$4.3 Million in Civil Monetary Penalties Awarded for Encryption Failures under HIPAA

June 29, 2018

An administrative law judge for HHS upheld an award of $4.3 million in civil monetary penalties (the ?ÃÂ£***Penalties***?ÃÂ¥) against a Texas-based healthcare provider for violations of the HIPAA privacy and security rules (the ?ÃÂ£***HIPAA Rules***?ÃÂ¥). The provider is a ?ÃÂ£covered entity?ÃÂ¥ under HIPAA (?ÃÂ£***CE***?ÃÂ¥), and the Penalties are the fourth largest ever awarded to the Office of Civil Rights (?ÃÂ£***OCR***?ÃÂ¥), the HHS agency that enforces the HIPAA Rules, by an administrative law judge or secured via a settlement for HIPAA violations. The Penalties stemmed from an OCR investigation of the CE in response to three separate HIPAA breach reports the CE filed with OCR during 2012 and 2013 involving the theft of an unencrypted laptop computer and the loss of two unencrypted thumb drives, which resulted in the impermissible disclosure of electronic protected health information (?ÃÂ£***EPHI***?ÃÂ¥) of over 33,500 individuals. OCR?ÃÃs investigation found that, although the CE had written encryption policies going as far back as 2006 and the CE?ÃÃs own risk analysis had concluded that the lack of device-level encryption posed a high risk to the security of EPHI, the CE did not begin to adopt an enterprise-wide solution to implement encryption of EPHI until 2011 and had not completed it as of January 2013. As a result of its findings, OCR requested the Penalties, calculated based on $2,000 per day for each day the CE failed to encrypt its electronic devices (for a total of approximately $1.3 million) and $1.5 million per year for 2012 and 2013 for the impermissible disclosure of EPHI (for a total of $3 million). The CE appealed OCR?ÃÃs determination, but the administrative law judge agreed with OCR?ÃÃs arguments and findings and upheld the imposition of the Penalties. This decision underscores the risks for HIPAA covered entities, including employer-sponsored group health plans, if they fail to comply with the HIPAA Rules.