Substitute Notice

Notice to our Patients About an Email Phishing Incident

District Medical Group ("DMG") is committed to protecting the confidentiality of our patients' information. Regrettably, this notice is to inform our patients of an incident that may have involved some of that information.

On March 11, 2020, we learned that an unauthorized person may have gained access to some DMG employee email accounts through an email phishing incident. We immediately secured the accounts, began an investigation, and a leading cyber security firm was engaged to assist in our investigation. The investigation confirmed the unauthorized person may have accessed a limited number of DMG employee email accounts between February 4, 2020, and February 10, 2020.

Our investigation determined that some patient information was contained in the email accounts, including patient names, medical record numbers, health insurance information, medical information, and in some instances, Social Security numbers.

Importantly, we have no reason to believe that any patient information was misused as a result of this incident. We recommend that affected patients review the statements they receive from their health insurers. If patients see services they did not receive, they should contact the insurer immediately. For those patients whose Social Security numbers were included in the email accounts, we are offering a complimentary membership of credit monitoring and identity protection services.

We began mailing letters to affected patients on May 8, 2020, and established a dedicated call center for patients to call with questions. If you believe you are affected by this incident, and do not receive a letter by July 8, 2020, please call 1-855-917-3471, Monday through Friday, 6:00 a.m. to 6:00 p.m., Arizona Time, excluding major U.S. holidays.

We take the privacy and confidentiality of our patients' information very seriously, and deeply regret any inconvenience or concern this incident may cause our patients. To help prevent something like this from happening again, we are implementing additional email security, reinforcing education with our employees on how to identify and avoid phishing emails, and enhancing our security infrastructure and systems.