

https://www.duncanbanner.com/community/affected-patients-to-receive-information-about-drh-data-security-incident/article_4e5b6b88-9c19-11ec-b6af-8353d6989d4c.html

FEATURED

TOP STORY

BREAKING

TOPICAL

Affected patients to receive information about DRH data security incident

By Charlene Belew The Duncan Banner
Mar 4, 2022



DRH logo



Officials with DRH Health, the leading healthcare provider in Stephens County, confirmed Friday, March 4 a data incident dating back to January of this year may have impacted protected health information for some patients.

On Jan. 20, DRH reported an incident affected on of their servers, although an investigation launched immediately and DRH's team brought systems back to normal operation within 24 hours, Cyndi Crook, executive director of PR and marketing for DRH, said at the time.

On March 4, information released shows the detected security incident impacted some of DRH's systems, and the hospital "immediately implemented its incident response protocols, disconnected access to all systems, and hired external cybersecurity experts to conduct a forensic investigation." According to DRH, "all systems were securely restored within 24 hours and DRH remained operational to provide care to its patients."

However, the forensic investigation determined some information stored outside of the hospital's "primary electronic medical record system may have been impacted, including names, addresses, demographic information, dates of birth, and some combination of Social Security numbers, medical record numbers, and limited treatment information," states information obtained from DRH.

Crook said the hospital has posted a notice to its website, along with a FAQ about the incident, and in addition to this, they are mailing letters to individuals affected. The bailouts began on March 4.

"These letters contain information about the incident and enrollment codes for free credit monitoring and identity restoration services," she said. "Cybercriminals continue to target the healthcare sector. Fortunately, DRH has incident response protocols in place that allow us to detect and respond to the threat with minimal disruption to operations or patient care. In addition to the security measures already in place, we have layered extra controls to enhance our security posture."

Those extra security measures include conducting a global password reset, Crook said, along with tightening firewall restrictions and implementing "endpoint threat detection and response monitoring software on workstations and servers."

According to DRH, law enforcement was notified of the event.

To determine whether you were affected by this incident, call 1-888-401-0543 from 8 a.m. to 10 p.m. Monday through Friday or from 10 a.m. to 7 p.m. Saturday and Sunday. Those who call should be prepared to provide engagement number B028450.



[DRH Health reports server 'incident' as fixed, under investigation](#)