Notification of Data Security Incident

April 12, 2024 - On February 14, 2024, our third-party management company discovered they were victimized by a sophisticated ransomware attack. Upon discovery, they immediately secured the network and promptly began an internal investigation. They further engaged third-party forensic specialists to perform a thorough investigation to confirm the nature and scope of the incident. While the investigation remains ongoing, based on the findings to date, they believe that protected health information (PHI) belonging to our patients may have been subject to unauthorized access during the attack. Although we are unable to confirm the specific information that may be affected at this time, we are providing notification of this incident in an abundance of caution as we value the security of our patients' information.

While the investigation remains ongoing at this time, we believe that the data at risk may include patient names, in combination with one or more of the following: address, date of birth, Social Security number, driver's license number, a limited medical and dental history, medical and dental diagnosis and/or treatment information, medication information, and/or medical and dental insurance information.

At this time, we are not aware of any evidence to suggest that any information has been or will be fraudulently misused. However, we are unable to rule out the possibility that the information may have been accessed during the attack. Therefore, in an abundance of caution, we are notifying potentially impacted individuals of this incident. If your information was impacted by this event, you will receive a written notification directly.

In response to this incident, our third-party management company has partnered with third-party forensic specialists to fully investigate the nature and scope of this matter, and to evaluate and reinforce existing security measures and facilities within the network to ensure optimal data security. Although there is no evidence of actual or attempted fraudulent misuse of any information as a result of this incident, individuals are nonetheless encouraged to monitor their account statements and explanation of benefits forms for suspicious activity and to detect errors.

Should you have additional questions or concerns regarding this matter, please do not hesitate to contact us at (405) 946-2455. You may also write to us at 3613 NW 56th St Ste 105 105, Oklahoma City, OK 73112.

We take the privacy and security of the information in its care seriously, and sincerely regret any worry or inconvenience this incident may have caused.

What steps can I take to protect my private information?

- If you detect suspicious activity on any of your accounts or explanation of benefits forms, you should promptly notify the financial institution or company with which the account is maintained. You should also report any fraudulent activity or any suspected incidents of identity theft to law enforcement.

- You may obtain a copy of your credit report at no cost from each of the three nationwide credit reporting agencies. To do so, visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three agencies appears at the bottom of this page.

- You can take steps recommended by the Federal Trade Commission to protect yourself from identify theft. The FTC's website offers helpful information at www.ftc.gov/idtheft.

Was my information specifically impacted?

The investigation into the data at risk remains ongoing. Should the investigation reveal that your information was impacted, written notice will be provided directly to you. Importantly, there is no evidence to suggest that any information was subject to actual or attempted misuse as a result of this incident.

How do I obtain a copy of my credit report?

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every twelve (12) months. To do so, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three agencies is included in the notification letter and is also listed at the bottom of this page.

How do I put a fraud alert on my account?

A fraud alert informs creditors of possible fraudulent activity within your report and requests that creditors contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact Equifax, Experian or TransUnion and follow the Fraud Victims instructions. To place a fraud alert on your credit accounts, contact your financial institution or credit provider. Contact information for the three nationwide credit reporting agencies is listed below.

Contact information for the three nationwide credit reporting agencies is as follows:

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information
You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.