<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Date>> (Format: Month Day, Year)
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Dear <<MemberFirstName>> <<MemberLastName>>,

We are contacting you as part of City of Hope's commitment to patient privacy. At City of Hope, our goal is to deliver the highest quality healthcare to our patients. Protecting our patients' confidentiality and privacy is a critical part of that goal and we take this responsibility very seriously. To that end, we want you to be aware of an incident involving our systems.

What Happened?

Despite all of the measures that we implement to protect our patients' information, we recently learned that City of Hope was the target of a phishing email. A phishing email is an attempt to acquire personal information such as account usernames and passwords by sending an email that looks like it is coming from a trustworthy source. This incident occurred on May 31st and June 2nd. Unfortunately, this incident resulted in unauthorized access to the email accounts of four staff members.

As part of our investigation into this matter, on **July 21st** we determined that three of the staff members' email accounts contained protected health information (PHI) which may have been accessed as a part of the incident. However, while we know that the email accounts were accessed, we were not able to identify the scope or nature of the access to individual emails within the accounts and, as a result, could not rule out the possibility that PHI had been viewed. Given that we could not rule out this possibility, we are sending this notification to you because your PHI was included in the affected email accounts.

What Information Was Involved?

The information in the email accounts may have included your name, medical record number, date of birth, address, email address, telephone number and clinical information such as diagnosis, diagnostic test results, medication information or dates of service. **The information in the email accounts did not contain your Social Security number, financial information or other identifying information.** We have no evidence that that the PHI contained in the email accounts was the target of the phishing incident; rather, we believe the accounts were accessed for the purposes of obtaining user credentials to send spam emails to other individuals.

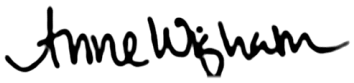
What Are We Doing to Protect You and How Can You Protect Yourself?

Upon identification of the phishing incident, City of Hope took prompt action to secure the email accounts and end the intrusion. Additionally, City of Hope retained a leading forensic information technology firm to assist with our investigation and to evaluate our systems and processes and further strengthen our protections in these areas. Please be assured that City of Hope is addressing this with the utmost seriousness. The matter has been reported to law enforcement and City of Hope is continuing to investigate other steps to mitigate any potential harm to affected individuals. To date, there is no evidence to suggest that any of the information has been withdrawn from the accounts or misused. Nevertheless, please remain cautious and regularly monitor your accounts.

We regret that this incident occurred and I sincerely apologize, on behalf of City of Hope, for any concern or inconvenience this may cause you. At City of Hope, we work very diligently to protect our patients' privacy. If you have any questions or

concerns regarding this incident, please do not hesitate to call the toll-free hotline we have established for this purpose at 855-205-6937. Please call Monday through Friday from 6:00 a.m. to 3:00 p.m. Pacific Time.

Sincerely,



Anne Wigham
Director, Compliance – Privacy & Security
Privacy Officer