MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Ryan C. Loughlin
Office: (267) 930-4786
Fax: (267) 930-4771
Email: rloughlin@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

October 26, 2020

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Trinity Health located at 20555 Victor Parkway Livonia, MI 48152, and are writing to notify your office of an incident that may affect the security of some personal information relating to approximately nine (9) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Trinity Health does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

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 is a world-leading provider of fundraising and donation customer relationship management tools for non-profit and higher education organizations and is used by Trinity Health and its affiliated Ministries for these services. 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. 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.

Blackbaud cannot confirm specifically whether any personal information included in the impacted databases was viewed by the unauthorized actor(s). However, the investigation confirmed that the information present in the accounts during the periods of unauthorized access included the following: name and address, phone numbers, email, and financial account information. The Social Security number of one (1) resident may also be impacted.

Notice to New Hampshire Residents

On or about September 14, 2020, Trinity Health began providing written notice of this incident to affected individuals, which includes approximately nine (9) New Hampshire residents whose personal information may be impacted. Written notice is being provided in substantially the same form as the letter included herein as ***Exhibit A***.

Other Steps Taken and To Be Taken

Information privacy and security are among Trinity Health's highest priorities. As part of its ongoing commitment to the privacy and security of personal information in its care, Trinity Health is in the process of reviewing its existing policies and procedures to mitigate risks associated with this incident and to better prevent future incidents.

Trinity Health is currently investigating the nature and scope of this incident and will work with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4786.

Very truly yours,

Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/mef

Exhibit A

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 Cyber-Attack Impacting Database Information

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. 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.

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, most recent donation date, date of birth, age, <<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. 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.

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

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	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 160	PO Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	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	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	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.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island Residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are X Rhode Island residents impacted by this incident.

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.