SOLUTIONS LAW PRESS

HIPAA ALERT

FEBRUARY 26, 2009

Get All The Latest At

March 25, 2009 HIPAA Update Teleconference

HIPAA HAPPENINGS HIGHLIGHTS

- √ **Covered Entities Must Review & Update PHI Data Disposal & Other HIPAA Practices**
- √ **HIPAA Now Applies to Business Associates & Employees**
- √ **OCR & FTC Teaming Up On Privacy Enforcement**
- √ **Privacy Breaches Carry Heightened Liability Risks**
- √ **Stimulus Bill Adds HIPAA Data Breach Notification Duties**
- √ **Stimulus Bill Adds New Limits on Uses & Disclosure**
- √ **Stimulus Bill Expands Criminal & Civil Penalties**
- √ **More**

HIPAA Risks Soar As CVS Agrees to Pay $2.25 Million To Resolve HIPAA Charges & Stimulus Bill Amends HIPAA

A recently announced CVS settlement agreement and newly enacted amendments to the Privacy & Security Standards of the Health Insurance Portability & Accountability Act ("HIPAA") require that employer sponsored and other health plans, health care clearinghouses and third party administrators and their other business associates review, update and tighten their practices governing the use, protection and disclosure of protected health information ("PHI") to guard against growing liability exposures under HIPAA and other federal and state laws. Business associates that have not already done so also must appoint privacy officers and adopt and implement privacy and data security policies and procedures fully compliant with HIPAA and other applicable federal and state rules.

On February 18, 2009, the U.S. Department of Health and Human Services ("HHS") Office of Civil Rights ("OCR") and the Federal Trade Commission ("FTC") jointly announced that CVS Pharmacy, Inc., the nation's largest retail pharmacy chain, will pay the U.S. government a $2.25 million settlement to resolve charges it violated HIPAA and other laws by disposing of pill bottles, prescriptions and other non-electronic records in dumpsters under the second Resolution Agreement announced by OCR. Under the Resolution Agreement, CVS also must take corrective action to ensure that it does not violate the HIPAA privacy rights of its millions of patients when disposing of non-electronic patient information such as identifying information on pill bottle labels. CVS also will conduct employee training on HIPAA compliance and impose sanctions for any noncompliance. In a coordinated action, CVS Caremark Corp., the parent company of the pharmacy chain, also signed a consent order with the FTC to settle potential violations of the FTC Act. The investigation resulting in the settlement marks the first instance where the OCR formally coordinated on investigation and resolution of a case with the FTC.

The CVS Resolution Agreement Announcement was released just one day after President Obama signed into law amendments to the HIPAA Privacy & Security Rules enacted as part of the American Recovery and Reinvestment Act of 2009 (the "Stimulus Bill"). Among other things, the Stimulus Bill:

- Added business associates to the list of parties required to comply with and which are subject to civil and criminal liability for violation of HIPAA's Privacy & Security Standards, so that HIPAA's requirements now apply to employer sponsored and other health plans, health care clearinghouses and their business associates ("covered entities");
- To prohibit the sale of PHI without prior written consent from the subject of the information and to further restrict and regulate certain uses and disclosures of PHI in certain other respects;
- To require covered entities provide certain notifications when a data breach involving PHI occurs to both OCR and the individuals whose information was breached;
- To allow state Attorneys' General to sue for civil damages when a covered entity's breach of HIPAA's Privacy or Security Standards damages citizens in their state; and
- To increase and modify HIPAA's criminal and civil sanctions and to comply with other tightened HIPAA obligations.

The CVS Resolution Agreement and the Stimulus Bill amendments reflect the growing obligations and enforcement risks that covered entities face when PHI is breached or HIPAA's requirements otherwise are not met. They follow the July 2008 announcement by OCR of its first Resolution Agreement with Seattle-based Providence Health & Services ("Providence") under which Providence agreed to pay a $100,000 settlement and implement a detailed Corrective Action Plan for appropriately safeguarding electronic PHI against theft or loss after certain unencrypted electronic PHI was lost or stolen. Covered entities must update policies and practices to avoid these growing liabilities.

HIPAA Privacy and Security Rules restrict the use, access and disclosure by covered entities of PHI and other individually identifiable health care information to those outlined within the Rules. Under HIPAA, covered entities also are responsible for establishing and enforcing policies and procedures that safeguard PHI against improper use, access or disclosure by employees, business associates, and other third parties. Noncompliance with the Privacy and Security Rules exposes a covered entity to criminal prosecution and penalties, civil penalties or both. The Privacy Rule requires covered entities to safeguard the privacy of patient information, including such information during its disposal and restrict use, access and disclosure of this information. The Stimulus Bill extends these requirements to business associates, tightens theme and expands penalties for noncompliance.

According to the Announcement, the CVS settlement applies to all of CVS's more than 6,000 retail pharmacies. It follows an extensive investigation by OCR for potential violations of the HIPAA Privacy Rule. OCR opened its investigation of CVS pharmacy compliance with the Privacy Rule after media reports alleged that patient information maintained by the pharmacy chain was being disposed of in industrial trash containers outside selected stores that were not secure and could be accessed by the public. At the same time, the FTC opened an investigation of CVS.

