PUBLICLY AVAILABLE EPHI LEADS TO $1.6 MILLION FINE

On November 7, 2019, the Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") announced that a Texas state agency ("State Agency") will pay a penalty of $1,600,000 for violations of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule and Security Rule.

According to the Notice of Proposed Determination, the State Agency notified OCR of a breach in June 2015, stating that electronic protected health information ("ePHI"), including names, addresses, social security numbers and treatment information, of 6,617 individuals was available on the internet. The State Agency identified a security vulnerability in a web application that was designed to collect and report utilization management review activities to the Centers for Medicare & Medicaid Services. This vulnerability occurred when the State Agency placed the web application on the State Agency's public server where credentials to access or review the ePHI were not required. The web application had previously been on a private secure server. The State Agency identified this breach after they were notified by an unauthorized user who was able to access the ePHI and was not required to use credentials for such access. The State Agency said that it had never performed a security risk analysis that was agency-wide, although it had performed certain risk assessment activities on an ad hoc basis.

In analyzing mitigating factors to determine the penalty, OCR did note that there were no *known* harms to patients, including physical, financial or reputational harms or inability to obtain health care services. The State Agency also acted quickly to remove the web application upon receiving the report that ePHI was publicly accessible.

PRACTICAL TAKEAWAYS

Covered entities and business associates should take note of the following in light of this civil monetary penalty:

- OCR expects both private and governmental covered entities to implement effective HIPAA compliance programs.
- This is the third OCR enforcement action in the past several weeks where OCR has cited the lack of an organizational-wide risk analysis as grounds for a HIPAA penalty. Not only is a risk analysis required by HIPAA, it is a cybersecurity best practice. Solely focusing on mitigating the risks to only certain components of technical infrastructure will not satisfy HIPAA's risk analysis requirements. All aspects of the organization must be evaluated for compliance.
- The fines included penalties for impermissible disclosures and lack of adequate access and audit controls. Under the HIPAA Security Rule, access controls and audit controls allow a covered entity or business associate to properly safeguard ePHI. Failure to comply with the HIPAA Security Rule requirements can lead to breaches of ePHI and result in violations of both the Privacy and Security Rule.

If you have any questions or would like additional information about this topic, please contact:

- Charise Frazier at (317) 977-1406 or cfrazier@hallrender.com;
- Patricia Connelly at (317) 429-3654 or pconnelly@hallrender.com; or
- Your regular Hall Render attorney.

For more information on Hall Render's HIPAA, Privacy & Security services, click here.