Blitman&King LLP

www.bklawyers.com

Client Alert
June 2011

OFFICE OF CIVIL RIGHTS IMPOSES $5.3 MILLION IN FINES FOR HIPAA PRIVACY RULE VIOLATIONS

In an unprecedented enforcement action, the Department of Health and Human Services' ("HHS") Office for Civil Rights ("OCR") recently imposed a $4.3 million civil monetary fine and reached a $1 million settlement as punishment for violations of the Health Insurance Portability and Accountability Act ("HIPAA"). The $4.3 million fine was the first civil money penalty issued by HHS for HIPAA Privacy Rule violations and may signify a change by HHS and OCR to enforce violations with a more heavy-handed approach.

Pursuant to HIPAA's Privacy Rule, covered entities[1] and business associates[2] are prohibited from unauthorized disclosure of protected health information ("PHI")[3], and may only disclose PHI under certain circumstances.[4] Disclosure is permitted if made:

(a) to the individual;
(b) for treatment, payment, or health care operations;
(c) incident to a use or disclosure otherwise permitted or required;
(d) pursuant to valid authorization or agreement; and
(e) as required by law or court order.

HIPAA's regulations also require that a covered entity provide a patient with a copy of their requested medical records within thirty days of the patient's request.[5] The covered entity must

[1] Under 45 CFR 160.103, covered entities include health plans, health care providers (including those providing medical or health insurances or services such as hospitals, physicians, dentists, etc.), health care clearinghouses, and business associates.
[2] Under 45 CFR 160.103, a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information.
[3] 45 C.F.R. § 160.103. Protected health information is all individually identifiable health information held or transmitted by a covered entity or business associate, in any form or media, whether electronic, paper or oral.
[4] 45 C.F.R. § 164.502.
[5] 45 C.F.R. § 164.524.

then make "reasonable efforts" to limit disclosure of PHI to the minimum necessary for the intended purpose of the use, disclosure or request.[6]

The OCR is granted the authority to impose civil monetary penalties upon a covered entity for violations of the Privacy Rule,[7] with the amount based on a list of factors set forth in the regulation. These considerations include the nature of the violation, circumstances and impact of the violation, degree of culpability, history of compliance by the covered entity, financial condition of the covered entity, and "such other matters as justice may require".[8] In addition to imposing fines, OCR also has the power to settle or reach compromise on penalties for alleged violations.[9]

Cignet Health Civil Monetary Penalty

HHS imposed a $4.3 million civil money penalty against Cignet Health of Prince George County for violations of the Privacy Rule. The assessed fines were for numerous violations, including failure to provide patient access to requested records, failure to cooperate with OCR's investigation, and willful neglect to comply with the Privacy Rule.

Between September 2008 and October 2009, forty-one patients requested access to their medical records, as allowed by HIPAA. Cignet failed to provide the records, and the patients filed individual complaints with OCR. During investigation of the complaints, OCR found that Cignet failed to cooperate by: (1) not initially responding to OCR's subpoena with records; (2) failing to resolve the complaints through informal means; and (3) a general willful neglect to comply with the Privacy Rule.

The OCR imposed a $1.3 million fine for the initial violation of failing to provide patients with their requested records and a $3 million fine for failing to cooperate during the complaint investigation process. The civil monetary penalty was an unprecedented action and marked the first time that HHS issued a civil monetary penalty for HIPAA Privacy Rule violations.

Massachusetts General Hospital Settlement

HHS also announced this year the settlement of potential HIPAA violations with Massachusetts General Hospital ("MGH") for the loss of PHI for 192 patients in MGH's Infectious Disease outpatient practice.

[6] 45 C.F.R. § 164.502(b).
[7] 45 C.F.R. § 160.402.
[8] 45 C.F.R. § 160.408.
[9] 45 C.F.R. § 160.416.

An MGH employee commuting to work left documents containing patients' PHI, including HIV/AIDS information, on a subway car. The documents included schedules which contained names and medical record numbers for 192 patients, and billing forms containing name, date of birth, medical record number, health insurer and policy numbers, diagnosis, and names of providers.

A complaint was filed by a patient claiming PHI was lost. OCR investigated and indicated that MGH failed to implement "reasonable, appropriate safeguards" to protect privacy when documents containing PHI were removed from MGH premises. MGH and OCR reached a settlement of $1 million, with the amount payable to the U.S. government.

In addition to the financial settlement, MGH agreed to enter into a Corrective Action Plan that: (1) requires the hospital to develop and implement policies and procedures to ensure PHI is protected when removed from the premises; (2) train workforce members in these policies; and (3) designate an internal monitor that must provide semi-annual reports to HHS for a 3-year period.

Practical Impact

It is clear that HHS and OCR are sending a message of increased HIPAA enforcement. In the Cignet Health press release, HHS Secretary Kathleen Sebelius was quoted as follows:

> Ensuring that Americans' health information privacy is protected is vital to our health care system and a priority of this Administration. The U.S. Department of Health and Human Services is serious about enforcing individual rights guaranteed by the HIPAA Privacy Rule.

A similar message was contained in the Massachusetts General Hospital press release, with OCR Director Georgina Verdugo stating:

> 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. . . . To avoid enforcement penalties, covered entities must ensure they are always in compliance with the HIPAA Privacy and Security Rules . . . A robust compliance program includes employee training, vigilant implementation of policies and procedures, regular internal audits, and a prompt action plan to respond to incidents.

The Cignet Health and Massachusetts General Hospital civil monetary penalties, and their significant amounts, should put all covered entities and business associates on notice of

HHS and OCR's increased enforcement efforts. Accordingly, covered entities and business associates should make every attempt to ensure compliance with the HIPAA Privacy Rule regulations.

* * *

This client alert is not intended to provide legal advice with respect to any particular situation and no decision should be based solely on its content. Please feel free to contact Daniel Brice, Esq. at (315) 422-7111 with any questions or concerns regarding HIPAA compliance or other issues raised in this client alert.