Among other issues, the reviews by OCR and the FTC indicated that:

- CVS failed to implement adequate policies and procedures to appropriately safeguard patient information during the disposal process; and
- CVS failed to adequately train employees on how to dispose of such information properly.

The Announcement indicated that HHS and FTC also will require CVS to actively monitor its compliance with the HHS Resolution Agreement (the "Agreement") and FTC Consent Order. The monitoring requirement specifies that CVS must engage a qualified, independent third-party to conduct assessments of CVS compliance and render reports to the federal agencies. The HHS Corrective Action Plan will be in place for three years. The FTC requires monitoring for 20 years. The CVS HHS Resolution Agreement and Corrective Action Plan can be found on the OCR Web site at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cvsresagrcap.pdf.

In addition to this Agreement, CVS also has faced sanctions under state data breach laws due to their conduct. In March 2008, Texas Attorney General Gregg Abbott announced that CVS would pay $315,000 to the State of Texas and implement safeguards to resolve charges of violation of Texas laws governing the disposal of customer records containing sensitive personal information. The Stimulus Bill Amendments grant new powers to states' Attorney Generals to seek civil damages when HIPAA Privacy Rule violations harm the state's citizens.

Following the Providence Resolution Agreement and a series of announced criminal convictions under HIPAA in recent years, the CVS Announcement is the latest in a series of HIPAA enforcement developments documenting the importance for covered entities to ensure their ability to demonstrate to federal regulators the effectiveness of their HIPAA compliance efforts by both adopting the written policies and procedures required by HIPAA and continuously monitoring and administering these safeguards. The Announcement also affirms that covered entities must comply with FACTA and other applicable privacy and data security laws as well. The Stimulus Bill changes further elevate the importance of taking these compliance steps.

In response to all of these warnings, covered entities should consider reviewing the adequacy of their current HIPAA Privacy and Security compliance practices taking into consideration the Stimulus Bill Changes, 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.

These and other developments make it imperative covered entities immediately review and update their HIPAA and other data security and privacy practices. If you need help complying with these rules or have questions, call Cynthia Marcotte Stamer at 972.419.7188. To learn more about Cynthia Marcotte Stamer click **here**. For important information concerning this communication click **here**. If you would like to update or remove your contact information for these communications, please click **here**.

MARCH 25
HIPAA UPDATE
TELECONFERENCE

Health care providers, health plans health care clearinghouses and their business associates must update their Privacy & Data Security policies and procedures in response to Stimulus Bill amendments to HIPAA, recent enforcement guidance, and other federal and state law developments. To get caught up on the latest HIPAA medical privacy and date security mandates are invited to participate in the "2009 HIPAA Update Teleconference" on March 25, 2009 from noon to 2:00 p.m. Central Daylight Time. The cost is $75 per registrant.

Register Now

2009 HIPAA Privacy & Security Update Teleconference

March 25, 2009

1:00 p.m. Eastern ~ Noon Central ~ 10:00 a.m. Pacific

MARCH 25

HIPAA UPDATE TELECONFERENCE

Catch Up On The Latest About:

- Stimulus Bill Amendments
- CVS Amendments
- New State Civil Damages Exposure
- New Criminal & Civil Monetary Penalties
- Latest Enforcement Steps You Must Take
- More

Name:

Title: | **Organization:**

Street Address:

City, State, Zip Code

Telephone: | **Fax:**

E-mail:

PAYMENT INFORMATION

I acknowledge and agree that the participation of any registrant named in this registration is conditional upon the receipt of Cynthia Marcotte Stamer, P.C. of the applicable registration fee for each registrant of $75.00. I hereby make payment as follows:

Payment Type: ***(circle applicable and for payment by credit card complete cardholder information)***

Master Card **Visa** **Attached Check/Money Order**

Account Number:

Security Code: | **Expiration Date:**

Cardholder Name:

Street Address:

City, State, Zip Code

By my signature below, I acknowledge and agree that I am authorizing the registration fee for my above registration to be charged to the credit card account set forth above. I represent that am the cardholder or an authorized user of the account of the cardholder and agree to pay in full the amount of such charges.

Cardholder Signature:

Date:

REGISTRATION POLICY: Payment by check or money order and completed registration form must be received at least 48 hours in advance of the program to complete registration. Returned checks shall not constitute payment and shall be subject to a $50.00 administrative charge. Persons not registered at least 48 hours in advance will only participate subject to space availability. CANCELLATION POLICY: In order to receive credit, cancellation (either fax or mail) must be received at least 48 hours in advance of the meeting. Refunds will be made by check via first class mail postmarked within 60 days of receipt of written cancellation notice. DISABILITIES ACCOMMODATION: If you are an individual with a disability who requires accommodation to participate, please let us know at the time of your registration. PROFESSIONAL CERTIFICATION OR CONTINUING EDUCATION CREDIT: Upon request, participants will receive a certificate of participation documenting their participation in the program for use in demonstrating participation for