

People Encouraging People - Notice of Data Privacy Event

People Encouraging People is providing notice of a recent event that impacts the confidentiality of information related to certain individuals who received treatment and related services at the facilities. Although we have no indications that any such information has been used to commit identity theft or fraud, we are providing information about the event, the steps taken we have taken in response, and resources available to individuals to help protect information from possible misuse, should they feel it is appropriate to do so.

What Happened? On or about December 21, 2024, People Encouraging People became aware of unauthorized activity on its computer network, including unauthorized encryption of certain data. We quickly responded by securing and restoring our environment. We learned that between December 18, 2024, and December 23, 2024, certain files stored within our environment were copied and taken by an unauthorized actor. We undertook a thorough review of the impacted patient data to identify the patients whose information was involved. Although we have no evidence of any identity theft or fraud in connection with this incident at this time, we are notifying you that some of your information was present within an impacted file.

What Information Was Involved. Our review determined that the following types of your information may have been impacted and varies between individuals: full name, address, date of birth, Social Security number, address, driver license number, financial account information, diagnosis information, medication information, and treatment information.

What People Encouraging People is Doing. Upon becoming aware of this event, People Encouraging People promptly took steps to investigate, assess the security of our systems, restore functionality to our environment, and notify potentially affected individuals. As part of our ongoing commitment to the privacy of personal information, we have safeguards in place to protect data in our care. We are working to review and further enhance these protections as part of our ongoing commitment to data security. We are also reporting this incident to the U.S. Department of Health and Human Services Office for Civil Rights and relevant state authorities.

What Affected Individuals Can Do. As a precautionary measure, we encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Additional resources can be found below in the *Steps You Can Take to Protect Personal Information*, which contains information on what you can do to better protect against possible misuse of your information.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call 833-456-5078 from 9:00 A.M – 5:00 P.M. ET, Monday through Friday, excluding major U.S. holidays. You may also write to us at 22 South Howard St., C U 1, Baltimore, MD 21201.

Steps You Can Take To Protect Personal Information

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 www.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 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 years. Should consumers wish to place a fraud alert, please contact any of the three 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:

- Full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security number;
- Date of birth;
- Addresses for the prior two to five years;
- Proof of current address, such as a current utility bill or telephone bill;
- A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
- 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 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; 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 and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by

writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately [#] Rhode Island residents that may be impacted by this event.