BakerHostetler

Baker&Hostetler LLP

2929 Arch Street
Cira Centre, 12th Floor
Philadelphia, PA 19104-2891

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

Eric A. Packel
direct dial: 215.564.3031
epackel@bakerlaw.com

September 8, 2020

VIA EMAIL (SECURITYBREACH@ATG.WA.GOV)

Office of the Washington Attorney General
Consumer Protection Division
800 5th Ave., Suite 2000
Seattle, WA 98104-3188

Re: Incident Notification

Dear Attorney General Ferguson:

We are writing on behalf of our client, Virginia Mason Medical Center ("VMMC"), as a courtesy, simply to make your office aware of a data security incident that will be press released by VMMC today. The incident occurred at one of its vendors, Blackbaud, Inc. ("Blackbaud"), which provides services related to VMMC's fundraising efforts.

VMMC is a covered entity under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and it is complying with the requirements of HIPAA in responding to the incident. This notice is being submitted to your office as a courtesy because, as addressed in further detail below, the incident would likely not subject Washington residents to a risk of harm per Wash. Rev. Code § 19.255.010. The incident did NOT involve Social Security numbers or other sensitive financial information.

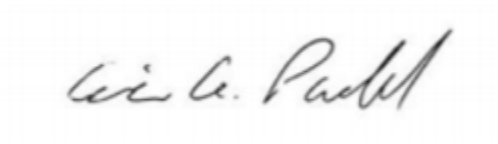
Blackbaud is a vendor used by VMMC for cloud based and data solution services related to its fundraising efforts. On July 16, 2020, VMMC received notice from Blackbaud stating that it discovered an unauthorized individual had gained access to Blackbaud's systems and may have acquired backup copies of databases used by its customers, including the database VMMC uses for fundraising efforts. VMMC immediately took steps to understand the extent of the incident and the data involved. VMMC's review of the affected database revealed that it contained some information belonging to VMMC patients, including their names, contact information, dates of birth, visit dates and locations, and/or treating physician names for 227,371 Washington residents.

The fundraising database involved does not include any substantive information about medical diagnoses or treatments. Moreover, Blackbaud informed VMMC that Social Security numbers, financial account information, and payment card information were encrypted and not accessible to the unauthorized individual. Also, this incident did not involve any access to VMMC's medical systems or electronic health records.

In accordance with HIPAA (45 CFR §§ 160.103 and 164.400 *et seq.*), VMMC began mailing letters to the Washington residents on September 8, 2020 (a copy of the notice letter is enclosed). VMMC also established a dedicated, toll-free call center where notified individuals may obtain more information regarding the incident. To help prevent something like this from happening in the future, VMMC is examining its vendor relationship with Blackbaud and evaluating their security safeguards.

Please do not hesitate to contact me if you have any questions regarding this courtesy notification.

Sincerely,



Eric A. Packel
Partner

Enclosure

Virginia Mason

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Virginia Mason Medical Center is committed to protecting the security and privacy of our patients, and all the individuals who support our fundraising efforts. Regrettably, this notice is regarding a recent incident that occurred at one of our third-party vendors, Blackbaud Inc. ("Blackbaud"), that may have involved some of your information.

What Happened?
Blackbaud is a vendor we use for cloud-based and data solution services related to our donors and fundraising. On July 16, 2020, Blackbaud informed us it had discovered that an unauthorized individual had gained access to Blackbaud's systems between February 7, 2020 and May 20, 2020. Blackbaud advised us that the unauthorized individual may have acquired backup copies of databases used by its customers, including a backup of a database we use for fundraising efforts. We immediately took steps to understand the extent of the incident and the data involved.

What Information was Involved?
Based on our review of the database, we have reason to believe that it contained some of your information, including your name, contact information - specifically email address and telephone number, gender, date of birth, visit date and location, treating physician(s), and/or concierge medicine status.

Importantly, Blackbaud informed us that your Social Security number and bank account and credit card account information were encrypted, and therefore not able to be accessed by the unauthorized individual. Also, this incident did not involve any access to medical systems or electronic health records. The incident affected our donor/fundraising database.

What We Are Doing:
We are notifying you of this incident because we take it very seriously and because we knew you would want to know. Blackbaud has informed us that they identified and fixed the vulnerability associated with this incident and are implementing additional security enhancements in response to the incident. In addition, we are undertaking a review of how our information is stored with Blackbaud and evaluating their security safeguards.

What You Can Do:
To date, we have no evidence that your personal information has been misused, and Blackbaud informed us that they believe the unauthorized individual did not retain any of the affected information. However, we recommend you review the statements you receive from your healthcare providers. If you see services you did not receive, please contact the provider immediately.

We deeply and sincerely regret any concern or inconvenience this incident may cause you. Should you have questions, please contact 1-???-???-????, Monday through Friday, from 8:00 a.m. to 5:30 p.m. Central, excluding major U.S. holidays. When calling, please refer to the Reference Number <<Member ID>>.

Sincerely,

Dean Schultz
Chief Information Security and Privacy Officer
Virginia Mason Medical Center