SOLUTIONS LAW PRESS

HR & BENEFITS UPDATE

Health Plans & Business Associates Face 2/17 Deadline To Update Policies, Contracts & Procedures For HIPAA Privacy Rule Changes

Connecticut Lawsuit Highlights Expanding Civil Damage Exposure Risks Of Noncompliance

February 16, 2010

By Cynthia Marcotte Stamer

By **Wednesday**, **February 17, 2010**, employer and other health plans and health insurers ("covered entities") and service providers performing functions on behalf of these entities ("business associates") must begin complying meet tighter federal requirements for the use, access, protection and disclosure of protected health information under Privacy & Security Standards of the Health Insurance Portability & Accountability Act (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH Act).

While the HITECH Act gave covered entities and business associates a year to complete the necessary arrangements to comply with these impending HITECH Act changes, many health plans and business associates have not completed the necessary arrangements despite expanding liability exposures that can result from noncompliance.

To mitigate these exposures, covered entities and their business associates should act quickly both to update their services agreements, plans and policies, practices, and procedures, and to implement the training, oversight, and other management procedures necessary to comply with the HITECH Act changes and to mitigate other HIPAA risks.

2/17/10 Deadline To Comply With HITECH Act HIPAA Amendments

On February 17, 2010, health plans and other covered entities and their business associates will become subject to the latest to take effect in a series of amendments to the HIPAA enacted under the HITEC Act. The new rules are part of a broader series of changes to HIPAA made by the HITECH Act that collectively both significantly expand the obligations of covered entities and their business associates to regarding the use, protection and disclosure of protected health information and the liability exposures that can result when covered entities or business associates violate these requirements.

The changes scheduled to take effect February 17, 2010 are likely to require that health plans and their business associates update their written policies, operational procedures, privacy notices and business associate agreements in several respects. For instance, effective February 17, 2010, the HITECH Act generally requires that covered entities and their business associates revise their written privacy policies, privacy notices and operating procedures:

- To meet expanded requirements to honor individual's requests for special restrictions on uses and disclosures of protected health information to health plans for payment purposes
- To restrict protected health information disclosures to the minimum necessary required to accomplish otherwise allowable purpose;

- To comply with new rules that require that the covered entity and its business associates treat any use, access or disclosure of any protected health information made for purposes of making communications about products or services as made for marketing, rather than operational, purposes which are prohibited by HIPAA except where HIPAA's requirements are met;
- To comply with new restrictions on certain fundraising communications made for operational purposes including expanded obligations to allow recipients to opt out of further fundraising communications;
- To prohibit covered entities or business associates from selling protected health information without meeting the amended requirements of HIPAA that a valid HIPAA authorization from the subject of the information and specific reassurances from the purchaser concerning its subsequent use of the protected health information except as otherwise permitted by HIPAA;
- To take into account these tightened restrictions on the use, access or disclosure of protected health information for purposes of complying with new HITECH Act breach notification requirements that took effect in September, 2009, which apply when a covered entity or its business associate knows or should know a breach of "unsecured protected health information" has occurred and for purposes of making the necessary changes in written policies and business associate agreements, training and operational procedures necessary to comply with these rules;
- To directly require business associates comply with HIPAA's requirements in the same manner as other covered entities and make it necessary or advisable that that service provider agreements between health plans and business associates be updated to reflect these and other changes to HIPAA; and
- To implement the necessary written policy changes, notification updates, business associate agreement amendments, training, management oversight and other procedural changes necessary to demonstrate fulfillment with these requirements.

Noncompliance with these and other HIPAA requirements subjects covered entities and business associates to civil penalties, criminal prosecution, civil damage awards under lawsuits brought by state attorneys general, and other legal remedies. In addition, timely update written policies, procedures, business associate agreements, training and documentation is imperative in order for covered entities and their business associates to fulfill their breach notification obligations under new rules enacted as part of the HITECH Act.

Under the HITECH Act, health plans and other covered entities and their business associates have been obligated since September 23, 2009 to notify individuals who are the subject of protected health information, the Department of Health & Human Services and in some cases the media if and when a breach of "unsecured protected health information occurs. Failing to timely update written policies, procedures and training increases the likelihood that health plans, other covered entities or business associates will be obligated to provide breach notifications under these new rules, in addition to their otherwise applicable exposures under HIPAA.

