20084

Membership #: <<Member ID>>

Call center (855) 935-6070

Trinity Health

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

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

Re: Patient: <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

You are receiving this letter because the patient listed above receives service from a hospital or health care provider that is a current or former member of Trinity Health*. The purpose of this letter is to notify you of an incident that may impact the privacy of certain confidential information related to the patient. Trinity Health was recently notified by Accellion, a third-party vendor, of a security incident. The Accellion File Transfer Appliance is used by Trinity Health and many other companies for large file transfer service. Trinity Health provides information technology services for its current and some former member hospitals and health care providers, including file transfer and email services (* please see included information about Trinity Health and the affected locations).

This letter provides you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so. While we are unaware of misuse of information, we encourage you to remain vigilant against incidents of identity theft and fraud. We have established a call center to answer your questions: **(855) 935-6070**.

What Happened? On January 29, 2021, Accellion informed Trinity Health of a security issue with its secure file transfer platform, used for sending secure email. Upon receiving this notice, Trinity Health immediately took the appliance offline and launched an investigation into the issue and its impact on both Trinity Health and our patients and colleagues. This investigation determined that certain files present on the appliance on January 20 were downloaded by an unknown user. The unauthorized user was able to take advantage of a previously unknown and unreported flaw in the security of the Accellion appliance.

What Information is Involved? Although the investigation is ongoing, on February 4, 2021, we determined file(s) were present on the appliance at the time of this event. The files contained certain protected health information, including some combination of the following, **patient's name, address, email, date of birth, healthcare provider, dates and types of health care services, medical record number, immunization type, lab results, medications, payment, payer name, and claims information.** <<b2b_text_1 (variable text sentence- SSN#, credit card information)>>

What We Are Doing. We take these matters extremely seriously. When we were alerted of the security issue, we immediately took steps to terminate access and use of the appliance and worked with Accellion to investigate the event. We also confirmed the security of our network. Additionally, while we go to great lengths to protect patient and colleague information entrusted to us, as part of our ongoing commitment to the security of information in our care, we are further evaluating our data security policies and procedures.

What You Can Do. We are providing notice of this event to you, so that you may take further steps to protect the patient's protected health information should you feel it is appropriate to do so. We encourage you to review the information in the attached "*Steps You Can Take to Protect Information.*"

Trinity Health is also offering the patient complimentary access to credit monitoring services as appropriate to the information impacted. Information on these services and enrollment directions are in the attached information.

For More Information. I want to assure you that we take the responsibility to safeguard protected health information very seriously. We apologize for any inconvenience or concern this situation may have caused you. If you have any additional questions or concerns, please do not hesitate to call (855) 935-6070 from 8:00 a.m. - 5:30 p.m. Central Time, Monday - Friday, or email THresponse@kroll.com

Español (Spanish) https://www.trinity-health.org/accellion-data-event/

Sincerely,

Trinity Health

Monica Lareau

Trinity Health, Privacy Official

Steps You Can Take to Protect Information

Credit Monitoring Services:

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 two years. 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, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

You have until **July 4, 2021** to activate your identity monitoring services.

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

If you are under 18 and wish to activate identity monitoring services, please email us at THresponse@kroll.com so that we can adjust the services offered as credit monitoring is not available to individuals under 18 years old.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938

Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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 North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

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

KROLL

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'll 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.

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.

Trinity Health

About Trinity Health

Trinity Health, based in Livonia, Mich., is one of the largest multi-institutional Catholic health care systems in the nation, serving diverse communities that include more than 30 million people across 22 states. Trinity Health includes 92 hospitals, as well as 113 continuing care locations that include PACE programs, senior living facilities, and home care and hospice services. Its continuing care programs provide nearly 2.5 million visits annually. For more information, visit www.trinity-health.org and Location Results (trinity-health.org). Trinity Health provides information technology services for the health care system and some former members of the health system, including email hosting and file transfer services. Trinity Health functions as a business associate (as defined by HIPAA) to its member hospitals and affiliated medical groups.

Trinity Health Current and Affected Former Member Organizations

Listed below are the locations of Trinity Health hospitals and medical groups affiliated with the hospitals

California (Fresno)
Saint Agnes Medical Center
www.samc.com

Connecticut (Hartford)
Trinity Health Of New England
www.trinityhealthofne.org

Delaware (Wilmington)
Trinity Health Mid-Atlantic
www.trinityhealthma.org

Florida (Fort Lauderdale)
Holy Cross Health Fort Lauderdale
www.holy-cross.com

Idaho (Boise, Nampa)
Saint Alphonsus Health System
www.saintalphonsus.org

Illinois (Greater Chicago)
Loyola Medicine
www.loyolamedicine.org

Mercy Hospital and Med. Center
www.mercy-chicago.org

Indiana (South Bend)
Saint Joseph Health System
www.sjmed.com

Iowa (Clinton, Sioux City, Dubuque, Mason City)
MercyOne
www.mercyone.org

Maryland (Silver Spring)
Holy Cross Health Silver Spring
www.holycrosshealth.org

Massachusetts (Springfield)
Trinity Health Of New England
www.trinityhealthofne.org

Michigan (Southeast)
Saint Joseph Mercy Health System
www.stjoeshealth.org

Mercy Health **(West)**
www.mercyhealth.com

New York
St. Peters Health Partners **(Albany)**
www.sphp.com

St. Joseph's Health **(Syracuse)**
www.sjhsyr.org

New Jersey
St. Francis Medical Center **(Trenton)**
www.stfrancismedical.org

Ohio (Columbus)
Mount Carmel Health System
www.mountcarmelhealth.com

Oregon (Baker City, Ontario)
Saint Alphonsus Health System
www.saintalphonsus.org

Pennsylvania (Greater Philadelphia)
Trinity Health Mid-Atlantic
www.trinityhealthma.org

On July 1, 2019 the below former Trinity Health locations joined Virtua Health. Trinity Health continued to provide information system services to these facilities in 2019 and 2020.

www.virtua.org
Virtua Our Lady of Lourdes Hospital, formerly known as Our Lady of Lourdes Medical Center **(Camden)**

Virtua Willingboro Hospital, formerly known as Lourdes Medical Center of Burlington County **(Burlington)**