

We regret to inform our patients that, on September 11, 2018, Maffi Clinics encountered unusual activity on one of our servers. We immediately instituted our security breach protocols which involved shutting down all of our computers and servers. Within hours of discovering the activity, an independent IT consulting firm was onsite at Maffi Clinics and determined that an unidentified source had gained remote access to our server and installed ransomware. Ransomware is a type of malware that attempts to deny access to a user's data by encrypting and then ransoming the data for payment.

The consulting firm promptly identified the unauthorized access point and terminated it; isolated and removed the ransomware; and restored all of our data. The consulting firm also determined the unauthorized access began approximately 5 hours before the system was shut down, at which point the access ended. The consulting firm found no evidence any of our data was viewed or downloaded and, to date, we have not received any ransom request. However, out of an abundance of caution, we recently mailed written notices to all of our patients whose information was subjected to the ransomware and published information regarding this matter in the Arizona Republic.

The types of information that was subjected to the ransomware was limited to first and last name, address, phone number, and pre- and post-operative records. **No social security numbers or credit card information was subjected to the ransomware.** Maffi Clinics does not keep this type of information on file.

Maffi Clinics take very seriously its role of safeguarding its patients' personal information and using it in an appropriate manner. Maffi Clinics regrets the stress and worry this situation may cause its patients. It has taken action to ensure this does not occur again, including implementing and continually evaluating, additional safeguards to limit the possibility of this occurring in the future.

If you detect any suspicious activity on any of your accounts, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. In addition, you can take steps recommended by the Federal Trade Commission to protect yourself from identity theft. The FTC's website offers helpful information at www.ftc.gov/idtheft.

You also can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Alternatively, contact information for the three nationwide credit reporting agencies is listed below.

Equifax
1-800-685-1111
www.equifax.com

Experian
1-888-397-3742
www.experian.com

TransUnion(FVAD)
1-800-888-4213
www.transunion.com

If you have any questions regarding anything discussed in this letter, please contact our Privacy Officer, Samantha. You can reach her during normal business hours at the following toll-free number: 866.883.9391.

Please accept our most sincere apology.