HIPAA Enforcement & Liability Exposures Real and Rising

Health plans and other covered entities, their business associates and others involved in health plan design and operations generally should resist the temptation to underestimate their potential HIPAA exposure based on the limited enforcement of HIPAA by the Office of Civil Rights between 2003 and 2009 for a variety of reasons.

First, the changes taking effect on February 17, 2010 follow the implementation changes to HIPAA's civil and criminal sanctions that took effect on February 17, 2009, when President Obama signed the HITECH Act into law and the new breach notification requirements added by the HITECH Act that took effect on September 23, 2009. The HITECH Act amendments to HIPAA's remedies significantly increase the risk that health plans and other covered entities and their business associates will face civil lawsuits, civil or criminal penalties or other consequences for violating HIPAA.

The expanded risks stem in part from the HITECH Act's amendments to HIPAA's remedy provisions. Among other things, the HITECH Act amended HIPAA to:

- Allow a State Attorney General to sue health plans or other covered entities, business associates or both that harm state citizens by committing HIPAA violations after February 16, 2009;
- Expand the mandate by the Office of Civil Rights to investigate violations and audit compliance with HIPAA;
- Require Office of Civil Rights to impose civil sanctions against health plans and other covered entities and their business associates involved in violations of HIPAA in accordance with tightened standards added to HIPAA by the HITECH Act;
- Revise the criminal sanctions that the Department of Justice can seek against health plans and other covered entities, their business associates and others for violations of HIPAA;
- Amend HIPAA to make clear that HIPAA's criminal sanctions also can imposed on business associates, workforce members and other persons that improperly use, access and disclose protected health information in violation of HIPAA.

A HIPAA civil lawsuit filed on January 13, 2010 demonstrates the willingness of at least some states to exercise the new authority created by the HITECH Act on February 17, 2009 to sue covered entities and business associates that violate HIPAA for civil damages.

The HITECH Act empowers a state attorney general to sue covered entities or business associates engaging in HIPAA violations that harms citizens of the state for statutory damages equal to the sum of the number of violations multiplied by 100 up to a maximum of $25,000 per calendar year plus attorneys fees and costs

On January 13, 2010 Connecticut Attorney General Richard Blumenthal sued Health Net of Connecticut, Inc. (Health Net) for failing to secure private patient medical records and financial information involving 446,000 Connecticut enrollees and promptly notify consumers endangered by the security breach. The suit also names UnitedHealth Group Inc. and Oxford Health Plans LLC, who have acquired Health Net. The first attorney general enforcement action brought based on amendments made to HIPAA under the HITECH Act, Connecticut charges that Health Net violated HIPAA by failing to safeguard protected medical records and financial information on almost a half million Health Net enrollees in Connecticut then allowing this information to remain exposed for at least six months before notifying authorities and consumers.

Even before the HITECH Act amendments, however, the Office of Civil Rights and Department of Justice already were stepping up HIPAA investigation and enforcement. The Department of Justice has obtained a variety of criminal convictions against violators of HIPAA. See, e.g., **2 New HIPAA Criminal Actions Highlight Risks From Wrongful Use/Access of Health Information.** Meanwhile, the Office of Civil Rights in February, 2009 announced that CVS Pharmacies, Inc. would pay $2.25 million to resolve HIPAA charges. This announcement followed the Office of Civil Rights announcement in July, 2008 that Providence Health Care would pay $100,000 to resolve HIPAA violation charges. While not resulting in the significant payments involved in CVS or Providence, the Office of Civil Rights also taken HIPAA enforcement actions against a broad range of other covered entities to redress HIPAA violations or other compliance concerns. To review examples of these other actions, see **here.**

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.

Health Plans & Business Associates Should Take Timely Action To Comply & Manage Risks

As a consequence of these collective HITECH Act changes and growing HIPAA-related exposures, both health plans and business associates generally will find it necessary or advisable among other things to:

- 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.

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 impending HIPAA changes scheduled to take effect on February 17, 2010, 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.

