[buck research]

A Xerox Company

fyi© for your information©

Volume 34 | Issue 24 | March 22, 2011

Recent HIPAA Enforcement Actions Signal Increased HHS Enforcement

HHS recently imposed its first civil money penalty for violation of HIPAA's privacy rules. The $4.3 million penalty was soon followed by HHS settling another entity's violation of HIPAA's privacy rules for $1 million. The two enforcement actions strongly suggest that HHS is investigating violations of HIPAA's privacy rules vigorously and imposing substantial penalties for violations of the rules.

Background

In 2001, the Department of Health and Human Services (HHS), pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), promulgated national standards to protect individuals' medical records and other personal health information from disclosure (Privacy Rule). The Privacy Rule applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. Under the Privacy Rule, covered entities must adopt safeguards to protect the privacy of personal health information. The Privacy Rule also sets limits and conditions on the uses and disclosures that may be made of such health information without patient authorization.

The Secretary of HHS is authorized to impose civil money penalties (CMP) against any entity that violates HIPAA's Privacy Rule. The Health Information Technology and Clinical Health Act (HITECH Act), which was enacted as part of the American Recovery and Reinvestment Act of 2009, expanded HIPAA's Privacy Rule requirements, substantially increased the penalties for noncompliance with the Privacy Rule, and mandated penalties in certain circumstances. Under the HHS tiered penalty structure, the amount of the penalty depends on the severity of the violation. For violations of the Privacy Rule that occur after the enactment of the HITECH Act, the minimum CMP that can be imposed is $100 per violation and the maximum penalty that can be imposed per year is $1.5 million for identical violations. The penalty amount varies depending on whether the violation was unknown, due to reasonable cause, or due to willful neglect. (See Our November 18, 2009 *For Your Information*.) HHS has not yet issued the HITECH Act's final regulations.

> ***BUCK COMMENT.*** *Historically, HHS has not vigorously enforced HIPAA's Privacy Rule. Even after enactment of the HITECH Act, the agency did not immediately impose any enhanced penalties.*

Recent HHS HIPAA Enforcement Actions

Recently, HHS has stepped up its enforcement of HIPAA's Privacy Rule, including employing its authority under the HITECH Act to impose a substantial CMP against an entity that violated the Privacy Rule and failed to cooperate with HHS's investigative efforts.

Cignet Health

In February 2011, HHS issued a Notice of Final Determination finding that Cignet Health of Prince George's County, Maryland (Cignet) violated HIPAA's Privacy Rule. HHS imposed a CMP of $4.3 million on Cignet for its violations.

HHS concluded that Cignet violated patients' rights by denying them access to their medical records when requested. The CMP imposed for these violations was $1.3 million. HHS also found that during 2009 and 2010, Cignet failed to cooperate with its investigations of the patients' complaints, concluding that the failure to cooperate was due to Cignet's willfully neglecting to comply with the Privacy Rule. HHS imposed a CMP of $3 million ($1.5 million for each year of noncompliance) for Cignet's failure to cooperate.

> ***BUCK COMMENT.*** *The penalty imposed on Cignet represented the first CMP issued by HHS for a covered entity's violations of the Privacy Rule.*

Massachusetts General Hospital

Less than two weeks after announcing the CMP imposed on Cignet, HHS announced a $1 million settlement with Massachusetts General Hospital (MGH) for alleged violations of HIPAA's Privacy Rule. In that case, a MGH employee took home documents containing protected health information and left the documents, secured with only a rubber band and not placed in a secured envelope or folder, on a subway while returning to work. In addition to the $1 million settlement, MGH agreed to a three-year corrective action plan (CAP) aimed at improving its compliance with HIPAA's requirements. The CAP requires MGH to (1) develop and implement policies that better protect protected health information, (2) train employees on the new policies, and (3) semi-annually report to HHS.

> ***BUCK COMMENT.*** *In the MGH announcement, HHS stated that the following are components of a robust HIPAA compliance program: (1) employee training; (2) vigilant implementation of policies and procedures; (3) regular internal audits; and (4) prompt action responding to suspected violations of HIPAA's rules.*

Conclusions

HHS is stepping up its enforcement of HIPAA's requirements by imposing substantial penalties for noncompliance and requiring extensive corrective action. In announcing the MGH settlement, the Director of HHS's Office of Civil Rights (OCR) stated that he "hope[s] the health care industry will take a close look at this agreement and

recognize that OCR is serious about HIPAA enforcement." While the Cignet and MGH actions involved health care providers, group health plans and plan sponsors should also be vigilant about HIPAA compliance in the wake of the recent enforcement actions.

Buck will continue to monitor new developments in HHS HIPAA enforcement. Buck's consultants are available to assist your organization in conducting risk assessments, reviewing and updating HIPAA policies, investigating suspected HIPAA violations, and responding to HHS inquiries.