C/O ID Experts
P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
(833) 928-1941
Or Visit:
https://ide.myidcare.com/crozer
Enrollment Code:
<<XXXXXXXX>>

<<First Name>> <<Middle>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

September 1, 2020

Dear <<First Name>> <<Middle>> <<Last Name>>,

I am writing on behalf of <<Hospital-Site>> to inform you of a recent cybersecurity incident that impacted a small portion of 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 and personal information was involved, as described below.

What data was affected?

To meet reporting, billing and other obligations, our hospital must track certain information related to patients who receive COVID-19 tests while at our facility. Together with our affiliated hospitals, we aggregate our COVID testing data for government regulatory purposes. This information included your name, date of birth, medical record number (i.e., a unique hospital tracking number), admit and discharge dates, lab ordering information, ordering physician's name, and lab test results. The information did not include your treatment, underlying diagnoses, but it did include your social security number.

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 was used in an improper way. Nonetheless, we recommend that you take certain precautionary measures, which are good practices regardless of this incident.

We recommend that you place a fraud alert on your credit files. A fraud alert requires potential creditors to use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name. A fraud alert lasts for 90 days. You can place a 90-day fraud alert through any of the reporting agencies listed below.

Equifax	**Experian**	**TransUnion**
800.525.6285	888.397.3742	800.680.7289
P.O. Box 740241	P.O. Box 9532	Fraud Victim Assistance Division
Atlanta, GA 30374	Allen, TX 75013	P.O. Box 6790
www.equifax.com	www.experian.com	Fullerton, CA 92834
		www.transunion.com

We also recommend that you obtain a credit report from one of the three credit bureaus; Experian, Equifax or TransUnion. You can do so at: www.annualcreditreport.com. Following such reviews, you should promptly report any suspicious activity to the proper law enforcement authorities including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC") at www.ftc.gov.

You should carefully check all credit card and other financial account information that you receive. If you detect any unauthorized or suspicious activity in any of these accounts, you should contact your credit card company or other account issuer immediately.

In addition, we have arranged to offer free credit monitoring and other identity recovery services for one year. You can enroll in these services by going to https://ide.myidcare.com/crozer and using the Enrollment Code provided below. You also may call for assistance at any time Monday through Friday from 6 am to 6pm Pacific Time. Please note the deadline to enroll is **<<enrollment deadline>>**.

You will need to reference the following enrollment code below when calling or enrolling on the website, so please do not discard this letter.

Your Enrollment Code: <<XXXXXXXX>>

For More Information

Please call (833) 928-1941 or visit our website at: https://ide.myidcare.com/crozer 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,

Sandra Puka

Sandra Puka
Compliance Officer
Crozer-Keystone Health System