Cynthia Marcotte Stamer, P.C.
SOLUTIONS LAWYER™

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 1st HIPAA Privacy, Security & Breach Notification Compliance Audits Begin

November 8, 2011

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.

Audit Targets

According to OCR, every covered entity and business associate is eligible for an audit. Selections in the initial round will be designed to provide a broad assessment of a complex and diverse health care industry. OCR is responsible for selection of the entities that will be audited. OCR plans to audit "as wide a range of types and sizes of covered entities as possible." However, OCR does not plan to audit business associates in this first round of audits.

Expected Audit Process

Based on information shared by OCR, a covered entity selected for an audit can expect that OCR will ask them to provide documentation of their privacy and security compliance efforts when notifying the covered entity of its selection. In this pilot phase, OCR says every audit will include a site visit and result in an audit report. During site visits, auditors will interview key personnel and observe processes and operations to help determine compliance. Following the site visit, auditors will develop and share with the entity a draft report; audit reports generally describe how the audit was conducted, what the findings were and what actions the covered entity is taking in response to those findings. Prior to finalizing the report, OCR says the covered entity will have the opportunity to discuss concerns and describe corrective actions implemented to address concerns identified. The final report submitted to OCR will incorporate the steps the entity has taken to resolve any compliance issues identified by the audit, as well as describe any best practices of the entity.

OCR will review the final reports, including the findings and actions taken by the audited entity to address findings. The aggregated results of the audits will enable OCR to better understand compliance efforts with particular aspects of the HIPAA Rules. Generally, OCR will use the audit reports to determine what types of technical assistance should be developed, and what types of corrective action are most effective. Should an audit report indicate a serious compliance issue, OCR may initiate a compliance review to address the problem. OCR will not post a listing of audited entities or the findings of an individual audit which clearly identifies the audited entity.

Audit Objectives

The audit program serves as a new part of OCR's health information privacy and security compliance program. OCR will use the audit program to assess HIPAA compliance efforts by a range of covered entities, Audits present a new opportunity to examine mechanisms for compliance, identify best practices and discover risks and vulnerabilities that may not have come to light through OCR's ongoing complaint investigations and compliance reviews. According to OCR, it intends that these audits serve primarily as compliance improvement activity. OCR will broadly share best practices

gleaned through the audit process and guidance targeted to observed compliance challenges via this web site and other outreach portals.

Audit Timing & Staging

The pilot audit program is a three step process. The first step entailed developing the audit protocols. Next, a limited number of audits will be conducted in an initial wave to test these protocols. OCR expects the initial audits to begin in November 2011.The results of the initial audits will inform how the rest of the audits will be conducted. The last step will include conducting the full range of audits using revised protocol materials. All audits in this pilot will be completed by the end of December, 2012.

More information regarding OCR's Pilot Audit Program is available on the OCR website at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html

Enforcement Actions Highlight Growing Exposures

Recent enforcement actions by OCR highlight the potential sanctions that covered entities failing to take appropriate steps to comply with HIPAA.

Other Signs of Rising Risks

The commencement of OCR HIPAA compliance audits is yet another sign that covered entities and their business associates should get serious about HIPAA compliance.

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. The Cignet CMP represents the first CMP issued by OCR for violations of the HIPAA Privacy Rule.

Subsequently on July 6, 2011, HHS entered into a resolution agreement with the University of California at Los Angeles Health System (UCLAHS) to settle potential violations of the HIPAA Privacy and Security Rules arising out of two separate celebrity patient complaints alleging that UCLAHS employees repeatedly and without permissible reason looked at the electronic protected health information of these and other UCLAHS patients.. In the agreement, UCLAHS agreed to settle for $865,500 and to administer a corrective action plan aimed at remedying gaps in its compliance with the rules. The UCLAHS is one of several high dollar resolution agreements achieved by OCR. See e.g., **Healthcare Providers Brace For New HIPAA Enforcement As OCR Announces Hospital Resolution Agreement Requiring $1 Million Settlement Payment**; **Rite Aid Pays $1 Million HIPAA Privacy Settlement As OCR Tightens HIPAA Regulations; HIPAA Risks Soar As CVS Agrees To Pay $2.25 Million To Resolve HIPAA Charges & Stimulus Bill Amends HIPAA**; **Providence To Pay $100,000 & Implement Other Safeguards To Settle HIPAA Penalty Exposures Under HIPAA**.

