

Notice to Denton Heart Group Patients of Theft of Hard Drive

Denton Heart Group (the “Clinic”), a member of HealthTexas Provider Network (HTPN) is committed to protecting the security and confidentiality of our patients’ information. Regrettably, this notice concerns an incident involving some of that information.

On January 11, 2017, we learned that an external computer hard drive was stolen from the Clinic on or about December 29, 2016. The external computer hard drive was used by the Clinic to back-up or store patient information from the Clinic’s electronic health record system and was secured in a locked closet within the Clinic. We promptly reported the theft to law enforcement authorities and we are working with law enforcement in its investigation.

The health information contained on the external hard drive for Clinic patients and guarantors may have included certain demographic information (such as patients’ names, dates of birth, addresses and phone numbers), driver’s license numbers, Social Security numbers, medical record numbers, clinic account numbers, insurance providers’ names, insurance group and/or policy numbers, physicians’ names and clinical information (including diagnosis/conditions, lab test results and medications) related to medical care received at the Clinic between 2009 and 2016.

To date, the Clinic has no indication that any of the information has been further disclosed or used by any other unauthorized individuals or entities. However, as a precaution, we began mailing letters to affected patients and guarantors on March 10, 2017, and have established a dedicated call center to answer any questions they may have. We also are offering eligible patients one year of credit monitoring and identity theft protection services through Experian. If you believe you may be affected and have not received a letter by March 20, 2017, please call 1-855-667-7934. Monday through Friday between 8:00 a.m. and 8:00 p.m. Central Time.

We regret any inconvenience caused by this incident. Necessary corrective actions have been taken to safeguard against similar incidents in the future, and we are taking steps to re-evaluate the security of computer devices within our clinics to further protect our patient’s information.