

James J. Giszczak
Direct Dial: 248-220-1354
E-mail: jgiszczak@mcdonaldhopkins.com

RECEIVED

JAN 04 2022

CONSUMER PROTECTION

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

December 29, 2021

VIA U.S. MAIL

John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Psych Care Consultants and Reimbursement Solutions – Incident Notification

Dear Mr. Formella:

McDonald Hopkins PLC represents Psych Care Consultants (“Psych Care”) and Reimbursement Solutions. I am writing to provide notification of an incident at a third-party vendor, QRS, Inc. (“QRS”) that may affect the security of personal information of approximately three (3) New Hampshire residents. Psych Care and Reimbursement Solutions’ investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Psych Care and Reimbursement Solutions do not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

QRS provides Psych Care and Reimbursement Solutions with an electronic patient portal. Psych Care and Reimbursement Solutions was recently informed by QRS that they had experienced a cyber-attack and that an unauthorized individual may have accessed one QRS dedicated patient portal server. QRS initially indicated to Psych Care and Reimbursement Solutions that it became aware of a potential security incident beginning on August 26, 2021 but that it had not determined if any personal information was impacted. QRS stated that upon discovery of the incident they immediately took the server offline, began an investigation, and notified law enforcement. QRS also engaged a forensic security firm to confirm the security of its network, analyze the incident, and determine the extent of the personal information that may have been accessed or acquired by the third party. On or about October 1, 2021, QRS’ investigation determined that between August 23, 2021 and August 26, 2021 the attacker accessed the single server and that Psych Care and Reimbursement Solutions patients’ personal information was potentially acquired. The files on the server contained the residents’ personal information, including their name, address, date of birth, Social Security number, patient identification number, portal username, and/or medical treatment or diagnosis information.

To date, QRS, Psych Care and Reimbursement Solutions are not aware of any reports of identity fraud as a direct result of this incident. Nevertheless, out of an abundance of caution, Psych Care and Reimbursement Solutions are informing you (and the affected residents) of the incident and to explain the steps being taken to help safeguard affected residents. QRS provided the affected residents with written notification of this incident commencing on November 26, 2021 in substantially the same form as the letter attached hereto. QRS is advising the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining a free credit report.

At Psych Care and Reimbursement Solutions, protecting the privacy of personal information is a top priority. Psych Care and Reimbursement Solutions is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. In connection with this incident, Psych Care and Reimbursement Solutions verified with QRS that it had taken significant steps to remove the intruder from its systems and prevent further compromise. Psych Care and Reimbursement Solutions continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at (248)-220-1354 or jgiszczak@mcdonaldhopkins.com.

Sincerely,



James J. Giszczak

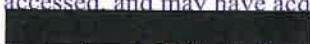
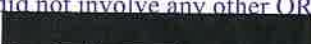
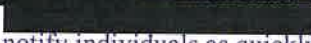

Encl.



RE: NOTICE OF DATA BREACH

Dear 

QRS, Inc. ("QRS") hosts the electronic patient portal for . QRS takes the protection of your information seriously and is writing to inform you about a recent incident that involved some of your personal information.

What Happened? On August 26, 2021, QRS discovered that an unknown, unauthorized third party accessed a QRS server associated with our patient portal and may have acquired certain protected health information ("PHI") stored in the server. Upon discovering the incident, we immediately took the server offline and began an investigation. We also engaged a forensic security firm to confirm the security of our network, analyze the incident, and determine the extent of the PHI that may have been accessed or acquired by the third party. Our investigation has determined that the third party accessed the server from August 23, 2021, to August 26, 2021. During this time, the third party accessed, and may have acquired, files in the server that contained your PHI. This incident did not involve any other QRS or  systems. We provided an initial notification of the incident to  on September 7, 2021. Following additional investigation, we provided further notification of the incident to  on or about October 1, 2021. We have since been working with  to notify individuals as quickly as possible.

What Information Was Involved? Our investigation determined that the incident involved unauthorized access, and potentially unauthorized acquisition, of your personal information, including your name, Social Security number, date of birth, patient number, and portal username. The accessed or acquired information may have also contained an address and limited medical treatment or diagnosis information if it was uploaded to the QRS portal. At this time, we are not aware of any identity theft or fraud to any person as a result of this incident.

What We Are Doing. Data security is one of our highest priorities. As discussed above, upon discovering the incident, we immediately took the server offline, began an investigation, and engaged a forensic security firm to confirm the security of our network. We will keep this particular server offline permanently. We have taken steps to further secure our network and reduce the risk of a similar incident occurring in the future, including implementing multifactor authentication on core QRS systems for key administrators and implementing a Security Information and Event Management System (SIEM). QRS is also reviewing and updating its information security policies.

What You Can Do. Although we are not aware of any instances of fraud or identity theft involving your information, you can find more information on steps to protect yourself against identity theft or fraud in the enclosed *Additional Important Information* sheet.

For More Information. We value the trust placed in us to protect your privacy, take our responsibility to safeguard your personal information seriously, and apologize for any inconvenience or concern this incident might cause. For further information and assistance, please call [REDACTED] from 9 a.m. – 9 p.m. EST, Monday through Friday. This toll-free number is provided on behalf of [REDACTED].

Sincerely,

QRS, Inc.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 2000
Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze can be placed without any charge and is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze
1-888-298-0045
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
www.transunion.com
P.O. Box 160
Woodlyn, PA 19094

This notification was not delayed by law enforcement.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Rhode Island Residents: We believe that this incident affected [XX] Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).