Gold Coast Health Plan℠
A Public Entity

Integrity • Accountability • Collaboration • Trust • Respect

**October 5, 2018**

RE: Substitute Notice of Data Breach

Gold Coast Health Plan (GCHP) values its relationship with its members and takes its commitment to protecting your information very seriously. Therefore, this Substitute Notice of Data Breach is to notify GCHP's members of a recent data security incident that may have involved their protected health information.

**What happened?**
GCHP recently discovered that it suffered a phishing email attack that had compromised an employee email account and resulted in potential disclosure to an unauthorized third party of member health information. GCHP's investigation indicated that member information was contained as attachments in some of the compromised emails.

The phishing attack permitted the attacker to access the employee's email account between June 18, 2018 and August 1, 2018. GCHP discovered the incident on August 8, 2018, immediately stopped the attack, and engaged a leading cybersecurity firm to assess the potential disclosure of protected health information.

**What information was involved?**
The investigation determined that the compromised email account that was accessed affected GCHP members whose claims information was sent by email. The claims information included health plan identification numbers, dates of medical service, and in some cases, member names, dates of birth, and medical procedure codes.

**No social security numbers or financial information were accessed or disclosed.**

GCHP is not aware of any misuse or attempted misuse of the affected health information. According to computer forensics experts and law enforcement, these types of attacks are usually financially motivated. Based on our investigation, we believe the perpetrators of the attack were trying to fraudulently transfer GCHP funds to their account.

**What has GCHP done to prevent this from happening in the future?**
Upon discovering the incident, GCHP immediately stopped the attack and launched an investigation with a leading cybersecurity firm. GCHP also promptly notified law enforcement. Based on what we learned, we activated a series of enhanced security

measures to improve security and to prevent an incident like this from happening again. GCHP conducted education for its employees to help them recognize and avoid phishing emails, which are becoming more and more sophisticated.

**What can you do to protect your information?**
GCHP wants to help protect you from potential misuse of your information. Therefore, due to this incident, GCHP is offering identity theft protection services through ID Experts, a data breach and recovery services expert, to provide affected members with MyIDCare. MyIDCare will help you resolve issues if your identity is compromised.

For information on your medical privacy rights, we suggest that you visit the website of the California Office of the Attorney General at https://oag.ca.gov/privacy.

You can also order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. You can order your reports from the three credit reporting agencies free each year by calling 1-877-322-8228 or going to the Annual Credit Report website at www.annualcreditreport.com.

**More Information**
We regret this incident occurred and are sorry for the inconvenience this may have caused the affected members. If you want to find out if you were affected by this data breach, please do not hesitate to call the toll-free hotline GCHP established for this purpose at (888) 599-2126. Please call Monday through Friday 5 a.m. to 5 p.m. PST.