29358

CommonSpirit

<<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>>,

CommonSpirit Health and its affiliated entities ("CommonSpirit") take the protection and proper use of your personal information very seriously. With that in mind, we are writing to tell you about a data security incident involving some of your personal information. While we have no evidence of misuse of your personal information, we are writing to you directly to explain the incident, our response to it, and steps you can take in addition to those you take every day to protect your personal information, should you feel it appropriate to do so.

CommonSpirit Health is the parent organization to Catholic Health Initiatives and Dignity Health facilities. CommonSpirit Health also is or has been associated with Centura Health and MercyOne (Iowa).

**What happened?**
On October 2, 2022, CommonSpirit detected a ransomware attack on our IT network. We immediately took steps to secure the network, which included proactively taking some systems offline, and began an investigation with the assistance of an external forensics vendor. The investigation determined that an unauthorized third party gained access to our network between September 16, 2022 and October 3, 2022. While the unauthorized third party did not retrieve data directly from CommonSpirit's Electronic Medical Records systems, during that time the unauthorized third party obtained copies of some of the data on our systems, including files from two file share servers that contained some employee information. CommonSpirit had used the data on the file share servers in performing various operational functions, and some of the data dates back several years. With respect to the data on the file share servers, determining what and whose data was impacted has required a detailed and time-consuming review of each individual file on each file server to identify the specific individuals whose information may have been impacted, and the type of information associated with each such individual. The initial phase of this part of the investigation was completed on February 21, 2023. Once this component of the review concluded, we worked to identify the individuals' relationship to CommonSpirit and determined that some of the data was associated with a limited number of both current and former CommonSpirit employees. We then worked to identify accurate address information to provide notice to potentially affected individuals and only recently completed these efforts.

**What information was involved?**
Our information shows that you may work or have worked at a CommonSpirit or associated location, or are a dependent of a current or former employee. You are being notified because some of your information was identified in the file share server files that were compromised.

The information in the files may have included personal information such as your <<b2b_text_3(name, address, data elements)>><<b2b_text_4(data elements cont.)>>. Importantly, your Social Security number was included in the information.

**What we are doing.**
Upon discovering the ransomware attack, CommonSpirit quickly mobilized to protect its systems, contain the incident, begin an investigation, and maintain continuity of care. In addition, CommonSpirit notified law enforcement. Once secured, systems were returned to the network with additional security and monitoring tools.

To help relieve concerns and restore confidence following this incident, CommonSpirit has secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll 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.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
*You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.*
Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

**Actions you may wish to take.**
Though CommonSpirit has no evidence that any of the personal information in these files has been misused as a result of the incident, it is always prudent for you to undertake your own steps and measures to secure your personal and credit information. Additionally, please review the enclosed "Additional Resources" section of this letter. That section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to contact the major credit bureaus along with how to place a free fraud alert or a security freeze on your credit file(s) if you desire to do so.

**For more information.**
If you need more information about this event, we have established a special call center with a trusted third-party partner, Kroll, that can answer specific questions about this event. To contact this special call center, please call (866) 869-0312, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding U.S. holidays.

We apologize for any concern this may cause. Protecting your information is important to us. We trust that this notification and additional resource information demonstrates our continued commitment to you.

Sincerely,

Lori Lamb
Privacy Officer
CommonSpirit Health

**ADDITIONAL RESOURCES**

**Contact information for the three nationwide credit reporting agencies:**

**Equifax**, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
**Experian**, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
**TransUnion**, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

**Free Credit Report.** It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

**For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:** You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

**Fraud Alerts.** There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

**Security Freeze.** You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

**Federal Trade Commission and State Attorneys General Offices.** If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

**For Maryland residents:** You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

**For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

**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 Connecticut residents:** You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

**For Massachusetts residents:** You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

**Reporting of identity theft and obtaining a police report.**

**For Iowa residents:** You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

**For Massachusetts residents:** You have the right to obtain a police report if you are a victim of identity theft.

**For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

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.