SALT LAKE CITY — The state's executive director of technology services, Stephen Fletcher, has been terminated over the data breach that compromised personal medical information of an estimated 800,000 Utahns.

Gov. Gary Herbert also said Tuesday two Department of Technology Services employees are under investigation in relation to the mistakes that led to the breach and he pledged the state will find a way to more securely handle confidential data.

"There needs to be some accountability for the lack of oversight and leadership," Herbert said.

"He has not built the kind of system we need going forward," Herbert said, in explaining why he asked Fletcher to step down.

Legislative leaders agreed with Fletcher's forced resignation and said changes need to be made to protect Utahns personal information. Sen. Stuart Reid, R-Ogden, is drafting a bill that would give patients control over how their health insurance details are shared with the government and tightening data security.

"I'm not looking to point fingers. I'm not looking to blame. What I'm looking to do is solve the problem so it doesn't happen in the future," Reid said.

The data breach was detected in March after a server was improperly protected, allowing hackers from Eastern Europe to access the state's Medicaid database. Tuesday's action comes after weeks spent notifying individuals whose information may have been compromised.

"We know from a review we've done already of this process, that the breach was a direct result of employees who neglected to adhere to and establish security protocols, and in this particular instance, there is just no room for error," Herbert said.

The governor apologized, saying the state has "failed to honor a commitment" to the people who trusted the government to protect personal information. He said much is being done to not only protect those
whose information was compromised, but also to correct the action and restore public trust in the system.

"When it comes to the private data that the public gives to our state, we take it very seriously," Herbert said. "This is a responsibility that every employee takes very seriously, and certainly I do."

The state has enlisted the help of Deloitte & Touche, an auditing and risk security agency, as well as the London-based law firm of Hogan Lovells, which will assess the way the state has responded to the victims of the breach.

The governor also said technical experts from the public and private sectors are coming together to review the processes in place and develop a plan for the future of data protection within the state.

"This incident is a tragic reminder that it is a different world in which we live," Herbert said, adding that the attack has been personal, as members of his family and those of his staff have been impacted.

**More changes coming**

Reid said he got involved in drafting legislation after his wife was contacted by the state concerning the loss of information. Other lawmakers said they have been hearing nonstop from angry constituents, who are worried about how their personal information may be used.

"This is a significant issue that demands accountability," House Speaker Becky Lockhart, R-Provo, said. "If I were a person who had been affected, I think I would have had some frustration."

Lockhart said not only do Utahns need reassurance about what happened to their data, they need to know it will be safeguarded in the future. That may require a reassessment of the state's centralized technology services that have been in place since 2005.

Senate President Michael Waddoups, R-Taylorsville, said the state is already spending millions of dollars fixing the problem and for credit monitoring for those affected, and still faces the possibility of federal penalties and a class-action lawsuit.

Waddoups estimated the current cost at less than $10 million.

No one else has attached a price tag yet to the breach, but Herbert said there is likely room within existing budgets to cover the costs, and there is no reason to call a special session to appropriate additional funds.

The Senate president called the governor's actions Tuesday "sufficient" and said the impact of what information was shared was "probably exaggerated" because it did not include credit card numbers or medical conditions.

Of the nearly 800,000 individuals impacted by the breach, approximately 280,000 had their Social Security numbers compromised. Those individuals have been offered one year of free credit monitoring services through the national credit-reporting agency Experian. Less than 3,000 have yet to be notified of this, due to insufficient data or other issues with the information.

Birth dates, names, addresses and other personal information of approximately 500,000 were also stolen from the server, and those individuals have been told to closely monitor their credit.
The Utah Department of Health is still analyzing the data within nearly 100,000 of the stolen claims and approximately 210,000 are duplicates and partial data that is indecipherable.

Mark VanOrden, a veteran IT director with the Department of Workforce Services, will take on the position as interim director of the technology department, and Herbert appointed Sheila Walsh-McDonald to the newly created position of health data security ombudsman to work with the public, offering case management, credit counseling and other resources and providing community outreach.

Walsh-McDonald is already working with victims of the breach through her advocacy position within the Salt Lake Community Action Program. She said people — specifically the homeless, non-English-speakers and refugees — are slipping through holes and are not aware of or taking advantage of the services available to them.

Individuals are encouraged to call 1-855-238-3339 or visit www.health.utah.gov for additional information.

"As of today, I feel hope for the victims," said Utah Health Policy Project director Judi Hilman. "Today I know the governor is taking this seriously."

Hilman said she trusts Walsh-McDonald, who works with a variety of community-based organizations that have the trust of individuals impacted by the Medicaid breach.

"Letters and hotlines are not enough. This needs to be a multidisciplinary effort … she will leave no stone unturned," Hilman said.

Herbert said the state has no evidence that the compromised data has been used thus far. He said new protection measures have been put in place to prevent additional exposure.

Claim data sent to state servers now remains encrypted throughout the duration of the less than 24 hours it is there, instead of just during transit, as it was when the breach occurred.

"Cyber-security is the modern battlefront and we are all enlisted — you, me, our state agencies, the Legislature — all of us have a critical role to play," Herbert said.

Lawmakers will further address issues surrounding the Medicaid breach Wednesday, Rep. Mike Noel, R-Kanab, chairman of the Public Utilities and Technology interim committee, said he expects to be briefed on the matter and hear about what is being done to help those impacted and prevent other potential breaches from happening again and in the future.

"I know there are a lot of constituents concerned," he said. "It's a real concern."

**Contributing:** John Daley