The Price of Delaying HIPAA Compliance

Insights 02.09.17

The Office for Civil Rights of the Department of Health and Human Services announced a civil money penalty of $3.2 million against a Dallas hospital on February 1. The penalty stems from the loss in 2010 of an iPad with protected health information of 22 individuals, and the theft in 2013 of an unencrypted laptop with PHI of 2,462 individuals.

OCR's press release on this penalty is entitled, "Lack of timely action risks security and costs money." This case is unusual because OCR typically settles investigations before they reach the formal assessment of civil money penalties. Evidently attempts at informal settlement failed in this case. The assessment provides insight into how OCR calculates penalties for HIPAA violations.

HIPAA has a scale of penalties for non-compliance, starting at $100 for each violation if the offender did not know and could not reasonably have known of the violation. The next tier is for failures due to "reasonable cause," but not willful neglect; the penalty at this tier starts at $1,000 for each violation (and runs as high as $50,000 per violation). The highest penalties are for violations due to willful neglect – these begin at $10,000 for each violation. Penalties are capped at $1,500,000 per year for identical violations. OCR says that in 2007 and 2008 two consulting firms had conducted security reviews for the hospital, and had recommended encrypting laptops and other devices.

OCR determined that the appropriate penalty tier was reasonable cause – the middle tier. It imposed the minimum penalty for this tier of $1,000 per violation, because the lack of encryption did not result in any known physical, financial or reputational harm to anyone, nor did it hinder anyone's ability to obtain health care. OCR found that the hospital failed to comply with two requirements of the HIPAA security rule, and one of the privacy rule:

- It failed to implement encryption or an equivalent alternative measure until April 9, 2013
- It failed to implement appropriate device and media controls until it completed a full inventory of its information systems on November 9, 2012
- It impermissibly disclosed the PHI of 2,484 people.

For the security rule violations, OCR treated each day as a separate violation, beginning six years prior to the date of its notice of proposed penalties, and ending on the date the violation was remedied – $833,000 for the failure to implement encryption, and $688,000 for the failure to implement device and media controls. The penalty for the impermissible disclosures was $1,522,000. OCR treated the loss of each individual's data as a separate violation – $22,000 for the loss of the iPad, and $1,500,000 for the loss of the laptop (but for the annual cap, the fine here would have been $2,462,000).

This approach is evidently based on the HIPAA enforcement rule (45 CFR § 160.408), which allows OCR to determine the number of violations of a HIPAA provision based on the nature of the covered entity's or business associate's obligation to act or not act under the provision that is violated, such as its obligation to act in a certain manner, or within a certain time, or to act or not act with respect to certain persons. In the case of continuing violation of a provision, the rule says a separate violation occurs each day the covered entity or business associate is in violation of the provision.

Although OCR cites separate regulations, there is arguably some duplication in fining a hospital separately for failing to encrypt a laptop, and again for disclosing PHI when the laptop is stolen. Apparently, however, the hospital in this case did not fight the assessment. In its press release on this penalty, OCR emphasizes that the lack of timely action risks security and costs money. It certainly does, if each day of non-compliance makes for a new violation.

Hooper, Lundy & Bookman provides a range of legal services relating to health information privacy, security and technology. For more information, please contact: In San Francisco, Paul Smith or Steve Phillips at 415.875.8500 ; in Los Angeles, Hope Levy-Biehl at 310.551.8140; in Washington, D.C., Bob Roth at 202.580.7701; or in Boston, Amy Joseph at 617.532.2702.

RELATED CAPABILITIES

Health Information Privacy and Security