June 27, 2023

ITASCA COUNTY HEALTH & HUMAN SERVICES
NOTICE OF DATA SECURITY INCIDENT

To Whom it May Concern:

Recently, Itasca County Health & Human Services ("Itasca HHS") discovered that there was an unauthorized activity involving one Itasca HHS employee's email account. On June 27, 2023, we mailed notifications to individuals whose protected health information and/or personal information may have been subject to unauthorized access and acquisition. Unfortunately, we did not have sufficient contact information to provide written notice to some individuals. To notify those individuals for whom we do not have sufficient contact information, we are posting this notice on our website and providing a toll-free telephone number, **(833) 804-0771**, which can be called Monday through Friday, 8 AM – 10 PM CST, and Saturday through Sunday 10 AM – 7 PM CST (excluding major U.S. holidays) to determine whether an individual's personal information was included in the data potentially impacted by this incident. Please be prepared to provide the following engagement number: **B097607**.

At this time, we are not aware of any misuse of the information involved in this incident. Nonetheless, we are providing this notice to inform potentially impacted individuals, offer complimentary identity monitoring services to those whose Social Security number and/or driver's license number was involved, and suggest ways that individuals can protect their information.

What Happened

In April, we learned that one Itasca HHS employee's email account was sending unauthorized spam emails. We began an investigation with the assistance of a nationally recognized digital forensics team, to further understand what happened and whether there was unauthorized access to the email box. On April 28, 2023, we determined there was intermittent unauthorized access to the Itasca HHS employee's email account between April 7 and April 11, 2023, and that the contents of the email box appeared to have been copied by the unauthorized actor. Once we learned this, we reviewed the contents of the email box to establish what information may have been involved, who may have been affected, and where those people reside so that we could provide notice.

What Information Was Involved

The impacted emails contained information that we maintain to help us provide services to the people of Itasca County including an individual's name or partial name, together with some or all of the following kinds of information: address, date of birth, Social Security number, and information regarding services provided to individuals and/or paid for by Itasca HHS, such as provider names, locations of service, dates of service, case numbers or unique identifiers related to services provided by Itasca HHS, demographic or family referral information, and/or insurance or billing information. The information may have also included insurance identification number, information regarding physical, medical, or mental health conditions, diagnoses, and/or treatment, medications, or information related to substance use. For one individual, a driver's license number was also impacted.

What We Are Doing About It

Because of this incident we have taken steps to ensure the security of all Itasca HHS email accounts and worked to review the contents of the impacted email account. To further strengthen the security of the information we maintain, and to help prevent similar incidents in the future, we have taken or will be taking the following steps:

1. Limiting outside access to our network;
2. Enhancing employee cybersecurity awareness training by including additional training on recognizing phishing attempts; and
3. Engaging a third-party vendor to provide incident response planning and cybersecurity testing services.

Additionally, we are providing notice of this incident to the United States Department of Health and Human Services and appropriate state regulators.

What You Can Do

We recommend that you take the following preventative measures to help protect your information:

1. If your Social Security number and/or driver's license was impacted by this incident, enroll in a complimentary, one-year membership with Experian. This membership will provide you with identity monitoring services, including a copy of your credit report at signup; credit monitoring; identity restoration; Experian IdentityWorks ExtendCARE; and up to $1 million in identity theft insurance. If you did not receive a notification letter and believe you may be eligible for these services, you can reach out to us at our toll-free number.

2. Remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements, free credit reports, and any health insurance Explanation of Benefits (EOB) forms for unauthorized or suspicious activity. Information on additional ways to protect your information, including how to obtain a free credit report and free security freeze, can be found at the end of this letter.

3. Report any incidents of suspected identity theft to your local law enforcement, state Attorney General and the major credit bureaus.

For More Information

Please accept our apologies that this incident occurred. We remain fully committed to maintaining the privacy of personal information in our possession and will continue to take many precautions to safeguard it.

Sincerely,

Eric Villeneuve
Itasca County HHS Director

MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit https://www.experian.com/blogs/ask-experian/category/fraud-and-identity-theft/ for general information regarding identity protection. You can obtain additional information about fraud alerts, security freezes, and preventing identity theft from the consumer reporting agencies listed below and the Federal Trade Commission (FTC) by calling its identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at https://consumer.ftc.gov/features/identity-theft. The FTC's address is: Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You have the ability to place a security freeze on your credit reports by contacting the following agencies.

National Credit Reporting Agencies Contact Information

Equifax	**Experian**	**TransUnion**
P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 www.equifax.com	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain your credit reports from each of the national consumer reporting agencies. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies listed above. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/articles/pdf/pdf-0093-annual-report-request-form.pdf and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report. You may be able to 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.

If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

Fraud Alerts

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. As soon as one credit bureau confirms the fraud alert, they will notify the others. Additional information is available at www.annualcreditreport.com.

Security Freeze

You have the ability to place a security freeze on your credit report at no cost to you. 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 be able to use an online process, an automated telephone line,

or a written request to all three of the 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 five years; (5) a legible copy of a government-issued identification card, (6) proof of current address, such as a legible copy of a recent utility bill or bank or insurance statement, (7) a legible copy of a recent W-2, pay stub, or Social Security card, and (8) if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. **Under federal law, you cannot be charged to place, lift, or remove a security freeze.**

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.

Additional Helpful Information

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 at the information provided above. This notice was not delayed as a result of a law enforcement investigation.

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.