DATA INCIDENT NOTIFICATION

What Happened

Medical Oncology Hematology Consultants, P.A. ("the Practice") was victimized by a cyber attack (the "Incident") that impacted a Practice email account. On March 14, 2019, the Practice, through its extensive investigation of the Incident, determined that personal health information ("PHI") and/or personally identifiable information ("PII") relating to you may have been subject to unauthorized access or acquisition as a result of the Incident.

We commenced the foregoing investigation immediately upon learning of the Incident for the purpose of determining its scope, the impact on our information systems, and the identities of those potentially affected. We engaged third party experts to assist us with our investigation and, during that investigation, coordinated extensively with the third party that hosts our email environment. Through our investigation, we determined that the attack occurred on or about June 7 and June 8, 2018. We have not found any evidence that your information was misused as a result of the Incident.

What Information Was Involved

The personal information subject to this incident may have included your name, health information, medical information, dates of birth, Social Security Number, government issued identification number, and/or financial account information.

What We Are Doing

The Practice is providing notice to potentially affected individuals so that they can take steps to minimize the risk that their information will be misused. As an added precaution, the Practice has arranged for TransUnion to provide potentially affected individuals 12 months of free credit monitoring and related services. To find out whether you were among those whose information was potentially affected, please contact (855) 424-2585, Monday through Friday, from 9 am to 9 pm Eastern Time (except holidays).

The Practice treats all sensitive information in a confidential manner and is proactive in the careful handling of such information. Since learning of the attack, the Practice has taken a number of steps to further secure its systems. Specifically, it has, among other things: established a new portal for delivery of secure emails from external sources; implemented malware blocking measures; facilitated suspicious email reporting; established notifications to alert users that they may be attempting to send un-encrypted sensitive data; facilitated encryption of outgoing emails; and provided additional data security training. Further, the Practice will soon implement multi-factor authentication and take additional steps to bolster its email phishing defenses.

What You Can Do

In addition to enrolling in the free credit monitoring and related services mentioned above, we recommend that you remain vigilant and take the following steps to protect your personal information:

1. Contact the nationwide credit-reporting agencies as soon as possible to:

    - Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
    - You can also receive information from these agencies about avoiding identity theft, such as by placing a "security freeze" on your credit accounts.
    - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
    - Receive and carefully review a free copy of your credit report by going to www.annualcreditreport.com.

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(800) 525-6285	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com/consumer	www.transunion.com

2. Carefully review all bills and credit card statements you receive to see if there are items you did not contract for or purchase. Also review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

3. The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft, such as by setting up fraud alerts or placing a "security freeze" on your credit accounts. The FTC can be contacted either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you should contact local law enforcement, and you can also contact the Fraud Department of the FTC, which will collect all information and make it available to law enforcement agencies. The FTC can be contacted at the website or phone number above, or at the mailing address below:

   Federal Trade Commission
   Consumer Response Center
   600 Pennsylvania Avenue
   NW Washington, DC 20580

4. *Maryland Residents:* To obtain additional information about avoiding identity theft, please contact the Maryland Attorney General's Office, using the contact information below:

   Maryland Attorney General's Office
   200 St. Paul Place
   Baltimore, MD 21202
   Phone: (410) 576-6300
   Toll-Free (in Maryland): (888) 743-0023
   Website: https://www.oag.state.md.us/contact.htm

For More Information

If you have questions or concerns, please contact (855) 424-2585, Monday through Friday, from 9 am to 9 pm Eastern Time (except holidays). We sincerely apologize for this situation and any inconvenience it may cause you.

4826-8485-9028, v. 1