HHS SETTLES HIPAA SECURITY CASE WITH STATE AGENCY FOR $1.7 MILLION

On June 26, 2012, the Department of Health and Human Services ("HHS") announced that it had reached a settlement with the Alaska Department of Health and Social Services ("Alaska DHSS") arising from potential violations of the Security Rule under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). HHS learned of the circumstances giving rise to the enforcement action through the notification provided by Alaska DHSS to HHS under the Breach Notification provisions of the Health Information Technology for Economic and Clinical Health Act ("HITECH"). This marks the first HIPAA enforcement action against a state agency and the second enforcement action arising from information divulged to HHS under the Breach Notification Rule.

The underlying facts involved the theft of a portable USB hard drive that was stolen from the vehicle of an Alaska DHSS employee. The portable drive contained electronic protected health information ("ePHI") of more than 500 Alaska Medicaid beneficiaries, which required Alaska DHSS to notify the affected individuals and HHS under the HITECH Breach Notification Rule.

The HHS Office for Civil Rights ("OCR") investigated the reported breach and found that Alaska DHSS had failed to implement appropriate safeguards to adequately protect ePHI. In particular, OCR found that Alaska DHSS did not have adequate policies and procedures in place and had not completed a risk analysis, implemented sufficient risk management measures, completed security training for its workforce members, implemented device and media controls or addressed device and media encryption as required by the HIPAA Security Rule. As a result, OCR and Alaska DHSS entered into a Resolution Agreement whereby Alaska DHSS agreed to pay HHS a $1,700,000 settlement payment and to perform the following obligations under a Corrective Action Plan:

- Develop, maintain and revise, as necessary, written policies and procedures relating to the completion of a risk analysis, risk management measures, security training for workforce members, device and media controls and device and media encryption. The policies and procedures must include procedures for tracking, safeguarding, encrypting and disposing/reusing devices containing ePHI, responding to security incidents and applying sanctions to workforce members who violate the policies and procedures.
- Obtain HHS's approval of the policies and procedures; distribute them to all workforce members with access to ePHI within 30 days of beginning service; obtain a written or electronic compliance certification from each such workforce member; and assess, update and revise, as necessary, the policies and procedures at least once annually. Alaska DHSS workforce members who do not receive the policies and procedures within 30 days of beginning service may not have access to ePHI until the workforce member receives the policies and procedures and provides the compliance certification.
- Conduct training for all Alaska DHSS workforce members who have access to ePHI, and obtain a written or electronic compliance certification from each such workforce member. Alaska DHSS workforce members who do not receive the policies and procedures within 30 days of beginning service may not have access to ePHI until the workforce member receives the training and provides the compliance certification.
- Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI held by Alaska DHSS, and implement security measures sufficient to mitigate those risks and vulnerabilities to a reasonable and appropriate level.
- Engage an independent individual or entity to monitor and review Alaska DHSS's compliance with the Corrective Action Plan. The monitor must conduct quarterly progress meetings with Alaska DHSS officials and workforce members and provide a quarterly report to HHS for a period of three years.
- Prepare and file an initial implementation report and annual reports tracking compliance with the Corrective Action Plan for three years.

In the press release announcing this enforcement action, OCR Director Leon Rodriguez was quoted as saying that "covered entities must perform a full and comprehensive risk assessment and have in place meaningful access controls to safeguard hardware and portable devices." He also indicated that OCR expects organizations to comply with their HIPAA privacy and security obligations regardless of

THIS IS AN ADVERTISEMENT
© 2002-2024. Hall, Render, Killian, Heath & Lyman, P.C. All Rights Reserved.

whether they are private or public entities. In light of this development, covered entities of all types should take the necessary steps to ensure that their HIPAA compliance programs are effective, including:

- Conducting a risk assessment to determine where vulnerabilities exist in current practices and systems, paying close attention to portable electronic devices;
- Reviewing policies and procedures affecting privacy and security to ensure that they are thorough and complete;
- Actively monitoring compliance, particularly when there is a material change in processes, personnel or functions;
- Consistently enforcing policies and procedures when conduct occurs that is in violation of them; and
- Considering the use of encryption for all media and devices that store, transmit or maintain protected health information.

More information on this enforcement action, including the Resolution Agreement and the HHS press release, is available here.

Hall Render's HIPAA Impact Series has provided in-depth analysis of HIPAA issues and developments since the passage of HITECH. Our HIPAA Impact Series may be accessed at www.hallrender.com/impact.

If you need additional information about HIPAA/HITECH, please contact Mark Swearingen at 317.977.1458 or mswearingen@hallrender.com or your regular Hall Render attorney.

THIS IS AN ADVERTISEMENT
© 2002-2024. Hall, Render, Killian, Heath & Lyman, P.C. All Rights Reserved.