Breach of faith

By jason cooke

Published: April 21, 2012 01:01AM
Updated: April 21, 2012 01:01AM

The dust has begun to settle around the recent security breach involving the personal information of roughly 750,000 Utahns who are enrolled in Medicaid.

The state departments of Health and Technology Services work diligently to deal with the fallout, while law enforcement seeks to track down the cyber thieves.

Community groups are trying to reassure and assist families with whom they work.

But for years after things return to normal, the families of those affected — mostly children, pregnant women, the elderly and people with disabilities — will struggle to keep tabs on their credit, living in fear that their identities have been stolen.

Whether the state is going far enough in helping the affected families deal with a very real threat to their financial future is an open question. In the meantime, policymakers have a legitimate opportunity to make something good come out of the disaster.

Let’s see what we can learn that will help avoid another catastrophe and improve the way government delivers services.

First, we should assess the relationship between the breach and the decision to centralize all state government information technology activities. Did we save money by downsizing the state’s IT workforce, increasing the workload of the remaining IT staff as well as the chances for human error?

The Department of Technology Services has audited its procedures and verified the security of other data in the state’s systems.
But let’s go the extra step of examining the decision to centralize state data systems to be sure we are not missing the policy forest because we’re focused on the technology trees.

Then let’s look at how the state manages change — what happens during the transition from the old ways of doing business to the new to ensure no interruption in critical services. Regardless of how the U.S. Supreme Court or the electorate rules on Obamacare, massive change is headed our way.

We need to be comfortable that we will meet that change with adequate and appropriate resources.

We should ask ourselves whether, in our rush to condemn the federal government for intruding in our lives, we are failing to do what makes sense, and upholds the dignity and financial security of our fellow citizens.

For example, there appears to be no federal requirement to encrypt Medicaid claims data while those data are in storage or “at rest.” But is that our idea of good government? Judging from the encryption requirements around the All Payer Claims Database, it would appear that it is not. Except when it comes to the personal information of individuals enrolled in Medicaid and CHIP.

We need to look at the adequacy of our contingency planning and how we carry it out. What was the state’s contingency plan for this kind of breach? Did anyone review it to ensure that it included the vital component of communicating effectively with affected consumers?

We must re-imagine government’s partnership with the community so that we can engage all of the resources at the state’s disposal to deal with a catastrophe on this scale. Why wouldn’t we pull together in response to a security breach like we do in the face of natural disaster?

Finally, we need to revisit how we view taxpaying Utahns who depend on government programs as they get back on their feet after a layoff or maintain their independence despite having a disability.

Where were the voices of the policymakers expressing concern for the security of Medicaid personal information?

It’s enough to make a reasonable person wonder: Would a similar breach of the state’s hunting and fishing license database have been met with the same response?

Jason Cooke is Medicaid research and policy director with the Utah Health Policy Project and former director of Texas Medicaid and CHIP.