May 12, 2023

VIA ELECTRONIC MAIL
Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete, LLP represents Uintah Basin Healthcare ("UBH"), a healthcare system located in Utah, in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with New Hampshire's data breach notification statute.

Nature of the Security Incident

On November 7, 2022, UBH became aware of unusual activity on its network. In response, UBH immediately took steps to secure its digital environment and engaged a leading cybersecurity firm to assist with an investigation. Through the investigation, UBH learned that personal and protected health information may have been accessed or acquired by an unauthorized individual. Specifically, on or around April 7, 2023, UBH determined that personal and protected health information belonging to patients that received care with UBH between March 2012 and November 2022 may have been accessed or acquired without authorization during the incident. UBH then began the process of locating mailing information to effectuate notification to the identified UBH patients, which was completed on April 10, 2023.

The information affected may have included employees'

. Please note that we have no current evidence to suggest misuse or attempted misuse of personal information involved in the incident.

Number of New Hampshire Residents Involved

On May 10, 2023, UBH notified eighteen (18) New Hampshire residents of this data security incident via U.S. First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

Steps Taken to Address the Incident

In response to the incident, UBH is providing individuals with information about steps that they can take to help protect their personal information, and, out of an abundance of caution, it is also offering individuals complimentary credit monitoring and identity protection services through IDX. Additionally, to help reduce the risk of a similar future incident, UBH has implemented additional technical security measures, including performance of a global password reset throughout the environment and deployment of SentinelOne, a sophisticated endpoint detection and response tool with 24/7 monitoring.

Contact Information

UBH remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at .

Sincerely,

Laura K. Funk
Partner
CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

Enclosure: Sample Notification Letter

Uintah Basin Healthcare

Return to IDX:
PO Box 480149
Niles, IL 60714

To Enroll, Please Call:
1-888-567-0240
Or Visit:
https://response.idx.us/UBH
Enrollment Code:
<<XXXXXXXX>>

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

May 10, 2023

Re: Notice of Data <<Variable Text 1>>

Dear <<FirstName>> <<LastName>>,

We are writing to provide you with information about a recent data security incident experienced by Uintah Basin Healthcare ("UBH"), a healthcare system located in Utah, that may have involved your personal and protected health information. At UBH, we take the privacy and security of all information within our possession very seriously. This is why we are notifying you of the incident, providing you with steps you can take to help protect your personal and protected health information, and offering you the opportunity to enroll in complimentary credit monitoring and identity protection services.

What Happened. On November 7, 2022, UBH became aware of unusual activity on our network. In response, we immediately secured the environment and engaged a leading cybersecurity firm to assist with an investigation and determine whether sensitive, personal, or protected health information may have been affected. On or around April 7, 2023, UBH determined the personal and protected health information of patients that received care with UBH between March 2012 and November 2022 may have been accessed or acquired without authorization during the incident. UBH then diligently worked to identify the names of individuals potentially impacted and locate relevant address information to effectuate notification to such individuals, which was completed on April 10, 2023.

What Information Was Involved. The potentially affected information varied between individuals but may have included

.

Please note that there is no evidence to suggest misuse or attempted misuse of personal or protected health information. Nonetheless, out of an abundance of caution, we are notifying all patients who were seen between March 2012 and November 2022 of this incident and offering resources to help you protect your personal and protected health information.

What We Are Doing. As soon as we discovered this incident, we took the steps described above. Further, we notified the Federal Bureau of Investigation and will cooperate with any resulting investigation. As part of the response process, we implemented additional measures to reduce the risk of a similar incident occurring in the future.

Additionally, UBH is providing you with information about steps that you can take to help protect your personal and protected health information and, as an added precaution, is offering you free of charge identity theft protection services through IDX, a ZeroFox Company. These identity protection services include: <<12/24 months>> of credit and CyberScan monitoring, an identity theft insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do. We recommend that you activate your complimentary IDX services by calling or going to and using the enrollment code shown on the letterhead of this document. Representatives are available from 7:00am to 7:00pm Mountain Time from Monday to Friday. Please note that deadline to enroll is August 10, 2023. In addition, we recommend that you review the guidance included with this letter about additional steps you can take to protect your personal and protected health information.

For More Information. If you have questions or need assistance, please contact IDX at 1-888-567-0240, Monday through Friday from 7:00am to 7:00pm Mountain Time, excluding major U.S. holidays. IDX representatives are fully versed on this incident and can answer questions you may have regarding the protection of your personal and protected health information.

UBH takes this matter very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Uintah Basin Healthcare
250 W 300 N
Roosevelt, UT 84066

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 740241
Atlanta, GA 30374
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC (1-877-438-4338 or www.ftc.gov/idtheft) or to the Attorney General in your state.

Utah Attorney General
350 North State Street
Suite 230
SLC, UT 84114
attorneygeneral.utah.gov
1-800-244-4636

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.