FIRST THREE HIPAA ENFORCEMENT ACTIONS OF 2017

In continuation of its active beginning to the new year, the Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") announced on February 1, 2017, that it imposed a HIPAA civil money penalty of $3.2 million on a Texas medical center ("Medical Center"). OCR issued the penalty for wrongful disclosure of unsecured electronic protected health information ("ePHI") and for extended non-compliance with HIPAA requirements.

The Medical Center filed breach notification reports with OCR following incidents in 2009 and 2013 that affected the ePHI of thousands of individuals. Specifically, the breaches stemmed from the loss of an unencrypted, non-password protected personal device and the theft of an unencrypted laptop from a Medical Center location. OCR's investigation determined that the Medical Center failed to implement risk management plans and to utilize encryption or a comparable security measure on its devices. In addition, OCR found that the Medical Center was aware of its security and privacy deficiencies, as they had been previously identified by third-party assessments, yet did not implement critical recommendations to ensure the confidentiality and protection of ePHI.

The penalty paid by the Medical Center follows two HIPAA settlements announced by OCR this year. On January 18, 2017, OCR announced a settlement of $2.2 million with a Puerto Rico insurance company ("Insurer") for potential non-compliance with the HIPAA Privacy and Security Rules. The Insurer reported a breach of ePHI resulting from the theft of a USB storage device from the Insurer's IT department, which did not have sufficient safeguards in place. OCR determined that the Insurer failed to perform a risk analysis, implement risk management strategies and utilize encryption or a similar alternative on its devices containing PHI, which is similar to OCR's findings in the Medical Center case.

On January 9, 2017, OCR announced its first-ever HIPAA settlement based on a lack of timely breach notification under HIPAA's Breach Notification Rule.

PRACTICAL TAKEAWAYS

These recent enforcement actions exhibit OCR's continued emphasis on covered entities' obligations under the HIPAA Privacy, Security and Breach Notification Rules. In particular, covered entities should consider the following with respect to their HIPAA compliance efforts.

- It is critical to not only identify potential security gaps in mobile devices, laptops and storage devices but to implement corrective remedies in a timely manner. In determining the amount of a HIPAA enforcement action penalty, OCR may consider the length of time that a known compliance deficiency remained uncorrected.
- It is critical to ensure breach notification is made without undue delay and no more than 60 days from the date a breach is discovered. Remember that large breaches (affecting 500 or more individuals) must be reported to individuals, the media and OCR within 60 days. Small breaches (under 500 individuals) must be reported to individuals within 60 days and to OCR by March 1 of the following calendar year.

Additional information on these enforcement actions is available at the HHS website.

If you have any questions, please contact:

- Elizabeth Callahan-Morris at (248) 457-7854 or ecallahan@hallrender.com;
- John Weber at (248) 457-7816 or jweber@hallrender.com; or
- Your regular Hall Render attorney.

Please visit the Hall Render Blog at http://www.hallrender.com/resources/blog/ or click here to sign up to receive Hall Render alerts on topics related to health care law.