HEALTH

Hospital data breach may affect local residents

Staff report

People who registered on a patient portal/personal health record used by the state and Twin Lakes Regional Medical Center may have their protected health information jeopardized by a national data security breach.

TLRMC participated in the Kentucky Health Information Exchange, an electronic network that supports health information exchange among healthcare providers and organizations throughout Kentucky. The KHIE contracted with Xerox Corp. to use its NoMoreClipboard patient portal product.

NoMoreClipboard, a national company, was the target of a cyber attack which has compromised the security of some protected health information, the hospital announced Monday, July 27.

To be included in the breach, patients must have registered for the MyHealthNow patient portal through NoMoreClipboard during a visit to TLRMC between Dec. 1, 2014, and March 12, 2015, or March 23 to April 8, 2015. Patients must then have taken the additional step of going on the NoMoreClipboard website, registered, and uploaded their personal information.

Patients whose information may have been compromised will be contacted by NoMoreClipboard, not Twin Lakes Regional Medical Center.

The information will include what to do and contact information for questions. The public is asked not to contact TLRMC since the breach did not involve any information stored by the hospital or by any local doctor's office.

To better assist those who may potentially have been affected, a confidential, toll-free hotline has been established to answer questions. This hotline is available Monday through Friday, 8 a.m. to 8 p.m. CDT and can be reached at 866-328-1987.

A news release from NoMoreClipboard says it is emailing users with instructions on how to change their passwords.

The affected data may include patients' names, home addresses, email addresses, dates of birth and Social Security numbers. No financial or credit card information was compromised, as this information is not collected or stored. The investigation indicates the unauthorized access to the network occurred on May 7 through May 8, 2015. The attackers regained unauthorized accessed to the network again on May 25, 2015.

Not every patient who registered at TLRMC during the time periods listed is affected by the situation. At this time, it is not possible for the hospital to determine the number of people this affects. However, it is believed the number should be kept to a minimum since the system was only recently put into place.

As the investigations continue, NoMoreClipboard is offering credit monitoring and identity protection services to affected individuals, free of charge, for the next 24 months. Participants can call the toll-free call center to answer questions relating to this data security event and the support and services being provided.

More information can be found at www.nomoreclipboard.com.