Notification of Data Security Incident

[**11-06-24**] – On or around July 1, 2024, Oklahoma Spine Hospital ("OSH") became aware of potential unauthorized access to one employee email account. Upon discovery, we took immediate action to secure the email tenant and investigate the event. This included resetting passwords for the impacted accounts and engaging a third-party team of forensic experts to investigate the incident and determine the full nature and scope of the event. Following a thorough investigation, on September 24, 2024, we confirmed that a limited amount of protected health information may have been accessed in connection with this incident.

Although the forensic investigation could not rule out the possibility that an unknown actor may have accessed this information, there is no indication whatsoever that any information has been misused at this time. The type of information contained within the affected data included first and last name, in combination with one or more of the following: Date of birth, Financial account number and routing number, Health insurance information, Medical information, Payment card information, and Driver's license information. Importantly, the information potentially impacted may vary for each individual, and may include all, or just one, of the above-listed types of information.

OSH is notifying potentially affected individuals for whom we have addresses for as quickly as possible via U.S. mail to their most recent address on file. Furthermore, in an abundance of caution, OSH provided potentially impacted individuals with complimentary credit monitoring services. Additionally, in response to this incident, OSH has implemented additional security measures within its network and facilities and is reviewing its current policies and procedures related to data security. Although OSH has no evidence of actual misuse of 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. Potentially impacted individuals may also wish to contact the three major credit agencies to place a fraud alert on their credit report – the credit agencies' contact information is: Equifax (888-378-4329); TransUnion (833-395-6938); and Experian (888-397-3472).

OSH has established a toll-free call center to answer questions about the incident and to address related concerns. The call center is available Monday through Friday from 9 AM - 9 PM Eastern Time and can be reached at 1-866-595-5664. You may also contact us by writing to 14101 Parkway Commons Drive, Oklahoma City, OK 73134.

The privacy and protection of information is a top priority for OSH, and we deeply regret any inconvenience or concern this incident may cause.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit 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 credit freeze 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 credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

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.