Notice of Email Phishing Incident

Park Royal Hospital ("Park Royal") is committed to protecting the security and privacy of the information we maintain. This notice provides information about an email phishing incident we experienced, measures that we took, and some steps patients can take in response.

Park Royal recently identified and addressed an email phishing incident that resulted in unauthorized access to one employee's email account and SharePoint account. Upon learning of this incident on January 17,2025, we immediately took steps to secure the email account and launched an investigation with the assistance of a third-party forensic investigation firm. The investigation confirmed that this incident was limited to the one employee's email account and SharePoint account, and did not involve Park Royal's electronic health records systems. Importantly, this incident did not disrupt Park Royal's services or operations.

Through our investigation, we determined that an employee mistakenly disclosed their email account credentials in response to a phishing email that they thought was legitimate. As a result, an unauthorized party used the credentials to access the employee's email account and SharePoint account between January 14, 2025 and January 15, 2025. While in the email account and SharePoint account, the unauthorized party accessed certain emails and files. Park Royal reviewed the emails and files that were accessed and determined that one or more contained information, including patient names and one or more of the following: dates of admission, provider information, and status as a patient at Park Royal.

On March 18, 2025, we began mailing notification letters via United States Postal Service First-Class mail to patients whose information was involved in the incident. We also established a dedicated, toll-free incident response line to answer questions that individuals may have. If an individual believes their information was involved and has any questions about this incident, they should call (888) 408-3029, Monday through Friday, between 9:00 a.m. – 9:00 p.m., Eastern Time, except for major U.S. holidays.

For patients whose information was 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 take this incident very seriously and sincerely regret any concern this may cause. To help prevent something like this from happening again, we have implemented additional safeguards and technical security measures to further protect and monitor our systems.