Cynthia Marcotte Stamer, P.C.
SOLUTIONS LAWYER™

Cynthia Marcotte Stamer
Board Certified – Labor and Employment Law
Texas Board of Legal Specialization
Primary Telephone: (214) 452-8297
24-Hour Telephone (469) 767.8872
Addison Telephone (972) 588.1860
cstamer@solutionslawyer.net

Helping Management Manage

Primary Office
16633 Dallas Parkway, Suite 600
Addison, Texas 75001

Mail Room/Plano Office
3948 Legacy Drive
Suite 106, Box 397
Plano, Texas 75023

April 17, 2012

Arizona Physicians Group To Pay $100,000 To Settle HIPAA Charges

The nailing of an Arizona physicians group by the Department of Health & Human Services (HHS) Office of Civil Rights (OCR) for violations of the Health Insurance Portability & Accountability Act of 1996 (HIPAA) demonstrates the need for all health care providers, health plans, health care clearinghouses and their business associates to maintain appropriate HIPAA compliance and risk management procedures and documentation.

Arizona-based Phoenix Cardiac Surgery, P.C. (PCS) will pay the U.S. Department of Health and Human Services (HHS) Office of Civil Rights (OCR) a $100,000 settlement and take corrective action to implement policies and procedures to safeguard the protected health information of its patients to settle OCR charges PCS violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules. Health care providers and other HIPAA-covered entities should heed the PSC and other recent settlements as the latest signal of the risks that health care providers and other covered entities run by failing to adequately implement and administer appropriate HIPAA compliance practices.

The PCS settlement follows an extensive OCR investigation of a report that PCS posted clinical and surgical appointments for its patients on a publically accessible Internet-based calendar. Among other things, the Resolution Agreement documenting the PCS settlement states that OCR's investigation found that PCS violated HIPAA by inappropriately posting patient appointments on a publically accessible website and otherwise failed to establish, administer and train its workforce on HIPAA policies and procedures between 2003 and 2009.

According to the Resolution Agreement, failures by PSC to implement and train workers on required HIPAA policies and procedures contributed to numerous violations of HIPAA over a period of years, including:

- From July 3, 2007 until February 6, 2009, PCS posted over 1,000 separate entries of ePHI on a publicly accessible, Internet-based calendar;
- From September 1, 2005 until November 1, 2009, PCS daily transmitted ePHI from an Internet-based email account to workforce members' personal Internet-based email accounts;
- From September 1, 2005 (when PCS began sending ePHI by email) until April 16, 2009, PCS failed to identify a security official;
- From September 1, 2005 (when PCS began sending ePHI by email) until November 30, 2009, PCS failed to conduct an accurate and thorough assessment of the potential risks and

©2012 Cynthia Marcotte Stamer. All rights reserved.

vulnerabilities to the confidentiality, integrity and availability of the ePHI held by the covered entity;

- From September 1, 2005 until December 3, 2009, the failure by PCS to obtain satisfactory assurances in business associates agreements from the Internet-based calendar and from the Internet-based public email providers that these entities would appropriately safeguard the ePHI received from PCS resulted in PCS permitting the entity providing the Internet-based email account to receive, store, maintain and transmit ePHI on the PCS's behalf without obtaining satisfactory assurances in a business associate agreement with the entity from September 1, 2005 until November 1, 2009; and PCS permitting the entity providing the Internet-based calendar application to receive, store, and maintain ePHI on its behalf without obtaining satisfactory assurances in a business associate agreement with the entity from July 3, 2007 until December 3, 2009.

Under the PCS HHS Resolution Agreement available **here**, PCS will pay a $100,000 settlement amount and a corrective action plan that includes a review of recently developed policies and other actions taken to come into full compliance with the Privacy and Security Rules. Following the announcement by OCR last month that Blue Cross Blue Shield of Tennessee (BCBST) would pay $1,500,000 to resolve HIPAA violations charges, and the latest in a series of Resolution Agreements announced by OCR in recent years, the PCS highlights the willingness to sanction health care providers and other covered entities of all sizes. "The case is significant because it highlights a multi-year, continuing failure on the part of this provider to comply with the requirements of the Privacy and Security Rules," said Leon Rodriguez, director of OCR. "We hope that health care providers pay careful attention to this resolution agreement and understand that the HIPAA Privacy and Security Rules have been in place for many years, and OCR expects full compliance no matter the size of a covered entity."

Enforcement Actions Highlight Growing HIPAA Exposures For Covered Entities

Like the BCBST Resolution Agreement and other previously announced OCR Resolution Agreements, the PCS provides more evidence of the growing exposures that health care providers, health plans, health care clearinghouses and their business associates need to carefully and appropriately manage their HIPAA responsibilities. See **$1.5 Million HIPAA Settlement Reached To Resolve 1st OCR Enforcement Action Prompted By HITECH Act Breach Report**; **HIPAA Heats Up: HITECH Act Changes Take Effect & OCR Begins Posting Names, Other Details Of Unsecured PHI Breach Reports On Website.** Covered entities are urged to heed these warning by strengthening their HIPAA compliance and adopting other suitable safeguards to minimize HIPAA exposures.

Health plans, health care providers, health care clearinghouses and their business associates should tighten privacy policies, breach and other monitoring, training and other practices to reduce potential HIPAA exposures in light of recently tightened requirements and new enforcement risks.

In response to these expanding exposures, all covered entities and their business associates should review critically and carefully the adequacy of their current HIPAA Privacy and Security compliance policies, monitoring, training, breach notification and other practices taking into consideration OCR's investigation and enforcement actions, emerging litigation and other

©2012 Cynthia Marcotte Stamer. All rights reserved.

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.

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 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,

©2012 Cynthia Marcotte Stamer. All rights reserved.

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 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 in fact operating properly and reliably;
- 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 Representation, Training & Other Resources

If you need assistance monitoring HIPAA and other health and health plan related regulatory 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 may be able to 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 24 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.

Scheduled to serve as the scribe for the ABA Joint Committee on Employee Benefits agency meeting with OCR, 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, Ms. Stamer for the second year will serve as the appointed scribe for the ABA Joint Committee on Employee Benefits Agency meeting with OCR. Her insights on HIPAA risk management and compliance frequently appear in medical privacy related publications of a broad range of health care, health plan and other industry publications 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

©2012 Cynthia Marcotte Stamer. All rights reserved.

plan, insurance and financial services, education, employer 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 publications and resources and additional information about the other experience of Ms. Stamer **here.** Examples of some recent publications that may be of interest include:

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.**

©2012 Cynthia Marcotte Stamer, P.C. All rights reserved.

©2012 Cynthia Marcotte Stamer. All rights reserved.