PLEWS SHADLEY RACHER & BRAUN LLP
ATTORNEYS AT LAW

October 9, 2015

Client Alert

OIG Increases HIPAA Enforcement

By: Shelley M. Jackson and Ashley N. Osak

Recent actions by the Department of Health and Human Services Office of the Inspector General ("OIG") reflect heightened scrutiny and enforcement activity relating to HIPAA privacy and security matters. This is noteworthy because most HIPAA compliance oversight is delegated to the Office of Civil Rights ("OCR"). The OIG has responsibility and resources for audits, investigations and enforcement on a range of health care matters, so it is giving notice of its expanding role in this area. As discussed below, this has immediate implications for Indiana health care providers and business associates.

On September 29, 2015 the OIG released two reports discussing the need for the OCR to increase its health privacy and data breach enforcement efforts. The reports detail deficiencies in OCR enforcement efforts and suggest improvement opportunities for oversight. The reports were created because the OIG believes that "covered entities such as doctors, pharmacies, and health insurance companies … do not adequately safeguard patients' protected health information, [which] could expose patients to an invasion of privacy, fraud, identity theft, and/or other harm." The two reports can be found here: OCR Should Strengthen Its Oversight of Covered Entities' Compliance with the HIPAA Privacy Standards and OCR Should Strengthen Its Followup of Breaches of Patient Health Information Reported by Covered Entities.

The OIG reports coincide with a settlement with Indiana-based Cancer Care Group, P.C. ("CCG") in connection with alleged breaches of certain HIPAA Rules relating to security of electronically stored protected health information ("ePHI"). A full copy of the settlement agreement can be found here: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cancercare-

racap.pdf, and the HHS press release can be found here: http://www.hhs.gov/news/press/2015pres/09/20150902a.html.

The CCG matter arose from an incident occurring in July 2012 in which a laptop bag was stolen from an employee's unattended vehicle. In addition to the laptop, the bag contained unencrypted portable media, which contained ePHI for approximately 55,000 CCG clients. Upon CCG's report of the theft to HHS, an investigation ensued. Specifically, the investigation determined that:

- "… CCG failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by CCG[;]
- "… CCG failed to implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility[; and]
- "… CCG impermissibly disclosed the ePHI of approximately 55,000 individuals by providing access to the ePHI to an unauthorized individual … when it failed to safeguard unencrypted back-up tapes that were stolen from the unattended vehicle of one of its workforce members."
-

The settlement requires CCG to complete a corrective action plan and pay a fine of $750,000. Details of the plan are available at the above link. This settlement, in light of increased audit and enforcement activities, provides a strong reminder for business associates to be proactive in performing a thorough risk assessment and implementing strong policies and practices to reduce the likelihood of a breach.

If you have questions regarding this matter or steps to be taken as part of a HIPAA compliance program, please contact Shelley Jackson, Ashley Osak, or any of the healthcare attorneys at Plews Shadley Racher & Braun LLP.