In addition to these civil enforcement actions by OCR, the Department of Justice has secured several criminal convictions or pleas under HIPAA's criminal provisions. OCR data confirms that the covered entities involved in these actions included health care providers, health plans, and others. See, e.g., **2 New HIPAA Criminal Actions Highlight Risks From Wrongful Use/Access of Health Information.**

As a result of amendments enacted as part of the HITECH Act, Congress modified and expanded the HIPAA audit obligations of OCR, amended and expanded the potential penalties, made business associates liable for violation of the privacy rules like covered entities, added an obligation for covered entities and business associates to provide notification of breaches of unsecured PHI and tightened other HIPAA obligations. The HITECH Act also gave state attorneys general 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 will get

the right to share in a portion of certain HIPAA recoveries. See **HIPAA Heats Up: HITECH Act Changes Take Effect & OCR Begins Posting Names, Other Details Of Unsecured PHI Breach Reports On Website.**

Along side these governmental actions, state courts also increasingly are willing to allow individual plaintiffs to rely on violations of HIPAA as the basis for bringing state privacy, retaliation or other actions. While prior to the recent HITECH Act amendments, federal courts had ruled that private plaintiffs could not sue under HIPAA for damages they incurred from a covered entity's violation of HIPAA, state courts have allowed private plaintiff's to use the obligations imposed by HIPAA as the basis of a covered entity's duty for purposes of certain state law lawsuits. In *Sorensen v. Barbuto*, 143 P.3d 295 (Utah Ct. App. 2006), for example, a Utah appeals court ruled a private plaintiff could use HIPAA standards to establish that a physician owed a duty of confidentiality to his patients for purposes of maintaining a state law damages claim. Similarly, the Court in *Acosta v. Byrum*, 638 S.E. 2d 246 (N.C. Ct. App. 2006) ruled that a plaintiff could use HIPAA to establish the "standard of care" in a negligence lawsuit. Meanwhile, private plaintiffs employed by covered entities also are increasingly pointing to HIPAA as the basis for their retaliation claims. See, e.g., **Retaliation For Filing HIPAA Complaint Recognized As Basis For State Retaliatory Discharge Claim.** Coupled with the HITECH Act changes, these and other enforcement actions signal growing potential hazards for covered entities and their business associates that fail to properly manage their HIPAA compliance obligations and risks.

In addition to these HIPAA-specific exposures, wrongful use, access or disclosure of medical information also can expose Covered Entities, members of their workforce and others improperly using, accessing or disclosing protected health information to liability under other federal or state laws. Federal and state prosecutors may and increasingly do bring criminal or civil actions against organizations or individuals for improperly accessing or using medical or other personal information under a variety of other federal or state laws . See e.g., **Cybercrime & Identity Theft: Health Information Security Beyond HIPAA; NY AG Cuomo Announcement of 1st Settlement For Violation of NY Security Breach Notification Law; Woman Who Revealed AIDs Info Gets A Year.**

Act To Manage HIPAA Exposures

As stated by OCR Director Georgina Verdugo when announcing the Mass General Resolution Agreement, stating, "We hope the health care industry will take a close look at this agreement and recognize that OCR is serious about HIPAA enforcement. It is a covered entity's responsibility to protect its patients' health information."

"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."

Covered entities are urged to heed these warning by strengthening their HIPAA compliance and adopting other suitable safeguards to minimize HIPAA exposures. Health plans and other covered entities as well as their business associates should tighten privacy policies, breach and other monitoring, training and other practices to mitigate against exposures in light of recently tightened requirements and new enforcement risks. To minimize the potential that the health plan's sharing of information with the employer will create or spread HIPAA or other privacy risks to the employer or members of its workforce, employers and other plan sponsors and members of their workforce also should take steps to ensure not only that their health plan documents, policies and procedures, as well as those policies and practices applicable to the employer, its human resources, and benefits advisors when accessing or handling health plan or other medical information on behalf of the employer, rather than the plan, are appropriately designed and administered.

In response to these expanding exposures, health care providers and other covered entities should review the adequacy of their current HIPAA Privacy and Security compliance policies, monitoring, training, breach notification and other practices taking into consideration the Cignet, Rite Aid, Provident and CVS enforcement actions, emerging litigation and other enforcement data; their own and reports of other security and privacy breaches and near misses, and other developments to determine if additional steps are necessary or advisable.

