and Social Security numbers. WUSM reported the incident to law enforcement and continues to work with them in their investigation.

WUSM began mailing letters to approximately one New Hampshire resident pursuant to the requirements of the Health Insurance and Portability Act ("HIPAA"), 45 C.F.R. §§164.400-414 and state law in substantially the same form as the letter attached hereto. [1] The one New Hampshire resident's Social Security number and financial information were not affected by this incident.

WUSM has also established a dedicated call center that potentially affected individuals may contact with questions. To help prevent something like this from happening in the future,

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

WUSM is reinforcing education with its staff and faculty of existing protocols and resources regarding phishing emails, and reviewing enhancements to strengthen its business practices and user login authentication.

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

Sincerely,

Paulette M. Thomas

Paulette M. Thomas
Counsel

Enclosure

Washington University in St. Louis

SCHOOL OF MEDICINE

March 24, 2017

STATE OF NH
DEPT OF JUSTICE
2017 MAR 27 AM 9:43

Sample Customer
123 Sample St Apt 2
Dublin, OH 43017-1234

Dear Sample Customer:

Washington University School of Medicine (WUSM) is committed to protecting the security and confidentiality of our patients' information. Regrettably, we are writing to inform you about an incident involving some of that information.

On January 24, 2017, we learned that a "phishing" email was sent to employees of WUSM who had previously responded to an email on December 2, 2016, believing it to be a legitimate request. A "phishing" email is an email designed to look like a legitimate email but tricks the recipient into taking some action, such as providing login credentials. Upon learning of this, we secured the email accounts and began an investigation. The investigation could not rule out that an unauthorized third party may have gained access to some employees' email accounts. We conducted a thorough review of the employees' email accounts and confirmed that some of the emails contained patient information. That information may have included your name, date of birth, medical records number, diagnosis and treatment information, and other clinical information. Neither your Social Security number nor other financial information was included. We reported the phishing incident to law enforcement and continue to work with them in their investigation.

We have no indication that the information in the emails has been used in any way; however, as a precaution, we wanted to notify you of this incident and assure you that we take it very seriously.

We regret any inconvenience or concern this may cause you. To help prevent something like this from happening in the future, we are reinforcing education with our staff and faculty of existing protocols and University resources regarding "phishing" emails. We are also reviewing enhancements to strengthen our business practices and user login authentication process. If you have any questions, please call 1-(844) 641-5630, Monday through Friday between 9:00 a.m. and 5:00 p.m. Central Time.

Sincerely,

Chellie A. Butel

Chellie A. Butel, BSN, RN, JD
Interim Privacy Officer
Washington University School of Medicine

Washington University in St. Louis

SCHOOL OF MEDICINE

March 24, 2017

Sample Customer
123 Sample St Apt 2
Dublin, OH 43017-1234

Dear Sample Customer:

Washington University School of Medicine (WUSM) is committed to protecting the security and confidentiality of our patients' information. Regrettably, we are writing to inform you about an incident involving some of that information.

On January 24, 2017, we learned that a "phishing" email was sent to employees of WUSM who had previously responded to an email on December 2, 2016, believing it to be a legitimate request. A "phishing" email is an email designed to look like a legitimate email but tricks the recipient into taking some action, such as providing login credentials. Upon learning of this, we secured the email accounts and began an investigation. The investigation could not rule out that an unauthorized third party may have gained access to some employees' email accounts. We conducted a thorough review of the employees' email accounts and confirmed that some of the emails contained patient information. That information may have included your name, date of birth, Social Security number, medical records number, diagnosis and treatment information, and other clinical information. We reported the phishing incident to law enforcement and continue to work with them in their investigation.

We have no indication that the information in the emails has been used in any way; however, as a precaution, we wanted to notify you of this incident and assure you that we take it very seriously. Out of an abundance of caution, 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 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. **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 also recommend that you review the explanation of benefits that you receive from your health insurer. If you see services that you did not receive, please contact your health insurer immediately.

We regret any inconvenience or concern this may cause you. To help prevent something like this from happening in the future, we are reinforcing education with our staff and faculty of existing protocols and University resources regarding "phishing" emails. We are also reviewing enhancements to strengthen our business practices and user login authentication process. If you have any questions, please call 1-(844) 641-5630, Monday through Friday between 9:00 a.m. and 5:00 p.m. Central Time.

Sincerely,

Chellie A. Butel

Chellie A. Butel, BSN, RN, JD
Interim Privacy Officer
Washington University School of Medicine

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE **That You Enroll By: June 28, 2017** (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 #: PC107146

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; contact government agencies.
  - 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 877-288-8057 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 877-288-8057.

Additional Steps You Can Take

Even if you choose not to take advantage of this free credit monitoring, we recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may 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

* 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.

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, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-866-640-2273
Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 state. 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. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft