Report on Patient Privacy Volume 19, Number 2. February 28, 2019 Violate HIPAA, Go Straight to Jail? Not Always

By Theresa Defino

For years, the HHS Office for Civil Rights (OCR) has tried to walk the line between encouraging HIPAA covered entities and business associates to lawfully use and disclose protected health information (PHI) while taking enforcement actions when these activities cross the line.

Indeed, HHS recently published a request for information that solicits feedback on a variety of topics, including how the privacy and security rules might be revised to ensure a freer flow of PHI, particularly for treatment and to share with family members of patients (*RPP 1/19, p. 8*).

Appearing before Congress in 2013, then-OCR Director Leon Rodriguez testified that the agency has "never taken an enforcement action because a provider has decided, in the best interests of a patient, to disclose information to a third party" (*RPP 5/13, p. 1*).

But as some individuals who must comply with HIPAA have found out, OCR isn't the only enforcement agency on the block. The Department of Justice (DOJ) can, and does, bring both civil and criminal charges for "disclosure of identifiable health information" against both individuals and organizations.

The provisions for civil and criminal charges for HIPAA violations are found at U.S.C. § 1320d-5 and U S.C. § 1320d-6 (2000), respectively.

Civil penalties may reach $100 per violation, with a cap of $25,000 per calendar year for each violation. Criminal convictions range from $50,000 and/or one year in prison to $500,000 and 10 years in prison, with higher amounts imposed if the act was committed under false pretenses or "with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." Penalties are also based on federal sentencing guidelines.