

Information About Recent Security Incident

Community Health Center of Buffalo Inc., (“CHCB”) is issuing notice of a recent data security event involving patient information. We are providing you with information about the event, our response, and steps you can take to protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so.

What Happened?

On April 21, 2026, CHCB became aware of suspicious activity within its computer network. In response, CHCB promptly took immediate action to further secure its network to avoid any substantial interruption to patient care. Additionally, CHCB launched an investigation, with the assistance of digital forensic and cybersecurity specialists, to determine the nature and scope of the activity. The investigation determined that there had been access to CHCB’s network by an unknown actor on April 20, 2026 and April 21, 2026. During that period of unauthorized access, certain files were accessed and/or acquired without CHCB’s authorization. CHCB is currently conducting a detailed review of the involved data, and will be providing written notice of this event to potentially impacted individuals. In the meantime, CHCB is providing this notice on our website homepage to make patients aware of the event.

Which Patients / What Information was Affected?

CHCB’s review of the impacted data is ongoing. CHCB will be providing written notice to those individuals whose information was potentially impacted with an offer of complimentary credit monitoring and identity theft protection services. That being said, it is expected that the following types of information were impacted in the event: name, address, date of birth, Social Security number, driver’s license, and medical and/or health insurance information including, but not limited to, prescription information, treatment location and information, medical diagnosis/condition, lab results, medications, medical record numbers, provider name, patient medical history, health insurance policy information and identification numbers, and other similar types of information.

What We are Doing.

The privacy of patient information is one of CHCB’s top priorities, and we have significant security in place to protect patient information in our care. As part of our ongoing commitment to data privacy, we are also working to review our existing policies and procedures. We will also be mailing notification letters to potentially impacted individuals and are notifying regulators as required. The letters will include an offer of complimentary credit monitoring.

What Affected Individuals Can Do.

We encourage you to remain vigilant against incidents of identity theft by reviewing account statements and explanations of benefits for unusual activity, and to report any suspicious activity promptly to your insurance company, health care provider, or financial institution. Additional detail can be found below in the below Steps You Can Take to Help Protect Your Information.

For More Information.

If you have questions, please call our dedicated assistance line at Call Center (toll free), Monday through Friday, from 8am – 8pm Eastern Time (excluding U.S. holidays). You may contact the assistance line at the following number: 844-507-8852. You may also write to CHCB at 34 Benwood Ave, Buffalo, New York 14214.3

Monitor Your Accounts

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 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 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 your name without your consent. However, you should be aware that using a credit 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 credit freeze on your credit report.

To request a security freeze, you will need to provide 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, military identification, etc.); 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:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, 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 Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. 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. This notice has not been delayed by law enforcement.