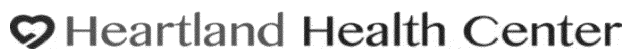
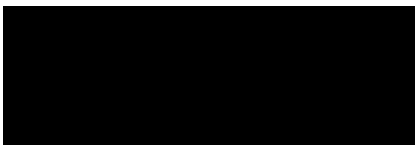


Heartland Health Center
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



Embracing people, inspiring health

a nebraska health⁺center



October 17, 2025

RE: Important Security Notification

Please read this entire letter.

Dear [REDACTED]

Notice of Data Incident

We are writing to inform you of an incident that may have affected some of your personal information. While there is currently no indication your personal information identified was used, there is reason to believe it may have been accessed during this incident.

What Happened

Heartland Health Center (hereinafter "Heartland Health") discovered it was the victim of an unknown third party gaining unauthorized access to the Heartland Health network environment. Heartland Health discovered the incident on February 4, 2025.

Upon learning of the issue, Heartland Health immediately engaged the appropriate forensic consultants to investigate the root of the incident, secure its systems, prevent this issue from reoccurring, and identify any sensitive or personal information that may have been impacted as a result.

Our investigation determined that data may have been exposed without authorization. Thereafter, Heartland Health conducted a thorough review of the contents of the files to determine if they contained any sensitive information. On June 3, 2025, after completing the extensive and exhaustive review, Heartland Health learned certain personal or sensitive information contained in its environment may have been exposed as result of the incident. Since that time, Heartland Health has been working diligently and exhaustively to identify and obtain sufficient information in order to provide you with this notice.

What Information Was Involved

This incident involved a combination of your name and Social Security number, date of birth, driver license number, financial account number, username and access information for a non-financial account, date of medical service, medical diagnosis information, individual health insurance policy number, physician or medical facility information, medical condition or treatment information, medical record number, Medicare or Medicaid number, patient account number, certificate or license number, full face photo and referral. As a result, your personal information may have been potentially exposed to others.

What We Are Doing

Please be assured that we have taken every step necessary to address the incident. We take our obligation to safeguard the information we receive seriously. Once the incident was discovered, we quickly took action to minimize risks, including securing the compromised systems and initiating an investigation into the unauthorized access. We also utilized additional resources in an effort to assess the impact of the incident and better protect Heartland Health from future instances like this one. We remain vigilant, continuously upgrading our already robust security measures to carefully safeguard against similar incidents.

000010103G0500

P

In response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do

If you believe there was fraudulent use of your information as a result of this incident, please review the Reference Guide at the end of this letter for additional steps on how to protect against identity theft and fraud.

To enroll in credit monitoring services at no charge, please visit **www.mytrueidentity.com** and follow the instructions provided. When prompted, please provide the following unique code to receive services: [REDACTED]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information

We sincerely regret any inconvenience or concern caused by this incident. Representatives are available Monday through Friday, from 8 a.m. to 8 p.m. Eastern Time, for 90 days from the date of this letter, to assist with any questions regarding this incident. Please call 1-833-426-5380 and supply the fraud specialist with your unique code listed above. To extend these services, enrollment in the monitoring services described below is required.

While call center representatives should be able to provide thorough assistance and answer most of your questions, you may still feel the need to speak with Heartland Health Center regarding this incident. If so, please contact our Operations Director, Laura Salber at inquiries@hhcne.org or (308) 646-3568.

Sincerely,

Tami Smith

Tami Smith
Chief Executive Officer
Heartland Health Center

REFERENCE GUIDE

Review Your Account Statements

Carefully review statements sent to you from your healthcare providers, insurance company, and financial institutions to ensure that all of your account activity is valid. Report any questionable charges promptly to the provider or company with which you maintain the account.

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the following contact information: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.ftc.gov/idtheft/.

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, GA 30348	1-888-766-0008	www.equifax.com
Experian	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a security freeze 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; 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, display your name and current mailing address, and the date of issue.



00001020380000

P

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	1-800-685-1111 www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	1-888-397-3742 www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	1-888-909-8872 www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

Provide Any Updated Personal Information to Your Health Care Provider

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so that they can make sure that all of your information is up to date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

Additional Information

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).

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Contact the District of Columbia Office of Attorney General for steps to avoid identity theft: (202) 727-3400, 400 6th Street, NW, Washington DC 20001, <http://oag.dc.gov>.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Maryland Attorney General: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

Massachusetts Residents: You have the right to obtain a police report and request a free security freeze as described above.

New York Residents: You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Attorney General at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755 or 1-800-7889898; <https://ag.ny.gov/>. You also may contact the Bureau of Internet and Technology (BIT), 28 Liberty Street, New York, NY 10005; 212-416-8433; <https://ag.ny.gov/about/about-office/economic-justice-division#internet-technology>.

North Carolina Residents: You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6400; www.ncdoj.gov.

Oregon Residents: We encourage you to report suspected identity theft to the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; 1-877-877-9392 or 1-503-378-4400; www.doj.state.or.us.

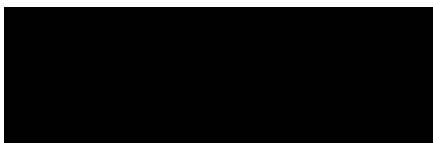
Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400.

South Carolina Residents: You can obtain information from the South Carolina Department of Consumer Affairs: 293 Greystone Blvd., Ste. 400, Columbia, SC 29210; 800-922-1594; www.consumer.sc.gov.

