Cherry Health
Comprehensive. Quality. *Healthcare.*

Heart of the City Health Center
100 Cherry Street SE
Grand Rapids, MI 49503

Cherry Street Services, Inc. - Notice of Data Privacy Event

June 18, 2026

Cherry Street Services, Inc. ("Cherry Health") is providing notice of an event that may involve information related to certain current or former patients and current or former staff members. Although **Cherry Health presently has no evidence that any such information has been used to commit identity theft or fraud**, Cherry Health is providing information about the event, the steps taken in response, and resources available to individuals to help protect their information from possible misuse, should they feel it is appropriate to do so.

What Happened. On or about April 19, 2026, Cherry Health became aware of suspicious activity relating to its network. Cherry Health promptly took measures to secure its environment and launched an investigation with the support of third-party specialists to determine the nature and scope of the activity. The investigation determined that certain information on Cherry Health's network was accessed and copied by an unauthorized individual.

Cherry Health is conducting a comprehensive review of the data involved, in partnership with third-party specialists, to determine which information was at issue and to whom it relates. Cherry Health will notify potentially affected individuals by written letter once the review is finalized, and will have call center representatives available to help answer questions. Potentially affected individuals can review the below *Steps You Can Take to Protect Personal Information*, which contains helpful guidance.

What Information Is Involved. While this review is ongoing, the affected data may include, but not be limited to, individuals' names along with addresses, phone numbers, dates of birth, health insurance information, health insurance ID numbers, patient ID numbers, provider names, service dates, and, in a limited number of cases, Social Security numbers. Importantly, the potentially impacted information may vary for each individual and may include several or just one of the above-listed types of data.

What Are We Doing. Cherry Health takes this event and the security of the information in its care very seriously. As part of its ongoing commitment to protecting the privacy of information in its care, Cherry Health is working to implement additional safeguards to reduce the likelihood of a similar incident in the future. Cherry Health is also providing individuals with guidance on how to protect against identity theft and fraud.

What Can I Do. Individuals should remain vigilant against incidents of identity theft by reviewing account statements and credit reports for unusual activity and errors. Any suspicious activity should be promptly reported to relevant parties. Additional information on protecting against identity theft and fraud can be found in the below *Steps You Can Take To Protect Personal Information*.

For More Information. Individuals seeking additional information regarding this event may write to Cherry Health at 100 Cherry St SE, Grand Rapids, MI 49503, or call (888) 204-2407.

Steps You Can Take To Protect Personal Information

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victims of identity theft, they are entitled to an extended fraud

alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069, Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, 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, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

Cherry Health
Comprehensive. Quality. *Healthcare.*

Heart of the City Health Center
100 Cherry Street SE
Grand Rapids, MI 49503

Cherry Street Services, Inc. - Aviso sobre Evento de Privacidad de Datos

18 de Junio de 2026

Cherry Street Services, Inc. ("Cherry Health") está proporcionando un aviso sobre un evento que podría involucrar información relacionada con ciertos pacientes actuales o anteriores, así como con ciertos miembros del personal actuales o anteriores. Aunque **Cherry Health actualmente no tiene evidencia de que dicha información haya sido utilizada para cometer robo de identidad o fraude**, Cherry Health está brindando información sobre el evento, las medidas tomadas en respuesta y los recursos disponibles para las personas, a fin de ayudarles a proteger su información de un posible uso indebido, en caso de que consideren apropiado hacerlo.

Qué sucedió. El o alrededor del 19 de abril de 2026, Cherry Health tomó conocimiento de actividad sospechosa relacionada con su red. Cherry Health tomó medidas de inmediato para asegurar su entorno e inició una investigación con el apoyo de especialistas externos para determinar la naturaleza y el alcance de la actividad. La investigación determinó que cierta información en la red de Cherry Health fue accedida y copiada por una persona no autorizada.

Cherry Health está llevando a cabo una revisión exhaustiva de los datos involucrados, en colaboración con especialistas externos, para determinar qué información estaba en cuestión y a quién corresponde. Cherry Health notificará a las personas potencialmente afectadas mediante carta escrita una vez que se finalice la revisión, y contará con representantes del centro de llamadas disponibles para ayudar a responder preguntas. Las personas potencialmente afectadas pueden revisar los siguientes *pasos que puede tomar para proteger su información personal*, los cuales contienen orientación útil.

Qué información está involucrada. Si bien esta revisión continúa en curso, los datos afectados pueden incluir, entre otros, los nombres de las personas, junto con direcciones, números de teléfono, fechas de nacimiento, información del seguro médico, números de identificación del seguro médico, números de identificación de pacientes, nombres de proveedores, fechas de servicio y, en un número limitado de casos, números de Seguro Social. Es importante señalar que la información potencialmente impactada puede variar para cada individuo y puede incluir varios o solo uno de los tipos de datos mencionados anteriormente.

Qué estamos haciendo. Cherry Health toma muy en serio este evento y la seguridad de la información bajo su cuidado. Como parte de su compromiso continuo de proteger la privacidad de la información a su cargo, Cherry Health está trabajando para implementar salvaguardas adicionales con el fin de reducir la probabilidad de que ocurra un incidente similar en el futuro. Cherry Health también está proporcionando a las personas orientación sobre cómo protegerse contra el robo de identidad y el fraude.