Further updating and tailoring of these and other provisions of services agreements has become even more important over the past year in light of the new breach notification mandates that took effect under the HITECH Act in September, 2009, changes to HIPAA's civil and criminal sanctions that took effect on February 17, 2009, and the impending extension by the HITECH Act to business associates of direct liability for compliance with HIPAA scheduled to occur on February 17, 2010.

Given these changes and the associated obligations and risks, both health plans and other covered entities and their business associates generally should act quickly to manage their own compliance and to minimize exposures that may result from the other's compliance deficiencies. As part of these efforts, both covered entities and their business associates generally should review and tighten business associate and other service agreement provisions to provide for more specific and comprehensive HIPAA-related contractual assurances, as well as improved cooperation, coordination, management and oversight.

Curran Tomko Tarski LLP Can Help

If your organization need advice or assistance in reviewing, updating, administering or defending its HIPAA or other privacy policies, practices, business associate or other agreements, notices or other related activities, consider contacting Curran Tomko Tarski LLP Partner Cynthia Marcotte Stamer.

A widely published author and speaker on HIPAA and other employee benefit and human resources related matters, Ms. Stamer has extensive experience advising health plans, their employer and other sponsors, health insurers, TPAs and other business associates and others about HIPAA and other health plan and privacy matters. Currently serving as both Chair of the American Bar Association (ABA) RPTE Employee Benefits & Other Compensation Group and as an ABA Joint Committee on Employee Benefits Council representative and Former Chair of the ABA Health Law Section Managed Care & Insurance Interest Group, Ms. Stamer has more than 23 years experience assisting employers, insurers, plan administrators and fiduciaries and others to design, implement, draft and administer health and other

employee benefit plans and to defend audits, litigation or other disputes by private parties, the IRS, Department of Labor, Office of Civil Rights, Medicare, state insurance regulators and other federal and state regulators. A nationally recognized author and lecturer, Ms. Stamer also speaks and writes extensively on these and other related matters. For additional information about Ms. Stamer and her experience or to access other publications by Ms. Stamer see **here** or contact Ms. Stamer directly. For additional information about the experience and services of Ms. Stamer and other members of the Curran Tomko Tarksi LLP team, see **here**.

Other Information & Resources

We hope that this information is useful to you. 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** or e-mailing this information **here** or registering to participate in the distribution of our Solutions Law Press HR & Benefits Update distributions **here**. Examples of other recent updates that may be of interest include:

- **COBRA, HIPAA, GINA, Mental Health Parity or Other Group Health Plan Rule Violations Trigger New Excise Tax Self-Assessment & Reporting Obligations**
- **Inapplicability of HIPAA Privacy To Disability Insurer Not License To Impose Unreasonable Claims Requirements**
- **New Mental Health Parity Regulations Require Health Plan Review & Updates**
- **Health Plans & Employers Can Expect Pressure To Pay For Childhood Obesity Counseling From New American Academy of Pediatrics Report**
- **New Labor Department Rule Allows Employers 7 Days To Deliver Employee Contributions To Employee Benefit Plans**
- **Certain Workforce Reductions Trigger Plant Closing Notice & Other Obligations**
- **Newly Extended COBRA Subsidy Rules Require Employers, Administrators Send Required Notices & Update Health Plan Documents & Procedures Quickly**
- **Rising Enforcement and Changing Rules Require Prompt Review & Update of Health Plan Privacy & Data Security Policies & Procedures**
- **Mishandling Employee Benefit Obligations Creates Big Liabilities For Distressed Businesses & Their Business Leaders**
- **DOL Plans To Tighten Employment Protections For Disabled Veterans & Other Disabled Employees Signals Need For Businesses To Tighten Defenses**
- **Employee Benefit Plan Sponsors & Fiduciaries Urged To Review Bonding, Credentials of Staff & Service Providers Under ERISA**
- **Added IRS Guidance For Correcting Employment Tax Overpayments Released**
- **Employer H1N1 Virus Risk Management Requires Employer Care To Manage Virus Risks Without Violating Employment Discrimination or Other Laws**
- **New GINA Genetic Information Based Employment Discrimination & Confidentiality Mandates Take Effect**
- **EEOC Prepares To Broaden "Disability" Definition Under ADA Regulations**

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 **here.**