The Salt Lake Tribune

Worker error exposes Utah Medicaid clients to hackers

Theft • Unusual volume of data found streaming from server.

By Patty Henetz

The Salt Lake Tribune

Published: April 4, 2012 10:31PM
Updated: April 5, 2012 07:15AM

A mistake by a state employee allowed hackers — suspected by state officials to be located in eastern Europe — to gain access to more than 24,000 files submitted to the Utah Department of Health for Medicaid recipients.

Officials initially said Wednesday that about 24,000 claims had been compromised. But by late afternoon, state officials said the breach likely included claims for far more patients.

"At this point it appears likely that at least, and most likely, more than, 24,000 unique clients would have had their information compromised," said Health Department spokesman Tom Hudachko.

The health department and state technology experts said they suspect hackers penetrated an incomplete layer of security protections on a single computer server on Friday. Active downloading of the information didn't begin until Sunday night, continuing to Monday morning, when the breach was discovered.

Officials are still determining how many of the state's 260,000 Medicaid clients may have been affected. The department is advising all Medicaid clients to monitor their credit and bank accounts for unusual activity.

When the agency determines specifically whose records were compromised, it will mail letters to the clients with information to assist them. They also will receive free credit-monitoring services, Hudachko said.

Judi Hilman, executive director of the Utah Health Policy Project (UHPP) and an advocate for Medicaid clients, said she learned of the data theft from a news report.

"We were not notified, which really bothers me," she said. "We need more information on exactly what happened. It really truly could be an innocent error."

But most important, Hilman said, is protecting Medicaid recipients wary of applying for the services and ensuring their safety. "An incident like this," she said, "detracts from that sense of safety."

Michael Hales, the Utah Department of Health's Medicaid director, said the lag time between the discovery on Monday and the public announcement on Wednesday was necessary, because agency managers needed to determine whether any of the 39 servers linked to the hacked one were affected, and to be sure they had correctly counted the 24,000 records.

The Health Department uses 125 of the state's 520 servers; only one was breached, said Hales. The Utah Department of Technology Services is reviewing every state government server to make sure property security is in place.

The stolen data also included information on medical providers, but did not include pharmacy records, Hales said.

Hudachko explained that is more efficient for hospitals, clinics and other providers to submit their Medicaid claims at one time. The Health Department runs the data once a week. Providers "will save up all week and then Friday ... will have multiple claims on multiple individuals."

The Utah Department of Technology Services detected an "unusual volume [of data] streaming out of the server" on Monday morning, Hales said at a regularly scheduled monthly meeting with UHPP and Utah Community Action Partnership.

Hales said it's likely that few Social Security numbers were on the records, as Medicaid clients have different identification numbers on their files. The greatest risk is for people who were entering the system and still using Social Security numbers as identifiers.

Stephen Fletcher, executive director of Technology Services, said that normally the state's computer servers are protected with several layers of security. That protocol wasn't followed with the breached server. An investigation is under way to determine how that happened and who might be responsible.

The state Attorney General's office, which sponsors the Identity Theft Reporting Information System, also is helping.

Fletcher said it appears the hackers used passwords to gain access, but investigators are still trying to figure out how that happened. The hackers "were very sophisticated," he said. "We are not sure how they circumvented [security]."

The invasive activity was traced to an Eastern European location, though investigators don't know whether that's where the hacking originated.

The claims records likely would have included some Social Security numbers along with health conditions, people's birth dates, addresses, physicians' names, and other private information. Thieves sell Social Security numbers.

Hospitals, providers, the Department of Workforce Services, Human Services and the governor's office have been provided with referral information should people call seeking help protecting their personal information.

The federal Social Security Administration says identity theft is one of the fastest growing crimes in America. Identity thieves can use stolen numbers to apply for credit in the victim's name or another name. People often don't know of the theft until bill collectors call.

In its annual Data breach Investigations Report released in March, the telecommunications company

Verizon, in cooperation with the U.S. Secret Service and police agencies in the Netherlands, Australia, Ireland and England, found that organized criminals were responsible for the majority of breaches in 2011. More than two-thirds originated in Eastern Europe; hackers needed only "low" or "very low" skill levels, the report said.

—

Recent large breaches

Breaches of health information that affect 500 or more people must be reported to the federal Secretary of Health and Human Services. To see recent reported breaches, visit http://1.usa.gov/3bnoX6.

Concerned Medicaid clients can visit www.health.utah.gov or call 1-800-662-9651 to get more information.
