Notice of a Data Incident

Compassion Health Care, Inc. ("CHC") recently became aware that an unauthorize third-party may have viewed and/or downloaded data stored on certain of CHC's systems containing patient and employee/vendor data. Below you will find additional information about what happened, what data was potentially impacted, steps CHC is taking, and additional guidance to help current or former CHC patients and employees/vendors protect themselves against potential fraud and/or identity theft.

***What Happened*:** On March 17, 2025, Compassion Health Care, Inc. ("CHC") detected suspicious activity on its network that resulted in a network interruption (the "Incident"). Upon learning of the Incident, CHC immediately initiated an investigation with the assistance of a third-party cybersecurity firm to determine the nature and scope of any potential unauthorized access to its computer systems.

***What Information Was Involved*:** On March 21, 2025, CHC learned that an unauthorized third-party potentially viewed and/or downloaded data stored on certain of CHC's systems containing patient and employee/vendor data. The potentially affected data includes, patients' names, addresses, phone numbers, dates of birth or ages, Social Security numbers, driver's license numbers, health insurance information, claims information, and clinical/diagnostic information related to medical services received from a healthcare provider engaged or employed by CHC. The potentially affected employee/vendor data includes, names, addresses, dates of birth, Social Security numbers, income information, financial account information, and possibly bank account and routing numbers.

***What We Are Doing and What You Can Do*:** On May 16, 2025, CHC sent written notification to all potentially impacted patients and employees/vendors for whom it has contact information. CHC has also arranged for complimentary credit monitoring and identity theft restoration services through HaystackID. If you do not receive written notification from CHC, but you are a current or former patient or employee/vendor of CHC, please contact the toll-free inquiry line provided below.

***More Information*:** Affected individuals should refer to the notice they will receive in the mail regarding steps they can take to protect themselves. In general, we recommend, as a precautionary measure, that individuals remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing their account statements and monitoring credit reports closely. If individuals detect any suspicious activity on an account, they should promptly notify the financial institution or company with which the account is maintained. They should also promptly report any fraudulent activity or suspected incidents of identity theft to proper law enforcement authorities, including the police and their state's attorney general.

You may also wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps that you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-Theft (1-877-438-4338). You may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, Washington DC 20580.

If you are a current or former CHC patient or employee/vendor and have any questions or concerns about this incident, please contact 855-260-8137 between 9:00 a.m. and 9:00 p.m. Eastern Standard Time, Monday through Friday, for further information and assistance.

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

CHC recommends that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed 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 for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze

You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert

You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission (FTC)

For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) at 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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. You can obtain further information on how to file such a complaint by way of the contact information listed above.

Internal Revenue Service (IRS)

Tax-related identity theft occurs when someone uses your stolen personal information, including your Social Security number, to file a tax return claiming a fraudulent refund. If you suspect you are a victim of identity theft, continue to pay your taxes and file your tax return, even if you must file a paper return. If your Social Security number is compromised and you know or suspect you are a victim of tax-related identity theft, the IRS recommends these actions:

- Respond immediately to any IRS notice: Call the number provided.
- If your e-filed return is rejected because of a duplicate filing under your Social Security number, or if the IRS instructs you to do so, visit irs.gov/victimassistance to complete Form 14039, Identity Theft Affidavit, attach it to the back of your completed paper tax return and mail to the IRS location based upon the state you reside. If you prefer, you have the option to submit the Form 14039 online and mail your paper return separately.
- Visit IdentityTheft.gov for steps you should take right away to protect yourself and your financial accounts.

You should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

This notification was not delayed by law enforcement.

Iowa Residents: Iowa residents are advised to report any suspected identify theft to local law enforcement or Iowa Attorney General. Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

District of Columbia Residents: District of Columbia residents can obtain information about preventing identity theft from the District of Columbia Attorney General's office at: 400 6th St. NW, Washington, D.C. 20001, Consumer Protection Division, (202) 442-9828, consumer.protection@dc.gov, https://oag.dc.gov

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, http://www.marylandattorneygeneral.gov/.

New Mexico Residents: Individuals have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; https://ag.ny.gov/consumer-frauds/identity-theft; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Oregon Residents: Oregon residents are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. Oregon residents can contact the Oregon Attorney General at 1162 Court St. NE, Salem, OR 97301-4096; 503-378-4400; https://www.doj.state.or.us/.

Rhode Island Residents: We believe that this incident affected X Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any police report filed regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Vermont Residents: If you do not have Internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

Contact Information

Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Credit Report	Add Fraud Alert	Add Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit--report-services
TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze