

**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

## **UCLA Health Systems Payment of \$865,500 To Settle HIPAA Charges Shows Rising HIPAA Risk**

*July 7, 2011*

The University of California at Los Angeles Health System (UCLAHS) has agreed to pay \$865,500 and to strengthen its health information privacy and security practices to settle charges made by the U.S. Department of Health & Human Services Office of Civil Rights (OCR) of violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules.

The latest in a series of high-dollar Resolution Agreements, the UCLAHS Resolution Agreement highlights the need for health care providers, health plans, health care clearinghouses and their business associates to implement and enforce the policies, systems and other management controls and training necessary to ensure that their organizations and their employees and other members of their workforce actually operationally comply with HIPAA.

### **UCLA Resolution Agreement**

The UCLAHS Resolution Agreement resolves two separate complaints filed with OCR on behalf of two celebrity patients who received care at UCLAHS. HIPAA generally requires that covered entities reasonably restrict access to patient information to only those employees with a valid reason to view the information and sanction any employee who is found to have violated these policies. The two complaints alleged that UCLAHS employees repeatedly violated this rule by looking at the electronic protected health information of these patients without a valid reason. OCR's investigation into the complaints revealed that from 2005-2008, unauthorized employees repeatedly looked at the electronic protected health information of numerous other UCLAHS patients.

To settle the two charges, the Resolutions Agreement requires UCLAHS pay a settlement payment of \$865,500 and comply with a corrective action plan that requires UCLAHS to implement Privacy and Security policies and procedures approved by OCR, to conduct regular and robust trainings for all UCLAHS employees who use protected health information, to sanction offending employees, and to designate an independent monitor who will assess UCLAHS compliance with the plan over 3 years.

### **Tightening Rules, Increased Sanctions and Risking Enforcement Fueling Risk**

Increased penalties, tighter rules and recent enforcement actions by OCR make it more important than ever that covered entities tighten their compliance and risk management policies and procedures. This Spring, OCR assessed its first civil monetary penalty (CMP) under HIPAA – a \$4.3 million against Cignet Health of Prince George's County, Md. (Cignet). Two days later, OCR followed up by announcing that General Hospital Corporation and Massachusetts General Physicians Organization Inc. (Mass General) has agreed to pay the U.S. government \$1,000,000 to settle potential HIPAA violation exposures.

According to OCR, Mass General, one of the nation's oldest and largest hospitals, signed a Resolution Agreement with HHS that requires it to pay \$1 million and develop and implement a comprehensive set of policies and procedures to safeguard the privacy of its patients. Like previously announced Resolutions Agreements with Rite-Aid, CVS Pharmacies, Inc. and Provident Health, the Mass General Resolution Agreement follows an extensive investigation by OCR.

The incident giving rise to the agreement involved the loss of protected health information (PHI) of 192 patients of Mass General's Infectious Disease Associates outpatient practice, including patients with HIV/AIDS. OCR opened its investigation of Mass General after a complaint was filed by a patient whose PHI was lost on March 9, 2009. OCR's investigation indicated that Mass General failed to implement reasonable, appropriate safeguards to protect the privacy of PHI when removed from Mass General's premises and impermissibly disclosed PHI potentially violating provisions of the HIPAA Privacy Rule.

The impermissible disclosure of PHI involved the loss of documents consisting of a patient schedule containing names and medical record numbers for a group of 192 patients, and billing encounter forms containing the name, date of birth, medical record number, health insurer and policy number, diagnosis and name of providers for 66 of those patients. These documents were lost on March 9, 2009, when a Mass General employee, while commuting to work, left the documents on the subway train that were never recovered.

Mass General also agreed to enter into a Corrective Action Plan (CAP), which requires the hospital to:

- Develop and implement a comprehensive set of policies and procedures that ensure PHI is protected when removed from Mass General's premises;
- Train workforce members on these policies and procedures; and
- Designate the Director of Internal Audit Services of Partners HealthCare System Inc. to serve as an internal monitor who will conduct assessments of Mass General's compliance with the CAP and render semi-annual reports to HHS for a 3-year period.

OCR's enforcement resolve is further evidenced by its assessment of a \$4.3 million CMP against Cignet. Announced just two days before the Mass General Resolution Agreement, the Cignet CMP announced February 22, 2011 is the first CMP ever assessed by OCR under the HIPAA Privacy Rule. The assessment resulted after OCR found Cignet violated 41 patients' HIPAA rights and committed other HIPAA violations. The \$4.3 million CMP against Cignet applies the expanded HIPAA violation categories and increased HIPAA civil monetary penalty amounts authorized by HIPAA amendments made by Section 13410(d) of the Health Information Technology for Economic and Clinical Health (HITECH) Act. [Read more details.](#)

### **Other Signs of Rising Risks**

Even before the Mass General Resolution Agreement and Cignet CMP announcements, HIPAA Privacy exposures of covered entities for failing to comply with HIPAA already had risen significantly. As of January 1, 2011, OCR reports that 12,781 of the cases it has investigated have been resolved by requiring changes in privacy practices and other corrective actions by the covered entities and has referred more than 484 Privacy Rule breach investigations to the Department of Justice for consideration for potential criminal prosecution. While OCR had not assessed any civil monetary penalties against any covered entity for violation of HIPAA before Cignet, OCR's collection of \$1 Million from Rite Aid in a 2010 Resolution Agreement, \$2.25 million from CVS Pharmacy, Inc. under a 2009 Resolution Agreement and \$100,000 from Providence Health & Services under a 2008 Resolution Agreement demonstrated that covered entities could face significant civil liability for willful violations of the Privacy Rules. See e.g., [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.](#)

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."

These warnings were reiterated by Ms. Vergugo in her announcement of the UCLAHS Resolution Agreement. "Covered entities need to realize that HIPAA privacy protections are real and OCR vigorously enforces those protections. Entities will be held accountable for employees who access protected health information to satisfy their own personal curiosity," said Director Verdugo. She also warned, "Covered entities are responsible for the actions of their employees. This is why it is vital that trainings and meaningful policies and procedures, including audit trails, become part of the everyday operations of any health care provider," In this regard, Ms. Vergugo cautioned, "Employees must

clearly understand that casual review for personal interest of patients' protected health information is unacceptable and against the law."

### **Act To Manage HIPAA Exposures**

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](#).

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