NOTICE OF DATA SECURITY INCIDENT

In October 2025, Unlimited Technology Systems, LLC ("Unlimited"), who provides practice management software to various health care organizations and providers, including Piedmont Cancer Institute ("PCI"), experienced a data security incident. Unlimited determined that certain PCI data may have been accessed without authorization and Unlimited is mailing notification letters to affected individuals for whom it has a postal address. Unlimited is also notifying applicable state regulators. PCI is providing notice of this incident as it may have impacted the privacy of information related to certain individuals for whom PCI doesn't have an address.

According to Unlimited, on October 19, 2025, Unlimited discovered unauthorized activity within its commercial datacenter. Upon discovering the unauthorized activity, Unlimited hired a cybersecurity forensic firm to conduct an investigation, notified law enforcement, and conducted a review of the data involved. Through this investigation, Unlimited determined that an unauthorized actor may have obtained a copy of certain individuals' personal information between October 5 and October 10, 2025. Unlimited provided PCI a list of the impacted individuals and is mailing letters to individuals for whom it has addresses. The type of information potentially impacted by this incident varies by individual, but may include name, and one or more of the following: Social Security number, health insurance and patient balance information (such as insurance policy numbers or claims/benefits information), medical information (such as medical record number, dates of service, and diagnosis information), scanned documents (such as driver's licenses or other government identification, insurance cards, and intake forms), and other personal information (such as date of birth, email, address, phone number, or demographic information).

PCI takes the confidentiality, privacy, and security of personal information seriously. Upon learning of the incident, PCI launched an investigation into the incident and took steps to review our policies and procedures relating to data privacy and security.

PCI encourages individuals to remain vigilant against incidents of identity theft and fraud by reviewing their account statements and credit reports for any unauthorized or suspicious activity. Individuals can also review the *Steps Individuals Can Take to Help Protect Their Information* below for further guidance.

Individuals who have questions about the incident that are not addressed in this notice may contact Unlimited's dedicated call center. Representatives are available to assist with questions from Monday through Friday, between the hours of 9 a.m. and 9 p.m. Eastern Time, excluding major U.S. holidays. Please call the help line at (844) 576-3063.

STEPS INDIVIDUALS CAN TAKE TO HELP PROTECT THEIR 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 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 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 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 their 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; 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.