

Healthcare Highways – Notice of Data Event

Frisco, TX – October 2, 2026 - Healthcare Highways, LLC (“HCH”) is providing notice of a recent event that may involve information pertaining to certain individuals. While there is no indication of actual or attempted fraud or identity theft associated with this event, HCH is providing information about the event, the steps taken in response, and resources available to individuals to help protect their information, should they deem it appropriate to do so.

What Happened. On August 4, 2026, HCH identified suspicious activity in its network environment. HCH promptly took steps to ensure the security of its network and launched an investigation. The investigation, while ongoing, determined that certain information on HCH’s network was accessed and copied by an unauthorized user between July 22, 2026, and July 27, 2026.

As part of the ongoing investigation, HCH is undertaking a comprehensive review of the data involved to determine what information may be affected and to whom the information relates. This review is ongoing. HCH will provide notice to potentially affected individuals once the review is finalized. Potentially affected individuals can review the below ***Steps You Can Take to Protect Personal Information***.

What Information Was Involved. While HCH’s review of the potentially affected data is ongoing, the information involved in the event varies and may include, but not be limited to, individuals’ names along with address, date of birth, Social Security number, dates of service, patient ID number, procedure codes, procedure costs, procedure and provider information, diagnosis, health insurance information, claim information, and information related to the payment of healthcare services.

What We Are Doing. HCH takes the confidentiality, privacy, and security of information in HCH’s care very seriously. Upon becoming aware of the suspicious activity, HCH promptly commenced an investigation to confirm the nature and scope of the event. HCH also reported the event to law enforcement and have implemented additional cybersecurity measures to further protect against similar events moving forward.

For More Information. If you have further questions, you may contact us at compliance@healthcarehighways.com, write to us at One Cowboys Way, Suite 290, Frisco, Texas 75034, or call toll-free at (866) 945-2292.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits and monitoring your free credit reports for suspicious activity and to detect errors. Any suspicious activity or errors 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.

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. To order a free credit report, visit <http://www.annualcreditreport.com/>, call toll-free 1-877-322-8228, or complete an Annual Credit Report Request Form and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax	Experian	TransUnion
P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285	P.O. Box 9532 Allen, TX 75013 1-888-397-3742	P.O. Box 2000 Chester, PA 19016 1-800-916-8800

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed above.

In order to request a security freeze, you may need to provide some or all of the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a one-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 consumer reporting agencies.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state attorney general.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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.