MULLEN
COUGHLIN

Jennifer A. Coughlin
Office: 267-930-4774
Fax: 267-930-4771
Email: jcoughlin@mullen.legal

1275 Drummers Lane, Suite 302
Wayne, PA 19087

INTENDED FOR ADDRESSEE(S) ONLY

Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Mr. Foster:

We represent Dr. Melissa D. Selke, 390 Amwell Road, Building 4 - Suite 405, Hillsborough, NJ 08844, and are writing to notify your office of an incident that may affect the security of protected health information relating to one (1) New Hampshire resident. The investigation into this incident is ongoing, and this notice will be supplemented with any substantive information learned after submission of this notice. By providing this notice, Dr. Selke does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On October 6, 2016, Dr. Selke discovered her information system had been infected with a virus that prohibited access to patient files. The integrity of the information system was immediately restored and an investigation was launched with the assistance of a forensic expert, to determine the capabilities of the virus and how it was introduced to the system. As part of the extensive investigation, on November 18, 2016, it was determined that this virus was introduced by an unknown third party that had access to a server on Dr. Selke's information system.

Notice to New Hampshire Resident

While the investigation is ongoing, and there is no evidence the unknown third party viewed or took information stored on the server, it has been confirmed that this server housed files and a software application containing information which may include patient or guarantor names, addresses, phone numbers, Social Security numbers, treatment and diagnosis information, driver's license information,

health insurance information, treating physician information, medical record number, and treatment date(s). Dr. Selke determined that the protected health information relating to one (1) New Hampshire resident may have been stored on the server. On December 2, 2016, Dr. Selke issued a press release regarding this incident to media serving New Jersey. See, ***Exhibit A***. Dr. Selke also conspicuously posted notice of this incident on the homepage of her website, where it will remain for ninety days, in substantially the same form as the press release attached hereto as ***Exhibit A***. Additionally, beginning on or about December 5, 2016, Dr. Selke is providing written notice of this incident to potentially impacted individuals. Notice is being provided to potentially impacted patients and guarantors of patients of Dr. Selke's practice in substantially the same form as the letter attached hereto as ***Exhibit B***.

Other Steps Taken and To Be Taken

Dr. Selke is providing potentially impacted individuals access to 1 free year of identity monitoring and restoration services through First Watch Technologies, Inc., and has established a dedicated hotline for individuals to contact with questions or concerns regarding this incident. Additionally, Dr. Selke is providing potentially impacted individuals with helpful information on how to protect against identity theft and fraud, including how to place a fraud alert and security freeze on one's credit file, the contact information for the national consumer reporting agencies, how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, state attorney general, and law enforcement to report attempted or actual identity theft and fraud. Dr. Selke is also providing written notice of this incident to the Department of Health and Human Services, the Centers for Medicaid and Medicare Services, as well as consumer reporting agencies and other state regulators as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4774.

Very truly yours,

Jennifer A. Coughlin of
MULLEN COUGHLIN LLC

JAC

Exhibit A

Melissa Selke, MD, PC
Family Medicine
Princeton Medicine

Media Contact: Carol Norris-Smith
609-252-8795

PHYSICIAN PRACTICE PROVIDES NOTICE OF DATA INCIDENT

Hillsborough, New Jersey – December 2, 2016 – A Somerset County physician is taking action after she recently became aware that there was an incident in which an unknown third party may have gained access to the data in her practice. Although there is no indication of actual or attempted misuse of patient information, Dr. Melissa D. Selke is notifying patients whose records may have been subject to unauthorized access and providing these patients with information and resources that can be used to better protect against the possibility of identity theft or fraud if they feel it is appropriate to do so.

"We take this incident, and patient privacy, very seriously," Dr. Melissa D. Selke stated. "We are taking steps to help prevent another incident of this kind from happening, and continue to review our processes, policies, and procedures that address data privacy," Dr. Selke said.

To better assist those who may potentially have been affected by this event, Dr. Selke has established a toll-free privacy line staffed with individuals familiar with this incident and how to better protect against the possibility of identity theft and fraud, and you can direct all questions and concerns to this line by calling 866-961-1460, between 9:00 a.m. and 7:00 p.m. EST, Monday through Friday, excluding major holidays and between 8:00 a.m. and 5:00 p.m. EST on Saturday, December 3 and Saturday, December 10.

