



Lindsay B. Nickle
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Lindsay.Nickle@lewisbrisbois.com
Direct: 214.722.7141

November 7, 2017

Via email to DOJ-CPB@doj.nh.gov

Attorney General Joseph Foster
Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Potential Data Security Incident

Dear Attorney General Foster:

We represent Little River Healthcare – Central Texas, LLC d/b/a Little River Waco Ear Nose and Throat (“Little River Waco Ear Nose and Throat”) with respect to a recent data security incident described in greater detail below. Little River Waco Ear Nose and Throat taking steps to prevent a similar incident from occurring in the future.

On July 7, 2017, Little River Waco Ear Nose and Throat separated from Waco Otolaryngology Associates, P.A. (the “Practice”). Consequently, the Practice is now operating the clinic as an independent medical practice separate from Little River Waco Ear Nose and Throat.

1. Nature of the security incident.

On June 26, 2017, it was discovered that Little River Waco Ear Nose and Throat was the victim of a ransomware attack that encrypted the data stored on some computers and servers. Action was immediately taken to secure the network, and an investigation was conducted. An independent computer forensic expert was retained to assist in the investigation and the expert confirmed the presence of ransomware. Little River Waco Ear Nose and Throat attempted to restore the infected data, and in the process of doing so discovered that some patient records were unfortunately irretrievably deleted. However, there is no evidence of the misuse of any information potentially involved in this incident, and Little River Waco Ear Nose and Throat has notified the potentially affected population.

2. Number of New Hampshire residents affected.

A total number of 2 residents of New Hampshire were affected by this security incident. Notification letters to these individuals were mailed on November 7, 2017 via first class mail. A sample copy of the notification letter is included with this letter.

November 7, 2017

Page 2

3. Steps taken relating to the incident.

Little River Waco Ear Nose and Throat wants to assure you that it is taking steps to prevent a similar event from occurring in the future, and to protect the privacy and security of all patient information. Computer systems are in the process of being analyzed and updated to ensure the security of sensitive data. In addition, potentially impacted individuals have been offered 12 months of identity protection services through ID Experts, at no charge.

4. Contact information.

Little River Waco Ear Nose and Throat remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (214) 722-7141, or by e-mail at lindsay.nickle@lewisbrisbois.com.

Please let me know if you have any questions.

Best regards,



Lindsay B. Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

LBN
Enclosure



C/O ID Experts
PO Box 10444
Dublin, Ohio 43017-4044

To Enroll, Please Call:
1-877-919-6852
Or Visit:
<https://ide.myidcare/enrollwacoent>
Enrollment Code:
<<XXXXXXXXXX>>

<<First Name>><<Last Name>>
<<Address1>>
<<Address2>>
<<City>><<State>><<ZIP>>

Re: Notice of Data Security Incident

November 07, 2017

To <<First Name>><<Last Name>>:

The purpose of this letter is to inform you of a potential data security incident involving Little River Healthcare – Central Texas, LLC d/b/a Little River Waco Ear Nose and Throat (“Little River Waco Ear Nose and Throat”) that may have resulted in the potential disclosure of your medical and personal information. We take the security of all patient information very seriously, and sincerely apologize for any inconvenience this incident may cause.

On July 7, 2017, Little River Waco Ear Nose and Throat separated from Waco Otolaryngology Associates, P.A. (the “Practice”). Consequently, the Practice is now operating the clinic as an independent medical practice separate from Little River Waco Ear Nose and Throat.

This letter contains information about steps you can take to protect yourself and resources we are making available to help you.

What happened.

On June 26, 2017, it was discovered that Little River Waco Ear Nose and Throat was the victim of a ransomware attack that encrypted the data stored on some of our computers and servers. Action was immediately taken to secure our network, and an investigation was conducted. An independent computer forensic expert was retained to assist in the investigation and the expert confirmed the presence of ransomware. Little River Waco Ear Nose and Throat attempted to restore the infected data, and in the process of doing so discovered that some patient records were unfortunately irretrievably deleted. However, there is no evidence of the misuse of any information potentially involved in this incident.

What information was involved.

The records that potentially have been impacted may include your name, address, date of birth, Social Security number, and medical information.

What we are doing and what you can do.

As stated above, while we are not aware of the misuse of any information potentially involved in this incident, we are notifying you out of an abundance of caution. As a precautionary measure to safeguard your information from potential misuse, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of credit monitoring, a \$1,000,000 insurance reimbursement policy, exclusive educational materials and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised. We encourage you to take full advantage of this offer. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information. The deadline to complete the enrollment process is February 7, 2018.

You will find detailed instructions for enrollment on the enclosed document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling on the website, so please do not discard this letter. Please call 1-877-919-6852 or go to <https://ide.myidcare/enrollwacoent> to enroll.

For more information.

We sincerely regret any inconvenience or concern that this matter may cause you and remain dedicated to protecting your information. Please do not hesitate to call 1-877-919-6852, Monday through Friday, 7:00 a.m. to 7:00 p.m. Central Time if you have questions about this event.

Sincerely,

Little River Waco Ear Nose and Throat
Now Known as Waco Otolaryngology Associates, P.A.

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the nationwide three credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorneys General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

Rhode Island Office of the Attorney General
Consumer Protection
150 South Main Street
Providence RI 02903
1-401-274-4400
www.riag.ri.gov

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Ave, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/bcp/edu/microsites/idtheft

For residents of Massachusetts:

It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three credit bureaus is below:

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, or regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a small fee to place, life, or remove a freeze, but is free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency. You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.freeze.equifax.com
800-525-6285

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

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
888-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.