



February 2011

EMPLOYEE BENEFITS AND PRIVACY UPDATE

In light of the increased HIPAA enforcement activity described below, covered entities such as group health plans should consider reviewing their current HIPAA compliance. Our lawyers regularly assist clients with this process, from providing an annual checkup to conducting a complete overhaul of HIPAA policies and procedures.

HIPAA Enforcement Activity Is On the Rise – Is It Time to Review Your Compliance Efforts?

The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) recently issued its first civil monetary penalty in response to violations of the federal privacy rules promulgated under the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA). In addition, Vermont, Connecticut and Indiana have recently settled lawsuits against insurance companies that failed to timely notify insureds about HIPAA violations.

HISTORY OF ENFORCEMENT ACTIONS

The HIPAA privacy rules have been in effect since 2003, but prior to February 2009, HHS and OCR generally did not aggressively penalize covered entities for violations of the rules. HHS and OCR did not conduct audits, but responded to complaints and worked with covered entities to help them achieve compliance. During that period, HHS and OCR resolved more than 8,000 cases by working with covered entities to make systemic changes to their privacy practices. There were only two cases in which covered entities entered into settlement agreements that included payment of monetary settlement amounts.

Conditions changed with the February 17, 2009 enactment of the Health Information Technology for Economic and Clinical Health Act (HITECH Act), which requires HHS and OCR to audit covered entities and assess penalties. The HITECH Act increased the minimum and maximum penalties and created a tiered penalty structure based on the level of the covered entity’s culpability. A covered entity that does not know or have reason to know of a violation and corrects it upon discovery is subject to a much lower penalty than a covered entity that willfully violates HIPAA and refuses to correct the violation.

FIRST CIVIL PENALTY

In February 2011, OCR issued the first HIPAA privacy civil monetary penalty against Cignet Health of Prince George’s County, Maryland. OCR found that Cignet willfully violated 41 patients’ rights by denying them access to their medical records. During the investigation, Cignet

© 2011 THOMPSON HINE LLP. ALL RIGHTS RESERVED.



reportedly was uncooperative with OCR and refused to resolve the complaints through informal means. As a result, OCR assessed a penalty of \$4.3 million.

About this penalty OCR Director Georgina Verdugo said, “Today the message is loud and clear: HHS is serious about enforcing individual rights guaranteed by the HIPAA privacy Rule and ensuring provider cooperation with our enforcement efforts.”

### **STATE ENFORCEMENT ACTIONS**

The HITECH Act also gave state attorneys general authority to enforce the HIPAA rules. The attorneys general of Connecticut, Indiana and Vermont have since filed separate federal lawsuits against insurance companies that have taken an unreasonably long time (from three to six months) to notify insureds of a data breach. The Connecticut lawsuit settled for \$250,000, the Indiana lawsuit settled for \$300,000 and the Vermont lawsuit settled for \$55,000.

### **LESSONS TO LEARN**

These enforcement activities highlight specific areas of HIPAA compliance, such as responding to an individual’s request for access and notifying individuals upon the occurrence of a breach. More generally, however, these enforcement activities point to the fact that HHS and the states are actively enforcing the HIPAA rules.

Covered entities should currently comply with all aspects of the HIPAA privacy, security and breach notification rules. They should also document their compliance through written policies, procedures and evidence of attendance at employee training sessions. Although many covered entities engaged in initial compliance activities in 2003, turnover, relationships with new vendors, physical relocation, changing technology, legal developments and other circumstances can cause compliance efforts to quickly become out of date. Covered entities should consider conducting an annual checkup to ensure that the HIPAA policies and procedures they have in place are appropriate for their organization.

### **FOR MORE INFORMATION**

For more information, please contact:

Kim Wilcoxon 513.352.6524 [Kim.Wilcoxon@ThompsonHine.com](mailto:Kim.Wilcoxon@ThompsonHine.com)

**IRS Circular 230 Disclosure:** To ensure compliance with requirements imposed by the IRS, we inform you that nothing contained herein is intended to be used, or can be used, to avoid penalties imposed under the Internal Revenue Code.

If you do not wish to receive future communications by email, please send an email with “Unsubscribe” in the subject line to [Unsubscribe@ThompsonHine.com](mailto:Unsubscribe@ThompsonHine.com).



---

This advisory may be reproduced, in whole or in part, with the prior permission of Thompson Hine LLP and acknowledgement of its source and copyright. This publication is intended to inform clients about legal matters of current interest. It is not intended as legal advice. Readers should not act upon the information contained in it without professional counsel.

This document may be considered attorney advertising in some jurisdictions. Some of the design images and photographs in this document may be of actors depicting fictional scenes.

© 2011 THOMPSON HINE LLP. ALL RIGHTS RESERVED.