[buck research]

fyi® for your information®

Volume 32 | Issue 80 | November 18, 2009

HHS Issues Interim Final Regulations on Increased Penalties for HIPAA Violations

The Department of Health and Human Services (HHS) recently issued interim final regulations implementing the provisions of HITECH that substantially increase penalties for noncompliance with the administrative simplification provisions (e.g., privacy security) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Background

Since the HIPAA privacy regulations took effect in 2003, HHS enforcement has been limited and few penalties have been assessed against covered entities. Among other things, the Health Information Technology for Economic and Clinical Health Act (HITECH), enacted as part of the American Recovery and Reinvestment Act of 2009, provided for increased enforcement activity and significantly increased penalties for noncompliance with the administrative simplification provisions of HIPAA. (See our April 27, 2009 *For Your Information*.) Now, HHS has issued interim final regulations that implement the increased penalty provisions.

Interim Final Regulations on New Penalty Structure

Effective February 18, 2009, HITECH increased civil penalties for HIPAA privacy and security violations based on a tiered penalty structure which depends on the severity of the violation. For violations that occurred prior to HITECH, civil penalties remain limited to $100 per violation with an overall limit of $25,000 per calendar year.

The regulations implement the new HITECH penalty structure as follows –

- If the covered entity was unaware or would not have known of the violation by exercising reasonable diligence, the minimum civil penalty is $100 per violation, with a maximum of $50,000, and an overall limit of $1,500,000 for identical violations during the calendar year.
- If the violation was due to reasonable cause and not to willful neglect, the minimum civil penalty is $1,000 per violation, with a maximum of $50,000, and an overall limit of $1,500,000 for identical violations during the calendar year.
- If the violation resulted from willful neglect but is corrected within a 30-day period after discovery, the minimum civil penalty is $10,000 per violation, with a maximum of $50,000, and an overall limit of $1,500,000 for identical violations during the calendar year.

- If the violation is due to willful neglect and is not corrected, the minimum civil penalty is $50,000 per violation, with an overall limit of $1,500,000 for identical violations during the calendar year.

For purposes of determining the penalty amount, the regulations provide that HHS has discretion to consider a variety of factors, including the nature of the violation, the resulting harm, and the covered entity's compliance history and financial condition. The regulations also confirm HHS' authority to partially or fully waive the civil penalties and reflect the revisions made by HITECH regarding affirmative defenses that may used to prevent HHS from assessing penalties for violations due to reasonable cause and not willful neglect.

Effective Date

The interim final regulations take effect on November 30, 2009, and apply to violations occurring on or after February 18, 2009.

Conclusion

The interim final regulations establish the significantly increased penalty structure for HIPAA privacy and security violations. Covered entities should assure that they can demonstrate full compliance with HIPAA requirements to avoid significant liability. Buck's consultants are available to review the new HIPAA regulations with you and to assist in your compliance efforts.