NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
Tabor Center
1200 17th Street, Suite 1000
Denver, Colorado 80202-5835
United States

Direct line +1 303 801 2758
kris.kleiner@nortonrosefulbright.com

Tel +1 303 801 2700
Fax +1 303 801 2777
nortonrosefulbright.com

January 27, 2017

By Certified Mail
Return Receipt Requested

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: Legal Notice of Information Security Incident

Dear Sirs or Madams:

I write on behalf of my client, Princeton Pain Management (PPM), to inform you of a potential data incident involving personal information for certain PPM customers that may have affected approximately 2 New Hampshire residents. PPM is notifying these individuals and outlining some steps they may take to help protect themselves.

PPM recently learned that a third party gained unauthorized access to portions of its network and may have been able to access certain patient information as a result. The incident could affect certain information, including names, addresses, telephone numbers, dates of birth, Social Security numbers, driver license or government identification numbers, medical and health insurance identifiers, and diagnostic and treatment information for certain individuals. Although the forensic investigation did not identify any evidence that any information maintained by PPM was actually acquired, PPM is notifying individuals and your office out of an abundance of caution.

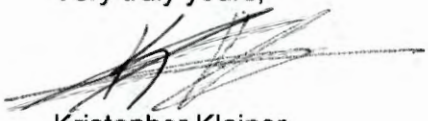
PPM takes the privacy of personal information seriously, and deeply regrets that this incident occurred. Upon learning of the incident, PPM promptly took steps to address the situation, including initiating an internal investigation and engaging outside forensic experts to assist PPM in investigating and remediating the situation. PPM has reconfigured various components of its network to enhance security and, although PPM is continuing to review security processes and updating system protections designed to help prevent this type of incident from recurring in the future, this incident has now been contained.

Pursuant to our obligations under the Health Insurance Portability and Accountability Act of 1996 and associated regulations, we are providing notice to potentially affected individuals and to the U.S. Department of Health and Human Services. Affected individuals are being notified

via written letter which will begin mailing on or around January 27, 2017. A form copy of the notice being sent to the affected New Hampshire residents is included here for your reference.

If you have any questions or need further information regarding this incident, please contact me at (303) 801-2758 or kris.kleiner@nortonrosefulbright.com.

Very truly yours,



Kristopher Kleiner

KCK
Enclosure

PRINCETON
PAIN
MANAGEMENT

[DATE]

[ADDRESS]

Dear [PATIENT NAME],

As a provider of pain management services, Princeton Pain Management (PPM) is committed to maintaining the privacy and security of our patients' information. Unfortunately, PPM recently learned that, like many other organizations, we may have been the victim of a data incident. We are writing to inform you of an incident involving some of that information and to share with you the steps we are taking to address it.

What Happened

On November 28, 2016, PPM discovered that a third party gained unauthorized access to certain data on its computer system. Although our investigation has not identified evidence that any patient records were removed from our systems, we are notifying you about this incident out of an abundance of caution.

What Information Was Involved

We believe that this incident may have affected certain information stored in our systems including names, addresses, telephone numbers, dates of birth, Social Security or Medicare numbers, driver license or government identification numbers, medical and health insurance identifiers, and diagnostic and treatment information.

What We Are Doing

PPM takes the responsibility to safeguard the privacy and security of patient information very seriously. Upon learning of this incident, we promptly commenced an internal investigation and retained a computer forensics firm to assist in the investigation. Additionally, we have reconfigured various components of our network to enhance security and will be reviewing our security processes and updating system protections designed to help prevent this type of incident from recurring in the future.

Although we have no evidence that any of your information has been taken or used inappropriately, we are offering twelve months of complimentary identity protection services from an identity monitoring services company. These services help detect possible misuse of your personal information and provide you with identity protection support focused on immediate identification and resolution of identity theft. For more information about these services and instructions on completing the enrollment process, please refer to the "Information about Identity Theft Protection" reference guide attached to this letter. This reference guide also

includes recommendations from the Federal Trade Commission regarding identity theft protection.

What You Can Do

While we are not aware of any fraud or identity theft arising out of this incident, we want to make you aware of steps that you can take as a precaution:

- **Activating the Complimentary Identity Protection Services.** As outlined above, we are offering one year of identity theft protection and credit monitoring services at no charge to you. For more information about these services and instructions on completing the enrollment process, please refer to the "Information about Identity Theft Protection" reference guide attached to this letter. Note that you must complete the enrollment process by April 30, 2017.

- **Checking Credit Reports.** We recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office, file a police report for identity theft, and get a copy of it. You may need to give copies of the police report to creditors to clear up your records.

- **Reviewing Explanation of Benefits Documents.** We also recommend that you regularly review the explanation of benefits statements that you receive from your health insurer or health plan or review for persons whose medical bills you assist with or pay (such as your child). If you identify services listed on the explanation of benefits that were not received, please immediately contact your insurer or health plan.

- **Consulting the Identity Theft Protection Guide.** Finally, please review the "Information about Identity Theft Protection" reference guide, included here, which describes additional steps that you may take as a precaution, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

For More Information

If you have questions or would like any additional information about this matter, contact us toll-free at 855-474-3904 between 8 a.m. and 5 p.m. Eastern Time, Monday through Friday. Again, we deeply regret any concern this incident may cause.

Sincerely,

Chu-Kuang Chen, MD, PhD
Medical Director

Information about Identity Theft Protection

We have engaged Experian® to offer you complimentary fraud resolution and identity protection services for one year. These services help detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. To enroll, visit **www.protectmyid.com/redeem** by **April 30, 2017** and use the following activation code: [**ACTIVATION CODE**]. You may also enroll over the phone by calling 877-288-8057 between the hours of 9:00 AM and 9:00 PM (Eastern Time), Monday through Friday and 11:00 AM and 8:00 PM Saturday (excluding holidays). Please provide the following engagement number as proof of eligibility: **PC106101**.

We also recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: 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.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For residents of Rhode Island You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, http://www.riag.ri.gov.

Review Accounts and Credit Reports: You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

Equifax (www.equifax.com)
General Contact:

P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Fraud Alerts:
P.O. Box 740256, Atlanta, GA 30374
Credit Freezes:
P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)
General Contact:

P.O. Box 2002
Allen, TX 75013
888-397-3742

Fraud Alerts and Security Freezes:
P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)
General Contact:

P.O. Box 105281
Atlanta, GA 30348
877-322-8228

Fraud Alerts and Security Freezes:
P.O. Box 2000, Chester, PA 19022
888-909-8872