

Data Breach Update

What happened?

In March 2012, computer hackers illegally gained access to a Utah Department of Technology Services (DTS) computer server that houses personal health information. DTS detected the security breach on Monday, April 2 and immediately shut down the server. The breach occurred due to an error on the server at the password authentication level, allowing the hacker to circumvent the security system. DTS has processes in place to ensure the state's data is secured, but this particular server was not configured according to normal procedure.

What kind of information was on the server?

Data from Medicaid and CHIP (Children's Health Insurance Program) claims payments as well as data from eligibility inquiries (inquiries sent from health care providers to determine if patients are enrolled in Medicaid or CHIP) were housed on the server. This data includes sensitive, personal health information from individuals and health care providers. Such information could include Social Security numbers (SSN), names, dates of birth, addresses, diagnosis codes, national provider identification numbers, provider taxpayer identification numbers, and billing codes.

Why are individuals who have no history with Medicaid or CHIP receiving letters stating their personal information was part of the breach?

The breached DTS server is primarily used to process Medicaid and CHIP payment claims. However, the server also contained information about individuals who may not have any history with the Medicaid or CHIP programs. Information on these individuals was submitted to the state by a health care providers or their third-party billing entities in a transaction called a Medicaid Eligibility Inquiry to determine if their patients are enrolled in Medicaid for billing purposes. These are routine business transactions, and providers submit this information with the expectation the state will keep it secure

How many victims are there?

Up to 780,000 people had personal information compromised as part of the breach. Approximately 280,000 of these people had their Social Security numbers (SSN) stolen. As many as 500,000 other people had less sensitive information, such as names, dates of birth, and addresses stolen.

What is being done?

The Utah Department of Health and the Department of Technology Services have implemented a number of steps to help victims protect themselves and to help inform the community about the breach. Such steps include:

- Governor Gary Herbert announced the creation of the Health Data Security Ombudsman to provide personal assistance to victims of the breach.
- The state has sent 277,000 letters to people who had their SSN stolen and 175,000 letters to people who had less sensitive information stolen.
- The state is offering one year of free credit monitoring to everyone who had their SSN stolen, the credit monitoring also includes identity theft insurance.
- The state established a 24-hour toll-free hot line to provide information (855-238-3339).
- Web site dedicated to the breach (www.health.utah.gov/databreach) has additional information on how people can protect their credit, along with contact information for the nation's three credit bureaus.

- The web site has also helped to publicize the Attorney General's Child Identity Protection Program.
- UDOH has conducted informational presentations to community groups and also hosted a public forum.
- The state has issued contracts for two independent audits. The first is an IT assessment of the entire state's data security and data storage systems, this assessment will also include a forensic analysis of the breach. The second contract is an assessment of the state's efforts to respond to victims in order to ensure the state is providing the best service possible in helping individuals protect their private information.
- The data that was compromised during this breach is now encrypted while it is "at rest" on state servers.
- DTS has analyzed all state servers and has conducted vulnerability assessments on them as well.
- DTS is reviewing all security policies and procedures and ensuring all staff are properly trained.
- UDOH conducted an internal security review of all of its data systems.
- The UDOH is working with the Digital Health Services Commission to review health information security and privacy policies.
- DTS is cooperating in a criminal investigation with the FBI.