Trinity Health

September 14, 2020

[redacted] P20T1067

RE: St. Mary's Hospital, a member of Trinity Health:

Notice of Cyber-Attack Impacting Database Information

Dear Patient,

At Trinity Health, safety is a top priority – including the safety of our patients' and donors' personal information. In that regard, we are notifying you about a data security incident involving Blackbaud, a vendor that supplies Trinity Health's donor database technology. The data security incident may have impacted certain personal information of donors and certain patients. Blackbaud has verified that the cybercriminal did not access your credit card information, bank account information or social security number.

What Happened? On July 16, 2020, Blackbaud notified Trinity Health and other customers of a cyber-attack involving Blackbaud's network, including ransomware, that impacted certain donor database backup files maintained by Blackbaud, including Trinity Health's donor database. Blackbaud reported the cyberattack occurred between April 18, 2020 - May 16, 2020. Blackbaud reported that based on its investigation, the cybercriminals responsible for the attack could have obtained access to various types of information in the client backup files. Upon receiving this notice, Trinity Health took immediate steps to begin its own investigation to determine what, if any, sensitive Trinity Health data was potentially impacted. Please note that this attack did not occur within the information systems of Trinity Health or any affiliated Ministry.

What information was involved? Our forensic investigation determined that some data fields were encrypted and would not be accessible to the cybercriminals. Other fields were not encrypted and could have been accessible to the cybercriminals including information such as: donor relation to patient, patient discharge status, patient insurance and patient department of service. This database information spans from 2000 to 2020.

Your personally identifiable information and protected health information data elements that could have been exposed in the cyberattack are: full name, address, phone numbers, email, most recent donation date, date of birth, age, inpatient/outpatient status, dates of service, hospital location, patient room number, and physician name.

How did Blackbaud secure the data? Blackbaud reported that they quickly locked out the cybercriminals and resolved the issue. Additional details about the security incident is available by visiting Blackbaud's website at https://www.blackbaud.com/securityincident, which includes information about Blackbaud's steps to ensure this issue does not happen again.

We continue to work with Blackbaud on the measures they are taking to further secure the information in their care. We deeply regret that this incident occurred and apologize for any concern or inconvenience you may experience from this notification. Thank you for trusting Trinity Health with your care and your support of our Mission. If you would like additional information and local contact information, please visit our website at https://www.trinity-health.org/blackbaud-incident.

Sincerely,

Monica C. Lareau
Director, HIPAA Compliance, Privacy Official
Trinity Health