SuperCareHealth
Return to IDX
P.O Box 989728
West Sacramento, CA 95798-9728

TO ENROLL, PLEASE CALL:
1-833-648-2050
OR VISIT:
https://response.idx.us/supercare
Enrollment Code: <<Enrollment>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

March 25, 2022

RE: <<Variable1>>

Dear <<First Name>> <<Last Name>>,

SuperCare Health is disappointed to be among the hundreds of healthcare-related entities that have experienced a data security incident in recent years. We are writing to inform you of this data security incident as it involved your <<Variable2>>. Please read this letter carefully as it contains information about the incident, our response efforts, the type of information involved, and steps you can take to help protect your personal information.

What Happened: On July 27, 2021, we discovered unauthorized activity on our systems. In response, we immediately began containment, mitigation, and restoration efforts to terminate the activity and to secure our network, systems, and data. In addition, we retained independent cybersecurity experts to conduct a forensic investigation into the incident and assist us in determining what happened.

The forensic investigation revealed that an unknown party had access to certain systems on our network from July 23, 2021 to July 27, 2021. Based on that information, we worked diligently to identify the potentially affected files and their contents. On February 4, 2022, we determined that the potentially impacted files contained some of your information. As of the date of this letter, **we have no reason to believe your information was published, shared, or misused** as a result of this incident. Nevertheless, we are notifying you of the incident and providing you with helpful resources.

What Information Was Involved: The data involved may include: <<Variable3>>.

What We Are Doing: In addition to the response efforts as described above, we implemented additional security measures to protect our digital environment and minimize the likelihood of future incidents. We also reported the incident to the Federal Bureau of Investigation and will cooperate to help identify and prosecute those responsible.

In addition, we are offering you <<12/24>> months of free identity theft protection services through IDX, a data breach and identity recovery services expert. The identity protection services include credit monitoring, dark web monitoring, $1 million identity theft reimbursement insurance, and fully managed identity recovery services at no cost to you. To receive these services, you must be over the age of 18 and have a Social Security number, an established credit file, and a residential address in the United States that is associated with your credit file.

What You Can Do: You can enroll in the free identity protection services offered in this letter by calling **1-833-648-2050** or visiting **https://response.idx.us/supercare** and using the Enrollment Code provided at the top of

this letter. Please note that the deadline to enroll is **June 25, 2022**. You can also review the enclosed sheet that provides additional information.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the identity protection services offered, please call 1-833-648-2050, Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific Time.

The privacy and security of patient information is a top priority for SuperCare Health. We take this incident very seriously and we regret any worry or inconvenience this may cause you.

Sincerely,

SuperCare Health

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
www.consumer.ftc.gov and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
www.oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet & Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
www.ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
www.oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete

inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.