



# Alert

Life Sciences and Health Care Client Service Group

To: Our Clients and Friends

March 4, 2010

## Covered Entities Are Hit Hard Under HIPAA Privacy Rule

Last week, the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) issued two separate press releases about failures to comply with the privacy rule of the Health Insurance Portability and Accountability Act (HIPAA) and the heavy price of non-compliance.

### Cignet Health

In the first case, OCR imposed its first civil monetary penalty on a covered entity for violating HIPAA, ordering Cignet Health (“Cignet”) – a health center based in Maryland – to pay \$4.3 million. \$1.3 million of the penalty was assessed against Cignet for its failure to provide 41 patients with copies of their medical records from September 2008 to October 2009. The other \$3 million was assessed against Cignet for its failure to cooperate with HHS’ investigation.

The HIPAA privacy rule requires covered entities to provide patients with their medical records within 30 (and no later than 60) days from the date of the patient’s request. This is one of the basic rights granted by HIPAA.

According to the HHS press release, the investigation began when a number of Cignet patients filed individual complaints with OCR, indicating they had requested, but had not received, access to their medical records. When OCR requested the records, Cignet failed to respond. OCR then served Cignet with a federal subpoena. When Cignet failed to respond to the subpoena, OCR filed a petition to enforce the subpoena in the U.S. District Court of Maryland. On March 30, 2010, after Cignet failed to respond to the petition, the District Court awarded HHS a default judgment.

Although Cignet subsequently produced the medical records, OCR found that Cignet failed to cooperate with its investigation on a daily basis from March 17, 2009 to April 7, 2010. The agency further stated: “Cignet’s failure to cooperate with OCR’s investigation of each complaint constitute[d] a separate violation of [the privacy rule], and each day that the violation continued... counts as a separate

This Client Alert is published for the clients and friends of Bryan Cave LLP. Information contained herein is not to be considered as legal advice. This Client Alert may be construed as an advertisement or solicitation. © 2011 Bryan Cave LLP. All Rights Reserved.

violation.” According to the release, each “violation was due to Cignet’s willful neglect of its obligations to comply” with the privacy rule.

This is the first time HHS used its expanded authority under the Health Information Technology for Economic and Clinical Health Act (HITECH), which was part of the 2009 economic stimulus package. HITECH increased HHS’ authority to impose civil monetary penalties for HIPAA violations and increased the amount of the penalty that could be imposed per violation.

## **Mass General**

In the second case, the General Hospital Corporation and Massachusetts General Physicians Organization Inc. (“Mass General”) agreed to pay the federal government \$1 million to settle potential violations of the privacy rule.

The incident giving rise to the settlement involved the loss of protected health information (PHI) of 192 patients of Mass General, including patients with HIV/AIDS, in 2009. Specifically, a Mass General employee left documents containing the PHI on a subway train. The documents (which included a patient schedule containing names and patient medical record numbers and billing encounter forms containing the name, birth date, medical record number, health insurer and policy number, diagnosis and name of providers for 66 of the patients) were never recovered.

OCR’s investigation indicated that Mass General failed to implement reasonable, appropriate safeguards to protect the privacy of PHI when removed from Mass General’s premises. Under the Resolution Agreement, Mass General agreed to enter into a Corrective Action Plan (CAP) - which requires Mass General to develop and implement a comprehensive set of policies and procedures to safeguard the privacy of its patients, to train workforce members on these policies and procedures and to designate an internal monitor who will conduct assessments of Mass General’s compliance and send semi-annual reports to HHS for the next 3 years.

According to OCR Director Georgina Verdugo, “OCR is serious about HIPAA enforcement.” The question remains whether these cases represent a fundamental change in HHS’ enforcement of HIPAA rules or whether these are unusually egregious situations that had to be addressed and penalized. Regardless, the actions certainly send a message to covered entities that they need to take HIPAA seriously, to implement appropriate safeguards to protect PHI and to cooperate in investigations concerning violations of the privacy rule.

If you have any questions, please contact any member of the Bryan Cave [Life Sciences and Health Care](#) team.