

Oklahoma State Department of Health

Data Theft Q & A

What Happened?

An Oklahoma State Department of Health (OSDH) laptop computer and other items were stolen from a personal vehicle while an agency employee was in Yukon on April 6, 2011. A database related to the Oklahoma Birth Defects Registry was on the laptop computer. The Oklahoma Birth Defects Registry (OBDR) provides statewide surveillance of birth defects to reduce the prevalence of birth defects through prevention education, monitoring trends and analyzing data. The laptop was used to record data from hospital medical records. The data includes information on nearly 35,000 children with birth defects. In addition, 50 paper files containing abstracted medical information were also taken in the theft. The theft was reported to the Yukon Police Department and the OSDH is working closely with them on their investigation.

How will I know if my information was included in this security breach?

The OSDH is notifying nearly 133,000 individuals that their names and some personal information may have been contained on the laptop computer. The OSDH has posted the letter on the OSDH website with information about the data theft and the kinds of personal information that could potentially be accessed. The OSDH is also making available identity protection services. If interested or if you have questions, call toll free 1-866-278-7134 during the hours of 8 am to 5 pm Monday through Friday; or email the OSDH at contactosdh@health.ok.gov; or visit <http://www.health.ok.gov> for more information.

Checking your credit report periodically is one way to help you spot problems and address them quickly. The Fair Credit Reporting Act guarantees you access to your credit report for free once per year. Go to annualcreditreport.com to obtain your free credit report along with other useful information.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, you should promptly call your local law enforcement agency and file a police report. Keep a copy of the report for your records. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission recommends that you check your credit reports periodically.

You may also consider placing a fraud alert on your credit files. A fraud alert tells creditors to contact you personally before they open any new accounts. In order to register a free fraud alert, contact any of the three major credit bureaus listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others to place fraud alerts.

- TransUnion, PO Box 6790, Fullerton, CA 92834-6790, 1-800-680-7289, www.transunion.com
- Experian, PO Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
- Equifax, PO Box 740241, Atlanta, GA 30374-0241, 1-800-525-6285, www.equifax.com

What else should I do?

You should carefully review any bills that you receive in the near future, especially credit card transactions, to ensure that the charges associated with your accounts are accurate. Get additional

[information about identity theft](#) (link opens in new window) or call toll free 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261.

If my information was among the files exposed or stolen, does this mean that I'm a victim of identity theft?

No. The fact that someone may have had access to your information doesn't mean you are a victim of identity theft or that they intend to use the information to commit fraud. We wanted to let you know about the incident so that you can take appropriate steps to protect yourself. The best way to protect yourself is to place a free fraud alert on your credit file and review your credit reports.

What is the Department of Health's policy regarding data security?

While the OSDH has strict policies in place to protect against incidents such as this, these policies are being reviewed to strengthen safeguards and better protect the confidentiality of the data collected by the agency to ensure a similar incident cannot happen again.

The OSDH offers its apologies to those who may be affected by this data theft. We are committed to the proper handling of confidential personal information and we are doing all we can to ensure a similar incident cannot happen again.

Reporting a Suspected Security Incident

Report any improper use of OSDH resources or exposure of personal information to:

Oklahoma State Department of Health
Privacy Officer
1000 Northeast Tenth Street
Oklahoma City, OK 73117-1299
Phone 1-866-278-7134