Utah guv fires tech director over health data breach, creates security czar

He fires the technology service director and hires an ombudsman to help victims of breach.

Gov. Gary Herbert apologized to the 780,000 victims of the health data security breach on Tuesday.

To restore the public’s trust, he announced Tuesday that he fired Department of Technology Services director Stephen Fletcher and hired an ombudsman to shepherd victims through the process of protecting their identities and credit.

“The people of Utah rightly believe that the government will protect them, their families, and their personal data. When they interface with us that is in fact our charge,” Herbert said at an afternoon news conference, adding that one of his family members was among those whose information was compromised.

“As a state government we have failed to honor that commitment,” he said. “For that, as your governor and as a Utahn, I am deeply sorry.”

He said Fletcher was asked to resign, saying the director lacked “oversight and leadership.”

The governor said the status of two other technology
employees is also being reviewed. They could be reprimanded or fired.

Herbert declined to give details of what protocols the employees failed to follow that allowed hackers, likely from Romania, to swipe the Social Security numbers and other data from health department servers on March 30. He said they are being investigated, but added that the breach was related to the failure to change a default password.

Data will now be encrypted while it is on state servers and not just when it is in transit, he said.

Herbert also announced the creation of a new “health data security ombudsman” in the health department and appointed Sheila Walsh-McDonald, a long-time advocate for low-income Utahn at the Salt Lake Community Action Program. She will help victims navigate the programs available to them to protect their information.

Hired full-time — she was handpicked by the health department — Walsh-McDonald will eventually extend her work beyond the breach to address other health data issues.

She said she will be a “portal for victims, to listen, to hear, to make sure that the public is as proactive as possible in taking advantage of what has been made available, and then assessing what else we need to do.”

She can be reached through the hotline at 1-855-238-3339.

The programs include free credit monitoring and free enrollment in identity theft insurance for coverage up to $1 million for individuals and $2 million for families. They must enroll in the insurance program by Aug. 31. Information is available through the hotline.

And the Utah Attorney General’s Office has a free Child Identity Protection Program, at cip.utah.gov, to prevent thieves from getting credit with children’s information.

Senate President Michael Waddoups, R-Taylorsville, said Tuesday he feels the steps taken by the governor are sufficient.

“I believe that there is probably an exaggeration to the impact this could have on the public, in that there’s no credit card numbers out there,” he said. “At the same time, this never should have gotten out.”

Herbert also terminated a contractor who provided software without encryption safeguards, he said.

“In my mind, more important than the termination of Fletcher, more important than the ombudsman, is the termination of the contractor,” Waddoups said.

Herbert warned Utahn to be wary of scammers taking advantage of the breach by claiming to be from the state and asking victims for their Social Security numbers or banking information. The state will not ask for that information, he said.

Judi Hilman, executive director of the Utah Health Policy Project, applauded the governor’s announcements regarding Fletcher and Walsh-McDonald, saying it was the first time she had hope that the state was “on the right track.”

She added: “It’s a good day for the victims of the breach. It’s the first day of hope.”

Hilman said Fletcher had to leave to show victims that the government was taking the mistake seriously.
And Walsh-McDonald “has always looked out for the needs of the consumer in this.”

Mark VanOrden, director for the Utah Department of Workforce Services, will serve as the acting director of Technology Services.

Fletcher was appointed in 2005 by then-Gov. Jon Huntsman to serve as the chief information officer in the state’s newly-centralized information technology department, managing technology programs across state government.

Before being appointed as CIO, Fletcher was the deputy assistant secretary for management and later chief information officer and chief technology officer at the U.S. Department of Education.

Fletcher graduated from the University of Utah and received an MBA from the University of Dallas with an emphasis in engineering management.

The moves come on the heels of the state seeking a public relations firm to handle “crisis communications” and rebuild trust with the public.

On March 30, hackers broke into a poorly protected Medicaid eligibility server, putting the personal information of 780,000 people at risk.

On that server were Medicaid claims and the names, birth dates, addresses, and in some cases, Social Security numbers, of retirees on Medicare, the privately insured and uninsured — information sent by health providers and billing companies to inquire about a patient’s eligibility for Medicaid.

The stolen information is not yet known to have been misused.

The governor also ordered a security audit of the state’s information technology systems across the state by Deloitte & Touche. And Hogan Lovells was hired to assess whether the state is following the federal Health Insurance Portability and Accountability Act in how it is notifying victims.

Tribune reporter Robert Gehrke contributed to this report.

hmay@sltrib.com

Was your information hacked?

Protect yourself » If you’ve been to a Utah health provider in the past four months, or possibly the last year, your personal information may have been exposed in a state data breach. To find out, call 1-855-238-3339.

Costs of the breach

Senate President Michael Waddoups, R-Taylorsville, said Tuesday he expects the response to data breach to cost between $2 million and $10 million — and more if the state faces federal fines or lawsuits. Among the costs so far:

A health data security ombudsman has been hired to fill the new position.
Victims are being offered free credit monitoring and free enrollment in identify theft insurance.

The state is hiring a public relations firm to handle “crisis communications” and rebuild trust with the public.

Deloitte & Touche has been hired to audit the security of the state’s information technology systems.

Hogan Lovells has been hired to assess whether the state is following federal law in how it is notifying victims.

© 2012 The Salt Lake Tribune