PHYS.ORG

Theft of data on 4M patients part of wider problem

November 18 2011, By DON THOMPSON and MARCUS WOHLSEN , Associated Press

The theft of a computer containing information on more than 4 million patients of a major Northern California health care provider may be among the largest breaches of health care data in recent years, but it's far from the only incident of its kind.

Over the last two years, health care organizations have reported 364 incidents involving the loss or theft of information ranging from names and addresses to Social Security numbers and medical diagnoses on nearly 18 million patients - equivalent to the population of Florida.

A thief stole medical information on more than 4 million patients of Sacramento-based Sutter Health last month by the simple act of breaking a window with a rock at the affiliated Sutter Medical Foundation. Stolen over the weekend of Oct. 15 were monitors, keyboards and a desktop computer containing patient information dating to 1995.

Employees reported the theft to Sacramento police when they returned to work that Monday, Oct. 17, said Sgt. Andrew Pettit, but they didn't notify the public until Wednesday, a month later. The company said in announcing the theft Wednesday that some patients might not receive mailed notices until early next month.

"If that machine is that valuable, then there should be more security measures where that is protected. There's got to be something in place to make sure that that doesn't happen," Pettit said.

Police were investigating the burglary as a routine smash-and-grab property theft, he said, and so far there is no indication that the information in the computer has been used.

Since federal health care data breach notification rules took effect in 2009, Health and Human Services records show that the Sutter theft was exceeded only when the U.S. military's health insurance program lost backup tapes in September containing information on more than 4.9 million patients.

While Sutter said the computer was password-protected, the data on patients was not encrypted, drawing criticism from privacy and computer security experts.

"Had this data been encrypted, you and I wouldn't be having this discussion. It would be a nonissue," said Beth Givens, director of the Privacy Rights Clearinghouse, a nonprofit consumer education and advocacy organization based in Sacramento.

On a computer in which data is encrypted, a user would typically have to enter another password in addition to the computer's general password to access that specific data.

Information on about 3.3 million patients included name, address, date of birth, phone number, email address, medical record numbers and the name of the patient's health insurance plan. Information on another 943,000 patients also included dates of services and descriptions of medical diagnoses and procedures.

Sutter spokesman Bill Gleeson said the company waited a month because it took that long to determine which patients' information was contained in the computer. The company properly notified the federal government as well as others beyond what was required, he said, and hired a private investigator who so far has turned up no leads on the stolen computer.

The stolen computer was scheduled to be encrypted "very soon," he said. Sutter initially concentrated on encrypting hand-held and laptop computers because those were deemed more likely to be lost or stolen.

"We deeply regret that that computer was stolen and that information about our patients was included. We have no reason to believe that computer was taken for that information," he said. He added that Sutter has heightened security for the building and was working on encrypting all of its computers.

The stolen computer did not contain patient financial records, Social Security numbers, health plan identification numbers or actual medical records, Sutter said.

Though encrypting patient information is "highly recommended" by the federal government, Verizon health care and data security expert Dr. Peter Tippett said the health care industry lags behind the financial and high-tech industries by 10 to 15 years when it comes to protecting personal data.

"Overall, the health care system needs a lot of work at being more secure," Tippett said.

In most cases, Tippett said, computer thieves are simply looking to make a little cash reselling the stolen computer itself. Sometimes they may try to ransom the computer back to its original owner. If the data itself is accessed, usually by organized crime operations, he said criminals would generally try to use it to blackmail prominent people with potentially embarrassing diagnoses or steal patients' identities to fraudulently bill health insurers for medical procedures that weren't really performed.

The worst consequence an average patient could expect would be a bill for a co-pay for a procedure they never received, he said.

Tippett said blaming any incident of identity theft on the stolen Sutter computer would be tough. If exploited, the patient information on the stolen computer would simply be added to the insecure data available on most everyone already floating around on the world's computer networks.

"It's real. It will hurt some people. But it won't hurt the average person in Sacramento," he said.

Sutter appears to have followed state and federal law and faces little investigation at least from California, officials said, particularly if no damage results to individuals.

California Department of Managed Care spokeswoman Denise Schmidt said her agency is "looking into whether there may be an impact," but she couldn't say what that might entail.

State Department of Insurance spokesman Dave Althausen said his department would only become involved if there are fraudulent insurance claims as a result.

Sutter notified the state Department of Public Health, but didn't need to, said department spokesman Ralph Montano. His department would only have jurisdiction if the breach was from a hospital or nursing home, he said, not a medical foundation or physician services group.

Joanne McNabb, chief of the California Office of Privacy Protection, said Sutter was only required to notify the U.S. Department of Health and Human Services, which it did within the required 60 days.

It was also required to notify affected patients in "the most expedient time possible without unreasonable delay," she said, quoting a 2008 state law. A one-month delay might be reasonable because it could have taken that long to determine what information was on the computer, she said.

Consumers should watch out for bogus medical procedures showing up on health care notices, and should be careful not to be caught by crooks using their information to seek Social Security numbers or other information, she said. But she said the data on the computer is relatively limited in the damage that could be done with it directly.

Citation: Theft of data on 4M patients part of wider problem (2011, November 18) retrieved 29 April 2024 from https://phys.org/news/2011-11-theft-4m-patients-wider-problem.html