Community Health Systems Data Breach Involves 4.5 Million Patients

August 19, 2014 - Community Health Systems (CHS), a company based in Franklin, TN, has begun notifying patients that their personally identifiable information may have been breached by Chinese hackers. The breach took place from April to June of this year and involves data on an estimated 4.5 million patients. The company is saying that medical records were not compromised but that other personal information including names, addresses, phone numbers, dates of birth and social security numbers were.

CHS is the largest operator of hospitals in the United States. The company has 206 hospitals in 29 states.

The data breach affects patients treated at any of the company's facility or patients that were referred to or treated by doctors affiliated with one of the company's hospitals.

CHS has said that it will offer some type of identity theft protection service to affected patients. This may not offer enough protection from identity theft however. Anyone who receives notification from CHS, or who has reason to suspect that their information was exposed in this breach, should seriously consider placing a security freeze on their credit file. This is the only way that we are aware of that can stop financial identity theft.

Victims of this breach should closely monitor credit card and banks statements for fraudulent activity. Additionally, the information stolen in this hack could be enough for the hackers to commit medical identity theft. Even though CHS has stated that medical information was not revealed, the hackers already know that patients were treated at CHS facilities. They may be able to use that information to gain access to other items including insurance policy information. Therefore, victims of this breach also need to closely monitor their medical insurance statements and challenge any treatments that they don't recognize.

And since victim telephone numbers were also compromised in the breach, victims should be especially cautious about phone calls they receive in which they are asked for personal information, such as credit card or account numbers.

CHS doesn't appear to have posted any information relating to the breach on the company website, other than a filing with the SEC. The filing states that the company's computer system was hacked. The SEC filing has the mundane name of "Report of unscheduled material events or corporate event" and was mandated by law since the data breach could impact the company's stock price. The fact that the company hasn't set up a resource page or announcement for victims

is very disappointing but not surprising. The healthcare industry is largely regarded by privacy advocates as being well behind the times for protection of patient data.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Jim Malmberg on Twitter Counter

Follow ACCESS