

Subject: Notice of Data Security Incident

This is to notify affected individuals about a data security incident that involved a limited number of our clients' personal information. NorthCare Network ("NorthCare") takes the protection of your information very seriously. For this reason we are posting this notification on our website to explain the circumstances of the incident and provide you with information about additional steps you can take to protect your personal information. At present, we have no evidence that any of the personal health information at issue was misused; however, in an abundance of caution, we want to notify you of the IT incident and offer you the resources discussed below.

What Happened? On or about August 17, 2021, NorthCare became aware of unusual activity on the one of its email accounts. Upon discovery, NorthCare immediately secured the email account and began an investigation with the help of independent IT forensic investigators to determine the scope and extent of unauthorized access and whether any sensitive information was affected. At the end of September, the investigation confirmed that a single email account had been subject to unauthorized access from August 3-18, 2021. NorthCare then conducted a by-hand review of emails in the email account to determine all individuals affected and what type of information may have been involved. This review was completed on or about January 5, 2022. NorthCare believes that the information of 327 individuals may have been affected.

What Information Was Involved? While we have no confirmation of what information may have been viewed or accessed, the following information may have been involved: medical data including clinical information and non-clinical information such as mailing addresses and health insurance information. In some instances, the emails contained personally identifiable information like credit card/financial account numbers.

What Are We Doing? We take the security of sensitive information very seriously. Upon discovery of this incident, NorthCare immediately secured our system and took steps to prevent further unauthorized access. Additionally, we conducted a thorough investigation with the assistance of legal and cyber-security experts. We were able to determine access to the NorthCare email account, who and what information may have been affected as outlined above. We are providing notice by U.S. mail to those individuals whose addresses we were able to ascertain.

While at this time we have no indication that any information has been misused, we want to make sure you have the information you need so that you can take steps to help protect yourself and your identity. We encourage you to remain vigilant and to regularly review and monitor relevant account statements and credit reports and report suspected incidents of identity theft to local law enforcement, your state's Attorney General, or the Federal Trade Commission (the "FTC"). We have included more information on these steps below.

Complimentary Identity Protection and Credit Monitoring Services Because of the potential release of private information, we are offering at no charge identity theft protection services through Equifax. Please call the number below to learn more information and enroll in services.

What Else Can You Do? In addition to enrolling in the complimentary credit monitoring services being offered, we recommend you carefully review the enclosed *Steps You Can Take to Protect Your Information* for additional information on how to protect against identify theft and fraud.

For More Information/How to Enroll In Services

If you have questions about the Incident or whether you qualify for services and how to enroll, please call 1-844-795-2557, Monday through Friday from 9:00 a.m. to 9:00 p.m. (EST).

On behalf of NorthCare Network, we genuinely regret this incident occurred and apologize for any inconvenience this may cause you. We can assure you that we are doing everything we can to protect you and your information, now and in the future. If you have questions about this notice or this incident, or require further assistance, you can reach us at 888-333-8030 or 906-225-7254, Monday through Friday between the hours of 8:00 a.m. and 5:00 p.m. (EST).

Sincerely,

Dr. Tim Kangas, CEO

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

ADDITIONAL RESOURCES

Fraud Alert Information

Whether or not you enroll in credit monitoring, we recommend that you place a “Fraud Alert” on your credit file. Fraud Alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. Call only one of the following three nationwide credit reporting companies to place your Fraud Alert: TransUnion, Equifax, or Experian. As soon as the credit reporting company confirms your Fraud Alert, they will also forward your alert request to the other two nationwide credit reporting companies so you do not need to contact each of them separately. The contact information for the three nationwide credit reporting companies is:

Equifax
PO Box 740256
Atlanta, GA 30374
www.equifax.com
1-800-525-6285

TransUnion
PO Box 2000
Chester, PA 19016
www.transunion.com/fraud
1-800-680-7289

Experian
PO Box 9554
Allen, TX 75013
www.experian.com
1-888-397-3742

Free Credit Report Information

Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the Federal Trade Commission (FTC) at www.identitytheft.gov or at 1-877-ID-THEFT (1-877- 438-4338). Your complaint will be added to the FTC’s Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations. Also visit the FTC’s website at www.ftc.gov/idtheft to review their free identity theft resources such as their comprehensive step-by-step guide “*Identity Theft - A Recovery Plan*”.

Security Freeze Information

You can request a “Security Freeze” on your credit file by sending a request in writing, by mail, to each of the three nationwide credit reporting companies. 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. When a Security Freeze is added to your credit report, all third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. The Security Freeze may delay, interfere with or prohibit the timely approval of any subsequent request or application you make that involves access to your credit report. This may include, but is not limited to, new loans, credit, mortgages, insurance, rental housing, employment, investments, licenses, cellular phone service, utility service, digital signature service, Internet credit card transactions and extension of

credit at point of sale. There may be a fee for placing, temporarily lifting, or removing a Security Freeze with each of the nationwide consumer reporting companies, although that fee is waived if you send the credit reporting company proof of eligibility by mailing a copy of a valid identity theft report, or other valid report from a law enforcement agency to show you are a victim of identity theft and are eligible for free Security Freeze services.

To place a Security Freeze on your credit files at all three nationwide credit reporting companies, write to the addresses below and include the following information:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
<http://www.freeze.equifax.com>
1-800-349-9960

TransUnion Security Freeze
PO Box 160
Woodlyn, PA 19094
<http://transunion.com/freeze>
1-888-909-8872

Experian Security Freeze
PO Box 9554
Allen, TX 75013
<http://experian.com/freeze>
1-888-397-3742

- Your full name (first, middle, last including applicable generation, such as JR., SR., II, III, etc.)
- Your Social Security Number
- Your date of birth (month, day and year)
- Your complete address including proof of current address, such as a current utility bill, bank or insurance statement or telephone bill
- If you have moved in the past 2 years, give your previous addresses where you have lived for the past 2 years
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
- Include applicable fee. Call or visit each of the credit reporting company websites listed above for information on fees for Security Freeze services. Forms of payment are check, money order, or credit card (American Express, Discover, MasterCard and Visa), or a copy of a valid identity theft report, or other valid report from a law enforcement agency to show you are a victim of identity theft and are eligible for free Security Freeze services.

Within 5 business days of receiving your request for a security freeze, the consumer credit reporting company will provide you with a personal identification number (PIN) or password to use if you choose to remove the freeze on your consumer credit report or to authorize the release of your consumer credit report to a specific party or for a specified period of time after the freeze is in place.

Additional Information for residents of the following states:

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

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

District of Columbia: You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov

Kentucky: 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: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

Massachusetts: Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

New Mexico: 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: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

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

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

West Virginia: You have the right to ask that nationwide consumer reporting agencies place fraud alerts in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.