

Notice of Data Breach

September 11, 2025: HealthCall of Detroit (“HealthCall”) takes privacy and security very seriously. As part of that commitment, we are notifying you of a data privacy incident involving the protected health information of certain HealthCall patients. We were unable to locate addresses of the individuals whose information was involved. As a result, we are issuing this public notice to inform all potentially impacted individuals. This notice explains the incident, our response, and steps you can take to help protect your personal information.

What Happened: On April 24, 2025, HealthCall became aware of technical issues related to systems in our network. Upon discovery, we took immediate action to secure our network and to address the incident, which included engaging outside cybersecurity specialists to investigate. After a thorough investigation, we learned that an unauthorized actor gained access to our systems between April 21, 2025 and April 24, 2025. After a comprehensive review, on June 2, 2025, we determined that system folders containing certain patients’ protected health information, including names, dates of birth, gender, and diagnosis/condition information, were accessed and acquired by the unauthorized actor.

What We Are Doing: We have notified law enforcement and are implementing further additional security safeguards. We also include information that identifies resources that are available to you regarding information security and credit protection in the enclosed “*Steps You Can Take to Help Protect Your Information.*”

What You Can Do: As a general matter, it is important to be vigilant against incidents of identity theft and fraud by reviewing your credit reports and account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, you should promptly contact the financial institution or company. We have provided additional information below, which contains steps you can take to help protect yourself against fraud and identity theft, should you feel it appropriate to do so.

For More Information: If you believe your information may have been involved in this incident or have any questions, please do not hesitate to contact our dedicated assistance line through TransUnion at 1-800-405-6108 between the hours of 8:00 am and 8:00 pm EST, Monday through Friday, excluding holidays.

Please know that the security of our patients’ information is of the utmost importance to us. We remain committed to safeguarding the trust our patients have placed in us and are deeply grateful for your continued support during this time.

Sincerely,

HealthCall of Detroit

Enclosure: *Steps You Can Take to Help Protect Your Information*

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts and Credit Reports: One may be vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors.

Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended “fraud alert” on a credit 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, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your express authorization. The credit 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 credit freeze 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 credit freeze on your credit report. To request a credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788
--	--	--

Woodlyn, PA 19094	Allen, TX 75013	Atlanta, GA 30348-5788
-------------------	-----------------	------------------------

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them.

The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.