The Salt Lake Tribune

Official: Utah Medicaid data breach caused by 'a mistake'

Improper security • Computer server launched without adequate controls by known, but unnamed, state information technology worker.

By Patty Henetz

The Salt Lake Tribune

Published: April 5, 2012 12:51PM
Updated: April 5, 2012 12:55PM

State officials said Thursday they are still trying to determine how many individuals were affected by hackers who penetrated an inadequately protected computer server that contained information on Utah Medicaid clients, but they know who was responsible for not following security protocol.

Boyd Webb, chief information security officer for the Utah Department of Technology Services, said he was not ready to talk about who launched the server without setting the proper layer of security because the investigation of the incident is still active.

"We know who works on that server," Webb said. "I believe it was just a mistake."

On Wednesday, the Utah Department of Health announced more that 24,000 Medicaid files were stolen sometime between Sunday night and Monday morning, when the breach that occurred Friday was discovered and the server shut down.

Officials are still trying to count how many of the state's 260,000 Medicaid clients were affected, Health Department spokesman Tom Hudachko said Thursday morning. But they do know that 24,000 files would have contained information on far more individuals, as hospitals, clinics and other providers commonly gather and consolidate Medicaid claims and submit them to the state in batches, or files.

Letters will be sent to affected clients as soon as they can be identified. In the meantime, Hudachko advised people to check their bank accounts and credit for unusual activity.

Michael Hales, the Health Department's Medicaid director, said Wednesday the lag time between the discovery on Monday and the public announcement on Wednesday was necessary because department 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 files.

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 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. But Hales also 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.

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

Technology Services detected an "unusual volume [of data] streaming out of the server" on Monday morning, Hales said.

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.

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

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.

Officials directed concerned people to call the health department, where a series of prompts eventually lead to a customer service representative. Judi Hilman, executive director of the Utah Health Policy Project and advocate for people on Medicaid, said that shouldn't be considered adequate.

"When something like this happens they are supposed to say right up front, 'if you're calling about the data breach,' click [this number]," she said.

But there is a greater concern, Hilman said. "When you have a breach like this, and now we're reasonably certain it's an employee," she said, "maybe we don't have enough security around the servers. We pride ourselves on our lean government. But when you have a breach like this, you have to ask whether you have adequate staffing."

—

Investigation continues into Medicaid hack

State officials say they don't yet know how many of Utah's Medicaid clients had their information stolen when a computer server's security was breached. Concerned Medicaid clients can visit www.health.utah.gov or call 1-800-662-9651 to get more information.