Data Breach Update
April 13, 2012

What happened?

In March 2012, computer hackers illegally gained access to a Utah Department of Technology Services (DTS) computer server that stores Medicaid and CHIP claims data. The thieves began removing data from the server. DTS detected the security breach on Monday, April 2 and immediately shut down the server. As its investigation proceeded, DTS discovered data from eligibility inquiries (inquiries sent from health care providers to determine if patients are enrolled in Medicaid) was also stored on the server. This additional data included information from individuals who may not be Medicaid or CHIP clients.

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?

Claims payment and eligibility inquiries contain 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.

Who had their information stored on the server?

In the claims data, Medicaid and CHIP recipients and their providers had information stored on the server. Other potential victims include people whose information was sent to the state by their provider in a transaction called a Medicaid Eligibility Inquiry to determine their status as possible Medicaid recipients. These victims are likely to be people who have visited a health care provider in the past four months. Some may be Medicaid or CHIP recipients; others are individuals whose health care providers were unsure as to their status as Medicaid recipients.

How many victims are there?

The most sensitive information stored on the server was individual's SSNs. Approximately 280,000 individuals had their SSNs stolen. This includes Medicaid and CHIP clients, providers and other individuals who had their information sent to the state by their provider to inquire about their status as a Medicaid recipient. Other less sensitive information, such as names, dates of birth, and addresses was also stored on the server. As many as 500,000 individuals may have had this type of information compromised.

What is being done?

Victims will be receiving a letter from the Utah Department of Health (UDOH). UDOH has already begun sending letters and will continue to send them until everyone with compromised information is notified. If a SSN was accessed, the letter will also provide information on how to take advantage of free credit monitoring services for one year. Additionally, the data breach hotline is available to find out if their SSN was compromised **(1-855-238-3339).**

Possible victims should be aware that nobody from DTS or UDOH will be contacting them and asking for information over the phone or via e-email regarding this incident. Scammers may

attempt to reach victims in this manner. We strongly recommend that people do not provide private information in response to telephone or e-mail contacts they have not initiated.

DTS is cooperating in a criminal investigation with the FBI and Utah Department of Public Safety. At this point, there have been no reports of identity theft related specifically to this incident. However, given the sensitive nature of the stolen data, and information law enforcement has been able to compile about the thieves, including their potential whereabouts and their high level of sophistication, it is likely the motive for the breach is to use the stolen information in a fraudulent manner.

What can potential victims do to protect themselves from identity theft?
We advise all potential victims to closely monitor their credit and bank accounts. There are a number of other steps you can take to protect yourself from identity theft, including freezing your credit or placing a fraud alert on your personal credit file. You must initiate these activities on your own with each of the nation's three credit bureaus. For information on how to do this, visit http://idtheft.utah.gov.

For regularly updated information, please visit http://www.health.utah.gov/databreach or call the data breach hotline at **1-855-238-3339.**

If you work with potential data breach victims, including your patients or Medicaid/CHIP clients, please encourage them to be proactive in protecting their personal information and credit files. Specific ways in how to do this can be found on our web site, http://www.health.utah.gov/databreach. Additional resources are also listed below.

Additional Resources
To obtain a copy of your credit, place a fraud alert or freeze your credit, contact one of the nation's three credit bureaus:

- **TransUnion**
  http://www.transunion.com, 1-800-888-4213
- **Experian**
  http://www.experian.com, 1-866-200-6020
- **Equifax**
  http://www.equifax.com, 1-800-685-1111

The Utah Attorney General's Office sponsors a Child Identity Protection program, as well as the Identity Theft Reporting Information System to assist victims of identity theft. For more information visit, http://idtheft.utah.gov.