



300 Held Drive
Northampton, PA 18067

<<Name 1>> <<Name 2>> <<Date>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

Dear <<Name 1>> <<Name 2>>:

Precision Medical, Inc. (“Precision”) is writing to make you aware of a recent incident that may affect the privacy of some of your personal information. You are receiving this notice as you are the current or former employee of Precision. We write to provide you with information about the incident, our response, and steps you can take to help protect against the possible misuse of your information, should you feel it is appropriate to do so.

What Happened? On September 9, 2022, Precision discovered suspicious activity within certain systems in our environment. In response, we quickly took steps to secure our network and began an investigation to determine the nature and scope of the activity. Our investigation confirmed an unauthorized individual accessed certain information in our environment between September 5, 2022 September 9, 2022. Given that certain information was accessed without authorization, we undertook a comprehensive review of the affected data to understand the specific information potentially impacted and to whom it related for purposes of providing notification to potentially impacted individuals. We completed those efforts on February 2, 2023, and thereafter worked to provide notification to potentially impacted individuals. We are notifying you because your information was present in the files accessible to the unauthorized individual, and therefore may have been accessed during this incident.

What Information Was Involved? Our investigation determined that the information related to you that may have been impacted includes your name and [Extra 1 – Data Elements].

What We Are Doing. We take the security of the information in our care very seriously. After discovering the suspicious activity, we promptly took steps to confirm our system security, and conducted a comprehensive investigation of the incident to confirm its nature, scope, and impact. We also promptly notified federal law enforcement of the incident. Further, as part of our ongoing commitment to the privacy and security of personal information in our care, we are reviewing and enhancing existing policies and procedures relating to data protection and security. We have instituted additional security measures to better protect against future similar incidents. We are also notifying relevant regulatory authorities, as required.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing account statements and monitoring your free credit reports for suspicious activity and to detect errors. You should report any such activity to law enforcement. Information on these resources is included below under *Steps You Can Take to Help Protect Personal Information*.

For More Information. We understand that you may have questions that are not addressed in this notice. If you have additional questions or concerns, please email inquiry@precisionmedical.com.

We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

Precision Medical, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

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 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 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, 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 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
888-298-0045	1-888-397-3742	1-800-916-8800
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.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.