20361

careSOUTH carolina

C/O IDX
PO Box 4129
Everett WA 98204

ENDORSE

NAME
ADDRESS1
ADDRESS2
CSZ
COUNTRY

SEQ
CODE 2D
Ver 2A24

BREAK

To Enroll, Please Call:
(833) 664-2012
Or Visit:
https://response.idx.us/caresouth-netgain-incident
Enrollment Code: <<XXXXXXXX>>

May 17, 2021

Notice of Data Breach

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

At CareSouth Carolina, we take seriously our responsibility to protect the privacy and security of your personal information. We are writing to tell you about an incident that involved personal information maintained by our vendor, Netgain Technology, Inc. ("Netgain"). Netgain provides online data storage and other services for CareSouth Carolina.

What Happened

On December 1, 2020, Netgain informed CareSouth Carolina that it was investigating an IT security incident. At that time, CareSouth Carolina had no reason to believe that patient information was involved. On January 14, 2021, Netgain informed CareSouth Carolina that its investigation found that some of the servers that it maintained for CareSouth Carolina were affected as part of a ransomware attack on December 3, 2020. On April 13, 2021, CareSouth Carolina received a copy of the records that Netgain believed were affected by the attack. On April 27, 2021, CareSouth Carolina completed its review of the records and determined that your information was involved.

What Information Was Involved

CareSouth Carolina determined that the following information **was not** involved in this incident: your financial information (credit card and bank account numbers). CareSouth Carolina determined that the following information **was** involved in this incident: your name, date of birth, address, diagnosis/conditions, lab results, medications and other clinical information. For a small number of patients, Social Security numbers were involved.

What CareSouth Carolina Is Doing

In response to this incident, we required our employees to change their passwords for the affected systems and we are implementing additional security software for our networks. We also reported this incident to the federal government and to consumer reporting agencies.

We are also offering you identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What Netgain Is Doing

Netgain reported this incident to law enforcement and worked with cybersecurity experts to address, contain and recover from this incident. Netgain also paid a significant amount to the attacker in exchange for promises that the attacker will delete all copies of the data and that it will not publish, sell, or otherwise share the data. In addition, Netgain's

cybersecurity experts conducted dark web scans for the affected files, but such searches have not found that any data involved in this incident has been posted for sale or otherwise shared. Netgain also took several steps to strengthen the security of its environment following the incident.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling (833) 664-2012 or going to https://response.idx.us/caresouth-netgain-incident and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is August 17, 2021.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call (833) 664-2012 or go to https://response.idx.us/caresouth-netgain-incident for assistance or for any additional questions you may have.

Sincerely,

Ann Lewis
CEO, CareSouth Carolina
(Enclosure)

Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to https://response.idx.us/caresouth-netgain-incident and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at (833) 664-2012 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

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

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.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 agencies 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 a 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. You can 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.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

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

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

Description of Breach

Background: CareSouth Carolina ("Care South") is a private, non-profit community health center delivering patient-centered health and life services in the Pee Dee region of South Carolina. CareSouth operates centers in Bennettsville, Bishopville, Cheraw, Chesterfield, Dillon, Hartsville, Lake View, Latta, McColl and Society Hill. Services provided by CareSouth include family practice, internal medicine, pediatrics, women services, OB/GYN, HIV/AIDS primary care, dental, chiropractic services, pharmacy, geriatrics, social services, clinical counseling, laboratory, 4D ultrasound, X-Ray, migrant services and veterans choice provider.

Since 2011, CareSouth has contracted with Netgain Technology, LLC ("Netgain"), a third-party cloud storage provider. Because the CareSouth servers and systems maintained by Netgain contain protected health information ("PHI"), Netgain is a business associate and CareSouth and Netgain executed a business associate agreement.

Notice of Netgain Security Incident: On December 1, 2020, Netgain informed CareSouth that Netgain was investigating an IT security incident At the time, CareSouth had no reason to believe that its servers or its patients' information was affected by Netgain's IT security incident.

Notice of Netgain Breach: During a conference call on January 14, 2021, Netgain informed CareSouth that Netgain experienced a ransomware attack on December 3, 2020, and that CareSouth's servers were impacted. During the call, Netgain could not confirm which of CareSouth's servers, systems, or records were affected. Netgain stated it would send an email identifying the affected CareSouth servers and including a copy of the affected data.

CareSouth did not receive the promised email from Netgain until February 8, 2021, and only after CareSouth's CIO followed up with Netgain to request the information. Netgain forwarded an email from January 15, 2021, which CareSouth had not received, and in which Netgain stated it investigated, contained and eradicated the threat; reported the incident to law enforcement; and paid the threat actors, recovered the affected data, and monitored for signs the data was posted for sale. Attached to the email was a "tear sheet" documenting that several CareSouth servers were accessed on November 12, 2020, and data from one server was exfiltrated on November 14, 2020. The email stated that Netgain was "working to make a copy of this data available in a secure location for your review and will follow-up with additional information in a separate communication."

Identification of Affected Individuals: CareSouth did not receive the copy of the affected data until April 13, 2021, when CareSouth's CIO followed up with Netgain to report he had not received the promised "separate communication." The copied data from Netgain included over 400,000 pdf documents from a CareSouth document management system. The copied data from Netgain included documents from 2018, 2019 and 2020. Although the data management system maintains patient information dating back to 2011, Netgain stated that its investigation found that only data from 2018, 2019 and 2020 was exfiltrated. The documents contained demographic and clinical information.

On April 27, 2021, CareSouth concluded its review of the data. CareSouth decided to notify all patients with PHI maintained in the document management system because Netgain did not provide evidence that the breach was limited to only patient information from 2018, 2019, and 2020. In addition to notifying affected individuals by mail and posting substitute notice, CareSouth notified prominent media outlets in South Carolina and North Carolina, notified the national credit bureaus and offered affected individuals free credit monitoring.