NOTICE OF DATA SECURITY INCIDENT

Conceptions Reproductive Associates, Inc., of Colorado, (the "Practice") is notifying current and former patients and their partners about an incident that may have involved some their information. The Practice takes the privacy and security of all patient information very seriously and deeply regrets any concern or inconvenience that may result from this notification.

Recently, the Practice unfortunately joined the long and growing list of health care providers victimized by ransomware attacks. In such an attack, cybercriminals gain unauthorized access to computer systems for the purpose of using data to try to extort system owners to pay ransoms. According to data recently published by the U.S. Cyber Threat Intelligence Integration Center and by Sophos, such attacks on the healthcare sector nearly doubled year over year and nearly two thirds of healthcare organizations recently surveyed had experienced such an attack within the prior twelve months.

In mid-April, the Practice became aware that some legacy computer systems were affected by an unauthorized intrusion earlier that month, in which attackers extracted certain patient information. The Practice immediately initiated its incident response and recovery procedures and worked quickly to investigate the situation and to further secure its systems. It promptly notified law enforcement and undertook a thorough process to determine the scope of the attack. As a result of that diligent work, which recently concluded, the Practice is now able to notify current and former patients whose information may have been within scope. The Practice has mailed notification letters directly to all such individuals for whom it has current contact information and is posting this notice to inform any other current or former patients about the incident. The Practice also has taken steps to further strengthen the security of its systems including reconfiguring network infrastructure, enhancing password length and complexity requirements, and strengthening remote access security including multi-factor authentication.

While the specific data elements within scope varied by person, the data generally may have included one or more identifiers about a patient (e.g., name, date of birth, home address, phone number, etc.) along with certain clinical data (e.g., tests ordered, test results, vital signs, physical examination findings, diagnostic imaging, etc.). For a very small percentage of individuals, it may also have included Social Security Number, driver's license number (or other government-issued identification number), checking account number, and/or credit or debit card number (which, in many cases, was no longer current as of the time of the incident).

The Practice's ongoing monitoring efforts have found no indication that any of the data has been used or further disclosed for purposes of identity theft, fraud, or any purpose other than to try to extort a ransom from the Practice itself. Nonetheless, out of an abundance of caution, the Practice is offering credit monitoring and identity theft protection services to current and former patients/partners at no charge, as a courtesy. The Practice is also reminding patients that it is always a good idea to regularly review account statements and free credit reports, to detect and report any errors or suspicious activity. Individuals can obtain a free copy of their credit report online at www.annualcreditreport.com, by calling toll-free (877) 322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. The Practice has set up a toll-free number to answer patients' questions about the incident and to enroll in the complimentary monitoring services if desired. Current or former patients of the Practice, or their partners, may call 855-285-8960, from Monday to Friday 9:00 AM to 9:00 PM Eastern, excluding major U.S. Holidays, for more information.

December 4, 11, 18, 2024
NO. 585712