

Medical-data breach said to be major

October 21, 2010

By Jane M. Von Bergen
Inquirer Staff Writer

A computer flash drive containing the names, addresses, and personal health information of 280,000 people is missing - one of the largest recent security breaches of personal health data in the nation.

"We deeply regret this unfortunate incident," said Jay Feldstein, the president of the two affiliated Philadelphia companies, Keystone Mercy Health Plan and AmeriHealth Mercy Health Plan.

The breach, which involves the records of Medicaid recipients, is the first such Medicaid data breach in Pennsylvania since at least 1997, according to the state's Department of Welfare, which has oversight.

"We take compliance [with federal privacy laws] very seriously," department spokeswoman Elisabeth Myers said Wednesday.

The security failure, one of the several largest in nearly two years, involves nearly two-thirds of the insurers' subscribers. It became known only after The Inquirer requested information Tuesday evening. The insurers said the drive was missing from the corporate offices on Stevens Drive in Southwest Philadelphia. It noted that the same flash drive was used at community health fairs.

"That seems grossly irresponsible," said Dr. Deborah Peel, a Texas psychiatrist who heads Patient Privacy Rights, an advocacy group.

"Why would you be hauling around private patient information to a health fair," she said. "I can't imagine what they were thinking, taking this data out of a locked room at company headquarters.

"What's tragic is that this is a particularly vulnerable group of people," Peel said. "They tend to be vulnerable to identity theft, vulnerable to discrimination." Medicaid recipients are low-income people.

The companies said that as of Tuesday, there had been no reports of anyone trying to use the information stored on the drive.

The news of the breach comes at a time when there is more emphasis - and billions of dollars in federal funding - to develop protocols for electronic medical records, with information being shared among providers, insurers, and consumers.

The idea is to eliminate duplicated record-keeping and improve patient health by allowing doctors, hospitals, and others to be quickly informed about medical conditions, prescriptions, allergies, and treatments.

"It's scary when you think about electronic patient records, which have many potential benefits, but there's also the concern about loss," said Susan Grant, director of consumer protection for the Consumer Federation of America, an association of nearly 300 consumer groups.

Paul Stephens, director of policy for the Privacy Rights Clearinghouse, said that data breaches in the finance and retail sectors tended to involve more people, but that health data are very sensitive and may also contain payment information.

The most infamous security breach occurred in 2006, when records of 2.65 million veterans were stolen from a Veterans Administration employee working from his home.

The Privacy Rights Clearinghouse in California maintains a database of reports on breaches culled from the media and websites. It listed 184 medical data incidents in 2009 and 2010 involving the records of 5.2 million people.

The Keystone and AmeriHealth case, if it had been listed, would have been among the top five by number of people involved.

In the Keystone and AmeriHealth case, the company said that of the 280,000 people affected only seven members' Social Security numbers were included on the flash drive, along with the last four Social Security numbers of an additional 801 clients.

The affiliated companies have been tight-lipped about the breach, which they said occurred Sept. 20.

Until The Inquirer asked for information, the company had not disclosed the data breach to affected members, most of whom live in Philadelphia and nearby counties.

Federal patient-privacy laws, which have been strengthened as the push toward electronic medical records advances, require that companies report major data breaches to the individuals, to the U.S. Secretary of Health and Human Resources, to the media, and to appropriate "business associates," in this case defined as the Pennsylvania Department of Public Welfare.

The federal website explaining the law says that breaches must be reported "without unreasonable delay and in no case later than 60 days."

Medicaid is funded jointly by federal and state governments. Pennsylvania's agreement appears to require a report within two days. Myers said it was unclear when the companies reported the incident. The federal government did not respond on time.

On Wednesday, the companies refused to offer any explanation of how the incident happened.

They would not say how they know the computer drive was lost, not stolen. They would not comment on the riskiness of taking the drive to health fairs, nor would they say whether the data on the drive was encrypted.

The companies refused to say whether they reported the incident to the federal government, as required.

At 4 p.m. Wednesday, after many requests for follow-up information, the companies issued this statement:

"At Keystone Mercy Health Plan and AmeriHealth Mercy Health Plan, our number one priority is our members. Since reporting this unfortunate incident to the Department of Public Welfare, we have actively and responsibly executed a multifaceted plan to inform those affected, while also evaluating and enhancing our security measures to ensure this does not happen again."

Keystone Mercy Health Plan provides insurance to 300,000 Medicaid members in Philadelphia, Bucks, Montgomery, Delaware, and Chester Counties. AmeriHealth serves 100,000 in a 15-county arc running from Harrisburg to northeastern Pennsylvania.

The two companies are jointly owned by Independence Blue Cross and the Mercy Health System.

Contact staff writer Jane M. Von Bergen at 215-854-2769 or jvonbergen@phillynews.com.