UnityPoint Health
Des Moines Foundation

[redacted]

[redacted]

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

[redacted]

Dear [redacted]:

UnityPoint Health deeply values the trust and support of our patients, friends and donors, and we take our responsibility to safeguard the information you share with us very seriously. That's why we're reaching out to make you aware of a recent data security incident involving Blackbaud, a third-party software and service provider used by UnityPoint Health ("UPH") and many other non-profit organizations around the world for fundraising and donor engagement.

Blackbaud recently notified us of a wide-reaching security incident that impacted its clients across the globe and may have involved some of the information you provided to us. We are committed to transparency and want to share more about what happened and the measures taken to protect your information.

What Happened

On July 16, 2020, Blackbaud reported to us that they identified a ransomware attack in progress on May 20, 2020. Blackbaud informed us that they stopped the ransomware attack and engaged forensic experts to assist in their internal investigation. That investigation concluded that cybercriminals intermittently removed data from Blackbaud's systems between February 7, 2020 and May 20, 2020. Blackbaud paid a ransom to ensure the data was permanently destroyed.

What Information Was Involved

The information potentially compromised during this incident may have included personal information, including your full name, address, date of birth, phone number, provider name(s), date(s) of service, and/or hospital department(s) in which you may have received treatment. Your philanthropic giving history, such as donation dates and amounts, may have also been removed during the incident. **It is important to note the incident did not involve your Social Security number, and your financial account information and/or payment card information were also not exposed. Similarly, our electronic health record system was not impacted by this incident.**

What We Are Doing

Upon learning of the issue, we requested detailed information from Blackbaud about the nature and scope of the Blackbaud security incident, and we continue to correspond with Blackbaud regarding their investigation. As part of our mitigation efforts, we engaged experts to assist us in determining what information was potentially impacted and steps we can take to mitigate harm to our donors from this incident at Blackbaud. Further, we are reviewing our agreements and evaluating our ongoing relationship with Blackbaud. Please know we are taking this incident very seriously.

What Blackbaud Is Doing

Blackbaud has assured us they closed the vulnerability that allowed the incident and are taking steps to enhance their security controls to guard against incidents like this in the future. **According to Blackbaud, there is no evidence that any data has been misused, disseminated, or otherwise made publicly available. Blackbaud indicates that it has hired a third-party team of experts, including a team of forensics accountants, to continue monitoring for any such activity.**

What You Can Do

This letter provides precautionary measures you may wish to take to protect your personal and medical information. Specifically, we have included information on protecting your medical information. Even though Social Security numbers and financial information was not involved, we have also enclosed information on how to place a fraud alert and/or security freeze on your credit files, and/or obtain a free credit report from each of the three major credit reporting agencies as a courtesy for your reference. As a general precaution, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity and report any suspicious activity.

For More Information

Please know the security of our patients' and donors' information is our top priority, and we deeply regret any worry or inconvenience the Blackbaud incident may cause. **We remain fully committed to maintaining the privacy of personal information and take many precautions to safeguard it. We continually evaluate and modify our practices, and those of our third party service providers, to enhance the security and privacy of your personal information. Should you have questions regarding this incident, please call our dedicated and confidential toll-free response line at [redacted].** The response line is available Monday through Friday from [redacted]

As always, we deeply appreciate your continued trust and support.

Sincerely,

[redacted]

– OTHER IMPORTANT INFORMATION –

1. Protecting Your Medical Information.

We have no information to date indicating that your medical information involved in this incident was used for any unintended purposes. As a general matter, however, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review the "explanation of benefits statement" that you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

2. Placing a Fraud Alert on Your Credit File.

Even though no Social Security numbers or financial information was involved in this incident, at any time you may place an initial one (1) year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, at any time you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-349-9960

Experian Security Freeze
PO Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: (515) 281-5164.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.