Written by By Beth Blakeman Managing Editor
Friday, 05 March 2021 06:16

Says her credit agencies found her data on the dark web

The former Health Insurance Portability and Accountability Act privacy officer for Rehoboth McKinley Christian Healthcare Services has been told her name and other identifying information is on the dark web.

Dr. Phyllis Miller told the *Sun* Feb. 22, that two credit agencies she subscribes to, but does not wish to name, reported to her that in the months of December 2020 and January 2021, some of her information was found on the dark web.

She doesn't know what types of information were reportedly discovered. But she said she is concerned that some of it may be protected health information. In order for Miller to know more specifics, she said she would have to pay someone and do a deeper investigation.

The dark web or the dark nets are part of the internet that is not visible to search engines and is accessed using an anonymizing browser, specific software, or authorization.

Miller said this is the first time she has ever been told of any personal content of hers appearing on the dark nets.

Miller was a 2019 Volunteer of the Year award winner at RMCHCS. In November of that year she became the hospital's director of health information management, and by 2020 she was also the hospital's HIPAA privacy officer.

Miller was fired from the hospital on July 21, 2020, but not before she resigned her HIPAA privacy officer position after blowing the whistle about an alleged violation of an employee's HIPAA privacy rights at a board meeting May 23.

In the month before she left, she had some 50 posters printed, using the Snoopy character, with special permission, to inform hospital personnel, patients and visitors about HIPAA, privacy issues, and not talking about protected health information. The posters were displayed on the walls around RMCHCS before she left.

She continued to see RMCHCS health care providers after she was no longer an employee, and during a return to a clinic for an appointment, she discovered the posters were gone.

"I told them all of the [privacy] weaknesses and what they needed to do and it fell on deaf ears," Miller said of her time as the HIPAA privacy officer for the hospital.

On Feb. 18, Miller filed a letter with the Office of Health and Human Services and the Office for Civil Rights concerning the credit agency notices she received. In the letter she expressed her dissatisfaction with what she called reckless disregard of HIPAA Rules and Regulations and said "such breaches may cause me future harm."

Miller added that she has been unable to obtain copies of recent medical records from RMCHCS. She wasn't sure why.

On the same day she sent that letter, the hospital released a statement acknowledging that it had recently learned of unauthorized activity on its computer network and said it took immediate steps to prevent any further such activity. The release said RMCHCS was conducting an

investigation.

“Due to the ongoing nature of this investigation, we are unable to comment further at this time,” were the final words of the release.

No further media statements have been issued by the hospital as of Feb. 25.

Miller, who stated in her letter to HHS and OCR, that RMCHCS is obligated to notify her of any breach of her personal health information, said that as of Feb. 25, she has not heard anything from the hospital concerning a data breach.

Miller said she did not inform the hospital about this letter. She said that under HIPAA regulations, she is not obligated to do so.

Online, however, there are articles hinting at the possibility that there has been a data breach at RMCHCS.

Healthitsecurity.com mentions the hospital in a February 2021 article about ransomware actors who have allegedly leaked data from healthcare-related entities. One of those named by author Jessica Davis in connection with the Conti ransomware group, is Rehoboth McKinley Christian Health Care Services.

Davis stated that the dark web posting includes information from passports, drivers’ licenses and bills of sale.

The Conti malware is known for updating rapidly, being able to quickly encrypt a system, and for auto-spreading functionality according to the Cybereason’s Nocturnus Team report. Cybereason Nocturnus Team is a Boston, Mass. I-T company that solves hacks.

Davis was unavailable for comment as of press time.

By Beth Blakeman
Managing Editor