Substitute Notice – Possible Exposure of Patient Information
Fordland Clinic

Fordland Clinic ("Fordland") is committed to protecting patient confidentiality and privacy. Despite the security program implemented by Fordland, a security incident has occurred that potentially permitted unauthorized access to electronically stored patient information.

On May 28, 2019, Fordland discovered that an unauthorized individual had gained access to a Fordland employee's email account through a phishing attack. "Phishing" emails are sent by hackers in order to gain access to the victim's computer or network. While logged in to the employee's email account, it is possible that the unauthorized individual viewed emails containing electronic protected health information ("ePHI") contained in the employee's account. Fordland immediately investigated the incident, and required changes of all passwords. Fordland did not identify any removal of ePHI from the Fordland system, or any unapproved changes to the data. However, because unauthorized viewing of ePHI that was located in the employee's inbox was possible, Fordland is treating this as a breach of privacy and security, and is notifying all affected patients.

The ePHI that was viewed consisted primarily of the name of the patient and limited medical information, such as a diagnosis, medication, or treatment location. For 18 patients, social security numbers were visible. Those patients whose social security numbers were visible have received special notification and identity theft protection. In total, 881 individuals were affected.

Fordland is taking steps to mitigate this incident by notifying affected individuals via letter and posting this substitute notice. Identity monitoring and protection services are being offered free of charge to individuals whose social security numbers were potentially affected. Additionally, we are re-training personnel and re-emphasizing the importance of secure passwords, and risks of unknown links and documents that are received in email. We are evaluating other technical and operational approaches to strengthen defenses against phishing and other social engineering attacks, including additional use of encryption.

Please be assured, we are committed to fully protecting all of the information that has been entrusted to us and appreciate the opportunity to be of service to you.

Should you have any questions regarding this matter, please contact the following toll-free number: 1-800-478-1607 at prompt press 9, Monday through Friday, 8:30 a.m. to 4:30 p.m. Central Time, with questions.