EXHIBIT 1

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Salud Family Health ("Salud") does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about September 5, 2022, Salud Family Health ("Salud") became aware of suspicious activity related to certain computer systems. Salud immediately launched an investigation, with the assistance of third-party forensic investigators, to determine the nature and scope of the activity. Salud's investigation determined that there was unauthorized access to certain files from between September 5, 2022, and September 6, 2022. Therefore, Salud undertook a comprehensive review of the contents of the impacted files to determine what, if any, sensitive information was contained within them and to whom the information related for purpose of notification.

The information that could have been subject to unauthorized access includes name, Social Security number, driver's license number or identification card number, financial account information/credit card number, passport number, medical treatment and diagnosis information, health insurance information, biometric data, and username and password.

Notice to Maine Residents

On or about November 4, 2022, Salud began providing written notice of this incident to impacted individuals, including fifty (50) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Salud moved quickly to investigate and respond to the incident, assess the security of Salud systems, and identify potentially affected individuals. Salud is also working to implement additional safeguards and employee training to recognize suspicious behaviors. Salud is providing access to credit monitoring services for at least twelve (12) months, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Salud is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Salud is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Salud notified law enforcement and is cooperating with its investigation. Salud is also notifying other required state regulators, and the U.S. Department of Health and Human Services.

EXHIBIT A

Salud Family Health

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

MISSION
To provide a quality integrated health care home to the communities we serve.

CORE VALUES
Commitment
Compassion
Creativity & Innovation
Dignity
Integrity
Quality & Excellence
Teamwork

COMMUNITIES SERVED
Aurora
Brighton
Commerce City
Estes Park
Fort Collins
Fort Lupton
Fort Morgan
Frederick
Longmont
Sterling
Trinidad
Mobile Unit

NOTICE OF SECURITY INCIDENT

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Salud Family Health ("Salud") writes to notify you of a network security incident that may affect the privacy of some of your protected health information. We take this incident seriously, and although we have no evidence to date of identity theft or fraud as a result of this incident, this letter provides details of the incident, our response, and steps you may take to better protect against possible misuse of your information, should you feel it appropriate to do so.

What Happened? Around September 5, 2022, we became aware of suspicious activity in certain computer systems. We immediately launched an investigation, with the assistance of third-party computer specialists, to determine the nature and scope of the activity. Our investigation determined that there was unauthorized access to the affected systems on September 5, 2022 and that certain data may have been accessed or taken. Although we have no evidence of any identity theft or fraud in connection with this incident, Salud is notifying its patients whose information was accessible within the files and subject to unauthorized access.

What Information Was Involved? We determined that the following information may have been accessed or taken as the result of this incident: your name, Social Security number, driver's license number or Colorado identification card number, financial account information/credit card number, passport number, medical treatment and diagnosis information, health insurance information, biometric data, and username and password.

What is Salud Doing? Salud takes the confidentiality, privacy, and security of information in our care seriously. Upon discovery of the incident, we immediately commenced an investigation to determine its nature and scope. Although Salud has policies and procedures surrounding data security which were in effect at the time of the incident, as part of our ongoing commitment to the security of information, we are reviewing and enhancing our policies and procedures relating to data privacy and security. Salud is taking steps to prevent a reoccurrence, to include measures to reduce the likelihood of a future incident, including increased network security measures.

In an abundance of caution, Salud is providing you with access to 12 months of identity monitoring services through Kroll at no cost to you. A description of services and instructions on how to activate can be found within the enclosed *Steps You Can Take to Help Protect Personal Information*. Please note that you must complete the activation process yourself, as we are not permitted to activate the services on your behalf.

What You Can Do. You can review the enclosed *Steps You Can Take to Help Protect Personal Information*. You can also activate the complimentary identity monitoring services through Kroll. We also encourage you to remain vigilant against potential incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have any questions, please contact our dedicated call center at (855) 926-1137, Monday through Friday, 7:00 a.m. to 4:30 p.m. Mountain Time, excluding major U.S. holidays.

Salud takes the privacy and security of the information in our care seriously. We sincerely regret any inconvenience or concern this incident may cause you, and appreciates your continued support of Salud Family Health.

Sincerely,

John Santistevan
President/CEO
Salud Family Health

Steps You Can Take to Help Protect Personal Information

Activate Identity Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.
Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring
You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

$1 Million Identity Fraud Loss Reimbursement
Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation
You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration
If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three (3) major credit reporting bureaus listed below to request a free copy of your 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 one (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 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 (1) of the three (3) 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report 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 security freeze, you will need to provide 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 (2) to five (5) 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 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:

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	1-833-395-6938
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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For California residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For District of Columbia residents: the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Kentucky residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

For Maryland residents: the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents: the New York 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/.

For North Carolina residents: the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Oregon residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

For Rhode Island residents: the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are twelve (12) Rhode Island residents impacted by this incident.

For All U.S. residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338).