Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

[Name]
[Address]
[City], [State] [Zip Code]

May 4, 2022

Dear [Name]:

On behalf of Vail Health Services, we are writing to inform you that we recently suffered a security incident affecting limited portions of protected health information for some of our patients, which included your information. After experiencing issues with our network systems, we promptly investigated and on April 5, 2022, we determined that a third party potentially viewed the information on February 11, 2022. Vail Health is providing this notice to give you more information on what happened and what we are doing in response.

**WHAT HAPPENED**
An unauthorized third party gained access to a restricted location in Vail Health's computer network that had a small number of files, a subset of which contained results for COVID-19 testing performed at various Vail Health locations. Based on our investigation, the third party potentially viewed the information in the files, but we have no reason to suspect the information was or will be misused, especially given the limited types of data at issue.

**WHAT INFORMATION WAS INVOLVED**
The small number of files contained information for individuals who received COVID-19 tests from Vail Health, including full name, date of birth, contact information, COVID-19 test results, and encounter numbers—an internal reference we use to track your interactions with Vail Health. It is important to note that the information in the files did not contain Social Security numbers, driver's license numbers, financial information, or other sensitive information.

**WHAT WE ARE DOING**
We hired third-party experts to help us investigate the extent of the incident, and we are further securing our systems to protect your information. While the location of the impacted files was already access-restricted to a small number of individuals with a legitimate need to work with the information as part of their duties, we have added an additional layer of security to further restrict the ability to access that file location and have removed the impacted files from that location.

**WHAT YOU CAN DO**
If you have questions about this matter, please call us at the phone number below. While the information that was affected is not the type that generally can lead to identity theft or fraud, we nonetheless encourage you to remain vigilant for such activity. Enclosed with this letter you will find additional steps you can take to protect yourself.

**FOR MORE INFORMATION**
Our patients and their information are important to us. Should you have any questions, you can contact us at (866) 985-2702, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Lisa Herota, RHIA, CHC, CHPS, CCS
Senior Director, Compliance & Privacy
Compliance & Privacy Officer

## ADDITIONAL STEPS YOU CAN TAKE

**Remain vigilant** – While the information that was affected is not the type that generally can lead to identity theft or fraud, we nonetheless encourage you to remain vigilant for such activity by reviewing your account statements and free credit reports.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.

- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling 1-877-322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

**Consider placing a fraud alert or security freeze on your credit file** – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency.

- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which will prevent them from extending you credit. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

**Report suspicious activity** – If you believe you are the victim of identity theft, consider notifying your Attorney General, local law enforcement, or the Federal Trade Commission. You can also file a police report concerning the suspicious activity and request a copy of that report.

**Contact relevant authorities** – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

| **Federal Trade Commission** | **Equifax** | **Experian** | **TransUnion** |
|---|---|---|---|
| 600 Pennsylvania Ave. NW | P.O. Box 740241 | P.O. Box 9701 | P.O. Box 2000 |
| Washington, DC 20580 | Atlanta, GA 30374 | Allen, TX 75013 | Chester, PA 19016 |
| (202) 326-2222 | (800) 685-1111 | (888) 397-3742 | (888) 909-8872 |
| www.ftc.gov | www.equifax.com | www.experian.com | www.transunion.com |