Notice of Cyber Incident

Colonial Behavioral Health (CBH), like many organizations across the country, has unfortunately been the victim of a security incident. This notice provides information about how this incident may have affected personal information for CBH customers and, as a preventative measure, provides steps that can be taken to protect such information.

What Happened?

On or about October 4, 2024, CBH discovered issues with our computer systems and quickly determined we were the victim of a ransomware incident. We immediately took steps to stop the ransomware and engaged outside cybersecurity experts to assist and investigate this event. Thankfully, we could continue to care for patients despite system disruptions. Based on the investigation into this incident, it appears it began on or around May 17, 2024, when an unauthorized user logged into our systems undetected. Certain sensitive information may have been inappropriately accessed and/or obtained before ransomware encryption occurred to our IT systems on or about October 4.

What Information Was Involved?

We have determined that the information accessed in this incident included personal identifying information, including health information, of some CBH customers. Specifically, the information involved may have included patient files and other records stored on the affected CBH systems, including one or more of the following types of information: demographic information (such as names, social security numbers, addresses, ZIP codes, driver's license numbers, dates of birth, and/or similar identifiers), clinical information (which may include diagnosis/conditions, lab results, medications, and/or other treatment information), or information related to insurance or claims information. Some of this information may also be related to guarantors who paid bills for healthcare services of others. The data that may have been accessed was not the same for everyone.

What We Are Doing

We have notified state and federal law enforcement, including the FBI's Cyber Crimes Division, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), and the Cyber Fusion Center of the Virginia State Police. CBH is supporting all law enforcement investigations into this matter.

In addition, CBH takes its obligation to safeguard personal information very seriously and continues to evaluate additional actions to strengthen our network security in the face of an ever-evolving cyber threat landscape.

On November 27, 2024, CBH mailed individuals believed to have had data implicated a letter with information concerning this incident and an offer for free credit monitoring. If you are a former or current CBH patient who wants to receive credit monitoring and you do not receive this letter, please email us at privacy@colonialbh.org.

What You Can Do

Please review the "Additional Resources" section below. This section describes steps you can take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

We appreciate your understanding and patience. We regret any inconvenience that this incident causes and are committed to supporting you.

ADDITIONAL RESOURCES

Review Your Account Statements and Obtain and Monitor Your Credit Report

As a precautionary measure, we recommend that you remain vigilant by regularly reviewing and monitoring account statements and credit reports to detect potential errors or fraud and identity theft resulting from the security incident. You may periodically obtain your free credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 9701	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for inaccurate information, such as a home address and Social Security number. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Notify Law Enforcement of Suspicious Activity

You should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including local law enforcement, your state attorney general, and the Federal Trade Commission (FTC). To file a complaint with the FTC, use the below contact information or website.

The Federal Trade Commission

600 Pennsylvania Avenue, NW

Washington, DC 20580

1-877-ID-THEFT (1-877-438-4338)

TTY: 1-866-653-4261

www.IdentityTheft.gov

Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company which the account is maintained.

Credit Freezes

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued when you initiate a freeze. A credit freeze is designed to prevent potential creditors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact **all three** major consumer reporting agencies listed below.

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1) Your full name, with middle initial and any suffixes;
2) Your Social Security number;
3) Your date of birth (month, day, and year);
4) Your current address and previous addresses for the past five (5) years;
5) A copy of your state-issued identification card (such as a state driver's license or military ID);
6) Proof of your current residential address (such as a current utility bill or account statement); and
7) Other personal information as required by the applicable credit reporting agency.

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request. More information regarding credit freezes can be obtained from the FTC and the major consumer reporting agencies.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert will stay on your credit file one (1) year. The alert informs creditors of possible fraudulent activity within your report and requires the creditor to verify your identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Should you wish to place a fraud alert, please contact any one of the three major consumer reporting agencies listed above. The agency you contact will then contact the other two. More information regarding fraud alerts can be obtained from the FTC and the major consumer reporting agencies.

Monitor Your Personal Health Information

If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number. You may want to order copies of your credit reports and check for any bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your records.

Additional Resources and Information

You can obtain additional information and further educate yourself regarding identity theft and the steps you can take to protect yourself by contacting your state attorney general or the FTC. The FTC's contact information and website for additional information is:

The Federal Trade Commission

600 Pennsylvania Avenue, NW

Washington, DC 20580

1-877-ID-THEFT (1-877-438-4338)

TTY: 1-866-653-4261

www.ftc.gov/idtheft

For Virginia residents: You may contact the Virginia Attorney General's Office at 202 North Ninth Street, Richmond, VA 23219; 1-804-786-2071; or https://www.oag.state.va.us/contact-us/contact-info.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General at 165 Capitol Avenue, Hartford, CT 06106; 1-860-808-5318; or https://portal.ct.gov/ag.

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia at 400 6th Street, NW, Washington, DC 20001; 1-202-727-3400; or https://oag.dc.gov/consumer-protection/consumer-alert-online-privacy.

For Iowa residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. The Iowa Attorney General's Office can be reached at 1305 E. Walnut Street, Des Moines, IA 50319; 1-515-281-5164; or www.iowaattorneygeneral.gov.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202; 410-576-6300; 1-888-743-0023 (toll free), or https://www.marylandattorneygeneral.gov/Pages/contactus.aspx.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General at 1 Ashburton Place, Boston, MA 02108; 1-617-727-8400; or https://www.mass.gov/orgs/office-of-the-attorney-general. You have the right to obtain a police report if you are a victim of identity theft.

For New Mexico residents: You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your credit file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or ww.ftc.gov.

For New York residents: The 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/. You may also contact the Bureau of Internet and Technology (BIT) at 28 Liberty Street, New York, NY 10005; 212-416-8433; or https://ag.ny.gov/about/about-office/economic-justice-division#internet-technology.

For North Carolina residents: The North Carolina Attorney General's Office may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 919-716-6400; or https://ncdoj.gov/contact-doj/.

For Oregon residents: We encourage you to report suspected identity theft to the Oregon Attorney General at 1162 Court Street NE, Salem, OR 97301; 1-877-877-9392; 1-503-378-4400; or www.doj.state.or.us.

For Rhode Island residents: You may contact the Rhode Island Office of the Attorney General at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; or https://riag.ri.gov/. You have the right to obtain a police report if you are a victim of identity theft. Three Rhode Island residents were impacted by this breach.