Health Law Alert: The Record $16 Million Data Breach Settlement and How You Can Avoid Similar Outcomes

October 24, 2018

On October 15, 2018, Anthem agreed to pay $16 million to the Office of Civil Rights (OCR) following one of the largest data breaches in history that exposed the electronic protected health information (ePHI) of nearly 79 million people. The settlement far surpasses the previous high of $5.55 million paid by Advocate Health Care Network in 2016.

OCR highlighted that this record-breaking settlement is in large part due to Anthem's failure to conduct and implement an enterprise-wide risk analysis—sending a warning to other organizations, large and small. The good news is OCR just updated its Risk Assessment Tool, which can be used by organizations to assist in reviewing implementation of the HIPAA Security Rule. The update adds additional functionality and makes the tool more user friendly. It also continues a trend in which OCR publishes helpful material that covered entities and business associates can use to assist with their own compliance efforts. The trade-off, however, is that the materials OCR has made available may mean the agency will be less receptive to arguments that a provider is too small, or lacks the necessary resources, to comply with HIPAA's many requirements.

All of this takes place against the backdrop of surprisingly negative results from the OCR Audit Program. The Audit Program found, for example, that 83% of audited entities did not perform an appropriate Security Rule risk assessment. Clearly, the stakes on assessing and managing risks under the Security Rule have increased dramatically.

The Record Setting Settlement

On January 29, 2015, Anthem, an independent licensee of the Blue Cross and Blue Shield association, discovered cyber-attackers had gained access to their IT system via an undetected continuous and targeted cyberattack for the apparent purpose of extracting data. Anthem filed a breach report with OCR on March 13, 2015, and then discovered that cyber-attackers had infiltrated their system through phishing emails. An email was sent to employees of an Anthem subsidiary, and at least one employee responded to the malicious email and opened the door to further attacks. The cyber-attackers gained access to names, social security numbers, medical identification numbers, addresses, dates of birth, email addresses, and employment information.

OCR stated that Anthem failed to implement appropriate measures for detecting cyberattacks, noting that organizations "are expected to have strong password policies and to monitor and respond to security incidents in a timely fashion or risk enforcement by OCR." In addition, OCR commented that one of the aggravating factors leading up to the record settlement is that Anthem failed to conduct an enterprise-wide risk analysis.

What You Can Do

On October 16, 2018, the day after reaching the record data breach settlement, the Office of the National Coordinator for Health Information Technology (ONC) and OCR provided an update to the popular Security Risk Assessment (SRA) Tool, which is often used as part of an enterprise-wide risk assessment. The SRA Tool is a software application that a health care provider can use, along with other tools and processes, to assist in reviewing its implementation of the HIPAA Security Rule. The update adds additional functionality and makes the tool more user friendly.

Now is the time to perform (or update) a HIPAA Security Risk Assessment for your organization. The SRA Tool is available at no cost and can be used with several operating systems, including Microsoft Windows for desktop and laptop computers, as well as Apple iOS for iPad. Once the program is downloaded, you will be prompted to answer questions and provide information that will be the basis for the assessment and scoring. While the assessment provided by the SRA Tool is not a guarantee of HIPAA compliance, the assessment does offer helpful guidance for covered entities and business associates to help them identify risks and vulnerabilities to ePHI.

Specifically, new features of the SRA Tools include:

- Enhanced user interface
- Modular workflow with question branching logic
- Custom assessment logic
- Progress tracking
- Improved threats and vulnerabilities rating

- Detailed reports
- Business associate and asset tracking
- Overall improvement of the user experience

The Windows version of the tool can be found at www.HealthIT.gov/security-risk-assessment and the previous iOS version is available at the Apple App Store (the newest version is not yet available on iOS).

The publication of the new SRA Tool continues a trend by which OCR has been publishing guidance on HIPAA compliance for providers, health plans, and business associates to use in structuring and monitoring their own operations. For example, OCR has published guidance on cloud computing, methods of de-identification, application of HIPAA to mental health and substance use disorders, mobile devices, accessing ePHI remotely, and guarding against ransomware. While all of these materials help covered entities and business associates understand their compliance obligations, the trade-off is that OCR and state attorneys general may assert that regulated parties have little excuse for failing to comply.

If you have questions about conducting a HIPAA Security Risk Assessment or general health care enforcement, please contact Jesse Berg (jesse.berg@lathropgpm.com or 612.632.3374), Tony Fricano (antonio.fricano@lathropgpm.com or 612.632.3236), or Julia Reiland (julia.reiland@lathropgpm.com or 612.632.3280).