BNA, INC.

HEALTH IT LAW & INDUSTRY

BNA Employee-Owned Since 1947

VOL. 3, NO. 18 REPORT MAY 2, 2011

HHS Issues First-Ever Civil Monetary Penalty for HIPAA Privacy Rule Violation



DAVID THOMAS, GERARD M. STEGMAIER, AND WENDY LYNN DEVINE

A record civil penalty demonstrates the importance of protecting health patient privacy and responding appropriately to federal regulators. The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) recently assessed a $4.3 million civil monetary penalty against Cignet Health of Prince George's County, Md., for violations of the HIPAA[1] Privacy Rule.

This is the first fine assessed by the agency since the rule took effect in April 2003. The fine follows an investigation into events that occurred between September 2008 and October 2009 that, the OCR concluded, resulted in 41 separate violations of the HIPAA Privacy Rule.

David Thomas is a partner in Wilson Sonsini Goodrich & Rosati's Palo Alto, Calif., office, where he advises clients ranging from multinational corporations to small businesses on issues related to compensation and employee benefits. He can be contacted at dthomas@wsgr.com. Gerard M. Stegmaier is a senior associate in the Washington office of Wilson Sonsini Goodrich & Rosati, where he advises clients on all aspects of privacy and information governance including litigation and regulatory and transactional matters. He can be contacted at gstegmaier@wsgr.com. Wendy Lynn Devine is an associate in the San Diego office of Wilson Sonsini Goodrich & Rosati, where her practice includes privacy and information governance, particularly in connection with health-related enterprises and data security. She can be contacted at wdevine@wsgr.com.

Failure to Provide Requested Medical Records

OCR initiated its investigations after receiving complaints from individuals that Cignet failed to provide requested health records within 30 days, and not later than 60 days after receiving a request, as required by the rules. OCR then directly requested the records from Cignet and issued a subpoena to compel their production.

Cignet produced the medical records eventually, but only after being ordered to do so by a federal court. OCR then imposed a $1.3 million civil monetary penalty on Cignet for failing to provide copies of the requested records within the mandated time.

OCR also determined that Cignet failed to cooperate on a continuing daily basis throughout the investigations. Cignet's lack of cooperation, OCR concluded, was

[1] Health Information Portability and Accountability Act of 1996.

 ISSN 2151-2876

the result of Cignet's willful neglect of compliance with the HIPAA Privacy Rule.

OCR imposed a $3 million civil monetary penalty for Cignet's failure to cooperate with the HHS investigations.

Willful Neglect

Under the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act amendments to HIPAA, the agency determines penalties for violations using a multi-level penalty scheme that limits HHS' discretion.[2]

Where a determination of willful neglect has been made, the amount of the fine is mandatory.[3]

Lessons for Entities Subject to HIPAA Compliance

Critics of HIPAA contended that inadequate enforcement resulted in lax compliance. This civil monetary penalty highlights the severity of potential penalties for HIPAA violations and OCR's efforts to demonstrate the seriousness of its approach to ensuring that businesses comply with the HIPAA requirements.

The penalties themselves illustrate the simple value of clear, up-to-date, and well implemented HIPAA compliance plans. Active compliance planning and monitoring could help an organization avoid fines and potential violations, thus mitigating related risks.

Notably, under the HITECH amendments, ''business associates''—those companies that process protected health information for covered entities such as insurers, hospitals, and other providers—are now directly subject to the rules, whereas previously their liability existed primarily through indemnification obligations with their customers.

Given that in this instance the fines amounted to almost $105,000 per person (and effectively per record set or file), the financial returns on improved compliance, especially from a pure risk-management perspective, could be substantial.

Finally, given the dramatic increase in privacy class action litigations, increased regulatory and enforcement activity, and the heightened importance attached to privacy by consumers and business customers, this latest action may signal that now is a worthwhile time to take a fresh look at privacy compliance.

[2] The minimum HIPAA fine is $100 per violation, with a calendar-year cap of $25,000 for identical violations. The maximum fine can be as high as $50,000 for each violation, with a $1.5 million calendar-year cap for identical violations.

[3] For more information on HITECH civil penalty provisions, see the WSGR Alert titled ''Health Privacy Changes Create Increased Risks and Obligations for Holders of Health Data,'' available at *http://www.wsgr.com/wsgr/Display.aspx?SectionName=publications/PDFSearch/wsgralert_HIPAA.htm* and dated July 7, 2009.

  HITR ISSN 2151-2876