NOTICE OF DATA BREACH

The Retina Group of Washington ("RGW" or "we") places a high value on maintaining the privacy and security of patient information. Regrettably, this notice is to inform you that we were recently the victim of a cybersecurity incident (the "Incident") that resulted in the unauthorized acquisition of some of our patients' information. This notice explains the Incident, the measures we have taken in response, and the proactive steps potentially impacted individuals can take.

What Happened? On March 26, 2023, we began experiencing difficulty accessing information in some of our systems. Immediately upon becoming aware that we were experiencing a potential security incident, we took steps to secure the affected systems. We determined that we were the victim of a cybersecurity incident, initiated a privileged and confidential investigation, and reported the incident to the Federal Bureau of Investigation. While our investigation of the Incident is ongoing, we have determined that the Incident resulted in the unauthorized acquisition of some of our patients' information, and we are in the process of identifying and notifying impacted patients.

What Information Was Involved? Although the information involved varied among the impacted patients, the information may have included patient name, Social Security number, driver's license number or other government-issued identification number, medical record number, address, telephone number, email address, date of birth, date of service, and/or other demographic information as well as health, payment, and/or insurance information. At this time, we do not have evidence of any misuse of any patient information.

What Are We Doing? Immediately upon becoming aware that we were experiencing a potential security incident, we took steps to secure the affected systems. We determined that we were the victim of a cybersecurity incident, initiated a privileged and confidential investigation, and reported the Incident to the Federal Bureau of Investigation. While our investigation of the Incident is ongoing, we have determined that the Incident resulted in the unauthorized acquisition of some of our patients' information, and we are in the process of identifying and notifying impacted patients. To help prevent similar incidents from happening in the future, we have implemented and are continuing to implement additional procedures and security measures to further strengthen the security of our systems.

What Can You Do? We regret that this Incident occurred and any concern it may cause. While we do not have evidence of any misuse of any patient information, we encourage patients to remain vigilant against incidents of identity theft and fraud, to review their account and explanation of benefits statements, and to monitor their free credit reports for suspicious activity and to detect errors. Please see the "Other Important Information" section below with additional information. Should our investigation determine your information was impacted, we will send you a notification letter by U.S. Mail that includes details on the information that was impacted and how to sign up for complimentary credit and identity protection services.

For More Information. If you have any further questions regarding this Incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at 1-844-539-0961. This response line is staffed with professionals familiar with this Incident and knowledgeable on what you can do to protect against misuse of your information. The response

line is available Monday through Friday (excluding holidays), 8:00 AM – 8:00 PM Eastern Time. Please note, unless our investigation has determined your information was impacted, and therefore you have received a notification letter by U.S. Mail, the call center may not have further details on your information specifically.

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

You may place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(800) 680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(888)-298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
(888) 397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
https://www.transunion.com/credit-freeze
(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

5. Protecting Your Medical Information.

We have no information to date indicating that your medical information involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.

- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.

- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.