316191

Colla Health, Inc.
c/o HaystackID Return Processing Center
555 Monster Rd SW | Renton, WA 98057

PRESORT
FIRST-CLASS MAIL
US POSTAGE
PAID
CHICAGO, IL
PERMIT NO 4187

Collahealth

Via First-Class Mail

1020_316191

[redacted]

November 16, 2026

Re: Notice of Data Breach

[redacted],

Colla Health, Inc. ("CHI") writes to inform you, as a current or former patient at CHI's partner—[redacted]—of a recent data security incident that may have impacted the security of your Personal Information ("PI") and/or Protected Health Information ("PHI"). We are providing you with details about the event, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

What Happened?

On or around August 18, 2026, CHI became aware that an unauthorized party had accessed a third-party application CHI uses, Metabase, who announced a previously unknown vulnerability. We promptly took steps to secure the application and engaged a specialized third-party cybersecurity firm to conduct a comprehensive forensic investigation to determine the nature and scope of the activity. The forensic investigation found evidence that certain data may have been taken from the application.

We engaged a third-party vendor to analyze the data the forensic investigation identified. The vendor reviewed the affected data to identify the types of information that may have been involved and the potentially affected individuals. The vendor completed its review on October 19, 2026. Following this review, we coordinated with Cancer Care Specialists to identify contact information to provide notifications to impacted individuals.

CHI completed the process of identifying impacted individuals and their contact information on November 6, 2026. We then organized mailing, call center, and credit monitoring services for the affected population. This process was necessary to accurately identify whose PI and PHI may have been affected and to provide notice to potentially impacted individuals. During this review, we determined that some of your PI and/or PHI may have been affected by the incident.

What Information Was Involved?

The PI and/or PHI that may have been impacted includes: full name, [redacted]. Please note the information impacted varies for each potentially impacted individual, and not every individual had all the listed information involved. **Importantly, this incident did not affect your driver's license (or other state identification number) or other financial information.**

What We Are Doing.

CHI takes this event and the security of information in our care very seriously. Upon discovery of the incident, we promptly commenced an investigation and assessed the security of the application with the assistance of outside experts.

We notified potentially impacted individuals through media notice on November 16, 2026. In addition, we have taken additional technical and administrative steps to further enhance the security of our systems and the patient data we maintain to mitigate the risk of future harm.

In response to the incident, we are offering 12-months of access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12-months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update occurs with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by HaystackID, a company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in the 12-month credit monitoring services at no charge, please log on to the following and follow the instructions provided: **www.equifax.com/activate**.

When prompted please provide the following activation code to receive services: [redacted].

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. Enrollment requires an e-mail account and may not be available to minors under the age of 18. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What You Can Do.

As a precautionary measure, we encourage you to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor credit reports for suspicious or unauthorized activity. We encourage you to enroll in the complimentary credit monitoring that we are offering to you at no cost. Additional information can be found below in the *Additional Resources to Help Protect Your Information* section.

For More Information.

If you have any questions or concerns not addressed in this letter, please call our dedicated line 888-213-4555 (toll free) Monday through Friday, during the hours of 9:00 a.m. and 9:00 p.m. Eastern Standard Time (excluding U.S. national holidays). Please have this letter ready if you call.

We sincerely regret any concern or inconvenience this matter may cause and remain dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Colla Health, Inc.

316191

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We recommend 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, or remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents 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, or representative, you can request a freeze for a minor 15 and younger. To add a security freeze, 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

For more information about credit freezes, fraud alerts, and other steps you can take to protect yourself against identity theft, 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.

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.

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 Your Credit Report	Add a Fraud Alert	Add a 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

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting https://oag.dc.gov, or emailing at consumer.protection@dc.gov.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting http://www.marylandattorneygeneral.gov/Pages/contactus.aspx. Colla Health, Inc.'s headquarters are located at 8080 Westpark Dr. #82185, Houston, TX 77063.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at https://dos.ny.gov/consumer-protection; by visiting the New York Attorney General at https://ag.ny.gov or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or https://www.identitytheft.gov/#/.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 716-6000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies. There were 15 residents of Rhode Island potentially impacted by this incident.

Please Recycle Me!