Dramatic Increases In HIPAA Privacy And Security Enforcement

Insights
5.01.11

(Benefits Update, No. 2, May 2011)

Health and Human Services' (HHS) Office for Civil Rights (OCR) has sent a strong message about its commitment to enforcement of the HIPAA Privacy and Security Rules by announcing two HIPAA Privacy Rule enforcements within one week, one of which includes the first ever use of civil monetary penalties for a HIPAA Privacy Rule violation.

Cignet Health of Prince George's County
HHS issued a Notice of Final Determination, finding that Cignet Health of Prince George's County, MD violated the Privacy Rule, imposing a civil money penalty of $4,351,600 for the violations. The penalty was based on the increased penalty amounts authorized by the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act (ARRA), better known as the stimulus package. OCR found that Cignet violated 41 patients' rights by denying them access to their medical records when requested. The patients had individually filed complaints with the OCR, which initiated the investigation.

The HIPAA Privacy Rule requires that a covered entity provide patients with a copy of their medical records within 30 (and no later than 60) days of the patient's request. Under the HIPAA Privacy Rule, each day that a violation continues (i.e., each day that access was not provided) for each individual counts as a separate violation. OCR assessed a penalty of $100 per day for each day that Cignet failed to timely respond to each individual's request for access (the minimum penalty under the new HITECH penalty structure). The total penalty for these violations was $1,351,600.

OCR then assessed the maximum penalty of $50,000 per day for Cignet Health's failure to cooperate with the HHS investigation, which would have resulted in $242 million in penalties for 2009 and $130 million for 2010, but because penalties for the same violation are capped at $1.5 million per year, the penalty for failure to cooperate was limited to $3 million. The total penalty came to $4,351,600.

Massachusetts General

The General Hospital Corporation and Massachusetts General Physicians Organization, Inc. (Mass General) agreed to pay $1,000,000 to settle violations of HIPAA's Privacy Rule. Mass General must also develop and implement a comprehensive set of policies and procedures to safeguard the privacy of its patients. This settlement follows an extensive investigation by the OCR to enforce the HIPAA Privacy and Security Rules.

The incident giving rise to the investigation involved the loss of protected health information (PHI) of 192 patients. These documents were lost on March 9, 2009, when a Mass General employee, while commuting to work, left the documents on the subway train. The documents were never recovered. OCR opened its investigation of Mass General after a complaint was filed by a patient whose PHI was lost. OCR's investigation found that Mass General failed to implement "reasonable, appropriate safeguards" to protect the privacy of PHI when removed from Mass General's premises and impermissibly disclosed PHI, potentially violating provisions of the HIPAA Privacy Rule.

A Marked Increase in HHS Enforcement

The original version of HIPAA had relatively small penalties. Penalties were capped at $100 per day of violation and at $25,000 for the same violation in any one year. HHS received much criticism for its informal enforcement of HIPAA; seeking voluntary, confidential compliance agreements from those who violated the law. Responding to this criticism, HHS finally entered into its first financial settlement in July 2008. Providence Health, which over a seven month period had experienced four separate incidents of lost computers, lost backup tapes and other storage media, agreed to pay a $100,000 financial settlement and to implement a corrective action plan.

In January of 2009, HHS entered into its second financial settlement. This involved a joint investigation by HHS and the Federal Trade Commission (FTC) over allegations that CVS retail pharmacies were improperly disposing of medical information in unsecured dumpsters. This settlement was $2.25 million. In July of 2009, HHS and the FTC entered into a settlement with Rite-Aid. As with CVS, the investigation involved allegations that Rite-Aid pharmacies had improperly disposed of medical information. The settlement amount was $1 million.

Meanwhile, Congress took action to increase the penalties under HIPAA. In February of 2009, Congress passed the HITECH Act to amend HIPAA, dramatically increasing the monetary penalties, which now range from a minimum of $100 to $50,000 per day of violation, with an annual cap of $1.5 million for the same violation in any one year. HITECH also requires HHS to engage in compliance audits and gives states' Attorneys General the right to enforce HIPAA as well. With these two recent enforcements, the message is clear that failure to comply with HIPAA's Privacy and Security Rules and failure to cooperate with an OCR investigation can have severe consequences, particularly now that the penalties have been increased.

Are You In Compliance?

HIPAA's Privacy and Security Rules apply to "covered entities": healthcare providers, insurance companies, healthcare clearinghouses and group health plans, such as employer-sponsored medical, dental, vision, EAP and healthcare flexible spending accounts (FSAs). They also now apply

medical, dental, vision, EAP and healthcare flexible spending accounts (FSAs). They also now apply directly to "business associates," which are plan vendors, like insurance brokers, consultants, actuaries and attorneys who have access to PHI. If you are a Covered Entity or Business Associate, you should have already completed your Privacy and Security compliance efforts and should be operating in compliance with the Privacy and Security Rules.