News

# Notice of Data Privacy Event

**January 6, 2026** – The Laurel Health Centers ("LHC" or "we") are providing notice that we experienced a cyber event. We take this event very seriously. In this notice, we provide information about the event, our comprehensive response to it, and resources available to help protect personal information. Potentially impacted individuals are being notified directly by letter. For more information or to confirm if you may have been impacted, please call our dedicated assistance line at **1-800-405-6108**.

**What Happened:**

On or about July 14, 2025, Laurel Health became aware of unusual activity in its email environment. Upon becoming aware, we immediately began an investigation into the scope and nature of the suspicious activity. We retained third-party forensic specialists and legal counsel to investigate the unusual activity. That investigation revealed certain information may have been viewed by an unauthorized individual as part of the event. This activity occurred between July 11, 2025, and July 25, 2025. While the investigation began promptly, it took time before we were able to conclusively determine the threat actor was out of our systems and did not have a way to get back in.

LHC and our forensic investigation team took prompt action to protect our data when first discovering the suspicious activity and remediated systems as quickly as reasonably possible. We then began a comprehensive review of the data set to determine what sensitive and/or personal information was potentially impacted and to whom it potentially related.

On December 30, 2025, we finished the review of the potentially impacted information and proceeded to notify potentially affected individuals and reporting agencies. This time was necessary to understand the scope of the situation as thoroughly as possible in order to make accurate notifications and determine the best course of action surrounding the event.

**What Information Was Involved:**

Our review found that certain identified individuals' names, date of birth, social security number (SSN), address, telephone number, email, medical record number, date of service, medical provider, Medicare information, insurance information, diagnostic information, treatment information, diagnosis information, insurance carrier, procedure codes, disability, dental, denture, immunization information, behavioral information, PA Account IDs, account number, credit card information, checking account information, and/or claim information were present within some or all of the viewed files; files may also have been copied.

While we are not aware of any actual or attempted misuse of this information to perpetrate fraud, out of an abundance of caution, we are notifying potentially impacted individuals and providing them with resources to further protect their information. Potentially impacted individuals are being notified directly by letter. If you have not received a letter and would like to confirm whether you could be impacted,

please call **1-800-405-6108**.

**What We Are Doing**:

We understand your concerns, and we take this event very seriously. The privacy, security, and confidentiality of information in our care are among our highest priorities. Due to their stringent security and safety measures, health systems are being targeted with increasingly sophisticated and complex cyber events.

Upon becoming aware of the event, we immediately retained additional systems experts to promptly investigate and respond to the event. While we are not aware of any actual or attempted misuse of this information to perpetrate fraud, we are notifying potentially affected individuals for whom we have a valid mailing address via U.S. mail out of an abundance of caution and offering them **free credit monitoring and identity protection services**. We are also notifying applicable regulators. We encourage those notified to err on the side of caution and take steps to protect against identity theft.

**How Will Individuals Know If They Are Affected by This Event?**

We are mailing a notice letter to individuals whose information was determined to be in the affected files for whom a valid mailing address is available. If an individual did not receive a letter but would still like to confirm if they could be affected, they may call our dedicated cyber event assistance line at **1-800-405-6108**.

**Who to Contact for More Information:**

Laurel Health has set up a dedicated assistance line specific to addressing questions about this event and providing help with next steps for affected individuals. If you have questions about this event or need support, please call our dedicated assistance line at **1-800-405-6108**, between the hours of 8:00 a.m. to 8:00 p.m. EST, Monday through Friday (excluding major U.S. holidays).

**What You Can Do:**

We encourage all individuals to remain vigilant against incidents of identity theft and fraud by **regularly reviewing their account statements** and **monitoring their credit reports** for suspicious or unauthorized activity. Please report any suspicious activity promptly to your bank, credit card company, or other applicable institution.

Potentially affected individuals are being offered **free credit monitoring and identity protection services** with instructions for how to sign up in their mailed notice letter. You may also personally place a **free security credit freeze** and/or **a free fraud alert** with the major U.S. credit bureaus, which advises the bureaus to contact you directly to verify your identity when there is an attempt to open new credit in your name.

Under U.S. law, individuals are 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

annualcreditreport.com or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (form available at https://consumer.ftc.gov/articles/free-credit-reports) to:

Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA, 30348-5281

**How to Place a Security Freeze (Credit Freeze)**:

You have the right to place a **security freeze on your credit report**. A security freeze or "credit freeze" is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a free security freeze on your credit report, you need to make a request to each consumer reporting agency: Equifax, Experian, and TransUnion. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found on the credit bureau websites (listed below).

The following information must be included when requesting a security freeze: (1) full name with middle initial and any suffixes; (2) social security number (SSN); (3) date of birth; (4) current address and any previous addresses for the past five years; (5) proof of current address, such as a copy of a government-issued identification card, a recent utility bill, or bank or insurance statement; and (6) other personal information required by the applicable credit reporting agency.

Note: if you are requesting a credit report for your spouse or a minor under the age of 16, this required information must be provided for him/her as well. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Pursuant to federal law, **consumers cannot be charged to place or lift a credit freeze on their credit report**. You **must contact each agency** to place a credit freeze, as placing a freeze with one bureau does not automatically freeze your credit with all bureaus.

You may obtain a free security freeze by contacting the following national consumer reporting agencies:

**Equifax Security Freeze**

P.O. Box 105788
Atlanta, GA 30348
1-888-298-0045

equifax.com/personal/credit-report-services/credit-freeze

**Experian Security Freeze**

P.O. Box 9554

Allen, TX 75013
1-888-397-3742

experian.com/freeze/center.html

**TransUnion Security Freeze**

P.O. Box 160
Woodlyn, PA 19094
1-800-916-8800

transunion.com/credit-freeze

**Fraud Alerts**:

You can also choose to place a free **fraud alert** with the national credit bureaus. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Unlike credit freezes where you must notify each bureau individually, you only need to submit a fraud alert request to one of the three major credit bureaus, and said bureau will notify the remaining two on your behalf. Placing a fraud alert adds another layer of protection, but do be aware it may delay processing time when you seek to obtain credit.

Fraud alerts can be placed with a credit bureau by phone or online:

**Equifax**: 1-888-298-0045 or equifax.com/personal/credit-report-services/credit-fraud-alerts. Equifax fraud alert form: https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf

**TransUnion**: 1-800-916-8800 or transunion.com/fraud-alerts

**Experian**: 1-888-397-3742 or experian.com/fraud/center.html

While we are not aware of any actual or attempted misuse of your information to perpetrate fraud, if you do experience identity fraud, you have the right to file or obtain a police report. Please note that in order to file a **crime report or incident report** with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. Instances of known or suspected identity theft should be reported to law enforcement or to the Attorney General's office in your home jurisdiction. This notice has not been delayed by law enforcement.

The Federal Trade Commission (FTC) also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information about how to file an FTC

complaint at identitytheft.gov or 1-877-ID-THEFT (1-877-438-4338) / TTY: 1-866-653-4261. You may also contact the FTC by mail at:

Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

For more information about identity theft prevention, fraud alerts, security freezes, and other steps you can take to protect yourself, please visit identitytheft.gov. You may also contact your consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

For more information about this cyber event, to confirm if you were possibly impacted, or for help with signing up for credit monitoring and identity protection services, please contact the dedicated assistance line at **1-800-405-6108**.