

NOTICE OF DATA PRIVACY INCIDENT

DATE: MAY 14, 2026

NJ Pain Care Specialists. (“NJPCS”) is writing to provide information about a recent event involving certain information relating to patients. Although we are unaware of any attempted or actual misuse of your information, this letter contains additional information about the event, our investigation and response, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened? We recently detected unauthorized activity on certain systems within our network. We promptly took steps to contain the activity and launched an investigation, with the support of third-party cybersecurity specialists. This investigation determined an unauthorized actor gained access to a limited number of systems and certain servers within our network between February 25, 2026, and February 28, 2025, and may have removed certain information stored within those systems. We then took steps to thoroughly review and analyze the data to determine what was present within the potentially involved files and the patients and individuals to whom it relates. This review was recently completed.

What Information Was Involved? Based on our investigation to date, we determined that the impacted information varies by individual but may include name, address, date of birth, medical record number, driver’s license or other state ID number, clinical or treatment information, medical procedure information, medical provider name, prescription information, or health insurance information.

What NJPCS is Doing. Information privacy and security are among our highest priorities. Upon learning of this event, we moved quickly to investigate and respond to the incident, assess the security of our systems, restore functionality to our IT network, and undertake the processes needed to notify potentially affected individuals. As part of our ongoing commitment to information privacy and security, we reviewed and enhanced our technical, administrative, and physical safeguards, policies, and procedures, to further secure the information on our systems. We also reported this incident to the Federal Bureau of Investigation, who is responsible for investigating these cyber events, and appropriate federal and state data privacy regulators. We remain committed to complying with all state and federal requirements and maintaining timely and transparent communication with our community.

What You Can Do. We encourage individuals to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Suspicious activity should be promptly reported to relevant parties including an insurance company, healthcare provider, and/or financial institution. Additional information and resources may be found below in the *Steps Individuals Can Take to Protect Personal Information* section of this notice.

For More Information. Individuals seeking additional information may contact us at (732) 720-0247 between 10:00 A.M. and 2:00 P.M. Eastern time, excluding major U.S. holidays. Individuals may also write to NJPCS at 1806 Highway 35, Suite 305, Oakhurst, NJ 07755.

STEPS INDIVIDUALS CAN TAKE TO 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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, 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, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been

a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.