22032

CAREPOINTE
EAR . NOSE . THROAT SINUS AND HEARING CENTER

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

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

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Notice of Data Breach

At CarePointe ENT, we take the security of your data very seriously and have tools in place to monitor the safety of it on an ongoing basis. We recently identified some suspicious activity involving patient data and initiated an investigation to determine what may have occurred. We've found that an unauthorized party may have obtained some of our patients' personal information. This notice explains the incident, measures that have been taken, and some steps you can take in response.

What happened?
On June 25, 2021, we were the target of a ransomware attack on our computer systems. Ransomware is a computer virus that encrypts computer systems until and unless we pay money (i.e., the ransom) demanded by the attackers. These rampant attacks continue to challenge everyone in the business and medical communities. We believe it is likely the attacker only wanted money and not the information on our computers but, in an abundance of caution, we are letting you know that your information was encrypted by the attackers.

What information was involved?
Our investigation revealed that the encrypted system contained your electronic healthcare records which may have included your name, address, date of birth, Social Security number (only if provided), medical insurance information, and related health information. **While our investigation did not find evidence that your information has been specifically misused**, we could not rule out the possibility that files containing some patient information may have been subject to unauthorized access as a result of this incident.

What we are doing.
We take the security of your information seriously and have taken measures to reduce the likelihood of a future cyber-attack, including increasing threat detection and further restricting remote access to meet the continually evolving cyber threat.

In an abundance of caution, we are offering the services of Kroll to provide identity monitoring for two years. Your identity monitoring services include Credit Monitoring, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
*You have until **November 21, 2021** to activate your identity monitoring services.*
Membership Number: <<Membership Number s_n>>

If you are under the age of 18, we are unable to provide identity monitoring services; however, Kroll will provide Fraud Consultation and Identity Theft Restoration for two years. Parents/Guardians need to call the call center to notify us if the letter recipient is a minor.

What you can do.
Although we have no reports of misuse of your or anyone's information, we encourage you to follow the instructions in this letter and activate the identity monitoring services we are providing. We also recommend that you review the "Additional Important Information" section included with this notice. This section describes additional steps you can take

to help protect yourself, including recommendations by the Federal Trade Commission (FTC) regarding identity theft protection and details on how to place a fraud alert or security freeze on your credit file. As an added precaution, you may want to closely monitor your personal accounts for any suspicious activity.

For more information.
If you have any questions, please call 1-???-???-????, Monday through Friday from 8:00 am - 5:30 pm Central Time, excluding major U.S. holidays. We appreciate your patience and understanding, and we sincerely apologize for any inconvenience or concern this incident may cause you.

Sincerely,

Dennis P. Han M.D.

Dennis Han, MD FACS

Additional Important Information

For residents of *Iowa*: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *New Mexico*: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights pursuant to the federal Fair Credit Reporting Act. Please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission listed below.

For residents of *District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island:*
You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

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

New York Attorney General
120 Broadway
3rd Floor
New York, NY 10271
800-771-7755
www.ag.ny.gov

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

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

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Ave, NW Washington, DC 20580
1-877-IDTHEFT (438-4338) www.identitytheft.gov

Massachusetts and Rhode Island residents: You have the right to obtain a police report if you are a victim of identity theft.

For residents of all states:
It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for unauthorized activity. You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (https://www.experian.com/fraud/center.html), or Transunion (https://www.transunion.com/fraud-victim-resource/place-fraud-alert). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze for yourself or your spouse or a minor under 16: (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) Proof of current address, such as current utility or telephone bill, bank or insurance statement; (6) legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
https://www.equifax.com/personal/credit-report-services/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013-9544
https://www.experian.com/help/
888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19014-0200
https://www.transunion.com/credit-help
800-680-7289