Ronald Snyder, M.D., Provides Notice of Data Security Incident

On April 18, 2019, Ronald Snyder, M.D., ("Dr. Snyder"), announced a recent event that may have impacted the privacy of personal information relating to certain individuals. While Dr. Snyder is unaware of any attempted or actual misuse of personal information in relation to the event, his office is providing potentially affected individuals with notice of the event, information about the event, his office's response to it, and steps individuals may take to better protect against the possibility of identity theft and fraud, should they feel it is necessary to do so.

What Happened? On January 9, 2019, Dr. Snyder's staff became aware that electronic information stored on his office's computer server had been encrypted as the result of a "ransomware" cyber-attack by an unknown actor. Because the server that was encrypted stored patient billing information, Dr. Snyder's immediate goals were to (1) ensure his office could still access patient information that had been encrypted so that his office could continue to care for patients without disruption; and (2) investigate what happened and confirm as quickly as possible if this incident resulted in any unauthorized access to, or theft of, patient information by the unknown actor. Because the office regularly creates backup copies of patient information, Dr. Snyder was able to quickly gain access to almost all patient information that had been encrypted and easily restored information that was not accessible. He also immediately began working with outside cybersecurity and computer forensics experts to determine whether any patient information was subject to unauthorized access.

Since Dr. Snyder learned about this issue on January 9, 2019, he has taken every necessary step to investigate this incident and the impact it may have on patient information, which included working with multiple industry-leading experts to recover the important information that was encrypted on the computer server. Unfortunately, after many efforts and attempts, Dr. Snyder learned on April 2, 2019 that he would be unable to determine whether this incident resulted in unauthorized access to patient information, due to the damage done to the computer server and the information stored on it.

Although Dr. Snyder has no indication that any patient information was specifically targeted, viewed, or stolen by an unauthorized actor in relation to this incident, he is notifying potentially affected individuals about this incident in an abundance of caution due to the uncertain nature of the incident.

What Information Was Involved? Dr. Snyder determined the server that was encrypted stored medical billing information, which may include: name, address, date of birth, gender, co-pay amount, patient status, employment status, telephone number, email address, and certain patients' insurance identification number, which may be a Social Security number. There is no indication that any such information was specifically targeted, viewed, or stolen by an unauthorized actor in relation to this incident. However, a complete investigation to make that determination was not possible.

What Dr. Snyder is Doing. Dr. Snyder takes this incident and the security of patient information in his practice's care very seriously. As part of his practice's ongoing commitment to the privacy and security of patient information, he is working to review existing policies and

procedures and to implement additional safeguards to further secure the information in his systems. He is also notifying the Department of Health and Human Services, other government regulators, as required, and prominent news media outlets in the state of New Jersey. Dr. Snyder also notified law enforcement of this incident.

In addition, while he is not aware or any actual or attempted misuse of personal information in relation to this incident, he is offering potentially affected individuals access to 1 year of complimentary identity restoration services through TransUnion.

What Potentially Affected Individuals Can Do. Potentially affected individuals can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Prevent Fraud and Identity Theft.* Potentially affected individuals can also enroll to receive the free identity restoration services being offered.

For More Information. If you are a potentially affected individual and have questions about this incident, please call our dedicated assistance line at 855-222-3630, Monday through Friday (except holidays), during the hours of 9:00 a.m. to 9:00 p.m., Eastern Time.

STEPS YOU CAN TAKE TO BETTER PROTECT YOUR INFORMATION

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, 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.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.