patients' electronic health records inappropriately in a scheme to file fraudulent tax returns.

Oct. 28, 2013

Oct. 28 — Two former Sentara Healthcare employees pleaded guilty this month to accessing patients' electronic health records inappropriately in a scheme to file fraudulent tax returns, the health-care system has revealed. Both were nurses' aides, according to Greg Burkhart, chief compliance officer. Sentara is a not-for-profit heal care organization with more than 100 locations in Virginia and northeastern North Carolina.

This is the second reported security breach of electronic records involving Sentara in less than a year.

The breach exposing patients' personal information — including name, date of birth, Social Security number and address — stretched from September 2011 to April 2013, but largely took place between mid-September 2012 and mid-February 2013. During that time, officials said, the aides accessed the records of about 3,700 patients, most at Sentara Virginia Beach General.

"The proper focus is on the patient, not the facility," Burkhart said, noting that patients move among facilities. The tax fraud "impacted fewer than 200," and they have been contacted by the IRS, which is working with them to repair the information, he added. All potentially affected have received a letter from Sentara explaining the situation and have been offered a year of free credit monitoring through ProtectMyID Alert, which comes with $1 million in theft insurance.

Lawrence Combs, Jr., a Newport News resident, received a letter. Combs, who recently turned 18, went to the emergency room at Sentara CarePlex in Hampton on a

couple of occasions last year. “The hospital is supposed to be a safe place. There are

Sentara's medication dispensing systems. The information, which potentially affected 56,000 Sentara patients treated in 10 hospitals over a three-week period in 2012, did not include Social Security numbers. “There is no indication that data has been accessed. It appears to have been a crime of opportunity, not for patient information,” said Sentara spokesman, Dale Gauding.

In reaction to the local breach, Sentara has implemented a new policy to mask Social Security numbers in the record. That should be complete within the next 30 days. The company is also working to add a new layer of security, FairWarning, to detect inappropriate access more effectively. The process has been under way since before the breach. “It's much like the banking industry. We're always trying to improve it,” said Burkhart. The system is scheduled for full implementation by the end of the first quarter in 2014.

Several thousand of Sentara's 26,000 employees have access to electronic records, including clerical and billing personnel, those in registration, in labs, and nurses and physicians. “Everybody who accesses leaves a digital signature. There are ways to track use,” said Gauding, contrasting it with paper files, which allow people to look through without leaving a trail. “These were two people charged in a criminal enterprise, individuals who violated a personal pledge to protect patient information. How many thousands do this properly every day?”

Still, Burkhart described it as “a breach of trust — a significant black eye for us.”

With electronic records now the industry standard, health systems have to be constantly on the alert. In May, two certified nursing assistants at Bon Secours Mary Immaculate Hospital in Newport News were terminated for improper use of the hospital's electronic records over the course of a year, from April 2012 to April 2013. They potentially compromised the records of 5,000 patients. The incident is still under criminal investigation, according to spokeswoman Lynne Zultanky.

“We regularly provide our workforce education and training including the penalties

———————————

Benefits • Income Tax • Small Business • Taxes