



**June 27, 2012**

**Statement from Commissioner Bill Streur concerning \$1.7 million resolution agreement between Health and Social Services and the U.S. Department of Health and Human Services' Office of Civil Rights**

(ANCHORAGE) — The Alaska Department of Health and Social Services has paid the U.S. Department of Health and Human Services' Office of Civil Rights (OCR) \$1.7 million in a resolution agreement to address possible violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule.

During the investigation of a portable hard drive that was stolen in 2009, OCR alleged possible Security Rule violations by DHSS. I would like to assure Alaskans that we believe no individual's personal data has been compromised and we take our security responsibilities seriously. We completed a thorough investigation at the time of this incident, and have not discovered or received reports that personal information was accessed or used in any way. Our department had security measures in effect before this incident that helped keep our data safe. This resolution is the result of possible security violations, not the loss of actual personal information of Alaskans.

I would also like to address some misleading statements that have come about from a HHS press release entitled "Alaska Medicaid settles HIPAA security case for \$1,700,000:"

- Entering into this agreement was not an admission of liability or that we believe DHSS was in violation of the Privacy Rule or the Security Rule. Agreeing to complete our HIPAA compliance measures and paying a settlement amount is the

- only way for both parties to avoid costly and protracted litigation – a process with no guaranteed result and that could end up being more expensive for the state.
- The title of the OCR release suggests that Medicaid data may have been compromised. We have absolutely no indication that Medicaid data or personal information was lost or at risk.
  - OCR stated that DHSS did not have a current risk assessment. We did have a risk assessment, but it was several years old. It has not been clear in our dealings with OCR what the definition of “current” is by OCR, or that there even is a definition. We have begun work on conducting a new risk analysis in light of OCR’s concerns.
  - OCR suggested that DHSS did not have sufficient risk measurement in place. At the time of the investigation, DHSS had identified risk management measures, and was in the process of putting them in place.
  - OCR determined that DHSS did not have device and media controls and encryption in place. DHSS did have administrative controls in place in 2009, and had crafted security and privacy policies that were up for review to implement robust controls and encryption. Even before this investigation, the department had purchased encryption software and was partway through the encryption of all PCs and storage devices in the department. Currently, all computers and devices are protected with encryption software.

Since 2009, I am pleased to report that DHSS has completed the adoption of the security measures that were being implemented at the time of the OCR investigation. We have trained all department staff on privacy and security safeguards and ensured that our equipment is well protected.

I would like to reassure Alaskans that we respect and properly safeguard all data the department uses in providing services. For more information on our security efforts,

please contact our Chief Security Officer, Thor Ryan, at 269-0076, or [thor.ryan@alaska.gov](mailto:thor.ryan@alaska.gov).

Sincerely,

William J. Streur  
Commissioner

# # #

**DHSS is now on Twitter.** Follow health updates at [www.twitter.com/Alaska\\_DHSS](http://www.twitter.com/Alaska_DHSS).