<<First Name/Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip code>>

<<Date>>

Notice of Data Breach

Dear <<First Name/Last Name>>,

Prism Medical Products, LLC ("Prism") is writing to notify you of a recent security incident that may have involved some of your personal information, which Prism maintains in connection with the healthcare products and services it provides to you. We understand the trust you place in Prism to protect your personal and health information, and we recognize that receiving this notice may be concerning. Please read this letter carefully as it contains details about this incident and resources you may utilize to help safeguard your personal information.

What Happened.
On October 19, 2026, Prism personnel identified suspicious activity within portions of its environment. In response, Prism immediately engaged third-party cybersecurity specialists to help determine the nature and scope of the incident.

The investigation revealed that an unauthorized third party gained access to portions of Prism's environment and appears to have accessed and obtained certain files belonging to Prism.

What Information Was Involved?

Prism promptly initiated a review and engaged a third-party vendor to help identify whose information may be potentially involved and to what extent. The specific categories of information affected by the security incident are different for each person depending on how you interacted with Prism. The information affected by the incident may include your name, address, phone number, and email address, along with one or more of the following: medical and clinical information, health insurance information, payment and financial account information, and certain identifiers, including government-issued identification numbers such as Social Security number, driver's license, and other forms of government identifiers.

What we are doing.

The confidentiality, privacy, and security of information maintained by Prism remain its top priority. Upon discovering the issue, we shut down impacted internal servers, disabled remote access, and reset credentials or disabled certain management and service accounts. Based on the steps we have taken, and the new secure environment we implemented, we believe our environment is safe and secure, and our operations are functioning properly.

As a precaution, Prism is also offering free credit monitoring and identity protection services through Cyberscout, a TransUnion company specializing in fraud assistance and remediation

services, to individuals who suspect their information may be involved in this incident. A description of these services and enrollment instructions are provided in the next section.

What You Can Do.

We encourage you to review the following resources:

1. **Register for Credit Monitoring Services.**

In response to the incident, we are offering you free credit and dark web monitoring services. If your minor child was impacted, you may also enroll your child as a parent or legal guardian at no charge for dark web monitoring services. These services provide alerts for 24 months from the date of enrollment when changes occur to your credit file. Credit alerts are sent on the same day that the change or update is reported to the bureau through the services. We are also providing proactive fraud assistance to help answer any questions you may have or assist you if you become a victim of fraud. These services will be provided by CyberScout, a TransUnion company specializing in fraud assistance and remediation services.

Key Features of the Services. The services offered include the following features:

- Single-bureau credit monitoring
- Single-bureau credit report
- Single-bureau credit score
- Dark web monitoring
- Health insurance plan number monitoring
- Medical record number monitoring
- Medical National Provider Identifier (NPI) monitoring
- Health savings account monitoring

How to Enroll. To enroll in the credit monitoring and related services at no charge, please call, toll-free, 1-855-711-8407, Monday through Friday, from 8:00 a.m. to 8:00 p.m. Eastern Time, excluding holidays. A call center representative will assist you with obtaining a unique enrollment code. Once you have the unique enrollment code, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted, please provide the unique enrollment code you received from the call center representative.

You must enroll within 90 days from the date this notice is published. Individuals under the age of 18 may not be able to enroll independently and will require a parent or legal guardian to assist with enrollment.

Parents Enrolling Minors. If you are a parent or legal guardian, you need to first complete enrollment for yourself by following the “How to Enroll” steps above. Once that is completed, click on your name in the top right of your dashboard and then “Add Family Member” to enroll your child. To complete the child’s enrollment, click on the child’s name and provide the requested information for monitoring.

The enrollment requires an internet connection and an email account. For your protection, you may be asked to verify personal information during enrollment to confirm your identity.

2. Review Your Accounts for Suspicious Activity.
We encourage you to remain vigilant by regularly reviewing your accounts and monitoring credit reports for suspicious activity.

3. Order a Credit Report.
If you are a U.S. resident, you are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. Contact information for the nationwide credit reporting agencies is provided in the next section.

