OCR ANNOUNCES FINE FOR LACK OF BAA AND FAILURE TO TERMINATE FORMER EMPLOYEE'S ACCESS TO PHI

On December 11, 2018, the Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") announced that a critical access hospital in Colorado (the "Hospital") will settle potential violations of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") by paying a civil penalty of $111,400 and adopting a corrective action plan.

The alleged violations of HIPAA arose from two impermissible disclosures of protected health information ("PHI") of 557 individuals. The first was the impermissible disclosure of such PHI to Google, who was acting as a business associate of the Hospital. OCR indicated that the disclosure was impermissible because there were no satisfactory written assurances from Google in the form of a business associate agreement ("BAA"). The second impermissible disclosure of PHI was to a former employee for approximately two months. The Hospital failed to deactivate the former employee's username and password to its web-based calendar, which contained PHI, upon termination of employment.

Covered entities are required to enter into BAAs with their business associates to receive satisfactory assurances that the business associate will safeguard PHI in accordance with HIPAA. Additionally, once an individual is no longer in a role that requires access to PHI or has been terminated, access to PHI should be immediately terminated. In commenting on this settlement, OCR Director Roger Severino emphasized the importance of covered entities being aware of who has access to PHI and who does not.

PRACTICAL TAKEAWAYS

This settlement highlights the importance of the following:

- Covered entities must have processes in place to immediately shut off a terminated employee's access to PHI and electronic PHI ("ePHI"). This may require coordination of efforts between human resources and information technology departments.
- Covered entities must have a process in place to determine whether a BAA is needed and ensure written BAAs are completed for all identified business associate arrangements.
- Covered entities should evaluate workers' access to ePHI by role – if an individual does not need ePHI to perform their job duties or functions, then no access to ePHI should be granted.

For further information about privacy and security compliance and data breach response, please contact:

- Charise R. Frazier at cfrazier@hallrender.com or 317-977-1406;
- Patricia E. Connelly at pconnelly@hallrender.com or 317-429-3654;
- Stephen D. Rose at srose@hallrender.com or 425.278.9337; or
- Your regular Hall Render attorney.