What Happened

On October 6, 2016, Dr. Selke discovered her information system had been infected with a virus that prohibited access to patient files. The integrity of the information system was immediately restored and an investigation was launched with the assistance of a forensic expert, to determine the capabilities of the virus and how it was introduced to the system. As part of the extensive investigation, on November 18, 2016, it was determined that this virus was introduced by an unknown third party that had access to a server on Dr. Selke' information system.

Information Affected

While the investigation is ongoing, and there is no evidence the unknown third party viewed or took patient information stored on the server, it has been confirmed that this server housed files and a software application containing information which may include patients' names, addresses, phone numbers, Social Security numbers, treatment and diagnosis information, driver's license information, health insurance information, treating physician information, medical record number, and treatment date(s).

Melissa Selke, MD, PC
Family Medicine
Princeton Medicine

Media Contact: Carol Norris-Smith
609-252-8795

Notification

Dr. Selke is mailing letters to impacted patients. Dr. Selke is also informing the U.S. Department of Health and Human Services, and state regulators about this incident.

Fraud Prevention Tips

Dr. Selke encourages affected individuals to remain vigilant against incidents of identity theft and fraud and to seek to protect against possible identity theft or other financial loss by regularly reviewing their financial account statements, credit reports, and explanations of benefits for suspicious activity. Anyone with questions regarding how to best protect themselves from potential harm resulting from this incident, including how to receive a free copy of one's credit report, and place a fraud alert or security freeze on one's credit file, is encouraged to call 866-961-1460, between 9:00 a.m. and 7:00 p.m. EST, Monday through Friday, and between 8:00 a.m. and 5:00 p.m. EST on Saturday, excluding major holidays

###

Exhibit B

Return mail will be processed by: IBC
PO Box 1122
Charlotte, NC 28201-1122
PO #122059

00002801

Draft

Melissa Selke, MD, PC
Family Medicine
Princeton Medicine

December 5, 2016

Dear :

I am writing to inform you of a recent event that may affect the security of your personal information. While we are unaware of any actual or attempted misuse of your personal information, out of an abundance of caution, we are providing you with information about the incident. We are also providing you with information regarding the steps we are taking in response, and steps you can take to protect against fraud should you feel it is appropriate.

What Happened? On October 6, 2016, we discovered our information system had been infected with a virus that prohibited our access to our files. We immediately restored our information system and launched an investigation, with the assistance of a forensic expert, to determine the capabilities of the virus and how it was introduced to our system. As part of our extensive investigation, on November 18, 2016, we determined that this virus was introduced by an unknown third party that had access to a server on our information system, and that information relating to you was stored on this server. While there is a potential that this third party gained access to your personal information, we are currently unaware of any attempted or actual access or misuse of your information.

What Information Was Involved? While our investigation is ongoing, we have no evidence the unknown third party accessed or acquired protected information stored on the server. Nevertheless, we have confirmed this server housed files and a software application containing information relating to you, which may include your name, address, phone number, Social Security number, treatment and diagnosis information, driver's license information, health insurance information, treating physician information, medical record number, and treatment date. Out of an abundance of caution, we are providing notice of this incident to you given we cannot rule out that unauthorized access to this information occurred.

What Is the Practice Doing? We take this matter, and the security and privacy of information on our information system, very seriously. Since the incident occurred, we have further enhanced the security of the information system and implemented additional monitoring tools to detect suspicious activity. We are also providing you with notice of this incident, as well as complimentary access to identity monitoring and identity restoration services and information on what you can do to better protect against the possibility of identity theft and fraud.

What Can You Do? While we have no evidence your information was subject to unauthorized access, or that your information has been or will be misused, you can take steps to better protect against the possibility of identity theft and fraud by enrolling to receive the complimentary identity monitoring and identity restoration services we are offering to you. You can also review the additional information on protecting against misuse of your information. This additional information, as well as instructions on how to enroll and receive the complimentary monitoring and restoration services, are included in the attached Privacy Safeguards.

