SHUMAKER
Shumaker, Loop & Kendrick, LLP

Client Alert

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

July 20, 2016


Aebel


Leahy

The Government Makes a Business Associate Pay:
What HIPAA Covered Entities and Business Associates Can Learn from this Settlement

Erin Smith Aebel, Partner | eaebel@slk-law.com | 813.227.2357
Kelly A. Leahy, Partner | kleahy@slk-law.com | 614.628.6815

The government has entered into its first settlement with a HIPAA business associate, including a $650,000.00 monetary penalty, ushering in a new period of enforcement for third parties who use Protected Health Information ("PHI") in providing services to providers and some payers. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") security rule regulations are designed to protect the confidentiality, integrity and security of electronic Protected Health Information ("ePHI"). Most providers, some payers and health care clearinghouses are required to comply with HIPAA. These groups are referred to as "covered entities" under the HIPAA rules. A business associate is a third party that performs activities or services on behalf of a covered entity and who receives, transmits, accesses or uses PHI for those activities or services. Business associates can be a variety of entities or individuals such as a third party billing company or a lawyer who needs to review patient records in order to provide legal services to a provider. Providers and other covered entities must have a contract with their business associates with certain required terms that ensure that the business associate protects the PHI. As of 2013, business associates also are directly liable to the government for compliance with certain HIPAA requirements including the security rule requirements for ePHI.

The Office for Civil Rights ("OCR") is the federal government agency charged with reviewing and investigating complaints and issuing penalties and other remedies to covered entities and their business associates. In 2013 individuals became able to submit complaints to the OCR for violations of HIPAA by business associates. Since 2009 when the OCR began keeping records of data breaches affecting 500 or more individuals, approximately 20% involved business associates. The first OCR complaint that resulted in penalties against a business associate was just announced this month.

The Catholic Health Care Services of the Archdiocese of Philadelphia ("CHCS") agreed to settle potential HIPAA violations of the Security Rule after the theft of a mobile device compromised PHI of hundreds of nursing home residents, including Social Security numbers and patient diagnosis and treatment information. CHCS was a HIPAA business associate because it provided management and information technology services to six nursing homes. The security breach resulted from the theft of a single iPhone that was unencrypted and was not password protected. As the OCR investigated the incident they found that CHCS had not performed a HIPAA security rule risk assessment and had no policies addressing the removal of mobile devices containing PHI from a facility or what to do in the event of a security incident. In addition to the monetary penalty, the OCR required CHCS to enter into a corrective action plan under which CHCS's HIPAA compliance will be monitored for two years. In announcing the settlement, the OCR stated "business associates must implement the protections of the HIPAA Security Rule for the ePHI they create, receive, maintain or transmit from covered entities." See the Resolution Agreement and Corrective Action Plan at www.hhs.gov/sites/default/files/chcs-racap-final.pdf.

Here is what covered entities and business associates can take away from this settlement:

Assess Readiness for a Security Incident

Business associates and covered entities should assess their readiness for a security incident. They can begin to do so by asking themselves these questions:

1. Do you have an individual assigned as a security official?
2. Do you have procedures for granting access to ePHI and are they being followed?
3. Have you performed an enterprise wide security risk assessment? Ask to see your business associates' or subcontractors' results. Inquire when the last one was performed and how often they are performed.
4. Have you implemented a security risk management plan? Ask your business associates or subcontractors to describe their physical, technical and administrative safeguards for PHI.
5. Are your HIPAA policies and procedures current? Ask your business associates or subcontractors when they last updated theirs. How do they communicate changes in policies and procedures?
6. How do you respond to security incidents? Ask your business associates or subcontractors how many security incidents they have had and to describe how they responded to them.
7. Do you have policies and procedures addressing removal of mobile devices from the facility to safeguard PHI taken off-site? Ask your business associates or subcontractors if they have had a laptop, jump drive, cell phone or other mobile device containing PHI lost or stolen and how they responded to it.
8. Have you conducted security training for your workforce? Ask your business associates or subcontractors when and how often they conduct security training.

Consider Implementing OCR's May 3, 2016 Recommendations

The OCR has been signaling to the industry for some time that business associates are in its crosshairs. It has done this through increased enforcement activity against covered entities that do not have agreements in place with business associates as well as communications to covered entities such as its May 3, 2016 email containing specific recommendations for covered entities. See OCR's Cyber-Awareness April 2016 Update at www.hhs.gov/sites/default/files/hipaa-cyber-awareness-monthly-issue-4.pdf. The OCR's recommendations include:

1. Define in the service agreement or business associate agreement how and for what purpose PHI can be used or disclosed so that any use or disclosure that is not provided for can be reported to you – including breaches of unsecured PHI as well as security incidents.
2. Specify in the service agreement or business associate agreement the timeframe that business associates or their subcontractors are required to report a breach, security incident or cyberattack to the covered entity or business associate as applicable.
3. Specify in the service agreement or business associate agreement the type of information that would be required to be reported by the business associate or subcontractor in a security or incident report. The report should include:
    - Business associate name and point of contact.
    - Description of what happened including the date of the incident and date of discovery of the incident.
    - Description of the types of unsecured PHI that were involved in the incident.
    - Description of what the business associate is doing to investigate the incident and to protect against further incidents.
4. Train workforce members on incident reporting and consider conducting audits to evaluate business associates' or subcontractors' security and privacy practices.

The OCR is enforcing its rules on an aggressive and expanded basis so business associates and covered entities need to focus on prevention now to prevent costly fines and burdensome settlements.

If you have questions, please contact Erin Aebel at (813) 227-2357 or eaebel@slk-law.com or Kelly Leahy at (614) 628-6815 or kleahy@slk-law.com.

Shumaker, Loop & Kendrick, LLP is a 90 year old law firm with offices in Ohio, Florida and North Carolina. It provides full service business law advice and has a robust health care industry team.