

OCR Exercises its Enforcement Discretion

March 1, 2011

On February 4, 2011, the U.S. Department of Health and Human Services Office for Civil Rights (OCR) imposed a civil money penalty (CMP) of \$4,351,600 against Cignet Health of Maryland (Cignet) for violating the Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy standards. This is the first time OCR has used its CMP enforcement authority under HIPAA. On February 14, 2011, OCR entered into a settlement agreement with Massachusetts General Hospital (MGH) under which MGH agreed to pay \$1 million to settle potential violations of the HIPAA privacy standards. Together, the Cignet CMP action and MGH settlement agreement suggest OCR is serious about enforcing HIPAA.

The CMP stemmed from Cignet's failure to provide 41 patients with copies of their medical records after receiving the patients' requests for them. Cignet did not respond to any of the 41 individuals' requests. After receiving a number of complaints, OCR notified Cignet that it had opened investigations into its failure to respond to the individuals' requests. Cignet failed to respond to OCR's complaint investigations. As a result, OCR issued a subpoena directing Cignet to produce medical records related to certain of the complaints. Again, Cignet did not respond to the subpoena.

After an additional, unsuccessful attempt by OCR to contact Cignet and obtain the requested medical records, the Department of Justice filed a petition to enforce the subpoena in the U.S. District Court for the District of Maryland. The court scheduled a hearing and ordered Cignet to appear, but Cignet failed to do so and did not defend the action. The court subsequently ordered Cignet to produce the requested medical records. In response to the court's order, Cignet delivered 59 boxes of original medical records to OCR, which included the requested medical records as well as the medical records for approximately 4,500 other individuals for whom OCR had not requested records.

OCR ultimately imposed a CMP of \$3 million for Cignet's failure to cooperate throughout OCR's investigation and \$1,351,600 for Cignet's failure to provide the patients access to their medical records. For more information about the HIPAA civil money penalty scheme, see [HHS Issues Interim Final Rule Conforming HIPAA Civil Money Penalties to HITECH Act Requirements](#) and [OCR Issues Proposed Modifications to HIPAA Privacy and Security Rules to Implement HITECH Act](#).

In connection with OCR's announcement of the MGH settlement agreement, Georgina Verdugo, the director of OCR stated, "We hope the health care industry will take a close look at this agreement and recognize that OCR is serious about HIPAA enforcement. It is a covered entity's responsibility to protect its patients' health information." In light of this statement, the Cignet CMP action and the MGH settlement, covered entities and business associates should begin now to reassess the adequacy and effectiveness of their HIPAA compliance programs. Such a reassessment should include at least the following basic steps required by the HIPAA privacy and security standards and HITECH security breach notification regulations:

- Conduct a security risk assessment that identifies the risks and vulnerabilities to its electronic protected health information
- Implement written security policies that reflect the results of the risk assessment
- Adopt written privacy policies implementing each provision of the HIPAA privacy standards
- Train each employee who handles protected health information regarding its privacy and security policies and document the employee names and the dates of the training sessions
- Notify employees that if they receive a written request from an individual or a government agency, to forward that request to the HIPAA privacy/security officer for processing

Many times, the failure to timely respond to an individual's request is simply due to a breakdown in an organization's HIPAA procedures. It is important for an organization to keep a record of and train its personnel on how to handle an individual or enforcement agency's HIPAA request. OCR routinely asks about an organization's policies and procedures in its complaint investigations and has stated that an organization's failure to implement policies and procedures may cause OCR to conclude that it has a higher culpability level and, therefore, is a candidate for a larger CMP.

The material in this publication may not be reproduced, in whole or part without acknowledgement of its source and copyright. On the Subject is intended to provide information of general interest in a summary manner and should not be construed as individual legal advice. Readers should consult with their McDermott Will & Emery lawyer or other professional counsel before acting on the information contained in this publication.

© 2010 McDermott Will & Emery. The following legal entities are collectively referred to as "McDermott Will & Emery," "McDermott" or "the Firm": McDermott Will & Emery LLP, McDermott Will & Emery/Stambrook LLP, McDermott Will & Emery Rechtsanwälte Steuerberater LLP, MWE Steuerberatungsgesellschaft mbH, McDermott Will & Emery Studio Legale Associato and McDermott Will & Emery UK LLP. McDermott Will & Emery has a strategic alliance with MWE China Law Offices, a separate law firm. These entities coordinate their activities through service agreements. This communication may be considered attorney advertising. Previous results are not a guarantee of future outcome.