4. Contact the Federal Trade Commission, Law Enforcement and Credit Bureaus.
You may contact the Federal Trade Commission ("FTC"), your state's Attorney General's office, or law enforcement, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's website at www.identitytheft.gov; call the FTC at 1-877-438-4338; or write to the FTC Consumer Response Center at 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
P.O. Box 105069 Atlanta, Georgia 30348 1-800-525-6285 www.equifax.com	P.O. Box 9554 Allen, Texas 75013 1-888-397-3742 www.experian.com	P.O. Box 2000 Chester, Pennsylvania 19016 1-800-916-8800 www.transunion.com

5. Additional Rights Under the FCRA.
You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here.

Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by: (i) visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf; or (ii) by writing to the Consumer Financial Protection Bureau, 1700 G Street, NW, Washington, DC 20552.

6. Request Fraud Alerts and Security Freezes.

You may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

Equifax Fraud Alert	Experian Fraud Alert	TransUnion Fraud Alert
P.O. Box 105069 Atlanta, Georgia 30348 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ 1-800-525-6285	P.O. Box 9554 Allen, Texas 75013 https://www.experian.com/help/fraud-alert/ 1-888-397-3742	P.O. Box 2000 Chester, Pennsylvania 19016 https://www.transunion.com/fraud-alerts 1-800-909-8872

In addition, you can contact the nationwide credit reporting agencies at the following numbers to place a security freeze at no cost to you:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788 Atlanta, Georgia 30348 https://www.equifax.com/personal/credit-report-services/credit-freeze/ 1-888-298-0045	P.O. Box 9554 Allen, Texas 75013 https://www.experian.com/help/credit-freeze/ 1-888-397-3742	P.O. Box 160 Woodlyn, Pennsylvania 19094 https://www.transunion.com/credit-freeze 1-800-916-8800

Placing a security freeze prohibits the agency from releasing any information about your credit report without your written authorization. Security freezes must be placed separately at each of the three nationwide credit reporting agencies. When requesting a security freeze, you may need to provide the following information:

- Your full name, with middle initial as well as Jr., Sr., II, etc.
- Social Security number
- Date of birth
- Current address and all addresses for the past two years

- Proof of current address, such as a current utility bill or telephone bill
- Legible copy of a government-issued identification card, such as a state driver's license, state identification card, or military identification.

For Iowa Residents. You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft at: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319; 1-515-281-5164; and www.iowaattorneygeneral.gov.

For Maryland Residents. You can obtain information about avoiding identity theft from the Maryland Attorney General at: Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023 (toll-free in Maryland) or 1-410-576-6300; www.marylandattorneygeneral.gov. Prism is located at 112 Church Street, Suite 101, Elkin, NC, 28621, and can be contacted at 1-855-711-8407.

For New York Residents. You can obtain information about security breach response, identity theft prevention, and identity protection information from the New York State Office of the Attorney General at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755 (toll-free) or 1-800-788-9898 (TDD/TTY toll-free line); https://ag.ny.gov/; and the Bureau of Internet and Technology (BIT), 28 Liberty Street, New York, NY 1000; 1-212-416-8433; and https://ag.ny.gov/resources/individuals/consumer-issues.

For North Carolina Residents. You can obtain information about avoiding identity theft from the North Carolina Attorney General at: North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 (toll-free in North Carolina) or 1-919-716-6400; and www.ncdoj.gov.

For Residents of Oregon. You may report suspected identity theft to law enforcement, including the Office of the Oregon Attorney General and the FTC. Contact information for the FTC is included in your notice. The Office of the Oregon Attorney General at: 1162 Court St. NE, Salem, OR 97301; 1-877-877-9392; and https://www.doj.state.or.us/.

For Rhode Island Residents. You can obtain information about avoiding identity theft from the Rhode Island Office of the Attorney General at: Rhode Island Office of the Attorney General, Consumer Protection Unit 150, South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. You have the right to obtain a police report, and to request a security freeze (charges may apply), as described above. Information pertaining to approximately 48 Rhode Island residents was potentially involved in this incident.

For Washington, DC Residents. You can obtain information about avoiding identity theft from the Office of the Attorney General for the District of Columbia at: Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, DC 20001; 1-202-727-3400; and www.oag.dc.gov. You have the right to request a security freeze (without any charge) as described above.

For More Information.

If you have concerns that are not addressed by this notice, Prism has established a dedicated toll-free call center for individuals to call should they have any additional questions or concerns.

The call center can be reached at 1-855-711-8407 (available Monday through Friday from 8:00 am to 8:00 pm ET, excluding holidays).

We are sorry for any concern or inconvenience this may cause. We appreciate the trust you place in Prism and remain committed to protecting your information while continuing to support your care.

Sincerely,
Prism Medical Products, LLC