UC Health

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

UC Health understands the importance of protecting our patients' information. Regrettably, we are writing to inform you of an incident that involves some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

On July 6, 2019, we first learned that an unauthorized person gained access to a limited number of employee email accounts beginning on July 2, 2019 and continuing through July 15, 2019. We immediately secured the accounts, began an investigation, and a leading computer forensic firm was hired to assist. The investigation was unable to determine whether the unauthorized person actually viewed any emails or attachments in the accounts. In an abundance of caution, we reviewed the emails and attachments in the accounts to identify patients whose information may have been accessible to the unauthorized person. From this review, we determined that some of your information was contained in one or more of the email accounts. This information may have included your <<b2b_text_1 (Impacted Data)>><<b2b_text_2 (Impacted Data)>>. Your Social Security number was not contained in the email accounts.

We have no indication that your information was actually viewed by the unauthorized person, or that it has been misused. However, we wanted to advise you of the incident and assure you that we take it very seriously. We recommend that you review any statements that you receive from your healthcare providers and health insurer. If you see services you did not receive, please contact the provider or insurer immediately.

We deeply regret any inconvenience or concern this incident may cause you. To help prevent something like this from happening in the future, we reset all employee passwords, limited external email access, blocked access to malicious sites and IP addresses identified through the investigation of this incident, increased monitoring of network activity, continued to educate users on how to identify and avoid malicious emails, and added additional authentication measures for remote email access.

If you have any questions, please call 1-???-???-????, Monday through Friday, between 9:00 a.m. and 6:30 p.m. Eastern Time.

Sincerely,

Aimee Cordrey

Aimee Cordrey
Director & Chief Privacy Officer
UC Health
3200 Burnet Avenue
Cincinnati, OH 45229

ELN-????-????