Website Notice

NOTICE OF DATA PRIVACY EVENT

On Thursday, July 16, 2020, Enloe received notification from one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"), of a cyber incident. Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to organizations, including Enloe. Upon receiving notice of the cyber incident, we immediately commenced an investigation to better understand the nature and scope of the incident and any impact on Enloe's data. This notice provides information about the Blackbaud incident, our response, and resources available to patients to help protect their information from possible misuse, should they feel it necessary to do so.

What Happened? Blackbaud reported that, in May 2020, it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that the data was exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. Upon learning of the Blackbaud incident, Enloe immediately commenced an investigation to determine what, if any, sensitive Enloe data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident. The Blackbaud event affected thousands of organizations across many different states and countries. Although not the target of the ransomware incident, Enloe was one of the countless organizations that were impacted.

What Information Was Involved? Our investigation determined that the impacted Blackbaud systems contained patient names, addresses, medical treatment discharge dates and departments where the patients received care. The system may have also contained patient date of birth, phone number and/or email address. **No Enloe patient Social Security numbers, credit card numbers or bank account information were present in the Blackbaud system and were therefore not impacted by this event.**

What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities, and we take this incident very seriously. As part of our ongoing commitment to the security of information in our care, we are working to review our existing policies and procedures regarding our third-party vendors, and are working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. We will also be notifying the United States Department of Health and Human Services and state regulators, as required.

What Can You Do? We recommend patients remain vigilant for attempts to obtain sensitive information from you using social engineering. This is when someone requests the individual provide sensitive information such as bank account information or Social Security number by using information about the patient's recent medical visit in an attempt to show the request is legitimate. In addition, as a best practice, individuals should always carefully review Explanations of Benefits for suspicious or unauthorized activity and report any instances of fraud to law enforcement.

Individuals with additional questions can call the dedicated assistance line we established for this incident at (855) 380-6161, Monday through Friday from 6:00 am to 8:00 pm PT and Saturday and Sunday from 8:00 am to 5:00 pm PT.