



CAMERON G. SHILLING
Direct Dial: 603.628.1351
Email: cameron.shilling@mcclane.com
Admitted in NH and MA
900 Elm Street, P.O. Box 326
Manchester, NH 03105-0326
T 603.625.6464
F 603.625.5650

January 22, 2021

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

RECEIVED

JAN 26 2021

CONSUMER PROTECTION

Re: Data Security Breach

To whom it may concern,

McLane Middleton, P.A. represents the ConvenientMD Urgent Care (“ConvenientMD” or “Company”), which is located at 111 New Hampshire Avenue, Suite 2, Portsmouth, New Hampshire 03801. We are writing to inform you about a data security breach that affects 130 individuals who are residents of the State of New Hampshire.

What Happened: On December 18, 2020, ConvenientMD sent an email to certain individuals informing them that the results of their coronavirus tests were available, and that those test results could be obtained by using their email address to log-on to the Company’s health care portal. On December 21, 2020, Convenient MD sent a similar email to certain other individuals. These December 18 and 21, 2020 emails (“Emails”) were sent to the email addresses that these individuals had provided to the Company at the time that they and/or other individuals associated with them (such as a family member) were tested for coronavirus by Convenient MD.

When ConvenientMD sent the Emails, the email addresses for all recipients were included in the “To” field of the Email instead of the “Bcc” field. As a result, recipients of each Email could have seen the email addresses of the other recipients of that Email and, if a person did so, that individual would have known that those other recipients (and/or individuals associated with them) were tested for coronavirus. ***No coronavirus test results were included in the Emails, since such results can be accessed only by logging-on to the Company’s health care portal. Similarly, no Email recipient could have logged-on to the portal using another’s email addresses in an attempt to obtain test results for others, because the Company’s portal verifies each individual’s identity by sending a message to the email account requiring confirmation prior to permitting access to the portal.***

What Information Was Involved: Individuals who received an Email could have viewed the email address of other individuals who received the same Email and, if so, would have known from the information in the Email that those other individuals, and/or other individuals associated with them, had a coronavirus test at a ConvenientMD facility. ***Again, no test results were included in the Emails, and no individual would have been able to log-on to the***

Office of the Attorney General
January 22, 2021
Page 2

Company's health care portal to obtain the test results or other personal or health information of other individuals.

What ConvenientMD Is Doing: In addition to sending the enclosed notification to affected individuals on January 12, 2021 and addressing any questions or concerns they have, ConvenientMD has modified its procedures for sending emails notifying individuals that information is available for them on our health care portal to ensure that the email addresses of recipients cannot be viewed by other recipients.

Thank you for your attention to this matter. Please contact us if you have any questions or we can be of any assistance with this matter.

Very truly yours,

Cameron G. Shilling

Cameron G. Shilling

Enclosure

Date

Via Email Only

First Name Last Name

Address

City, State Zip Code

Email address

Subject: Notice of Data Security Breach

Dear **First Name Last Name**,

We are writing to inform you about a data security breach at ConvenientMD Urgent Care (“ConvenientMD” or “Company”) that involved your protected health information (“PHI”). As a result, we encourage you to review this letter, and contact us at 1-800-528-0775 or riskresponse@convenientmd.com if you have any questions about this matter.

What Happened: On December 18, 2020, ConvenientMD sent an email to certain individuals informing them that the results of their coronavirus tests were available, and that those test results could be obtained by using their email address to log-on to the Company’s health care portal. On December 21, 2020, Convenient MD sent a similar email to certain other individuals. These December 18 and 21, 2020 emails (“Emails”) were sent to the email addresses that these individuals had provided to the Company at the time that they and/or other individuals associated with them (such as a family member) were tested for coronavirus at a Convenient MD facility. You are receiving this notice because you were a recipient of one of the Emails.

When ConvenientMD sent the Emails, the email addresses for all recipients were included in the “To” field of the Email instead of the “Bcc” field. As a result, recipients of each Email could have seen the email addresses of the other recipients of that Email and, if a person did so, that individual would have known that those other recipients (or individuals associated with them) were tested for coronavirus. ***Please be aware that no coronavirus test results were included in the Emails, since such results can be accessed only by logging-on to the Company’s health care portal. Similarly, no Email recipient could have logged-on to the portal using another’s email addresses in an attempt to obtain test results for others, because the Company’s portal verifies each individual’s identity by sending a message to the email account requiring confirmation prior to permitting access to the portal.***

What Information Was Involved? Other individuals who received the Email that you received from ConvenientMD on December 18 or 21, 2020 could have viewed your email address and, if so, would have known from the information in the Email that you and/or other individuals

associated with you had a coronavirus test at a ConvenientMD facility. ***Again, no test results were included in the Emails, and no individual would have been able to log-on to the Company's health care portal to obtain the test results or other PHI of other individuals.***

What Should You Do? ConvenientMD believes that the information contained in the Emails does not present a risk of compromise of your identity or credit. Nonetheless, if you are concerned, the Company encourages you to review the information found in the enclosed "*Steps You Can Take To Help Protect Your Information.*"

While ConvenientMD has not filed a police report, because the Company is not aware of any potential criminal conduct, if any such police report existed, you may have a right to receive a copy of it. Additionally, if you wish to pursue this matter with law enforcement, ConvenientMD encourages you to contact your local or state police department.

What Is ConvenientMD Doing? In addition to notifying affected individuals about this breach, ConvenientMD has modified its procedures for sending emails notifying individuals that information is available for them on our health care portal to ensure that the email addresses of recipients cannot be viewed by other recipients. If you have any questions or concerns about this matter, please contact us at 1-800-528-0775 or riskresponse@convenientmd.com. We appreciate the trust that you place in ConvenientMD to provide you with health care services, and therefore apologize for any concern or inconvenience this situation may cause.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Accounts

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.

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:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/cen-ter.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, 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:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services

Additional Information

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); and 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 and your state Attorney General.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. **Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300. **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023. **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 a violator. 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. You can 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. **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; <https://ag.ny.gov/>. **North Carolina Residents:** Office of the Attorney

General of North Carolina, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400, 877-566-7226 (toll free within NC). **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392. **Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 0 Rhode Island residents impacted by this incident. **Washington D.C. Residents:** the Office of Attorney General for the District of Columbia can be reached at: 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; <https://oag.dc.gov>. **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.