A Notice to our Clients

UCP Heartland is committed to protecting the confidentiality and security of our clients' information. Regrettably, this notice concerns a security incident that may have involved some of that information.

On February 24, 2020, we identified suspicious activity within one of our employee's email accounts. We immediately secured the account, launched an investigation to determine the nature and scope of the incident, and a leading computer forensic firm was engaged to assist. On March 6, 2020, the investigation determined that an unauthorized person accessed the employee's account between February 21, 2020 and February 24, 2020, and during that time may have downloaded emails and attachments in the account. The investigation was unable to determine which emails and/or attachments, if any, were viewed or acquired. In an abundance of caution, we reviewed the full contents of the account to identify client information that may have been accessible to the unauthorized person. Our review determined that emails or attachments in the account contained some clients' names, dates of birth, medical record or UCP Heartland identification numbers, and/or limited clinical information, such as diagnoses, prescriptions, and/or treatment information. In limited instances, clients' health insurance information, financial account information, Social Security numbers and/or drivers' license numbers were also included in the account.

This incident did not affect all UCP Heartland clients, but only those whose information was included in the affected email account.

We have no indication that any specific client's information was actually viewed or downloaded by the unauthorized person(s), or that it has been misused. However, we are mailing notification letters to clients whose information was identified in the account. We also established a dedicated, toll-free call center to answer clients' questions. If you have questions, please call 1-844-969-2517, Monday through Friday, from 8:00 a.m. and 5:30 p.m. Central Time. For those clients whose Social Security numbers and/or drivers' license numbers were found in the email account, we are offering complimentary credit monitoring and identity protection services. We also recommend that clients review any statements they receive from their health insurers or healthcare providers. If clients see charges for services not received, they should contact the insurer or provider immediately.

We regret any concern or inconvenience this incident may cause. We remain committed to protecting the confidentiality and security of our clients' information. To help prevent something like this from happening in the future, we have reinforced education with our staff regarding how to identify and avoid suspicious emails and are making additional security enhancements to our email environment.