FEBRUARY 19, 2019

REPEATED BREACHES OF EPHI RESULT IN A $3 MILLION FINE, CAPPING OFF OCR'S "RECORD YEAR" OF 2018 ENFORCEMENT ACTIONS

The Office for Civil Rights ("OCR") announced that a health system in California (the "System") was required to pay a $3 million fine and adopt an extensive corrective action plan to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The System operates several hospitals, including a rehabilitation hospital in California.

DETAILED ANALYSIS

The System reported to OCR two breaches of unsecured electronic protected health information ("ePHI") that affected over 60,000 individuals. One breach occurred in December 2013 and impacted approximately 50,197 individuals, and the other occurred in December of 2015 and impacted about 11,608 individuals.

The removal of server protections by a System contractor led to the first breach, where protected health information ("PHI") was available to anyone who could access the System's server who could also download files – even if they did not have a username and password.

PHI was accessible on the internet again due to an employee activating the incorrect website on a SQL server. This led to the second breach.

The resolution agreement indicated that the System failed to comply with the HIPAA Security Rule by not conducting an analysis of the potential risks to ePHI, not implementing sufficient security measures to reduce risks and vulnerabilities to a reasonable and appropriate level and not performing a technical evaluation after a contractor installed the Windows Operating System. The System also failed to enter into a business associate agreement that contained satisfactory assurances that the contractor would appropriately safeguard ePHI maintained on behalf of the System.

Additionally, in this announcement, OCR stated that 2018 was a "record year" for enforcing HIPAA. Ten cases were settled by OCR and an Administrative Law Judge granted summary judgment on a case as well. Included in this settlement figure was an American health insurance company settlement, which resulted in a $16 million fine, the largest fine yet. These 2018 enforcement actions resulted in $28.7 million in fines, a 22 percent increase from the earlier record year of $23.5 million in 2016.

Importantly, the potential financial impact of HIPAA noncompliance on covered entities and business associates is not limited to fines from OCR. These record figures do not include the costs covered entities and business associates incur when required to respond to an OCR investigation that does not result in direct fines and penalties.

PRACTICAL TAKEAWAYS

The increasing demands on technology infrastructure and capabilities as well as the accompanying demands on information technology staff have created a complex environment to manage for entitities that must comply with HIPAA. Entities subject to HIPAA should:

- Recognize the importance of a robust HIPAA compliance plan that is regularly reviewed and updated by all relevant internal parties;
- Ensure that sufficient resources are allocated to implement adequate security measures to address identified risks and vulnerabilities;
- Establish processes to regularly conduct system reviews for all systems and applications that maintain ePHI to reduce the chance that human error results in such a significant breach of ePHI; and
- Ensure that those responsible for contracting and procurement are fully apprised of the nature and scope of services a particular vendor is providing and that they work with information technology staff and business partners to properly address regulatory obligations, like business associate agreements.

For further information about HIPAA and security compliance, please contact:

- Charise R. Frazier at cfrazier@hallrender.com or 317-977-1406;

- Patricia E. Connelly at pconnelly@hallrender.com or 317-429-3654; or
- Your regular Hall Render attorney.

Hall Render has launched its Breach Response Hotline, a 24/7 resource for consultation if a breach is suspected. Call us at 1-833-BREACH8.