FISHERBROYLES®
A LIMITED LIABILITY PARTNERSHIP

Stuart A. Panensky
Partner
Mail: 420 Main St. #138, Tennent, NJ 07763
Office: 100 Overlook Center, 2nd Fl, Princeton, NJ 08540
Direct: 609.454.6957
Fax. 609.498.6039
Email: stuart.panensky@fisherbroyles.com
www.FisherBroyles.com

July 10, 2018

(Via E-Mail attorneygeneral@doj.nh.gov & Fax 603-271-2110)

State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03301

Re: Notice of Data Breach

Dear Madam / Sir:

The undersigned represents MedEvolve in connection with the above-referenced matter. In accordance with RSA 359-C:20(b), please accept the following from MedEvolve, in lieu of more formal notice of a data breach incident. MedEvolve is an Arkansas company with a principal place of business located at 1115 W 3rd Street, Little Rock, AR 72201. MedEvolve is a provider of electronic billing and record services to physicians and health facilities. Premier Immediate Medical Care ("Premier") is a customer of MedEvolve. This matter concerns the security of personal information relating to Premier patients, of which, 84 are New Hampshire residents.

Nature of the Data Event

On or about May 11, 2018, MedEvolve discovered that an FTP containing a file with information related to certain Premier patients was inadvertently accessible to the internet. Upon discovery, MedEvolve launched an investigation, with the help of third-party forensic investigators, to determine the contents of the file, how long the file was internet accessible, and whether the file was subject to unauthorized access. Through, the investigation, it was determined that the file was internet accessible from March 29, 2018 to May 4, 2018. The investigation also determined that the file was subject to unauthorized access on March 29, 2018. The file contained certain information including name, billing address, telephone number, the identification of patient's primary health insurer and the Social Security numbers for some of the individuals. The file did not contain any clinical information such as treatment or diagnosis or any financial information such as methods of payment. Additionally, we learned that a screenshot of the internet accessible file was taken and posted online in an article regarding this incident. The screenshot posted online contained the first names, city, state and zip code of fifteen (15) patients but did not include patients' last names or street addresses.

Notice to New Hampshire Residents

MedEvolve began providing written notice to potentially affected individuals, including 84 New Hampshire residents, by mail on or about July 10, 2018. Written notice was provided in substantially the same form as the letter attached here as Exhibit "A".

Other Steps Taken and to Be Taken

MedEvolve takes the security of information of its clients and their patients very seriously. Upon discovery, MedEvolve immediately secured the portal in question and took steps to prevent further access. MedEvolve also hired a third-party forensic investigator to conduct an exhaustive investigation of this matter. In an effort to mitigate the potential recurrence of an incident such as this, MedEvolve began conducting a review of its security practices, policies and procedures and updated them as appropriate. Further, MedEvolve also initiated updated Security Risk Analysis and Security Risk Management Plans. The employee responsible was sanctioned and work force members were retrained. Additional physical security measures were also put into place. MedEvolve is mailing letters to impacted individuals and providing those affected with two (2) years of credit monitoring services through TransUnion. MedEvolve is also informing the U.S. Department of Health and Human Services, additional required state regulators and the three consumer reporting agencies about this incident.

Thank you for your kind and early attention to this matter. Please feel free to contact the undersigned should there be any questions about this notification or any other aspect of this data security event.

Yours very truly,

FISHERBROYLES, LLP

Stuart A. Panensky, Esq.

Cc: Matthew Rolfes
President & CEO
MedEvolve

Exhibit “A”

medevolve

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Notice of Data Breach

Dear <<Name 1>>:

MedEvolve is writing to make you aware of a recent incident that may affect the security of your personal information. We take this incident seriously and are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so. MedEvolve provides electronic billing and record services to physicians and medical facilities, including Premier Immediate Medical Care ("Premier"), to streamline their processes. As part of these services, MedEvolve receives information from Premier related to its patients.

What Happened? On or about May 11, 2018, MedEvolve discovered that an FTP containing a file with information related to certain Premier patients was inadvertently accessible to the internet. Upon discovery, MedEvolve launched an investigation, with the help of third-party forensic investigators, to determine the contents of the file, how long the file was internet accessible, and whether the file was subject to unauthorized access. This investigation is ongoing. However, the investigation determined that the file was internet accessible from March 29, 2018 to May 4, 2018. The investigation also determined that the file was subject to unauthorized access on March 29, 2018. Additionally, we learned that a screenshot of the internet accessible file was taken and posted online in an article regarding this incident. The screenshot posted online contained the first names, city, state and ZIP Code of fifteen (15) patients, but did not include patients' last names or street addresses.

What Information Was Involved? The file that was inadvertently accessible contained your name, billing address, telephone number, primary health insurer and account number and Social Security number. The file did not contain any clinical information such as treatment or diagnosis nor any financial information such as methods of payment.

What Are We Doing? We take the security of information that our clients entrust in us very seriously. Upon discovery, we immediately secured the portal in question and took steps to prevent further access. We also hired a third-party forensic investigator to conduct an exhaustive investigation of this matter. 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 information in our systems. In addition to providing this notice to you, we are providing notice to the U.S. Department of Health and Human Services, relevant media outlets, and state regulators as required.

We want to make sure you have the information you need so that you can take steps to help protect yourself from identity theft. We encourage you to remain vigilant and to regularly review and monitor relevant account statements and credit reports and report suspected incidents of identity theft to local law enforcement, your state's Attorney General, or the Federal Trade Commission (the "FTC"). We have included more information on these steps in this letter.

Complimentary Credit Monitoring Service

As an added precaution, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for two years provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the *my*TrueIdentity website at **www.mytrueidentity.com** and in the space referenced as "Enter Activation Code", enter the following 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422.** When prompted, enter the following 6-digit telephone pass code **<<Insert static 6-digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Insert Date>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

Again, this protection is being offered at no cost to you, but you must contact TransUnion to activate your protection.

What Can You Do? You can review the enclosed *Steps You Can Take to Protect Your Information* for additional information on how to better protect against identify theft and fraud. You can also enroll in the complimentary credit monitoring services being offered.

For More Information. We are genuinely sorry that this incident occurred and apologize for any inconvenience this matter may cause you. We can assure you that we are doing everything we can to protect you and your information and to minimize any recurrence of this situation. If you have questions about this notice or this incident or require further assistance, you can reach us at 888-354-7159, between the hours of 9:00 a.m. and 9:00 p.m. (ET). You can also get more information at http://www.mytrueidentity.com. Please reference this letter when calling.

Thank you,

Matthew D. Rolfes
MedEvolve President & CEO

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

The following information is provided in accordance with certain state legal requirements.

Monitor Your Accounts

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits, and monitoring your free credit reports for suspicious activity and to detect errors. 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. At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from $3 to $15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.freeze.equifax.com	www.experian.com/freeze/	freeze.transunion.com

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting 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 encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be promptly reported to law enforcement, the Federal Trade Commission, and your state Attorney General. 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 crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. This notice has not been delayed as the result of a law enforcement investigation.

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

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