Health Law manatt

February 25, 2011

First Ever Civil Monetary Penalty Imposed for HIPAA Privacy Rule Violation

Authors: Robert D. Belfort | Susan R. Ingargiola

Leveraging the increased enforcement authority granted under the Health Information Technology for Economic and Clinical Health Act ("HITECH"), for the first time, the U.S. Department of Health and Human Services Office for Civil Rights ("OCR") imposed a civil monetary penalty on a health care organization for violating the Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule. On February 22, 2011, OCR ordered Cignet Health to pay a $4.3 million penalty for failing to provide patients with copies of their medical records and refusing to cooperate in OCR's investigation.

Cignet's Unusual Conduct

The Privacy Rule requires Covered Entities to provide patients with copies of their medical records within 30 to 60 days from the date of a request.[1] Cignet failed to provide copies of medical records to 41 patients between August 2008 and October 2009. Cignet is a physician group that offers family practice and other services at four locations throughout Maryland. It also claims to offer health insurance through "Cignet Health Plan" though its licensure to operate as a health insurer has been questioned in the press.

The announcement issued by OCR does not explain why Cignet failed to comply with its obligations under the Privacy Rule.

OCR began its investigation when a group of patients filed individual complaints against Cignet with OCR. Compounding its initial violations, Cignet failed to respond to OCR's request for the patients' records. Cignet then ignored a subpoena. OCR sought to enforce the subpoena in the United States District Court for the District of Maryland. The Court issued an order for Cignet to show cause and scheduled a hearing at which Cignet did not appear. Cignet neither responded to the petition nor defended the action. The Court then granted a judgment by default against Cignet and directed Cignet to produce copies of the medical records to OCR. Cignet subsequently produced the medical records along with copies of many other medical records not covered by the subpoena -yet another Privacy Rule violation. Cignet made no effort to resolve the patients' complaints.

Stiff Penalties Result

Under an October 30, 2009 Interim Final Rule implementing HITECH's heightened HIPAA sanctions, OCR is authorized to impose a range of civil monetary penalties of not less than $100 to more than $50,000 for each violation of the Privacy Rule occurring on or after February 18, 2009, provided that the total amount imposed for violations of an identical requirement during a calendar year does not exceed $1,500,000.[2] Prior to HITECH, OCR could only impose civil monetary penalties of up to $100 for each violation with an annual cap of $25,000 for all violations of an identical requirement during a calendar year.

Using its heightened sanction authority under HITECH, OCR imposed a civil monetary penalty of $100 per patient per day for the period during which Cignet failed to provide copies of records. This amounted to a total $1.3 million penalty.

OCR also imposed $3 million in civil monetary penalties based on Cignet's failure to cooperate with OCR's investigation.[3] Cignet's failure to cooperate with OCR's investigation of each complaint constituted a separate violation of the Privacy Rule. OCR found that Cignet's failure to cooperate with the investigation was due to willful neglect[4] not corrected within 30 days of when Cignet knew or with the exercise of reasonable diligence would have known of the violations, and thus assessed on Cignet the maximum penalty of $50,000 per day for each violation.

Implications of OCR's Enforcement Action

Whether OCR's imposition of civil monetary penalties against Cignet signals more aggressive enforcement of HIPAA remains to be seen. Cignet's failure to provide its patients with their medical records and refusal to cooperate with OCR's investigation is highly unusual, and OCR may simply be responding to this unique set of facts. It will take a less egregious case of non-compliance that triggers substantial penalties to confirm that OCR is prepared to use its heightened HIPAA sanction authority on a regular basis.

Meanwhile, OCR continues to resolve cases of non-compliance with the HIPAA Privacy and Security Rules through other means, including the execution of "resolution agreements." OCR entered into its latest resolution agreement on February 24, 2011 with The General Hospital Corporation and Massachusetts General Physicians Organization, Inc. ("Mass General") to settle claims involving the loss of Protected Health Information ("PHI") of 192 patients of Mass General's Infectious Disease Associates outpatient practice, including patients with HIV/AIDS. A Mass General employee left the PHI in a subway car.

Under the Resolution Agreement, Mass General agreed to pay $1,000,000 and enter into a Corrective Action Plan ("CAP"). Among other items, the CAP obligates Mass General to develop written policies and procedures governing the physical removal and transport of PHI, laptop encryption, and USB drive encryption. The CAP also obligates Mass General to train workforce members

who access and use PHI on the policies and procedures, designate an internal monitor to assess compliance with the CAP, and report the results to the Department of Health and Human Services on a semiannual basis for three years.