med:evolve

[redacted]

[redacted]

JAMES CARMODY

[redacted]

July 10, 2018

Notice of Data Breach

Dear James Carmody:

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. 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.