Return Processing Center:
PO Box 173071 | Milwaukee, WI 53217

Wilmington Community Clinic

[redacted]

Via First-Class Mail

December 10, 2025

Re: Notice of Data Breach

Dear [redacted]

Wilmington Community Clinic ("WCC") is writing to inform you of a recent data security incident that may have resulted in unauthorized access to some individuals' personal information. While we are unaware of any fraudulent misuse of personal information at this time, this notice is intended to provide details about the incident, steps we are taking in response, and resources available to help protect against the potential misuse of personal information.

What Happened?

On August 13, 2024, WCC discovered that its systems were potentially compromised by an unauthorized actor. Upon discovery of this incident, WCC immediately disconnected all access to the network and promptly engaged a specialized third-party cybersecurity firm and IT personnel to assist with securing the environment as well as to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The forensic investigation determined that that personal information may have been acquired by an unauthorized actor.

Based on these findings, WCC decided to proceed with an analysis of the compromised data for any potential sensitive personal information ("PII") or protected health information ("PHI"). WCC engaged a third-party vendor to review the data that was compromised. The data mining process took some time given the complexities of the types and the volume of the data analyzed, requiring multiple phases of automated and manual review. On October 13, 2025, WCC engaged a third-party notice vendor to assist with the mailings, call center, and provide identity theft protection services. Thereafter, WCC worked to verify the patient information and addresses for mailing. On November 18, 2025, WCC finalized the list of individuals to notify.

As of this writing, WCC has not received any reports of related identity theft since the date of the incident (August 13, 2024, to present).

What Information was Involved?

Although WCC has no evidence that any sensitive information has been misused by third parties as a result of this incident, we are notifying you out of an abundance of caution and for purposes of full transparency. Although the information varies by individual, based on the investigation, the following information may have been subject to unauthorized access: health insurance identification number, medical information, date of birth, driver's license number or state identification number and Name.

What We Are Doing:

Data privacy and security is among WCC's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Since the discovery of the Incident, we have taken and will continue to take steps to mitigate the risk of future issues. Specifically, we engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. Additionally, we disconnected all access to our network, restored operations in a safe and secure manner, enhanced our security measures, and took steps and will continue to take steps to mitigate the risk of future harm.

In light of the incident, we are also providing you with 12 months of complimentary credit monitoring and identity theft restoration services through HaystackID. While we are covering the cost of these services, you will need to complete the activation process by following the instructions below.

What You Can Do:

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

You may also activate the credit monitoring services we are making available to you at no cost. The deadline for enrolling is ninety (90) days from the date of this letter.

Credit Monitoring Enrollment Instructions

To enroll in the free credit monitoring services noted above, please log on to **app.identitydefense.com/enrollment/activate/WCC** 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 ninety (90) days from the date of this letter. Enrollment requires an internet connection and e-mail address and may not be available to minors under the age of eighteen (18) years of age. 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:

If you have any questions or concerns not addressed in this letter, please call 1-888-844-1319 (toll free), Monday through Friday, during the hours of 8:00 am to 11:00 pm Eastern time, and 9:00 am to 6:00 pm Eastern time (excluding U.S. national holidays).

We sincerely regret any concern or inconvenience this matter may cause and remain dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Wilmington Community Clinic

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze

You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert

You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission

For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) 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 should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

Contact Information

Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit--report-services
TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at https://dos.nysits.acsitefactory.com/consumerprotection; by visiting the New York Attorney General at https://ag/ny.gov or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or https://www.identitytheft.gov/#/.