Trinity Health

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

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

RE: << b2b_text_1 (Site of Care)>>, a member of Trinity Health:

Notice of Data Breach

At Trinity Health, safety is a top priority – including the safety of our patients' and donors' personal information. In that regard, we are notifying you about a data security incident involving Blackbaud, a vendor that supplies Trinity Health's donor database technology. The data security incident may have impacted certain personal information of donors and certain patients.

What Happened? On July 16, 2020, Blackbaud notified Trinity Health and other customers of a cyber-attack involving Blackbaud's network, including ransomware, that impacted certain donor database backup files maintained by Blackbaud, including Trinity Health's donor database. Blackbaud reported the cyberattack occurred between April 18, 2020 - May 16, 2020. Blackbaud reported that based on its investigation, the cybercriminals responsible for the attack could have obtained access to various types of information in the client backup files.

What We Are Doing. Upon receiving this notice, Trinity Health took immediate steps to begin its own investigation to determine what, if any, sensitive Trinity Health data was potentially impacted. Please note that this attack did not occur within the information systems of Trinity Health or any affiliated Ministry. Unfortunately, a sophisticated attack against Blackbaud circumvented Blackbaud's security measures protecting the information in their care leading to this incident. Trinity Health and its affiliated Ministries take security of your information seriously and makes significant investments in the protection of your information to reduce this type of event from occurring. Trinity and its affiliated Ministries are working with Blackbaud to keep this type of event from occurring again.

What information was involved? Our forensic investigation determined that some data fields were encrypted and would not be accessible to the cybercriminals. Other fields were not encrypted and could have been accessible to the cybercriminals including information such as: donor relation to patient, patient discharge status, patient insurance and patient department of service. This database information spans from 2000 to 2020.

Your personally identifiable information and protected health information data elements that could have been exposed in the cyberattack are: full name, address, phone numbers, email, <<b2b_text_2(ImpactedData)>>.

Why was patient information in the database? Limited patient information was included for the purposes of the Trinity Health Grateful Patient Program consistent with the permitted use of limited patient information for fund-raising under HIPAA.

How did Blackbaud secure the data? Blackbaud reported that they quickly locked out the cybercriminals and resolved the issue. Additional details about the security incident is available by visiting Blackbaud's website at https://www.blackbaud.com/securityincident, which includes information about Blackbaud's steps to ensure this issue does not happen again. We continue to work with Blackbaud on the measures they are taking to further secure the information in their care.

We deeply regret that this incident occurred and apologize for any concern or inconvenience you may experience from this notification.

What You Can Do. As an added precaution, Trinity Health is offering you access to 12 months of free identity monitoring services through Kroll at no cost to you. To activate your membership and start monitoring your personal information please follow the steps in the enclosed *Steps You Can Take To Help Protect Personal Information*.

For More Information. Thank you for trusting Trinity Health with your care and your support of our Mission. If you would like additional information, please visit our website at https://www.trinityhealth.org/blackbaud-incident or call our dedicated call center at 1-???-???-???? Monday through Friday, 8:00 a.m. CT to 5:30 p.m. CT, excluding U.S. holidays.

Sincerely,

Monica C. Lareau
Director, HIPAA Compliance, Privacy Official
Trinity Health

Steps You Can Take to Help Protect Personal Information

Enroll in Identity Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Fraud Consultation, and Identity Theft Restoration.

Visit **<<IDMonitoringURL>>** to activate and take advantage of your identity monitoring services.

*You have until **<<Date>>** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

Monitor Accounts

Trinity Health encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.