Clinic of North Texas, LLP Provides Notice of Data Security Incident

Clinic of North Texas LLP ("CNT") provides multi-specialty healthcare services to individuals. CNT is providing notice that it experienced a cybersecurity incident that may involve the personal and protected health information of some patients it serves. As such, CNT sent notification of this incident to potentially impacted individuals and is providing resources to assist them. CNT sincerely regrets any inconvenience that this incident may cause and remains dedicated to protecting all personal and health information.

What Happened:
On or about November 9, 2021, CNT first discovered that it was the victim of a cyber attack which may have resulted in unauthorized access to patient information stored on its systems. After learning about this Incident, CNT promptly engaged a third party cybersecurity firm to conduct a forensics investigation to analyze the nature and scope of the Incident, and to determine whether any patient information may have been exposed as a result.

On January 24, 2022, CNT concluded its initial investigation and determined the incident involved personal and protected health information. CNT has no evidence indicating misuse of this information. However, out of an abundance of caution, CNT is providing notification to all potentially impacted patients, regardless of the information not being subject to unauthorized access and/or acquisition.

What Information Was Involved:
The investigation confirmed that patient information contained in a folder stored on CNT's systems may have been subject to unauthorized access. The patient information contained in this folder was limited to patient's name, address, date of birth, and limited health information. **Please note that the patient information stored in this folder did not include social security numbers, driver's license numbers, other State identification numbers, financial account information, or debit or credit card numbers.**

What We Are Doing:
CNT takes the security of patient information very seriously, and has taken steps to prevent a similar event from occurring in the future. Since the incident, CNT changed all administrator passwords, implemented two-factor authentication and deployed end point detection and response and threat hunting tools to ensure that its information technology environment is secure.

The notification letter to the potentially impacted individuals includes steps that they can take to protect their information. In order to address any patient concerns and mitigate any exposure or risk of harm following this Incident, CNT has arranged for complimentary credit monitoring services, Dark Web monitoring services, and identity theft protection services to all potentially

impacted patients at no cost to them for a period of twelve (12) months. CNT recommends that individuals enroll in the services provided and follow the recommendations contained within the notification letter to ensure their information is protected.

What You Can Do:
As noted above, the information contained in the compromised folder did **not** include individuals' social security numbers, driver's license numbers, State identification numbers, financial account information, or debit or credit card numbers.

Nonetheless, as a precautionary measure, CNT recommends that individuals remain vigilant by closely reviewing their account statements and credit reports. If individuals detect any suspicious activity on an account, CNT strongly encourages individuals to promptly notify their financial institution. In addition, individuals should may report any fraudulent activity or any suspected incident of identity theft to law enforcement, their State Attorney General, and/or the Federal Trade Commission (FTC). To file a complaint or to contact the FTC, you can (1) send a letter to the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, D.C.; or (2) go to IdentityTheft.gov/databreach; or (3) call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement agencies.

CNT also encourages individuals to review the addendum to this notice titled "*Additional Important Information"* outlining additional steps they can take to protect their information.

For More Information:
For individuals seeking more information about the incident, please call CNT's dedicated toll-free helpline at 833-749-1690 (toll free) during the hours of 8 a.m. and 8 p.m. Central Standard Time, Monday through Friday (excluding U.S. national holidays).

Once again, CNT remains committed to protecting patient information and sincerely apologizes for this incident and any inconvenience it may cause.

Sincerely,

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon,* and *West Virginia*:
It is required by state laws to inform you that 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.

For residents of *Iowa*:
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*:
State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Arizona, Colorado, Maryland, Rhode Island, Illinois, New York, and North Carolina:
You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.
Maryland Office of the Attorney General Consumer Protection Division 200, St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us
Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street, Providence RI 02903 1-401-274-4400 www.riag.ri.gov
North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com
Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft
New York Office of Attorney General Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft
Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov
Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025
Illinois Office of the Attorney General Consumer Protection Division 100 W Randolph St., Chicago, IL 60601 1-800-243-0618 www.illinoisattorneygeneral.gov

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

For residents of all states:
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); TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). 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. As of September 21, 2018, 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. You may make that request 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 (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (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; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.