Leon Medical Centers, LLC Provides Update on 2020 Data Security Incident

Doral, Florida, May 14, 2021 – On January 8, 2021, Leon Medical Centers, LLC ("Leon Medical") announced a data security event that involved information relating to our patients and employees. Upon learning of the incident, Leon Medical conducted a thorough and time-consuming review of all potentially impacted information to identify affected or potentially affected individuals and the types of information involved. With the conclusion of this effort, Leon Medical provides the below update. Leon Medical takes the confidentiality, privacy and security of information in its care seriously. Please know that to date, Leon Medical has not received any reports of actual or attempted misuse of said information.

What Happened? On November 8, 2020, Leon Medical learned that it was the target of a cybercriminal attack and that portions of our computer network were infected with malware. We immediately took systems offline and, with the help of cybersecurity professionals, launched an investigation into the nature and scope of the incident. On November 9, 2020, we received confirmation that certain files stored within Leon Medical's environment that contain personal information had been accessed by the cybercriminals.

Later, on or about December 23, 2020, Leon Medical learned that the cybercriminals had exfiltrated information from its systems and began publishing the stolen files online. Since December 23, 2020, Leon Medical has been conducting a review of the contents of the illegally published records to identify affected or potentially affected individuals and the types of information involved. That process was recently completed.

What Information Was Involved? Leon Medical determined that the type of information potentially impacted may vary significantly by individual and that the following types of information may be impacted: name, address, date of birth, Social Security number, provider name, medical record number, treatment and diagnosis information, and/or health insurance information, including Medicare number, policy number, and group member ID.

What Leon Medical is Doing. Leon Medical takes the privacy and security of sensitive information within its care very seriously. In response to this incident, Leon Medical took immediate steps to identify and address the issues that allowed unauthorized access to its databases to occur. Leon Medical also conducted a thorough review to identify all individuals whose information was impacted by this incident. Following that review, Leon Medical provided written notice to all individuals that Leon Medical determined may have been impacted by this incident.

At this time, Leon Medical has already notified the U.S. Department of Health and Human Services (HHS), state regulatory authorities, the Federal Bureau of Investigation, and prominent news media outlets throughout the State of Florida.

What Potentially Affected Individuals Can Do? Individuals who believe they may be impacted by this incident can call the dedicated confidential assistance line detailed below or find out more about how to protect against potential identity theft and fraud in the below section *Steps You Can Take to Prevent Fraud and Identity Theft*.

For More Information. If you believe you may have been impacted by this incident and have questions, please call Leon Medical's dedicated assistance line at 855-914-4725 between the hours of 9am – 9pm ET. Please visit our website at http://www.leonmedicalcenters.com, where we have posted relevant information and updates about this situation since January 2021.

STEPS YOU CAN TAKE TO BETTER PROTECT YOUR INFORMATION

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

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.