Texas Residents: You can obtain information from the Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; www.texasattorneygeneral.gov/consumer-protection/.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

New Mexico: You have rights pursuant to the Fair Credit Reporting Act. These rights include knowing what is in your file and your credit score; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; to be told if information in your credit file has been used against you; as well as other rights. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. For more information about the FCRA, and your rights pursuant to the FCA, please visit https://files.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.



17 de octubre de 2025

RE: Notificación Importante de Seguridad

Lea esta carta completa.

Estimado/a ,

Aviso de Incidente de Datos

Le escribimos para informarle sobre un incidente que podría haber afectado parte de su información personal. Si bien actualmente no hay indicios de que se haya utilizado su información personal, existen motivos para creer que se pudo haber accedido a ella durante este incidente.

¿Qué sucedió?

Heartland Health Center (en adelante, "Heartland Health") descubrió que fue víctima de un acceso no autorizado a la red de Heartland Health por parte de un tercero desconocido. Heartland Health descubrió el incidente el 4 de Febrero de 2025.

Al enterarse del problema, Heartland Health contrató de inmediato a los consultores forenses correspondientes para investigar la causa del incidente, proteger sus sistemas, evitar que se repitiera e identificar cualquier información confidencial o personal que pudiera haberse visto afectada.

Nuestra investigación determinó que los datos podrían haber sido expuestos sin autorización. Posteriormente, Heartland Health realizó una revisión exhaustiva del contenido de los archivos para determinar si contenían información confidencial. El 3 de Junio de 2025, tras completar la revisión exhaustiva, Heartland Health tuvo conocimiento de que cierta información personal o confidencial de su entorno podría haber sido expuesta como resultado del incidente. Desde entonces, Heartland Health ha trabajado diligentemente y exhaustivamente para identificar y obtener información suficiente para enviarle este aviso.

¿Qué Información Estuvo Involucrada?

Este incidente involucró una combinación de su nombre y Número de Seguro Social, fecha de nacimiento, número de licencia de conducir, número de cuenta financiera, nombre de usuario e información de acceso para una cuenta no financiera, fecha de servicio médico, información de diagnóstico médico, número de póliza de seguro de salud individual, información del médico o centro médico, información de condición médica o tratamiento, número de registro médico, número de Medicare o Medicaid, número de cuenta del paciente, número de certificado o licencia, foto de rostro completo y referencia. Como resultado, su información personal podría haber sido expuesta a terceros.

Qué Estamos Haciendo

Le aseguramos que hemos tomado todas las medidas necesarias para abordar el incidente. Nos tomamos muy en serio nuestra obligación de proteger la información que recibimos. Una vez detectado el incidente, actuamos rápidamente para minimizar los riesgos, incluyendo la protección de los sistemas comprometidos y el inicio de una investigación sobre el acceso no autorizado. También utilizamos recursos adicionales para evaluar el impacto del incidente y proteger mejor a Heartland Health de futuros incidentes como este. Nos mantenemos alertas, actualizando continuamente nuestras ya robustas medidas de seguridad para protegernos cuidadosamente contra incidentes similares.

000010303000000

P

En respuesta al incidente, le brindamos acceso gratuito a los servicios de **Monitoreo de Crédito de Agencia Única/Informe de Crédito de Agencia Única/Puntaje de Crédito de Agencia Única**. Estos servicios le envían alertas durante doce (12) meses a partir de la fecha de inscripción cuando se producen cambios en su historial crediticio. Esta notificación se le envía el mismo día en que se realiza el cambio o la actualización con la agencia. Finalmente, le brindamos asistencia proactiva contra el fraude para ayudarlo con cualquier pregunta que pueda tener o en caso de ser víctima de un fraude. Estos servicios serán proporcionados por Cyberscout, una empresa de TransUnion especializada en asistencia y remediación de fraudes.

Qué Puede Hacer

Si cree que se ha producido un uso fraudulento de su información como resultado de este incidente, consulte la Guía de referencia al final de esta carta para obtener más información sobre cómo protegerse contra el robo de identidad y el fraude.

Para inscribirse en los servicios de monitoreo de crédito gratuitos, visite **www.mytrueidentity.com** y siga las instrucciones. Cuando se le solicite, proporcione el siguiente código único para recibir los servicios: [REDACTED]. Para recibir los servicios de monitoreo descritos anteriormente, debe inscribirse dentro de los 90 días posteriores a la fecha de esta carta. La inscripción requiere conexión a internet y una cuenta de correo electrónico, y podría no estar disponible para menores de 18 años. Tenga en cuenta que, al registrarse en los servicios de monitoreo, es posible que se le solicite que verifique su información personal para su propia protección y así confirmar su identidad.

Para Más Información

Lamentamos sinceramente cualquier inconveniente o inquietud ocasionada por este incidente. Los representantes están disponibles de Lunes a Viernes, de 8:00 a. m. a 8:00 p. m., hora del este, durante 90 días a partir de la fecha de esta carta, para ayudarlo con cualquier pregunta relacionada con este incidente. Llame al 1-833-426-5380 y proporcione al especialista en fraude su código único indicado anteriormente. Para ampliar estos servicios, es necesario inscribirse en los servicios de monitoreo que se describen a continuación.

Si bien los representantes Del centro de llamadas deberían poder brindarle asistencia completa y responder a la mayoría de sus preguntas, es posible que aún necesite hablar con Heartland Health Center sobre este incidente. De ser así, comuníquese con nuestra Directora de Operaciones, Laura Salber, a inquiries@hhcne.org o al (308) 646-3568.

Atentamente,

Tami Smith

Tami Smith
Chief Executive Officer
Heartland Health Center