DATA BREACH INCIDENT

Notice of Data Breach Incident

Crenshaw Community Hospital ("CCH") recently became aware that an unauthorized third-party may have viewed and/or downloaded data containing patient information. This notice is intended to provide details about the incident, steps we are taking in response, and resources available to help protect against the potential misuse of personal information.

What Happened: On June 16, 2025, CCH experienced a network disruption that impacted the functionality and access of certain computer systems. Upon discovery of this incident, CCH promptly engaged a specialized third-party cybersecurity firm to assist with securing its environment, as well as, to conduct a comprehensive investigation to determine the nature and scope of the incident. While the investigation remains ongoing, CCH learned that certain files were copied from our system without authorization.

CCH is diligently working to determine what, if any, patient information data may be affected. CCH is still in the process of identifying the specific individuals and the types of information that may have been compromised.

What Information Was Involved: Affected individuals will be notified by mail of the specific information that was impacted.

What We Are Doing: Upon completion of its ongoing review, CCH will determine the specific individuals whose information was contained in the impacted data. CCH will notify affected individuals by mail as the information becomes available.

What You Can Do: Affected individuals should refer to the notice they will receive in the mail regarding steps they can take to protect themselves. In general, we recommend, as a precautionary measure, that individuals remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing their account statements and monitoring credit reports closely. If individuals detect any suspicious activity on an account, they should promptly notify the financial institution or company with which the account is maintained. They should also promptly report any fraudulent activity or suspected incidents of identity theft to proper law enforcement authorities, including the police and their state's attorney general.

You may also wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps that you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-Theft (1-877-438-4338). You may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, Washington DC 20580.

If you or a family member are a current or former CCH patient and have any questions or concerns about this incident, please contact 833-426-7376 between 9:00 a.m. and 6:00 p.m. Eastern Standard Time, Monday through Friday (excluding U.S. national holidays), for further information and assistance.