LAKE WASHINGTON
VASCULAR

PRESS RELEASE

10 March 2025

Subject: Cybersecurity Breach

Shortly before 5:00 AM on February 14, 2025, our technology team was alerted that an outside intruder had accessed our network and was installing malware. Thanks to the quick response of our team, we were able to stop the attack and minimize the impact.

Since then, we have carefully inspected, reset, and restored every computer on our network. Although the malware encrypted the electronic medical record and practice management systems on our servers, we were able to use secure backups which are stored off-site to restore those systems with only minimal information loss.

Our electronic medical records and practice management systems contain personal and protected health information of approximately 30,000 patients, including names, dates of birth, addresses, payer identification numbers, government-issued identifications, diagnostic test results, medical histories, diagnoses and treatment information. However, we do not store credit card or banking information in our systems.

We cannot say for certain what personal or protected health information may have been extracted or viewed by the intruder. Because we take patient privacy seriously, we are informing our patients of this incident so that they can take extra precautions. In accordance with federal and state laws, we have also filed notices with the appropriate authorities and regulatory agencies.

We recommend that patients place a fraud alert on their credit files. They can do this by contacting any of the major credit reporting agencies:

- **Equifax:** (888) 766-0008 | www.fraudalert.equifax.com
- **Experian:** (888) 397-3742 | www.experian.com
- **TransUnion:** (800) 680-7289 | www.transunion.com

Patients with questions or need for further assistance may contact our call center at 888-408-2752 (Available M-F, 9:00 am – 9:00 pm Easter Time.)