

**Primary Office**  
16633 Dallas Parkway, Suite 600  
Addison, Texas 75001  
Mobile Telephone: (469) 767.8872

HELPING MANAGEMENT MANAGE

**Plano Office**  
3948 Legacy Drive  
Suite 106, Box 397  
Plano, Texas 75023

## **OCR 1<sup>st</sup> HIPAA Privacy, Security & Breach Notification Compliance Audits Begin**

*November 8, 2011*

The kickoff of a new compliance audit pilot program provides another reason for health care providers, health plans, healthcare clearinghouses and their business associates to get serious about compliance with the privacy, security and data breach requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

### **OCR Pilot Audit Program Begins**

On November 8, 2011, the Office of Civil Rights (OCR) of the Department of Health & Human Services (HHS) announced that it will begin auditing HIPAA compliance this month under a new pilot program.

As amended by the American Recovery and Reinvestment Act of 2009 in Section 13411 of the HITECH Act, requires HHS to provide for periodic audits to ensure covered entities and business associates are complying with the HIPAA Privacy and Security Rules and Breach Notification standards. To implement this mandate, OCR is piloting a program to perform up to 150 audits of covered entities to assess privacy and security compliance between November 2011 and December 2012.

The commencement of OCR HIPAA compliance audits is yet another sign that covered entities and their business associates should get serious about HIPAA compliance. The audit program serves as a new part of OCR's health information privacy and security compliance program. While OCR says that it presently views the pilot audits as primarily a compliance improvement tool, this does not mean violators should expect a free walk.

Even before the impending audits, HIPAA Privacy exposures of covered entities for failing to comply with HIPAA already had risen significantly. Earlier this year, OCR imposed a \$4.3 Million Civil Money Penalty (CMP) against Cignet Health of Prince George's County (Cignet) for violating HIPAA. Meanwhile, the Department of Justice has secured several criminal convictions or pleas under HIPAA's criminal provisions. Under amendments made by the HITECH Act, state attorneys general also now are empowered to bring civil lawsuits against covered entities and business associates that commit HIPAA violations that injure citizens in their state under certain circumstances. Eventually, individuals injured by HIPAA violations also will get the right to share in a portion of certain HIPAA recoveries.

These and other audit and enforcement activities send a strong message that covered entities and their business associates need to get serious about HIPAA compliance. As stated by OCR Director Georgina Verdugo when announcing the Mass General Resolution Agreement, "To avoid enforcement penalties, covered entities must ensure they are always in compliance with the HIPAA Privacy and Security Rules," Verdugo added, "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." Learn more [here](#).

### **For Help With Monitoring Developments, Compliance, Investigations Or Other Needs**

If you need assistance monitoring federal health reform, policy or enforcement developments, or to review or respond to these or other health care or health IT related risk management, compliance,

enforcement or management concerns, the author of this update, attorney Cynthia Marcotte Stamer, can help.

Vice President of the North Texas Health Care Compliance Professionals Association, a member of the American College of Employee Benefit Counsel, Past Chair of the ABA RPTE Employee Benefits & Other Compensation Arrangements Group, Past Chair of the ABA Health Law Section Managed Care & Insurance Section and the former Board Compliance Chair of the National Kidney Foundation of North Texas, Ms. Stamer has extensive experience advising and assisting health care providers, health plans, their business associates and other health industry clients to establish and administer medical privacy and other compliance and risk management policies. Ms. Stamer also regularly helps clients deal with OCR and other agencies, publishes and speaks extensively on medical and other privacy and data security, health and managed care industry regulatory, staffing and human resources, compensation and benefits, technology, public policy, reimbursement and other operations and risk management concerns. Her publications and insights appear in the Health Care Compliance Association, Atlantic Information Service, Bureau of National Affairs, World At Work, The Wall Street Journal, Business Insurance, the Dallas Morning News, Modern Health Care, Managed Healthcare, Health Leaders, and a many other national and local publications. Her insights on the required “culture of compliance” with HIPAA are frequently included in medical privacy related publications of the Atlantic Information Service, Modern Health Care, HealthLeaders and many others. Among others, she has conducted privacy training for the Association of State & Territorial Health Plans (ASTHO), the Los Angeles Health Department, the American Bar Association, the Health Care Compliance Association, a multitude of health industry, health plan, employee benefit and other clients, trade and professional associations and others. You can get more information about her HIPAA and other experience [here](#) or may contact her at (469) 767-8872 or via e-mail [here](#).

You can review other selected publications and resources and additional information about the employment, employee benefits and other experience of Ms. Stamer [here](#).

If you or someone else you know would like to receive future updates about developments on these and other concerns, please be sure that we have your current contact information – including your preferred e-mail – by creating or updating your profile [here](#). For important information concerning this communication click [here](#). If you do not wish to receive these updates in the future, send an e-mail with the word “Remove” in the Subject to [here](#).

*©2011 Cynthia Marcotte Stamer, P.C. All rights reserved.*