Notification of Data Security Incident

October 30, 2025 – On September 2, 2025, Harbor became aware of potential unauthorized access to an employee email account. Upon discovery, we immediately performed password resets for the affected account and subsequently engaged a third-party team of forensic investigators in order to determine the full nature and scope of the incident. On September 29, 2025, following a thorough investigation, Harbor confirmed that a limited amount of protected health information may have been accessed in connection with this incident.

Although the forensic investigation could not rule out the possibility that an unknown actor may have accessed this information, there is no indication whatsoever that any information has been misused. The type of information contained within the affected data included the name of the individual receiving services through Harbor Regional Center, their address, date of birth, Social Security number, medical record number, patient ID or account number, Medicare or Medicaid number, health insurance information, medical diagnosis and treatment information, medical history, prescription information, medical lab or test result, treatment location, treatment date, and provider name. Importantly, the information potentially impacted may vary for each individual, and may include all, or just one, of the above-listed types of information.

We are notifying potentially affected individuals as quickly as possible via U.S. mail to their most recent address on file. In an abundance of caution, we are providing potentially impacted individuals with complimentary credit monitoring services. Additionally, in response to this incident, we have implemented additional security measures within our systems and are reviewing our current policies and procedures related to data security. Although we have no evidence of misuse of information as a result of this incident, individuals served by Harbor are nonetheless encouraged to monitor their account statements and explanation of benefits forms for suspicious activity and to detect errors. Individuals may also wish to contact the three major credit agencies to place a fraud alert on their credit report – the credit agencies' contact information is: Equifax (888-378-4329); TransUnion (833-395-6938); and Experian (888-397-3472).

Harbor has established a hotline to answer questions about the incident and to address related concerns. The number for the hotline is 1-833-647-1407. You may also contact us by email Privacy.Records@harborrc.org, or by writing to Harbor Regional Center, Attention: Privacy Officer, 21231 Hawthorne Blvd., Torrance, California 90503.

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You 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-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion	Experian	Equifax
1-800-680-7289	1-888-397-3742	1-888-298-0045
website	website	website
TransUnion Fraud Alert: P.O. Box 2000 Chester, PA 19016-2000	Experian Fraud Alert: P.O. Box 9554 Allen, TX 75013	Equifax Fraud Alert: P.O. Box 105069 Atlanta, GA 30348-5069
TransUnion Credit Freeze: P.O. Box 160 Woodlyn, PA 19094	Experian Credit Freeze: P.O. Box 9554 Allen, TX 75013	Equifax Credit Freeze: P.O. Box 105788 Atlanta, GA 30348-5788