



C/O IDX
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Data Breach

Dear <<Name 1>>,

I am writing on behalf of Crozer-Keystone Health System to inform you of a recent cybersecurity breach that impacted certain hospital data.

What happened?

On June 14, 2020, we identified a malware incident that affected some of our hospital computer systems. The malware was promptly isolated, and the systems were quickly repaired and brought back to full functionality.

The event was determined to be “near-zero day” malware (i.e., “nearly unknown”) launched by a known ransomware cyber group. External security professionals were engaged to assist in conducting a full investigation of this incident.

During the course of the investigation, it was determined that the cybergroup had obtained copies of certain hospital data, all of which have been returned. Based on the nature of this attack, the actors involved, and the hospital’s recovery of all accessed data, we do not believe that any of the impacted data was misused, further distributed or made public nor do we believe that any such data is at risk for any future misuse or public disclosure.

As a precautionary measure, we are notifying you because some of your health information was involved, as described below.

What data was affected?

Your name, admission and discharge dates, service code, insurance information and information relating to your hospital payments were included on a hospital payor aging report. The report did not include any information regarding your treatment, diagnoses, or any sensitive personal or financial information that could result in the theft of your identity. Rather, the purpose of the report was to track accounts receivable for a particular period of time.

What have we done?

We are performing a full investigation and analysis regarding this incident and any data that may have been compromised. We took further measures to ensure that any impacted data was returned. As a result of this incident and part of our ongoing efforts to prevent similar attacks, we have continued to enhance our security detection and response processes so that we can proactively detect security vulnerabilities and potential exposures and act on them promptly. We have also implemented additional safeguards to enhance access controls to our systems.

What can you do?

We have no reason to believe that your information has been misused; however, we recommend that you review statements you received from your healthcare providers. If you see listed services that you did not receive, contact the provider immediately.

For More Information

Please call 1-833-791-1654 Monday through Friday from 9 am - 9 pm Eastern Time or visit our website at: <https://response.idx.us/ckhs> if you have any further questions about this incident.

We apologize for any inconvenience or concern that this notification may cause. As a patient of our hospital, we want to ensure that we do all that we can to maintain your trust and confidence.

Sincerely,

A handwritten signature in cursive script that reads "Sandra Puka".

Sandra Puka
Compliance Officer,
Crozer-Keystone Health System