

Notice of Potential Data Event

Cedarcrest Surgery Center LLC ("Cedarcrest") is providing notice an event that may involve some of our patient's personal information. This notice provides information about the event, our response, and resources available to help individuals protect their personal information, should they feel it is appropriate to do so.

What Happened? Cedarcrest recently learned of suspicious activity related to a single employee email account. In response, Cedarcrest quickly took steps to secure the email account, confirm the security of its email environment, and conduct a comprehensive investigation. The investigation determined that a single Cedarcrest employee email account was accessed without authorization between October 24, 2024 and December 31, 2024, by an unknown individual. We then reviewed the relevant emails to determine what information was present, and to whom the information related. Based on this review, on or around February 7, 2025, Cedarcrest determined that patient information was in the relevant emails.

What Information Was Involved? While the actual types of information affected may vary by individual, our investigation determined that the following types of information may be involved: name, date of service, billing date, payment date, physician name, payer name, date of birth, procedure, gender, zip code, policy number, policy type, group number, and subscriber policy number.

What We Are Doing. We take this event seriously, and the confidentiality, privacy, and security of information in our care are among our highest priorities. We moved quickly to investigate this incident, assess the security of our email environment, and notify patients. Additionally, we notified federal law enforcement of the event and are cooperating with their investigation. We recognize the evolving nature of cybersecurity. As part of our ongoing commitment to cybersecurity, we are reviewing our existing security policies and will continue to implement appropriate cybersecurity measures in the future. We are also notifying potentially affected individuals and providing details on steps they may take to protect their information, should they feel it is appropriate to do so.

For More Information. If you have additional questions, please call our dedicated assistance line toll-free at 1 (800) 405-6108 from 7:00 a.m. to 7:00 p.m. CT, Monday through Friday, excluding major U.S. holidays.

What You Can Do. We encourage individuals who may be affected to remain vigilant against incidents of identity theft and fraud by reviewing account statements and monitoring free credit reports for suspicious activity and to detect errors. Additionally, we encourage individuals to check their explanations of benefits regularly to ensure that there has not been any unexpected activity. Under U.S. law, a consumer is entitled to one free credit report annually from each of the three (3) major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit <https://www.annualcreditreport.com> or call, toll-free, 1 (877) 322-8228. Consumers may also directly contact the three (3) 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 one (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 (7) years. Should consumers wish to place a fraud alert, please contact any of the three (3) 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 (2) to five (5) 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 (3) 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 Fraud Alert, 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 Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

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; <https://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, the Federal Trade Commission, and the relevant state Attorney General. This notice has not been delayed by law enforcement.