Date: April 10, 2025

Notice of Data Breach

Laboratory Services Cooperative (LSC) is encouraging individuals to take precautionary measures to protect their information following a security incident.

LSC provides lab testing services to select Planned Parenthood centers. If you, or someone whose healthcare bills you pay for, visited one of these centers and had lab tests done or were referred for lab tests, your information might be part of this incident.

Please be advised that this incident did not involve all Planned Parenthood centers. It specifically may have impacted only those centers that received lab testing services from LSC. It is important to note that LSC began providing services to these centers at different times, with some partnerships starting as recently as the past few years. For a list of states where LSC partners with Planned Parenthood centers, please see the FAQ section of this website notice.

We encourage individuals to read this notice carefully, as it contains important details about the incident and steps you can take to help protect your information.

What Happened?

On October 27, 2024, LSC identified suspicious activity within its network. In response, LSC immediately engaged third-party cybersecurity specialists to determine the nature and scope of the incident and notified federal law enforcement. The investigation revealed that an unauthorized third party gained access to portions of LSC's network and accessed/removed certain files belonging to LSC.

LSC promptly initiated a review and engaged a third-party vendor to help identify whose information may be potentially involved and to what extent.

What Information Was Involved?

In February 2025, LSC received the initial results of the data review, revealing that certain LSC patient and worker-related data might be affected.

The specific information involved is not the same for everyone. It depends on the individual's relationship with LSC but may include contact details such as name, address, phone number, and email, along with one or more of the following categories:

- Medical/Clinical Information: This may include information such as date(s) of service, diagnoses, treatment, medical record number, lab results, patient/accession number, provider name, treatment location, and related-care details.
- Health Insurance Information: This may encompass plan name, plan type, insurance companies, and member/group ID numbers.
- Billing, Claims, and Payment Data: This could involve claim numbers, billing details, bank account details (including bank name, account number, and routing number), billing codes, payment card details, balance details, and similar banking and financial information.
- Additional Identifiers: This may include Social Security Number, driver's license or state ID number, passport number, date of birth, demographic data, student ID number, and other forms of government identifiers.

For LSC workers, the information involved may also include details about their dependents or beneficiaries if that information was provided to LSC.

What We Are Doing.

Upon detecting the suspicious activity, we moved quickly to investigate the incident and secure our environment. We then conducted a thorough review to determine whose information may be potentially involved.

The confidentiality, privacy, and security of information maintained by LSC remains its top priority. As a precaution, LSC has hired third-party cybersecurity specialists to monitor the dark web for any information that may have been accessed or taken without authorization during this incident. The dark web is a hidden part of the internet where unauthorized activities and data exchanges often happen.

The cybersecurity specialists hired by LSC are using tools and techniques to scan various dark web forums, marketplaces, and other platforms. As of this writing, they haven't found any evidence that information involved in this incident is on the dark web.

LSC is offering free credit monitoring and medical identity protection services through CyEx Medical Shield Complete 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 individuals to review the steps outlined in this notice to protect their information. Cybersecurity is an ongoing concern for everyone, as companies worldwide face cybersecurity threats. By following the steps below, individuals can better protect themselves.

1. Enroll in Medical Shield Complete or Minor Defense

    a. CyEx Medical Shield Complete: LSC is offering free credit monitoring and medical identity protection services through CyEx Medical Shield Complete to individuals potentially affected by this incident. LSC is paying the cost for these services for 12 or 24 months, depending on state of residence. Please see below for key features and enrollment instructions.

    Key Features:

    - 1-Bureau Credit Monitoring
    - Health Insurance Plan Number Monitoring
    - Medical Record Number Monitoring
    - Medical Beneficiary Identifier Monitoring
    - National Provider Number Monitoring
    - International Classification of Diseases Monitoring
    - Health Savings Account Monitoring
    - Dark Web Monitoring

    How to Enroll:

    1. **Get Your Activation Code:** Call LSC's dedicated call center at 1-855-549-2662 (available Monday through Friday, 9:00 AM to 9:00 PM ET) to receive your unique Activation Code.

    2. **Visit the Enrollment Website:** For adults, go to: app.medicalshield.cyex.com/enrollment/activate/lscms. For minors, go to: app.minordefense.com/enrollment/activate/lscmd.

    3. **Enter Your Activation Code:** Input your unique Activation Code.

    4. **Redeem Your Code:** Click "Redeem Code."

    5. **Create Your Account:** Follow the prompts to set up your account.

    Deadline to Enroll: The deadline to enroll is July 14, 2025. After this date, the enrollment process will close, and your Medical Shield Complete code will no longer be active. Please enroll before the deadline to take advantage of these services.

Need Help? If you need assistance with the enrollment process or have questions, please call CyEx directly at 1-866-622-9303. Please remember, however, that you will need to obtain your unique Activation Code first by calling LSC's dedicated call center at 1-855-549-2662 (available Monday through Friday, 9:00 AM to 9:00 PM ET).

Important Information Relating to Enrollment and Minors: Medical Shield Complete may not be available for individuals who do not have established credit, a U.S. address (or one in its territories), or a valid Social Security number. For minors, LSC is offering a separate monitoring service called Minor Defense. To learn more about Minor Defense and how to enroll, please call LSC's dedicated call center at 1-855-549-2662 (available Monday through Friday, from 9:00 AM to 9:00 PM ET).

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 740241 Atlanta, Georgia, 30374	P.O. Box 9701 Allen, TX 75013	P.O. Box 2000 Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-916-8800

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 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, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ 1-800-525-6285	P.O. Box 9554 Allen, TX 75013 https://www.experian.com/fraud/center.html 1-888-397-3742	P.O. Box 2000 Chester, PA 19016 https://www.transunion.com/fraud-alerts 1-888-909-8872

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, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-freeze/ 1-888-298-0045	P.O. Box 9554 Allen, TX 75013 http://experian.com/freeze 1-888-397-3742	P.O. Box 160 Woodlyn, PA 19094 http://www.transunion.com/creditfreeze 1-888-916-8800

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.

After receiving your request, each agency will send you a confirmation letter containing a unique PIN or password that you will need to lift or remove the freeze. You should keep the PIN or password in a safe place.

7. **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.

8. **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. LSC is located at 2001 E. Madison Street, Seattle, WA 98122 and can be contacted at 1-425-460-4522.

9. **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/internet/resource-center.

10. **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.

11. **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/.

12. **For Rhode Island Resident.** 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.

13. **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, LSC 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 1-855-549-2662 (available Monday through Friday from 9:00 AM to 9:00 PM ET).

We sincerely regret any concern this incident may cause and will continue to work hard to maintain the trust of our patients and partners.

Sincerely,

Laboratory Services Cooperative