LARGEST HEALTH DATA BREACH = LARGEST OCR SETTLEMENT IN HISTORY

On October 15, 2018, the Department of Health and Human Services (“HHS”), Office for Civil Rights ("OCR") announced that it had reached a record $16 million settlement with Anthem arising out of alleged violations of the Privacy and Security Rules under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The settlement comes after an OCR investigation into Anthem's 2015 breach of unsecured electronic protected health information ("ePHI") of nearly 79 million individuals, which still stands today as the largest health data breach in history. The penalty is nearly three times the largest HIPAA fine to date. However, the fine represents less than one percent of Anthem’s operating revenue.

OCR Director Roger Severino, at the joint OCR/NIST Safeguarding Health Information: Building Assurance through HIPAA Security conference on October 18, 2018 in Washington, D.C., commented that the Anthem case was an example of the "big, juicy enforcement" actions OCR is seeking to pursue, although the ultimate goal of OCR is to bring down the number of enforcement actions by supporting the industry's compliance efforts.

The 2015 breach occurred when a workforce member at an Anthem subsidiary responded to a malicious phishing email that allowed cyber attackers to gain undetected access to the Anthem IT system for nearly two months. Before the attackers' presence was discovered, they were able to steal the ePHI of almost 78.8 million individuals, including names, social security numbers, medical identification numbers, addresses, dates of birth, email addresses and employment information. OCR investigated the breach and concluded that Anthem had failed to conduct an enterprise-wide risk analysis, lacked sufficient procedures to regularly review information system activity, failed to identify and respond to suspected or known security incidents and failed to implement adequate minimum access controls to prevent the cyber attackers from accessing ePHI.

To resolve the enforcement action, HHS and Anthem entered into a Resolution Agreement for $16 million and a two-year "robust" Corrective Action Plan. Under the Corrective Action Plan, Anthem must, among other requirements, conduct a risk analysis and revise and distribute certain policies and procedures related to information system activity review and access controls.

PRACTICAL TAKEAWAYS

This settlement is a good reminder for covered entities and business associates to take steps to mitigate the risk of a successful cyber attack, including:

- Conducting an enterprise-wide risk analysis to determine where vulnerabilities exist in current practices and systems;
- Timely remediating vulnerabilities that are identified in the risk analysis;
- Training workforce members to be alert to potential phishing emails;
- Implementing technical safeguards against phishing attacks such as multi-factor authentication;
- Routinely patching and updating software and systems; and
- Being prepared to respond to cyber-attacks.

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

For information regarding the annual OCR/NIST Safeguarding Health Information: Building Assurance through HIPAA Security conference, click here.

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

- Mark Swearingen at (317) 977-1458 or mswearingen@hallrender.com;
- Elizabeth Callahan-Morris at (248) 457-7854 or ecallahan@hallrender.com;

- Patricia Connelly at (317) 429-3654 or pconnelly@hallrender.com; 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.