Business Associate Settles HIPAA Investigation for $650,000

July 6, 2016

The U.S. Office for Civil Rights (OCR), the agency responsible for enforcing the HIPAA Privacy and Security rules, has just sent a strong message that business associates are not immune from scrutiny. On June 24, 2016, in a settlement that is the first of its kind, Catholic Health Care Services of the Archdiocese of Philadelphia ("CHCS") agreed to pay $650,000 and enter into a corrective action plan to resolve alleged violations of its obligations under the HIPAA Privacy and Security Rules.

This settlement culminates the indications of increased business associate liability that OCR has made since the Omnibus HIPAA Regulations went into effect on September 23, 2013. In March and April of 2016, OCR entered into two separate settlement agreements with covered entities that involved failure to obtain required business associate agreements. In May 2016, business associates and covered entities began receiving the pre-audit questionnaires for Phase 2 of OCR's HIPAA Audit Program. On June 24, 2016, OCR entered into this first settlement agreement with a business associate.

CHCS, the business associate involved in the settlement, is a management and information technology services vendor for skilled nursing facilities. In February 2014, a CHCS employee lost a company-issued iPhone containing social security numbers, diagnosis and treatment information, medical procedures, and other demographic information of patients of six skilled nursing facilities. The iPhone was not encrypted or password protected. Each of the six nursing homes notified OCR of the breach, which affected a total of 412 patients.

Notably, OCR's investigation of CHCS indicated that CHCS had not implemented HIPAA policies and procedures, and had not performed a HIPAA security risk assessment. Related to the absence of a risk assessment, OCR determined that CHCS had not implemented reasonable and appropriate safeguards to protect electronic protected health information, including information stored on mobile devices. CHCS does not admit liability in the settlement but has agreed to pay $650,000 and submit to a two-year corrective action plan.

The facts and settlement terms of this agreement are not unique but should serve as a warning to all business associates that HIPAA obligations must be taken seriously. All business associates should be performing enterprise-wide risk assessments and implementing appropriate security measures including,

but not limited to, policies and procedures to maintain the privacy and security of protected health information.

For questions regarding HIPAA compliance obligations of business associates and covered entities, contact your Lathrop Gage attorney or the attorneys listed above.

For more information regarding data privacy and security, save the date for our upcoming Data Privacy and Security Seminar, scheduled for August 23, 2016 in our Kansas City office.