HINSHAW
& CULBERTSON LLP

Health Law ALERT

# Alaska Settles HIPAA Security Case for $1.7 Million; HHS Reinforces Need for Adequate Policies and Procedures for the Safeguarding of ePHI

## July 18, 2012

On June 25, 2012, the Alaska Department of Health and Social Services (Alaska DHSS) agreed to a $1.7 million settlement with the U.S. Department of Health and Human Services (HHS), stemming from the 2009 theft from a state computer technician's vehicle of an external hard drive potentially containing electronic protected health information (ePHI). The striking fact in this scenario is that the fine was driven primarily by Alaska DHSS's failure to show that it had adequate policies, procedures and staff training in place, rather than by an improper disclosure of ePHI.

The HHS Office of Civil Rights (OCR) conducted an investigation following a breach notification report submitted by Alaska DHSS, as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act. OCR's investigation included a review of Alaska DHSS's policies, procedures and training activities related to compliance with the HIPAA privacy and security rules, and interviews with members of the workforce. As a result of its investigation, the OCR determined that Alaska DHSS violated the HIPAA security rule, which protects health information in electronic form by requiring HIPAA-covered entities to use physical, technical and administrative safeguards to ensure that ePHI remains private and secure. Specifically, the OCR determined that Alaska DHSS had failed to: (1) complete a risk analysis; (2) implement sufficient risk-management measures; (3) complete security training of workforce members; (4) implement device and media controls; and (5) address device and media encryption. Ultimately, Alaska DHSS agreed to settle the potential violations for $1.7 million and to submit to a corrective-action plan, pursuant to which Alaska DHSS is required to develop, maintain and revise as necessary its written policies and procedures related to the violations and to train the members of its workforce. Members of the workforce are required to sign initial compliance certifications acknowledging that they have read, understand, and will abide by the policies and procedures. They must also certify that they have received the necessary training. In addition, Alaska DHSS must conduct a risk analysis and submit to a monitoring plan.

This settlement comes only months after a $1.5 million settlement reached with Blue Cross Blue Shield of Tennessee (BCBST) regarding potential HIPAA violations stemming from BCBST's notification involving a 2009 theft of computer hard drives containing ePHI. There, the OCR found that BCBST had failed to implement appropriate administrative safeguards to adequately protect information by not performing the required security evaluation in response to operational changes and by not having adequate facility-access controls, as required under the security rule. Pursuant to its settlement, BCBST was similarly required to review, revise and maintain its privacy and security rule policies and procedures, conduct regular trainings for members of the BCBST workforce, and to perform monitor reviews to ensure compliance with its corrective-action plan.

The OCR's recent enforcement activity highlights the need for HIPAA-covered entities to make certain that they have in place carefully designed and monitored HIPAA-compliance programs. In the $1.7 million settlement reached with the Alaska DHSS, Alaska DHSS's breach notification report indicated only that the stolen hard drive *potentially* contained ePHI. Despite the fact that there was no evidence of a definite impermissible disclosure of ePHI, the OCR's investigation revealed numerous violations of the security rule stemming from Alaska DHSS's failure to have in place adequate safeguards. Covered entities should take note of the OCR's careful attention to covered entities' policies and procedures and the training provided to members of the workforce, and should ensure that their compliance programs are up to date in such regards. Failure to do so can be an independent basis for the OCR to find a violation and could subject a covered entity to substantial monetary penalties and increased scrutiny from authorities.

For further information, please contact Danielle M. Costello or your regular Hinshaw attorney.

---