**MCALLEN SURGICAL SPECIALTY CENTER, LTD. PROVIDES NOTICE OF DATA PRIVACY EVENT**
**October 22, 2021**

McAllen Surgical Specialty Center, Ltd. ("McAllen Surgical") is providing notice of an incident that could affect the privacy of information of certain employees and patients for whom it provided medical care. While McAllen Surgical is unaware of any actual or attempted misuse of this information, McAllen Surgical takes this incident very seriously and are providing information about the incident, their response to it, and resources available to individuals to help protect their information, should they feel it appropriate to do so.

**What Happened?** On May 14, 2021, we discovered encrypted files on one of our servers. We immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. Our investigation determined that an unauthorized actor gained access to certain computers and servers between May 12, 2021 and May 14, 2021. We then worked diligently to identify which computers were impacted, what information was stored on those computers, and to whom the information on those computers relates. On July 22, 2021, as part of our investigation, we determined we were unable to rule out whether any computers or servers housing patient information were accessed. Therefore, although McAllen Surgical has no indication that any patient information was actually viewed or taken, they are providing notice in an abundance of caution because sensitive information was present on the network at the time of the unauthorized access.

**What Information Was Involved?** McAllen Surgical conducted a thorough review of the relevant systems to identify the types of information stored there and to whom it related. McAllen Surgical's review determined that sensitive information was present in the affected systems and it is possible that this information could have been accessed or acquired by an unauthorized actor. While the specific data elements vary for each potentially affected individual, the scope of information potentially involved includes: name; address; Social Security number; health insurance information; date of service; provider name; medical record number; and patient number.

**How Will Individuals Know If They Are Affected By This Incident?** McAllen Surgical is mailing notice letters to the individuals identified as impacted. If an individual did not receive a letter but would like to know if they are affected, they may call McAllen Surgical's dedicated assistance line, detailed below.

**What McAllen Surgical is Doing**. McAllen Surgical takes the confidentiality, privacy, and security of information in its care seriously. Upon discovery, McAllen Surgical immediately commenced an investigation to confirm the nature and scope of the incident. In response to this incident, McAllen Surgical is reviewing and enhancing existing policies and procedures.

**Whom Should Individuals Contact For More Information?** If individuals have questions or would like additional information, they may call McAllen Surgical's dedicated assistance line, 866-581-1076 between the hours of 8:00 a.m. and 10:00 p.m., Central Time, Monday through Friday.

**What You Can Do?** McAllen Surgical encourages individuals to remain vigilant against incidents of identity theft and fraud, to review account statements and explanation of benefits forms, and to monitor free credit reports for suspicious activity and to detect errors. Under U.S. law individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit 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, place a fraud alert, or a security freeze. Contact information for the credit bureaus is below:

Consumers have the right to place an initial or extended "fraud alert" on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer's 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 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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.); 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:

| **Equifax** | **Experian** | **TransUnion** |
|---|---|---|
| https://www.equifax.com/personal/credit-report-services/ | https://www.experian.com/help/ | https://www.transunion.com/credit-help |
| 888-298-0045 | 1-888-397-3742 | 833-395-6938 |
| Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069 | Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013 | TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016 |
| Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788 | Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013 | TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094 |

**Additional Information**

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 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. 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.

*For North Carolina residents*, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

*For New Mexico residents*, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

*For New York residents,* the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.Individuals can further educate themselves regarding identity theft, fraud alerts, security freezes, and steps to protect their information by contacting the Federal Trade

Commission. Instances of known or suspected identity theft should be reported to law enforcement and the state attorney general.