



RECEIVED

NOV 30 2017

CONSUMER PROTECTION

November 28, 2017

Gregory J. Bautista
914.872.7839 (direct)
Gregory.Bautista@wilsonelser.com

Via Regular Mail

Attorney General Joseph A. Foster
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03302

Re: Data Security Incident

Dear Attorney General Foster:

We represent Pulmonary Specialists of Louisville, PSC (“PSoL”) with respect to an incident involving the potential exposure of certain personal information described in detail below.

1. Nature of the possible security breach or unauthorized use or access

On September 26, 2017, PSoL identified possible unauthorized access to its electronic health record (EHR) system. After learning of this, PSoL worked with its IT department and computer experts to investigate whether its systems were at risk. The investigation determined that an unknown, unauthorized third party may have gained access to the practice’s EHR and could have viewed or accessed patients’ electronically stored information, including names, addresses, phone numbers, dates of birth, Social Security numbers, health insurance information and medical records. At this time, PSoL is not aware of any specific access to patient information.

2. Number of New Hampshire residents potentially affected

Approximately 2 New Hampshire residents were affected in this potential incident. PSoL sent the potentially impacted individuals letters notifying them of this incident on November 28, 2017. A copy of the notification sent to the potentially impacted individuals is included with this letter.

3. Steps you have taken or plan to take relating to the potential incident

PSoL has taken steps to secure patient information, including reviewing and revising its information security policies and procedures and updating the security systems on its EHR. PSoL has also notified the Department of Health and Human Services, Office of Civil Rights, as per the HIPAA Breach Notification Rule.

1133 Westchester Avenue • White Plains, NY 10604 • p 914.323.7000 • f 914.323.7001

Albany • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Grand City • Highcrest • Houston • Kentucky • Los Angeles • London
Los Angeles • Miami • Michigan • Milwaukee • New Jersey • New Orleans • New York • Orlando • Philadelphia • San Francisco • Stamford • Virginia
Washington, DC • West Palm Beach • White Plains

wilsonelser.com

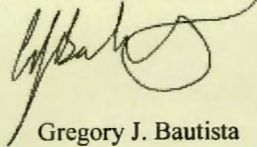
6790070v.1

4. Other notification and contact information.

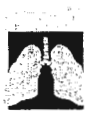
If you have any additional questions, please contact me at Gregory.Bautista@wilsonelser.com or (914) 872-7839.

Very Truly Yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Gregory J. Bautista



Return Mail Processing Center
P.O. 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>>
<<County>>

November 28, 2017

Dear <<Name 1>>:

We are writing to inform you of an incident that may have resulted in the disclosure of your information, including your name, Social Security number and medical records. We take the security of your information very seriously and sincerely apologize for any inconvenience this incident may cause. This letter contains additional information about what occurred.

On September 26, 2017, we identified possible unauthorized access to our electronic health record (EHR) system. In response, we worked with our IT department and computer experts to investigate whether our systems were at risk. The investigation determined that an unknown, unauthorized third party may have gained access to our practice's EHR and could have viewed or accessed your electronically stored information, including your name, address, phone number, date of birth, Social Security number, health insurance information and medical records. Although at this time we have no evidence that your information was actually accessed or viewed, or any indication of misuse of your information, we are sending this letter to you out of an abundance of caution. We also recommend that you monitor your accounts for unusual activity. Additional tips for protecting your information can be found on the reverse side of this letter.

We want to assure you that we have taken steps to prevent a similar event from occurring in the future, including reviewing and revising our information security policies and procedures to minimize this risk in the future and updating the security systems on our EHR.

We sincerely regret any inconvenience that this incident may cause you, and remain dedicated to protecting your personal information. Should you have any questions or concerns, please call 844-814-8802, Monday through Friday from 6:00 AM to 6:00 PM Pacific Standard Time.

Sincerely,

Dr. Ammar Almasalkhi
Pulmonary Specialists of Louisville

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/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
800-680-7289

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