NOTICE OF DATA PRIVACY INCIDENT
FEBRUARY 27, 2025

Unfortunately, the state of our world is riddled with cyber security incidents that impact businesses and individuals throughout the country. Even the highest levels of security protocols do not always prevent such actors from disrupting and gaining access to cyber networks. Like so many businesses and health care providers before us, Melbourne Terrace Rehabilitation Center ("Melbourne Terrace") experienced such an event and is providing notice of a data privacy incident.

What Happened? On May 17, 2024, evidence of suspicious activity was identified on the network and prompted an investigation. Upon detecting the issue, measures were quickly initiated to mitigate the threat and further secure the telecommunications network, computer systems and devices. An investigation was also launched with the support of industry leading cybersecurity specialists and in collaboration with federal law enforcement.

The investigation identified that the unauthorized actor may have viewed or copied certain personal information between May 8, 2024, and May 17, 2024. Personalized notices have already been mailed out to the few known impacted individuals. If you did not receive a personalized notice, then Melbourne Terrace does not have knowledge that any of your personal information was compromised.

What Information Was Involved? In general, the systems contain information including, but may not be limited to names, addresses, dates of birth, social security numbers, and health information.

What is Melbourne Terrace Doing? We take this event very seriously. Upon learning of the suspicious activity, we moved quickly to investigate and respond. The investigation included steps to access and secure the network, reviewing the systems involved and files, notifying law enforcement and regulators, and notifying potentially involved individuals as information became available. As part of our ongoing commitment to information security, we reviewed and continue to review our policies and procedures, as well as assessing new cybersecurity tools, to reduce the risk of a similar incident from occurring in the future.

What You Can Do. In general, individuals should remain vigilant against incidents of identity theft and fraud by reviewing account statements, explanations of benefits statements, and monitoring your free credit reports for suspicious activity and to detect errors. Suspicious activity should be promptly reported to relevant parties including an insurance company, healthcare provider, and/or financial institution. Additional information and resources may be found below in the *Steps You Can Take to Protect Personal Information* section of this notice.

For More Information. A dedicated incident support team to answer questions has been established. If you have any questions regarding this incident please call the toll-free number

1-877-804-2826 (Monday – Friday from 9:00am – 5:00pm EST).

Steps Individuals Can Take to Protect Their Personal Information

Monitor 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 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:

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/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
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

Additional Information

As a best practice, consumers should change all passwords to their personal accounts on a regular basis, use strong passwords, and refrain from using the same password for multiple accounts. 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.