

January 6, 2022

Via electronic-mail: DOJ-CPB@doj.nh.gov; AttorneyGeneral@doj.nh.gov

Attorney General Gordon McDonald

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re: Our Client : CGSR, Inc. dba Meadowbrook Healthcare
Matter : Data Security Incident on November 11, 2021
Wilson Elser File # : 16516.01688

Dear Attorney General McDonald:

We represent CGSR, Inc. dba Meadowbrook Healthcare (“Meadowbrook Healthcare”), located in Plattsburgh, New York, with respect to a potential data security incident described in more detail below. Meadowbrook Healthcare takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the security breach, the number of New Hampshire residents being notified, what information has been compromised, and the steps that Meadowbrook Healthcare is taking to secure the integrity of its systems. We have also enclosed hereto a sample of the notification made to the potentially impact individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

On November 11, 2021, Meadowbrook Healthcare was a target of a cybersecurity incident. This incident may have resulted in the exposure of personal information. Although we have found no evidence that any information has been specifically accessed for misuse, it is possible that the potentially impacted individuals’ name, mailing address, date of birth, social security number, protected medical and health information, and/or Medicare Health Insurance information could have been exposed as a result of this attack.

As of this writing, Meadowbrook Healthcare has not received any reports of related identity theft since the date of the incident (November 11, 2021 to present).

3348 Peachtree Road N.E., Suite 1400 • Atlanta, Georgia 30326 • p 470.419.6650 • f 470.419.6651

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston • Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans • New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Seattle • Stamford • Virginia • Washington, DC • Wellington • White Plains •

wilsonelser.com



2. Number of New Hampshire Residents Affected

A total of one (1) resident of New Hampshire was potentially affected by this security incident. A notification letter to this individual was mailed on January 6, 2022, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps Taken

Immediately upon learning of this incident, Meadowbrook Healthcare contacted a reputable third-party forensic team to assist with its investigation. Since then, Meadowbrook Healthcare has been working with law enforcement to help respond to this incident, along with cybersecurity experts to review all policies and procedures relating to the security of Meadowbrook Healthcare's systems.

Although Meadowbrook Healthcare is not aware of any evidence of misuse of personal information, Meadowbrook Healthcare extended to all potentially impacted individuals an offer for free credit monitoring and identity theft protection through IDX. This service will include 12 months of credit monitoring, along with a fully managed identity theft recovery service, should the need arise.

4. Contact Information

Meadowbrook Healthcare 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 Tawana.Johnson@WilsonElser.com or (470) 419-6653.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

A handwritten signature in black ink that reads "Tawana Johnson". The signature is fluid and cursive, with the first name being the most prominent.

Tawana Johnson, Esq.

Copy: Robert Walker, Esq. (Wilson Elser LLP)

Enclosure: *Sample Notification Letter*

3348 Peachtree Road N.E., Suite 1400 • Atlanta, Georgia 30326 • p 470.419.6650 • f 470.419.6651

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston • Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans • New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Seattle • Stamford • Virginia • Washington, DC • Wellington • White Plains •

wilsonelser.com

Meadowbrook Healthcare
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223



Via First-Class Mail

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

January 6, 2022

Notice of Data Breach

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

CGSR, Inc. d/b/a Meadowbrook Healthcare (“Meadowbrook Healthcare”) is a skilled nursing and rehabilitation facility in Plattsburgh, New York. As your existing or former employer, we are writing to inform you of a data security incident that may have exposed your sensitive personal information. We take the privacy and protection of patient information very seriously, so we sincerely apologize and regret any inconvenience this incident may cause.

What Happened

On November 11, 2021, Meadowbrook Healthcare detected that it was the target of a cybersecurity attack. An unauthorized third party attempted to infiltrate Meadowbrook Healthcare’s computer network and demand a ransom payment. Upon detecting this incident, we moved quickly to secure our network environment and launched a thorough investigation. The investigation was performed with the help of independent IT security and forensic investigators to determine the scope and extent of the potential unauthorized access to our systems and any sensitive information.

What Information Was Involved

After the comprehensive forensic investigation into this incident concluded, we discovered that your name, mailing address, date of birth, and/or Social Security number may have been exposed to the unauthorized party during the network compromise. We have had no reports of related identity theft as a result of this incident.

What We Are Doing

We take the security of all information in our control very seriously. Given this, we are taking steps to prevent a similar event from occurring in the future by implementing additional safeguards and enhanced security measures to better protect the privacy and security of information in our systems. We have also reviewed and taken steps to enhance our policies and procedures relating to the security of our systems and servers, as well as our information life cycle management.

