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

March 13, 2012

BCBST Agrees To Pay $1.5 Million In 1st OCR Enforcement Action Prompted By HITECH Act Breach Report

Resolution Agreement Also 1st Announced With Health Plan

Blue Cross Blue Shield of Tennessee (BCBST) has agreed to pay the U.S. Department of Health and Human Services (HHS) $1,500,000 and to take certain other actions specified in a corrective action plan to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules. The **BCBST Resolution Agreement** is particularly significant, both as:

- The first reported enforcement action directly resulting from the filing by a covered entity of a breach report required by the Health Information Technology for Economic and Clinical Health (HITECH) Act Breach Notification Rule; and
- The first reported resolution agreement reached with a covered entity that is a health plan.

These notable enforcement firsts demonstrate both the significance of the HITECH Breach Notification Rule's significance as an OCR HIPAA enforcement tool, and the readiness of OCR to sanction health plans that breach HIPAA's Privacy or Security Rules.

BCBST Breach & Resolution Agreement

The OCR investigation that lead to the BCBST settlement is the first to result from an investigation initiated in direct response to a covered entity filing a HITECH Act required large breach notice.

OCR opened the investigation against BCBST in response to the submission by BCBST of a notice required under the Breach Notification Rule, which requires covered entities to report an impermissible use or disclosure of protected health information, or a "breach," of 500 individuals or more to HHS and the media.*

In response to the Breach Notification Rule, BCBST reported to OCR that 57 unencrypted computer hard drives were stolen from a leased facility in Tennessee. The drives contained the protected health information (PHI) of over 1 million individuals, including member names, social security numbers, diagnosis codes, dates of birth, and health plan identification numbers. OCR's investigation found BCBST failed to implement appropriate administrative safeguards to

* The Breach Notification Rule also requires that covered entities report smaller breaches annually to OCR as part of a consolidated disclosure.

adequately protect information remaining at the leased facility by not performing the required security evaluation in response to operational changes. In addition, the investigation showed a failure to implement appropriate physical safeguards by not having adequate facility access controls; both of these safeguards are required by the HIPAA Security Rule.

To avoid OCR pursuing civil monetary penalties (CMPs) for HIPAA violations stemming from these findings under the strengthened enforcement rules and sanctions enacted as part of the HITECH Act, BCBST has agreed to pay $1,500,000 and adopt other corrective actions detailed in a corrective action plan. In addition to the $1,500,000 settlement, the agreement requires BCBST to review, revise, and maintain its Privacy and Security policies and procedures, to conduct regular and robust trainings for all BCBST employees covering employee responsibilities under HIPAA, and to perform monitor reviews to ensure BCBST compliance with the corrective action plan.

"This settlement sends an important message that OCR expects health plans and health care providers to have in place a carefully designed, delivered, and monitored HIPAA compliance program," said OCR Director Leon Rodriguez. "The HITECH Breach Notification Rule is an important enforcement tool and OCR will continue to vigorously protect patients' right to private and secure health information."

Enforcement Actions Highlight Growing HIPAA Exposures For Covered Entities

The BCBST Resolution Agreements, like the 1st-ever $4.3 million HIPAA CMP that OCR imposed against Cignet Health of Prince George's County, Md. (Cignet) in 2011 and a series of other high dollar Resolution Agreements that OCR has announced against various health care providers over the past few years highlight the significance of the HITECH Act amendments to HIPAA's enforcement and CMP rules, as well as the significance of its Breach Notification Rule as a tool in OCR's investigation and enforcement efforts.

BCBST's breach notification report clearly prompted the investigation that lead to the Resolution Agreement. The opening of the investigation in response to the BCBST Breach Notification report reflects the need for covered entities to be prepared to respond to an investigation when making Breach Notification Rule reports. Failure to timely file required Breach Notifications Rule reports can create additional liabilities for covered entities. However, covered entities reporting large breaches under the Breach Notification Rule need to understand that the making of the report almost certainly will lead to an investigation and very possibly sanctions or other consequences. OCR officials previously have stated that it is the practice of OCR to conduct an investigation into all breaches of the protected health information of 500 individuals or more reported to it under the Breach Notification Rule.

The BCBST Resolution Agreement provides yet another reminder to covered entities and their business associates of the need to carefully and appropriately manage their HIPAA responsibilities. See **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 mitigate against 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 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, 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 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 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 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.

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 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 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.**