

# The Salt Lake Tribune

---

## Utah Health Dept chief: hacked data stored too long

Community forum • Victims say they need help protecting their identities.

By Patty Henetz

The Salt Lake Tribune

Published: May 3, 2012 01:51PM

Updated: May 3, 2012 10:18AM

Medical data hacked in March from a state computer server languished in the state's electronic system instead of being erased within a day, which is normal security protocol, Utah Department of Health Executive Director David Patton said Tuesday.

At a community forum held by the department, Patton said Social Security numbers and other personal information stayed on the poorly protected server for three months. The information, he said, "should have been deleted the day after the inquiry."

By "inquiry," Patton meant the information routinely sent out by health care providers, as part of their billing, to check whether patients are covered by Medicaid. That means patient names, birth dates and Social Security numbers go through the Health Department's computer system.

That doesn't sit right with Sandy resident Rex Anderson, whose Social Security number was among the 280,000 that hackers grabbed between March 30 and April 2.

Anderson was among the 40 people who attended the community forum aimed at answering questions and helping victims, through the nationwide credit-reporting system, to minimize the threat of their identities being stolen. He demanded to know who sent the inquiry on him, as he has never been a Medicaid recipient.

"I want to go after the S.O.B. who sent it," Anderson said.

Patton replied the breach wasn't the fault of the providers — they were just doing their jobs. "They did not expect to see this [personal health information] saved on our server," he said. "The data should not have been there when it was compromised."

Hackers broke into an unprotected Department of Technology Services server by exploiting a weak password. As many as 780,000 people, many of them children, were affected.

The victims likely visited a health care provider in the past four months, officials say. This applies to

anyone who visited a hospital, family doctor or had home health care, and had private insurance, no insurance, Medicare or Medicaid. Patients agree to share their information with medical professionals when they sign a federal Health Insurance Portability and Accountability Act, or HIPAA, disclosure form.

Health Department Deputy Director Michael Hales said the investigation has even turned up compromised Social Security numbers for people living outside Utah.

The state is offering a year of free credit monitoring for those whose Social Security numbers were stolen. Patton said that so far, 20,000 people have signed up.

The FBI is investigating how the break-in occurred and who might have done it. While the breach was traced to an Eastern European location, investigators haven't said for certain that is where the hacking originated.

Twice at the Tuesday evening forum, attendees asked whether anyone at the Utah Department of Technology Services, which manages computer operations for all state agencies and was responsible for the lax security, had been fired or reprimanded.

Patton deflected the question. "We're in the mode of trying to help people," he said, "not find culprits."

---

© 2012 The Salt Lake Tribune