Notice of Data Security Incident

Whitman Hospital & Medical Clinics ("WHMC") experienced a data security incident that involved patient and WHMC's Group Health Plan information. This notice explains the incident, measures that have been taken, and some steps patients can take in response.

On February 28, 2025, we were alerted to unusual activity in our Information Technology ("IT") environment. In response, we initiated an investigation, took steps to secure our systems, and notified law enforcement. Additionally, a third-party forensic firm was engaged to assist in the investigation.

Through the investigation, we determined that an unauthorized party accessed certain systems in our IT environment between December 26, 2024 and February 28, 2025. While in the IT environment, the unauthorized party may have accessed and/or acquired files that contain information pertaining to patients and members of WHMC's Group Health Plan, including their names and one or more of the following: dates of birth, addresses, Social Security numbers, financial account information, diagnosis, lab results, medications, other treatment information, health insurance information, provider names, and/or dates of treatment.

On April 11, 2025, we began mailing letters to individuals whose information may have been involved in the incident. We are offering eligible individuals complimentary credit monitoring and identity protection services. If an individual believes their information was involved and have any questions about this incident, please call 855-549-2646, Monday through Friday, between 6:00 a.m. – 6:00 p.m., Pacific Time, except for major U.S. holidays.

For individuals whose information may have been involved in the incident, we recommend that they review the statements they receive from their healthcare providers and health insurance plans. If they see any services that were not received, they should contact the provider or health plan immediately.

We are committed to protecting the confidentiality and security of the information we maintain. We regret any inconvenience or concern this incident may cause and take this matter seriously. To help prevent something like this from happening again, we have implemented, and will continue to adopt, additional safeguards and technical security measures to further protect and monitor our systems.