March 7, 2022

Anjali C Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Online Portal

Attorney General Aaron Frey
6 State House Station
Augusta, ME 04333

Department of Professional & Financial Regulation
Bureau of Consumer Credit Protection
35 State House Station
Augusta, Maine 04333

Re: Data Security Incident
Client: Norwood Clinic
File No.: 15991.01112

Dear Attorney General Frey:

We represent Norwood Clinic ("Norwood"), a multi-specialty medical facility operating out of Birmingham, Alabama in regards to a recent data security incident. Norwood takes this matter very seriously and is taking measures to remediate the incident and provide notice to potentially affected individuals.

This letter will serve to inform you of the nature of the incident, what information may have been compromised, the number of Maine residents being notified, and the steps that Norwood has taken in response to the incident.

1. **Nature of the incident.**

On October 22, 2021, Norwood discovered that it was the victim of a cyber attack that resulted in the unauthorized access of data stored on its network. Immediately after discovering the incident, Norwood took steps to secure and safely restore its systems and operations. In addition, Norwood engaged cybersecurity experts to conduct a thorough forensics investigation to determine the nature and scope of the incident and to assist in the remediation efforts. The investigation revealed that an unauthorized party gained access to Norwood's servers that stored patient information. However, the investigation was unable to confirm the specific information that may have been accessed. Therefore, out of an abundance of caution, Norwood is providing notice to all of its patients, regardless of whether their information was in fact subject to unauthorized access or acquisition. Norwood has no reason to believe that any individual's information has been misused as a result of this event. Immediately after concluding its review procedures, Norwood procured credit monitoring for affected individuals and drafted notices to individuals and state and federal

regulators as appropriate.

The forensics investigation revealed that those who instigated the data security incident gained access to folders containing personal information. PII impacted includes name, contact information, date of birth, Social Security number, Driver's License number, limited health information, and/or health insurance policy number.

2. **Number of Maine residents affected.**

Norwood discovered that seven (7) residents of Maine were impacted by this incident. A notification letter was sent to these individuals on March 8, 2022. A sample notice letter that was sent to the impacted individuals is included as **Exhibit A**.

3. **Steps taken.**

Norwood takes the security of personal information in its control very seriously, and has taken steps to prevent a similar event from occurring in the future, including but not limited to: revising email settings and policies, updating and modifying network security technical hardware, adding additional password complexity rules, and instituting more secure login mechanisms for all accounts.

Norwood has also provided 12 months of credit monitoring, dark web monitoring, and identity theft protection services to the individuals whose PII was potentially accessed by an unauthorized individual.

4. **Contact information.**

Norwood remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

Enclosure

EXHIBIT A

Norwood Clinic, Inc.
P.O. Box 3923
Syracuse, NY 13220

341 Walker Chapel Plaza, Suite 305
Fultondale, AL 35068
(205) 250-6000 • (800) 272-6481
www.norwoodclinic.com

<Individual>
<Address 1>
<Address 2>

March 8, 2022

Notice of Data Security Incident

Dear <Individual>,

We are writing to inform you of a data security incident which affected Norwood Clinic ("Norwood"), a large multispecialty medical group practicing in Alabama. The data security incident may have resulted in the potential compromise of some of your personal data. While we have no indication that your information has been misused, this letter contains information about the incident and information about how to protect your personal information going forward. Norwood considers the protection of sensitive information a top priority, and sincerely apologizes for any inconvenience as a result of the incident.

What Happened

On October 22, 2021, Norwood discovered that it was the victim of a cyber attack that resulted in the unauthorized access of data stored on its network. Immediately after discovering the incident, Norwood took steps to secure and safely restore its systems and operations. In addition, Norwood engaged cybersecurity experts to conduct a thorough forensics investigation to determine the nature and scope of the incident and to assist in the remediation efforts. The investigation revealed that an unauthorized party gained access to Norwood's servers that stored patient information. However, the investigation was unable to confirm the specific information that may have been accessed. **Therefore, out of an abundance of caution, Norwood is providing notice to all of its patients, regardless of whether their information was in fact subject to unauthorized access or acquisition. Norwood has no reason to believe that any individual's information has been misused as a result of this event.**

What Information Was Involved

While we have no reason to believe that your information has been misused as a result of this incident, we are notifying you out of an abundance of caution and for purposes of full transparency. Based on the investigation, the unauthorized party may have had access to your name, contact information, date of birth, Social Security number, Driver's License number, limited health information, and/or health insurance policy number. **However, please note that the information did not include any individual's financial account information, debit or credit card numbers.**

What We Are Doing

The security and privacy of patient information contained within Norwood's systems is a top priority, and Norwood is taking additional measures to protect this information. Since the incident, Norwood has continued to strengthen its security posture by adding the following security controls: revising email settings and policies, updating and modifying network security technical hardware, adding additional password complexity rules, and instituting additional secure login mechanisms for all accounts.

We are also providing you with twelve (12) months of complimentary credit monitoring, dark web monitoring and up to $1,000,000 in identity theft protection. Norwood strongly encourages you to take advantage of these services. More information on how to sign up for the services can be found below.

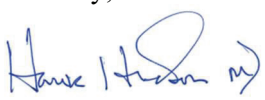
What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file.

Please review the enclosed *Additional Important Information*, to learn more about how to protect against the possibility of information misuse.

The protection of your information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause. If you have any questions, please do not hesitate to call Norwood's dedicated toll-free helpline at 1-833-770-0832 Monday through Friday between 8:00 am to 8:00 pm Eastern, excluding holidays. Representatives are available for 90 days.

Sincerely,



Norwood Clinic

Credit Monitoring

We are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score/Cyber Monitoring services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud, as well as a $1,000,000 insurance reimbursement policy. These services will be provided by Cyberscout through Identity Force, a company specializing in fraud assistance and remediation services.

How do I enroll for the free services?
To enroll in Credit Monitoring* services at no charge, please log on to **https://secure.identityforce.com/benefit/norwood** and follow the instructions provided. When prompted please provide the following unique code to receive services: **RSYUYJN5MC** In order for you to receive the monitoring services described above, you **must enroll within 90 days** from the date of this letter.

The enrollment requires an internet connection and an email account, and services may not be available to minors under the age of 18 years of age. When signing up for monitoring services, you may be asked to verify personal information for our own protection to confirm your identity.

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 Maryland, Rhode Island, Illinois, New York, and North Carolina:
You can obtain information from the Maryland and North Carolina 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

---

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:

Fair Credit Reporting Act: You are also advised that you may have additional rights under the federal Fair Credit Reporting Act.

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	**Experian Security Freeze**	**TransUnion (FVAD)**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
(800)-525-6285	(888)-397-3742	(800)-680-7289
https://www.equifax.com/personal/credit-report-services/credit-freeze/	www.experian.com/freeze	freeze.transunion.com

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