Qué puedo hacer. Las personas deben mantenerse alerta ante incidentes de robo de identidad mediante la revisión de sus extractos de cuentas e informes de crédito para detectar actividad inusual o errores. Cualquier actividad sospechosa debe informarse de inmediato a las partes correspondientes. Se puede encontrar información adicional sobre cómo protegerse contra el robo de identidad y el fraude en los siguientes *pasos que puede tomar para proteger su información personal*.

Para más información. Las personas que busquen información adicional sobre este evento pueden escribir a Cherry Health en 100 Cherry St SE, Grand Rapids, MI 49503, o llamar al (888) 204-2407.

Pasos que puede tomar para proteger su información personal

Según la ley de EE. UU., un consumidor tiene derecho a un informe de crédito gratuito por año de cada una de las tres principales agencias de informes crediticios: Equifax, Experian y TransUnion. Para solicitar un informe de crédito gratuito, visite www.annualcreditreport.com o llame, sin costo, al 1-877-322-8228. Los consumidores también pueden comunicarse directamente con las tres principales

agencias de informes crediticios que se enumeran más abajo para solicitar una copia gratuita de su informe de crédito.

Los consumidores tienen derecho a colocar una "alerta de fraude" inicial o extendida en su archivo crediticio sin costo alguno. Una alerta de fraude inicial es una alerta con vigencia de un año que se coloca en el archivo crediticio del consumidor. Al ver una alerta de fraude en el archivo crediticio de un consumidor, una empresa está obligada a tomar medidas para verificar la identidad del consumidor antes de otorgar nuevo crédito. Si los consumidores son víctimas de robo de identidad, tienen derecho a una alerta de fraude extendida, la cual tiene una duración de siete años. Si los consumidores desean colocar una alerta de fraude, por favor comuníquense con cualquiera de las tres principales agencias de informes crediticios que se indican más abajo.

Como alternativa a una alerta de fraude, los consumidores tienen derecho a colocar un "congelamiento de crédito" en su informe de crédito, lo que prohibirá que una agencia de crédito divulgue información del informe sin la autorización expresa del consumidor. El congelamiento de crédito está diseñado para evitar que se aprueben créditos, préstamos y servicios a nombre del consumidor sin su consentimiento. Sin embargo, los consumidores deben tener en cuenta que utilizar un congelamiento de crédito para tomar control sobre quién tiene acceso a la información personal y financiera en su informe de crédito puede retrasar, interferir o impedir la aprobación oportuna de cualquier solicitud o petición posterior que realicen en relación con un nuevo préstamo, crédito, hipoteca o cualquier otra cuenta que implique la extensión de crédito. De acuerdo con la ley federal, no se puede cobrar a los consumidores por colocar o levantar un congelamiento de crédito en su informe de crédito. Para solicitar un congelamiento de crédito, las personas pueden necesitar proporcionar parte o toda la siguiente información:

1. Nombre completo (incluyendo la inicial del segundo nombre, así como Jr., Sr., II, III, etc.);
2. Número de Seguro Social;
3. Fecha de nacimiento;
4. Direcciones de los dos a cinco años anteriores;
5. Comprobante de dirección actual, como un recibo de servicios públicos o de teléfono vigente;
6. Una fotocopia legible de un documento de identificación emitido por el gobierno (licencia de conducir estatal, tarjeta de identificación, etc.); y
7. Una copia del informe policial, del informe de investigación o de la denuncia presentada ante una agencia del orden público relacionada con el robo de identidad, en caso de ser víctima de robo de identidad.

Si los consumidores desean colocar un congelamiento de crédito o una alerta de fraude, por favor comuníquense con las tres principales agencias de informes crediticios que se enumeran a continuación:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069, Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, 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, P.O. Box 160, Woodlyn, PA 19094

Información adicional

Los consumidores pueden informarse más sobre el robo de identidad, las alertas de fraude, los congelamientos de crédito y las medidas que pueden tomar para proteger su información personal comunicándose con las agencias de informes crediticios, la Comisión Federal de Comercio (FTC, por sus siglas en inglés) o con el Fiscal General de su estado. La Comisión Federal de Comercio puede ser contactada en: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-

Heart of the City Health Center
100 Cherry Street SE
Grand Rapids, MI 49503

THEFT (1-877-438-4338); y TTY: 1-866-653-4261. La Comisión Federal de Comercio también alienta a aquellos que descubran que su información ha sido utilizada de manera indebida a presentar una queja ante ellos. Los consumidores pueden obtener más información sobre cómo presentar dicha queja a través de la información de contacto mencionada anteriormente. Los consumidores tienen derecho a presentar un informe policial si alguna vez son víctimas de robo de identidad o fraude. Tenga en cuenta que, para presentar un informe ante las autoridades por robo de identidad, es probable que los consumidores deban proporcionar alguna prueba de que han sido víctimas. Los casos de robo de identidad conocido o sospechoso también deben ser reportados a las autoridades policiales y al Fiscal General del estado correspondiente. Este aviso no ha sido retrasado por ninguna autoridad policial.