Group Offers Suggestions on How To Respond to Utah Health Data Breach

The Utah Health Policy Project has teamed up with community-based groups and consumer credit counseling agencies to provide state agencies with recommendations on how to restore trust in the security of state health programs after a recent data breach at the Utah Department of Health, the Salt Lake City Deseret News reports.

UHPP warns that the breach could result in an increasing number of eligible families not applying for Medicaid or the Children’s Health Insurance Program because of concerns about the security of their personal information (Schwarz, Salt Lake City Deseret News, 4/28).

Background on Data Breach

According to UDOH, the breach occurred on March 30 as Utah Department of Technology Services technicians were exchanging computer servers.

Stephen Fletcher -- executive director of UDTS -- said it appeared that "very sophisticated" hackers used passwords to access a server, but officials are uncertain about how the hackers bypassed security (iHealthBeat, 4/12).

The breach affected the personal information of about 800,000 Medicaid and CHIP beneficiaries. The stolen information included about 280,000 Social Security numbers.

Recommendations

To help restore trust in the security of state health programs, UHPP recommended:

- Issuing new Social Security numbers to children affected by the breach;
- Establishing a long-term plan to provide counseling and assistance to affected residents;
- Creating a step-by-step guide on how to apply for a credit freeze;
- Creating an advisory committee to advocate for individuals who have limited or no English proficiency, those with mental illnesses, seniors and those living in nursing homes or residential facilities; and
- Launching a marketing and outreach campaign with public service announcements (Salt Lake City Deseret News, 4/28).