SHUMAKER
Shumaker, Loop & Kendrick, LLP

Client Alert

Business Information for
Clients and Friends of
Shumaker, Loop & Kendrick, LLP

August 9, 2016

The Government Enters into Largest HIPAA Settlement to Date; What HIPAA Covered Entities and Business Associates Need to Know

Kelly A. Leahy, Partner | kleahy@slk-law.com | 614.628.6815

Advocate Health Care Network, which operates 12 hospitals and more than 200 other treatment centers in Chicago and central Illinois, has agreed to the largest settlement to date with the Office for Civil Rights ("**OCR**") for multiple potential violations of the Health Insurance Portability and Accountability Act ("**HIPAA**"). Advocate will pay $5.5 million and adopt a multi-year corrective action plan that stemmed from three incidents reported to OCR in 2013. The breaches involved Advocate's medical group subsidiary, Advocate Medical Group ("**AMG**"), which employs more than 1,000 physicians. In the first incident, four unencrypted desktop computers containing the electronic Protected Health Information ("**ePHI**") of approximately four million patients were stolen from an AMG administrative office. The computers were password protected but not encrypted. In the second incident, Advocate reported that the ePHI of approximately 2,000 AMG patients was compromised when an unauthorized third party accessed the computer network of an AMG billing services consultant. AMG did not have a business associate agreement with the billing services company. The third incident Advocate reported involved the theft of an unencrypted laptop which was stolen from the unlocked car of an Advocate employee and put the ePHI of approximately 2,200 patients at risk. Patient names, addresses, dates of birth, credit card numbers with expiration dates as well as demographic, clinical and health insurance information were contained in the patient records that were compromised in the three incidents.

As we mentioned in our recent Client Alert addressing OCR's first settlement agreement with a business associate http://www.slk-law.com/NewsEvents/Publications?find=145622, there are a growing number of HIPAA enforcement actions, many of them related to security of ePHI. In the Advocate resolution agreement OCR found that Advocate:

1. Failed to conduct an accurate and thorough risk analysis that covered all of its facilities, IT equipment, applications and data systems using ePHI;
2. Failed to implement policies and procedures to limit physical access to its electronic information systems housed in the administrative office from which the desktop computers were stolen;
3. Failed to reasonably safeguard the ePHI of nearly 4 million patients;
4. Failed to execute a business associate agreement with its billing services company;
5. Impermissibly disclosed the ePHI of approximately 2,000 individuals in the absence of a business associate agreement; and
6. Failed to reasonably safeguard the ePHI of approximately 2,200 patients when an AMG employee left an unencrypted laptop in an unlocked vehicle overnight.

The resolution agreement requires Advocate to:

1. Conduct a comprehensive and thorough risk analysis of the potential risks and vulnerabilities of the ePHI maintained by Advocate;
2. Develop and implement an enterprise-wide risk management plan to address and mitigate any security risks and vulnerabilities found in the risk analysis;
3. Implement a written process to regularly evaluate any environmental or operational changes that affect the security of Advocate's ePHI;
4. Develop an encryption report of the total number of devices and equipment that may be used to access, store, download or transmit Advocate ePHI;
5. Review and revise policies and procedures on device and media controls, facility access controls and business associates; and
6. Develop enhanced privacy and security awareness training.

OCR Director Jocelyn Samuels stated, "We hope this settlement sends a strong message to covered entities that they must engage in a comprehensive risk analysis and risk management to ensure that individuals' ePHI is secure. This includes implementing physical, technical, and administrative security measures sufficient to reduce the risks to ePHI in all physical locations and on all portable devices to a reasonable and appropriate level."

The Advocate resolution agreement follows two other significant July, 2016 settlements between OCR and covered entities. In a $2.7 million settlement with Oregon Health & Sciences University ("**OHSU**") the hospital was cited for widespread HIPAA vulnerabilities after it made multiple breach reports to OCR in 2013. One involved the theft of an unencrypted laptop stolen during a burglary at a surgeon's vacation home. The patient ePHI was located in the email system which was used to share daily surgery schedules with surgeons scheduled to operate in the OHSU operating rooms. Another breach report involved medical residents' use of Google Drive and Google Mail. The residents created spreadsheets of patients to provide up-to-date information about who was admitted to the hospital over a 2.5 year period. OHSU did not have a business associate agreement in place with Google for its cloud-based services. Although OHSU performed risk analyses in 2003, 2005, 2006, 2010 and 2013, OCR found they were not enterprise-wide and that OHSU failed to timely implement measures to address documented risks. In addition to the civil monetary penalty, OHSU entered into a three-year corrective action plan.

The University of Mississippi, on behalf of the University of Mississippi Medical Center ("**UMMC**"), also entered into a settlement with OCR in July, 2016 that included a $2.75 million civil monetary penalty and a three-year corrective action plan. In 2013, UMMC reported a breach of unsecured ePHI affecting approximately 10,000 individuals resulting from a laptop that went missing from UMMC's Medical Intensive Care Unit ("**MICU**") and which was believed to have been stolen by a visitor to the MICU. OCR's investigation revealed that although UMMC notified OCR and the media of the breach, it failed to notify each individual whose ePHI was compromised. Additionally, OCR found that from the April 20, 2005 compliance date of the HIPAA Security Rule, UMMC failed to assign a unique user name and/or number for identifying and tracking user identity in information systems containing ePHI, allowing workforce members to access ePHI through a generic account and preventing UMMC from tracking which users were accessing ePHI. OCR also determined that UMMC failed to implement its policies and procedures and was aware of risks and vulnerabilities in its systems; however, no risk management activity occurred until after the breach due largely to organizational deficiencies and insufficient institutional oversight.

In light of the growing number of recent enforcement actions by OCR here's what covered entities and business associates can do to prevent costly fines and burdensome settlements:

1. Take steps to perform a comprehensive and thorough assessment of systems and facilities on an enterprise-wide basis.
2. Take reasonable and appropriate actions to address deficiencies on a timely basis.
3. Perform an audit to ensure a business associate agreement is in place with all relevant persons and entities that have access to PHI in provision of their services.
4. Enhance privacy and security training and education and include the full range of members of the workforce as well as the medical staff and medical residents.
5. Regularly evaluate operational or environmental changes which may affect security of ePHI.
6. Update and implement HIPAA privacy and security policies and procedures as needed.

If we can assist you or if you have questions, please contact Kelly Leahy at (614) 628-6815 or kleahy@slk-law.com.