

# Notice of Data Security Incident

Maintaining the privacy and security of personal information is of the utmost importance to Lake Region Healthcare. We are notifying individuals of a data security incident that may have resulted in the exposure of certain data stored on our network.

On or about May 19, 2025, we detected unauthorized access to our network. Upon learning of this issue, we promptly took steps to secure our network and commenced a thorough investigation with the assistance of external cybersecurity professionals experienced in handling these types of incidents. The investigation included a comprehensive review of the affected data to assess and identify the individuals and information that may have been impacted, which concluded on June 5, 2026. We are providing notice to potentially impacted individuals via U.S. mail for whom a mailing address is available.

The potentially impacted data contained personal information of certain individuals that may include one or more of the following: name, date of birth, Social Security number, medical record number, patient account number, health insurance information, contact information, medical and/or treatment information, government-issued identification, and/or financial information. Not all of these data elements were affected for every individual.

While we are not aware of any unauthorized use of personal information as a result of this incident, we encourage all potentially impacted individuals to remain vigilant by reviewing financial account statements on a regular basis for any unauthorized activity. We also recommend reviewing explanation of benefits statements received from health insurance providers, as further described in the "Other Important Information" section below. We are providing complimentary identity theft protection services to all individuals. Potentially impacted individuals may contact the dedicated response line referenced below for information on additional precautionary measures or for enrollment support.

As a team of dedicated and caring professionals, we understand the importance of safeguarding personal and protected health information. We remain fully committed to maintaining the privacy of the information in our possession, and upon learning of the event, we took prompt action to protect information entrusted to our care. We continually evaluate our practices to enhance the security and privacy of personal information and have implemented additional safeguards to further strengthen our cybersecurity posture.

For further questions about this incident, or to determine if affected, please contact the dedicated toll-free response line at [1-844-507-9987](tel:1-844-507-9987). The response line is available between the hours of 7:00 a.m. to 7:00 p.m. Central Time, Monday through Friday, excluding holidays.

## **OTHER IMPORTANT INFORMATION**

### **Placing a Fraud Alert**

We recommend that you place a one-year “Fraud Alert” on your credit files, at no charge. A fraud alert tells creditors to take reasonable steps to verify your identity before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. Once one credit bureau confirms your fraud alert, it is required to notify the others.

---

#### ***Equifax***

Equifax Information Services LLC  
P.O. Box 105069, Atlanta, GA 30348

[www.equifax.com/personal/credit-report-services/credit-fraud-alerts/](http://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/)

1-888-EQUIFAX (1-888-378-4329)

#### ***Experian***

P.O. Box 9532, Allen, TX 75013

[www.experian.com/fraud](http://www.experian.com/fraud)

1-888-EXPERIAN (1-888-397-3742)

#### ***TransUnion***

Fraud Victim Assistance Department

P.O. Box 2000, Chester, PA 19016

[www.transunion.com/fraud-alerts](http://www.transunion.com/fraud-alerts)

800-916-8800; [800-680-7289](tel:800-680-7289)

---

# **Consider Placing a Security Freeze on Your Credit File**

You may also request a “Security Freeze” be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting any of the three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

---

## ***Equifax Security Freeze***

Equifax Information Services LLC

P.O. Box 105788, Atlanta, GA 30348

[www.equifax.com/personal/credit-report-services/credit-freeze/](http://www.equifax.com/personal/credit-report-services/credit-freeze/)

1-888-EQUIFAX (1-888-378-4329)

## ***Experian Security Freeze***

P.O. Box 9554, Allen, TX 75013

[www.experian.com/freeze](http://www.experian.com/freeze)

1-888-EXPERIAN (1-888-397-3742)

## ***TransUnion Security Freeze***

P.O. Box 160, Woodlyn, PA 19094

[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

800-916-8800; [888-909-8872](tel:888-909-8872)

---

To place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information such as a copy of a government-issued identification. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift

the freeze. If you do place a security freeze prior to enrolling in identity theft protection services, you will need to remove the freeze to sign up. After you sign up, you may refreeze your credit file.

## **Obtaining a Free Credit Report**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call [1-877-322-8228](tel:1-877-322-8228) or request your free credit reports online at [www.annualcreditreport.com](http://www.annualcreditreport.com). Once you receive your credit reports, review them for discrepancies, identify any accounts you did not open or inquiries from creditors that you did not authorize, and verify that all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

## **Protecting Medical Information**

As a general matter, the following practices can help deter, detect, and protect from medical identity theft. For more information visit [consumer.ftc.gov/articles/what-know-about-medical-identity-theft](http://consumer.ftc.gov/articles/what-know-about-medical-identity-theft). Only share health insurance cards with health care providers and other family members who are covered under the insurance plan or who help with medical care. Review the “explanation of benefits statement” provided by your health insurance company and follow up with the insurance company or care provider for any items not recognized. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date. Ask the insurance company for a current year-to-date report of all services paid for the impacted individual as a beneficiary. Follow up with the insurance company or the care provider for any items not recognized.

## **Additional Helpful Resources**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly. If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by visiting [www.identitytheft.gov](http://www.identitytheft.gov), by phone at 1-877-IDTHEFT (1-877-438-

4338), or by mail at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

**Iowa Residents:** You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319; [www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov); [515-281-5164](tel:515-281-5164).

**Maryland Residents:** You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202; <https://oag.maryland.gov>; [888-743-0023](tel:888-743-0023).

**Massachusetts Residents:** Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

**New Mexico residents:** 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. In addition, you have the right to obtain a security freeze (as explained above) or submit a declaration of removal. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act. For more information about the FCRA, please visit [www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf](http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf) or [www.ftc.gov](http://www.ftc.gov).

**New York Residents:** You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; [ag.ny.gov/consumer-frauds-bureau/identity-theft](http://ag.ny.gov/consumer-frauds-bureau/identity-theft); [800-771-7755](tel:800-771-7755).

**North Carolina Residents:** You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; [www.ncdoj.gov](http://www.ncdoj.gov); [877-566-7226](tel:877-566-7226) (Toll-free within North Carolina), [919-716-6000](tel:919-716-6000).

**Oregon Residents:** You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; [www.doj.state.or.us](http://www.doj.state.or.us); [877-877-9392](tel:877-877-9392).

**Rhode Island Residents:** You have the right to obtain a police report if one was filed, or alternatively, you can file a police report. Further, you can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903; [www.riag.ri.gov](http://www.riag.ri.gov); [\(401\) 274-4400](tel:401-274-4400). As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services. To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies can be contacted using the contact information provided above. In order to request a security freeze, you may need to provide the following information: your full name (including middle initial as well as Jr., Sr., II, III, etc.); Social Security number; date of birth; complete address; prior addresses; proof(s) of identification (state driver's license or ID card, military identification, birth certificate, etc.); and if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. When you place a security freeze on your credit report, within five (5) business days you will be provided with a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following: (1) the unique personal identification number or password provided by the consumer reporting agency; (2) proper identification to verify your identity; and (3) the proper information regarding the period of time for which the report shall be available to users of the credit report.

**Washington D.C. Residents:** You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, [oag.dc.gov/consumer-protection](http://oag.dc.gov/consumer-protection), Telephone: [202-442-9828](tel:202-442-9828).