What You Can Do

We are offering you credit monitoring and identity theft protection services through IDX, a leading identity protection technology company. These services include <<12/24>> months of credit monitoring, as well as fully managed identity theft recovery services. With this protection, IDX will help you resolve any issues if your identity is compromised.

We encourage you to contact IDX with any questions and enroll in free IDX services by calling 1-800-939-4170 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX is available Monday through Friday 9 am to 9 pm Eastern Time. Please note the deadline to enroll is April 6, 2022.

IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

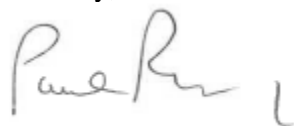
Enclosed, you will find additional information regarding the resources available to you, and the steps you can take to further protect your personal information.

For More Information

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call IDX services at 1-800-939-4170, Monday through Friday 9 am to 9 pm Eastern Time.

Meadowbrook Healthcare values the security of your personal data, and we apologize for any inconvenience this incident has caused.

Sincerely,

A handwritten signature in black ink, appearing to read "Paul Richards", with a stylized flourish at the end.

Paul Richards
Administrator/CEO,
Meadowbrook Healthcare

Additional Information

Credit Reports: 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.

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 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 www.transunion.com/credit-freeze
---	---	--

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.

File Police Report: You have the right to file or obtain a police report if you 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 proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further

information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

For 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 violators. 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. We encourage you to 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.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

For 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, and <https://ag.ny.gov/>.

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

Meadowbrook Healthcare
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223



Via First-Class Mail

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

To Enroll, Please Call:
1-800-939-4170
Or Visit:
[https://app.idx.us/account-
creation/protect](https://app.idx.us/account-creation/protect)
Enrollment Code: <<XXXXXXXXXX>>

January 6, 2022

Notice of Data Breach

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

CGSR, Inc. d/b/a Meadowbrook Healthcare (“Meadowbrook Healthcare”) is a skilled nursing and rehabilitation facility in Plattsburgh, New York. We are writing to inform you of a data security incident that may have exposed your sensitive personal information. We take the privacy and protection of patient information very seriously, so we sincerely apologize and regret any inconvenience this incident may cause.

What Happened

On November 11, 2021, Meadowbrook Healthcare detected that it was the target of a cybersecurity attack. An unauthorized third party attempted to infiltrate Meadowbrook Healthcare’s computer network and demand a ransom payment. Upon detecting this incident, we moved quickly to secure our network environment and launched a thorough investigation. The investigation was performed with the help of independent IT security and forensic investigators to determine the scope and extent of the potential unauthorized access to our systems and any sensitive information.

What Information Was Involved

After the comprehensive forensic investigation into this incident concluded, we discovered that your name, mailing address, date of birth, Social Security number, protected medical and health information, and/or Medicare Health Insurance information may have been exposed to the unauthorized third party during the network compromise. We have had no reports of related identity theft as a result of this incident.

What We Are Doing

We take the security of all information in our control very seriously. Given this, we are taking steps to prevent a similar event from occurring in the future by implementing additional safeguards and enhanced security measures to better protect the privacy and security of information in our systems. We have also reviewed and taken steps to enhance our policies and procedures relating to the security of our systems and servers, as well as our information life cycle management.

What You Can Do

We are offering you credit monitoring and identity theft protection services through IDX, a leading identity protection technology company. These services include <<12/24>> months of credit monitoring, as well as fully managed identity theft recovery services. With this protection, IDX will help you resolve any issues if your identity is compromised.

We encourage you to contact IDX with any questions and enroll in free IDX services by calling 1-800-939-4170 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX is available Monday through Friday 9 am to 9 pm Eastern Time. Please note the deadline to enroll is April 6, 2022.

IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Enclosed, you will find additional information regarding the resources available to you, and the steps you can take to further protect your personal information.

For More Information:

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call IDX services at 1-800-939-4170, Monday through Friday 9 am to 9 pm Eastern Time.

Meadowbrook Healthcare values the security of your personal data, and we apologize for any inconvenience this incident has caused.

Sincerely,

A handwritten signature in black ink, appearing to read "Paul Richards", with a stylized flourish at the end.

Paul Richards
Administrator/CEO,
Meadowbrook Healthcare

Additional Information

Credit Reports: 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.

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 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 www.transunion.com/credit-freeze
---	---	--

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.

File Police Report: You have the right to file or obtain a police report if you 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 proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further

information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

For 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 violators. 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. We encourage you to 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.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

For 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, and <https://ag.ny.gov/>.

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.