



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

RECEIVED
MAR 19 2019
CONSUMER PROTECTION

Edward J. Finn
Office: (267) 930-4776
Fax: (267) 930-4771
Email: efinn@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

March 15, 2019

***INTENDED FOR ADDRESSEE(S) ONLY
VIA U.S. 1ST CLASS MAIL***

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General MacDonald:

We represent Rutland Regional Medical Center (“Rutland Regional”) located at 160 Allen Street, Rutland, VT 05701 and are writing to notify your office of an incident that may affect the security of some personal information relating to twenty (20) New Hampshire residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Rutland Regional does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about December 21, 2018, a Rutland Regional employee identified a high volume of spam emails being sent from their email account. The employee reported this activity to Rutland Regional’s IT Department on December 29, 2018. Subsequently, on December 31, 2018, Rutland Regional’s IT Department determined the employee’s email account was subject to unauthorized access and immediately changed the employee’s password and locked the account.

Rutland Regional, with the assistance of a third-party forensic expert, further investigated this incident. Rutland Regional confirmed on February 6, 2019 that an unauthorized actor or actors had access to nine (9) employees’ email accounts at certain times between November 2, 2018 to February 6, 2019.

Attorney General Gordon J. MacDonald
March 15, 2019
Page 2

The information that could have been subject to unauthorized access includes: name and Social Security Number (most of which were part of a Medicare Health Insurance Claim Number).

Notice to New Hampshire Residents

On March 12, 2019, Rutland Regional began mailing, on a rolling basis, written notice of this incident to affected individuals. This rolling notice includes notice to twenty (20) New Hampshire residents who had information that is protected under the New Hampshire data incident notification law affected. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

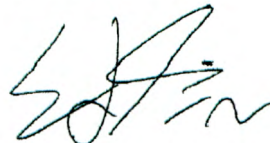
Upon discovering the event, Rutland Regional moved quickly to investigate and respond to the incident, assess the security of Rutland Regional systems, and notify potentially affected individuals. Rutland Regional is also working to implement additional safeguards and training to its employees. Rutland Regional is providing access to credit monitoring services for two years through AllClear ID to individuals whose Social Security numbers were potentially affected by this incident, at no cost to these individuals.

Additionally, Rutland Regional is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Rutland Regional is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4776.

Very truly yours,



Edward J. Finn of
MULLEN COUGHLIN LLC

EJF:ncl
Enclosures

EXHIBIT A



Processing Center • P.O. BOX 141578 • Austin, TX 78714



JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

[DATE]

RE: Notice of Data Security Incident

Dear John Sample:

Rutland Regional Medical Center (“Rutland Regional”) recently discovered a data security incident that may impact the security of your personal information. Rutland Regional writes to advise you of our investigation and the steps we are taking in response to this incident as well as steps you can take to protect your personal information should you feel it is appropriate to do so.

What happened? On December 21, 2018, a Rutland Regional employee identified a high volume of spam emails being sent from their email account. The employee reported this activity to Rutland Regional’s IT Department on December 29, 2018. Subsequently, on December 31, 2018, Rutland Regional’s IT Department determined the employee’s email account was subject to unauthorized access and immediately changed the employee’s password and locked the account.

Rutland Regional, with the assistance of a third-party forensic expert, further investigated this incident. Rutland Regional confirmed on February 6, 2019 that an unauthorized actor or actors had access to nine (9) employees’ email accounts at certain times between November 2, 2018 to February 6, 2019. The email accounts included, among other things, data files that contain the types of demographic information that is used for health care billing. On February 21, Rutland confirmed that your information was impacted. No Electronic Medical Record systems or other Rutland Regional internal systems were affected.

What Information Was Involved? The information in the email accounts that was potentially subject to unauthorized access and related to you includes your name, [DATA ELEMENTS AFFECTED].

Rutland Regional cannot confirm whether any specific information within the affected email accounts was actually accessed, viewed, or acquired without permission. We are providing this notification out of an abundance of caution to anyone whose information was accessible within the email accounts.



01-02-4

What We Are Doing. As part of our ongoing commitment to the security of personal information in our care, we are working to implement additional safeguards and security measures to enhance the privacy and security of our patient information. Information privacy and security remain one of our highest priorities. Rutland Regional has strict security measures and will continue to protect the information in our possession. As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-904-5761 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 1-year fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a \$1 million identity theft insurance policy. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-904-5761 using the following redemption code: Redemption Code.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

What You Can Do. You can enroll to receive the free credit monitoring and identity restoration services. You can also review the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud*. In addition, we advise you to report suspected incidents of identity theft to local law enforcement or the Attorney General.

For More Information. Rutland Regional has established a dedicated assistance line for individuals seeking additional information regarding this incident. Individuals may call 1-855-904-5761, 9 a.m. to 9 p.m. ET, Monday through Saturday with questions or if they would like additional information.

We sincerely apologize for this incident and regret any concern or inconvenience this has caused you.

Sincerely,



John Wallace
General Counsel
Rutland Regional Medical Center

Steps You Can Take to Protect Against Identity Theft and Fraud

Monitor Your Accounts. Rutland Regional encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

We recommend that you regularly review any Explanation of Benefits statements that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on your statement. If you do not receive regular Explanation of Benefits statements, you can contact your insurer and request that they send such statements following the provision of services in your name or number.

Credit Reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Fraud Alerts. You have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Equifax

P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian

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

TransUnion

P.O. Box 2000
Chester, PA 19022
800-680-7289
www.transunion.com

Security Freeze. You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Equifax

P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian

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

TransUnion

P.O. Box 2000
Chester, PA 19022
800-680-7289
www.transunion.com



Additional Information. To further educate and protect yourself against identity theft, fraud alerts, and security freezes, contact 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.