CARLTON FIELDS

A New Era of HIPAA Enforcement

June 15, 2015

Traditionally, HIPAA enforcement is assigned to the Department of Health and Human Services' Office for Civil Rights (OCR). In November 2013, Health and Human Services' Office of Inspector General sharply criticized OCR's HIPAA enforcement efforts. OCR responded with swift action regarding providers' data protection responsibility. The first sign of a new HIPAA enforcement era came in late December 2013, when OCR levied the first fine against an entity for failing to implement policies to address a data breach. The fine was issued even though there was no evidence that any individuals were harmed (or even that any patient files were accessed). Further evidence of this new era in provider enforcement came in April 2014 when Concentra Health Services agreed to a $1.7 million fine and a corrective action plan following the theft of a unencrypted laptop from a Missouri physical therapy center. Also in April 2014, QCA Health Plan, Inc. agreed to pay a $250,000 fine and a corrective action plan after an unencrypted laptop was stolen from an employee's car. Parkview Health Systems settled a rare low-tech HIPAA breach case in June 2014, agreeing to pay $800,000 in fines and to institute a corrective action plan. In June 2009, Parkview employees delivered 71 boxes of patient files to the home of a retiring physician. Knowing that the physician was not at home, the employees left the boxes in the physician's driveway. OCR noted that the boxes were left "unattended and accessible … within 20 feet of a public road and a short distance away from a heavily trafficked public shopping venue." May 2014 brought the largest HIPAA settlement to date. New York-Presbyterian Hospital and Columbia University collectively agreed to pay $4.8 million. The underlying breach occurred when the deactivation of a server by an individual physician, along with a lack of technical safeguards, allowed patients' electronic protected health information to be accessible through public Internet search engines. During OCR's investigation, the agency learned that neither the hospital nor Columbia University had undertaken any risk analysis or verified the server's security. OCR described the case against the joint entities as a means to "remind health care organizations of the need to make data security central to how they manage their information systems." The entities also agreed to a corrective action plan. In addition to taking stronger HIPAA enforcement actions, OCR has begun to refer HIPAA breaches for criminal prosecutions. Historically, criminal enforcement of HIPAA violations was rare. In one such prosecution, *United States v. Joshua Hippler*, Hippler allegedly obtained private health information with the intent to sell, transfer, or use it for personal gain. In Hippler's case, the government did not allege inadvertent disclosure or failure to

secure data, but rather an intentional effort to profit from private and personal data. Hippler pleaded guilty in August 2014 and was sentenced to 18 months. OCR's aggressive enforcement of HIPAA security requirements is expected to continue into 2015. In June 2014, an OCR Chief Regional Counsel, Jerome Meites, warned at an American Bar Association conference that the previous 12 months' enforcement efforts, through which OCR collected more than $10 million in HIPAA fines, would "be low in comparison to what's coming." He said OCR intended to focus on "high impact cases" to send strong messages about the importance of data security. Meites observed that the failure to conduct a thorough risk analysis was a common thread in the cases OCR identified. Additionally, he noted that portable media have become a particular vulnerability for health care providers. In an August regulatory filing, Community Health Systems announced that it had been hacked by a group believed to be based in China. The hackers stole identification data for 4.5 million patients. It will be interesting to see how OCR approaches the case in 2015, and what Community Health Systems discloses in its public filings concerning the possible prosecution of this matter.

Related Practices

Health Care

Related Industries

Health Care