For More Information. We understand you may have questions relating to this event and this letter. We have established a privacy line staffed with individuals familiar with this incident and how to better protect against the possibility of identity theft and fraud. You can direct all questions and concerns to this line by calling 866-961-1460, between 9:00 a.m. and 7:00 p.m. EST, Monday through Friday, excluding major holidays. This line can also be reached between 8 a.m. EST and 5 p.m. EST on Saturday, December 10, 2016.

We apologize for any inconvenience this incident may cause you, and remain committed to the privacy and security of our information.

Sincerely,

Melissa D. Selke M.D.

Draft

PRIVACY SAFEGUARDS

Although we are unaware of any actual or attempted misuse of your information, we have arranged monitoring of activity **within the United States** for 12 months at no cost to you. You can enroll in a professional identity monitoring service (First Watch ID) provided by First Watch Technologies, Inc. You can sign up for this service anytime between now and **March 3, 2017** using the verification code listed below. To enroll in this service, simply call **866-961-1460** Monday through Friday between the hours of 9:00 a.m. and 7:00 p.m. EST or go to www.firstwatchid.com and:

- Click on the Verification Code button.
- Enter the appropriate information, including your unique 12-digit verification code: .

After enrollment, you will receive 12 months of proactive identity monitoring. First Watch ID will monitor thousands of databases and billions of records on your behalf to look for suspicious activity that could indicate the beginning steps of identity theft. If suspicious activity is found, First Watch will place a personal phone call to you (at the telephone number that you provide) to determine if the suspicious activity is potentially fraudulent.

Additionally, if you enroll, First Watch provides you with easy online access to monitor your credit activity using the three major credit bureau services. Each credit bureau will provide you one free credit report annually. First Watch suggests you request your free credit report from one bureau at a time every four months. This allows you to monitor credit activity three times per year. First Watch will send you an email (at the email address you provide) every four months reminding you to request your free credit report from the appropriate bureau.

The First Watch ID service also includes up to $1,000,000.00 of identity theft insurance with $0 deductible, along with identity restoration coverage (certain limitations and exclusions may apply).

We encourage everyone to remain vigilant against incidents of identity theft and financial loss by:

- **Reviewing account statements, medical bills, and health insurance statements** regularly for suspicious activity, to ensure that no one has submitted fraudulent medical claims using your name and address. Report all suspicious or fraudulent charges to your account and insurance providers. If you do not receive regular Explanation of Benefits statements, you can contact your health plan and request them to send such statements following the provision of services.

- **Ordering and monitoring your credit reports** for suspicious activity. Under U.S. law, everyone is entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit http://www.annualcreditreport.com/ or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

- **Placing a "fraud alert" on your credit file.** A "fraud alert" will tell creditors to take additional steps to verify your identity prior to granting credit in your name; however, because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the credit bureaus verify your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your files. You may use the contact information listed above to contact the major credit bureaus and place a "fraud alert" on your credit report.

- **Placing a "security freeze" on your credit file,** that prohibits a credit reporting agency from releasing any information from your credit report without your written authorization but may delay, interfere with, or prevent the timely approval of any requests for new credit. If you have been a victim of identity theft, and provide the credit reporting agency with a valid police report, the credit reporting agency cannot charge to place, lift or remove a security freeze. In all other cases, a credit agency may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You must contact each of the credit reporting agencies separately to place a security freeze on your credit file:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-685-1111 (NY residents please call 1-800-349-9960) https://www.freeze.equifax.com	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 https://www.experian.com/freeze/center.html	TransUnion Fraud Victim Assistance P.O. Box 2000 Chester, PA 19022 Fraud Division 888-909-8872 http://www.transunion.com/credit-freeze/place-credit-freeze

- **Educating yourself further** on identity theft, fraud alerts, and the steps one can take to protect 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.ftc.gov/idtheft/; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. **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. Instances of known or suspected identity theft should also be reported to law enforcement.

- **Reporting suspicious activity or incidents of identity theft and fraud** to local law enforcement.