To minimize the potential that the health plan's sharing of information with the employer will create or spread HIPAA or other privacy risks to the employer or members of its workforce, employers and other plan sponsors and members of their workforce also should take steps to ensure not only that their health plan documents, policies and procedures, as well as those policies and practices applicable to employer, its human resources, and benefits advisors when accessing or handling health plan or other medical information on behalf of the employer, rather than the plan, are appropriately designed and administered. As part of this process, steps that concerned covered entities, business associates and employers should consider include:

- Reviewing the adequacy of the practices, policies and procedures of the Covered Entities, business associates, and others that may come into contact with protected health information within the scope of attorney-client privilege taking into consideration the Corrective Action Plan, published OCR noncompliance and enforcement statistics, their own and reports of other security and privacy breaches and near misses, and other developments to determine if additional steps are necessary or advisable;
- Updating policies, privacy and other notices, practices, procedures, training and other practices as needed to promote compliance and defensibility;
- Renegotiating and enhancing service provider agreements to detail the specific compliance obligations of each party; to clarify the respective rights, procedures and responsibilities of each party in regards to compliance audits, investigation, breach reporting, and mitigation; to clarify rights of indemnification; and other related relevant matters;
- Improving technological and other tracking, documentation and safeguards and controls to the use, access and disclosure of protected health information;
- Conducting well-documented training as necessary to ensure that members of the Covered Entity's workforce understand and are prepared to comply with the expanded requirements of HIPAA, can detect potential breaches or other compliance concerns, and understand as well as are prepared to follow appropriate procedures for reporting and responding to suspected violations;
- Tracking actual and near miss violations and making adjustments to policies, practices, training, safeguards and other compliance components as necessary to deter future concern;
- Establishing and providing well-documented monitoring of compliance;
- Establishing and providing well-documented timely investigation and redress of reported violations or other compliance concerns;
- Establishing contingency plans for responding in the event of a breach;
- Establishing a well-documented process for monitoring and updating policies, practices and other efforts in response to changes in risks, practices and requirements;
- Preparing and maintaining a well-documented record of compliance activities;
- Pursuing other appropriate strategies to enhance the Covered Entity's ability to demonstrate its compliance commitment both on paper and in operation.

As part of these compliance and risk management efforts, most covered entities and their business associates will find it advisable to devote significant attention to the business associate relationship and its associated business associate agreements.

Proper management of the expanded compliance obligations and liability exposures created by the HITECH Act generally will necessitate that health plans and other covered entities and their business associates focus significant attention on the reworking of their operating and contractual relationships.

Even before the HITECH Act changes took effect, a strong need for more detailed contracting and planning of these relationships already existed. Since the enactment of HIPAA, the practice of many covered entities and their business associates of appending generic "business associate" representations onto existing services contracts without specific tailoring and planning has created undesirable ambiguities in these agreements. In response to the HITECH Act and other recent developments, both covered entities and their business associates generally also should seek to tighten business associate and other service agreements to promote the improved cooperation, coordination, management and oversight required to comply with the new breach notification and other HIPAA requirements by specifically mapping out these details. Among other things, both covered entities and business associates generally will should:

- Conduct well-documented due diligence on each other's practices and procedures to improve their ability to demonstrate both their commitment to compliance and their realistic efforts to ensure that these commitments are operationalized in performance;
- Renegotiate their service provider agreements to detail the specific compliance obligations of each party relating to for auditing compliance, investigating potential breaches; providing required breach notifications; specify leadership and required cooperation in the event of a breach, charge, or other concern; indemnification and other liability allocations; and other related matters; and
- Pursue appropriate liability and other protection as appropriate.

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, 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 more than 23 years experience advising health industry clients about these and other matters. 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, to health care industry investigation, enforcement and other compliance, public policy, regulatory, staffing, and other operations and risk management concerns. She regularly designs and presents HIPAA and other risk management, compliance and other training for health plans, employers, health care providers, professional associations and others.

Ms. Stamer also regularly works 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. For instance, On May 3, 2011, Ms. Stamer served as the appointed scribe for the ABA Joint Committee on Employee Benefits Agency meeting with OCR and will moderate a teleconference featuring comments by OCR's Susan McAndrew for the Joint Committee on Employee Benefits scheduled for May 16. Her insights on the required "culture of compliance" with HIPAA also recently were quoted in medical privacy related publications of the Atlantic Information Service. 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**.

If you need assistance with these or other compliance concerns, wish to inquire about arranging for compliance audit or training, or need legal representation on other matters please contact Ms. Stamer at (469) 767-8872 or via e-mail **here.**

You can review other recent human resources, employee benefits and internal controls publications and resources and additional information about the employment, employee benefits and other experience of Ms. Stamer **here.**

If you need help investigating or responding to a known or suspected compliance, litigation or enforcement or other risk management concern, assistance with reviewing, updating, administering or defending a current or proposed employment, employee benefit, compensation or other management practice, wish to inquire about federal or state regulatory compliance audits, risk management or training, or need legal representation on other matters please contact Ms Stamer **here** or at (469) 767-8872.

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.**