Notice to Our Patients of Privacy Incident

Family Health Care, Inc. ("FHC") is committed to protecting the security and privacy of our patients' information. Regrettably, this notice explains an incident that may have involved some of that information.

We recently identified unusual activity within our computer network. We immediately initiated our incident response protocols, which included isolating potentially impacted devices and shutting off select systems. We also began an investigation with the assistance of a computer forensic firm. The investigation determined that an unauthorized person gained access to our network prior to March 8, 2022, and, during that time, accessed some of the documents on our system. On March 25, 2022, we learned that some of those documents contained patient information.

Our investigation could not rule out the possibility that information of our current and former patients was contained in the documents viewed or acquired by the unauthorized person. The information may have included patients' names, dates of birth, addresses, Social Security numbers, health insurance information, medical record numbers, and clinical information, such as diagnoses, provider names, and/or dates of service. This incident did not involve our electronic medical record and patient care was not affected.

We have no indication that any information has been misused as a result of this incident. However, as a precaution, we are mailing letters to our current and former patients. The letters include guidance on how patients can protect their information going forward, as well as details on an offer of complimentary credit monitoring and identity protection services through IDX.

We have also established a dedicated, toll-free call center to answer patients' questions. If you have questions regarding this incident, please call 833-909-4276, Monday through Friday, between 8:00 a.m. and 8:00 p.m. Central Time. You can also visit https://response.idx.us/fhc for more information on the IDX identity protection services and to enroll online.

We take this issue very seriously and are committed to taking steps to help prevent something like this from happening again, including implementing enhanced network monitoring tools and continuing to regularly audit our systems for any unauthorized activity.