



# HIPAA Solutions, LC

Special Alert On HIPAA Enforcement

*The Source for Comprehensive HIPAA Compliance Resources*

## **MASSIVE FINE LEVIED AGAINST CVS FOR HIPAA VIOLATIONS**

### **CVS Pays \$2.25 Million and Toughens Practices to Settle HIPAA Privacy Case**

**February 18, 2009 - The U.S. Department of Health and Human Services and the Federal Trade Commission today announced that CVS, the nation's largest retail pharmacy chain, will pay the U.S. government a \$2.25 million settlement and take corrective action to ensure it does not violate the privacy of its millions of patients when disposing of patient information such as identifying information on pill bottle labels.**



The settlement, which applies to all of CVS's more than 6,000 retail pharmacies, follows an extensive investigation by the HHS Office for Civil Rights (OCR) for potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule.

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 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>.

OCR has posted new FAQs that address the HIPAA Privacy Rule requirements for disposal of protected health information. They can be found on the OCR Web site at

<http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfqs.pdf>.

Information about the FTC Consent Order agreement is available at [www.ftc.gov](http://www.ftc.gov).

---

## **ECONOMIC STIMULUS BILL ADDS TEETH TO HIPAA PRIVACY AND SECURITY REGULATIONS**

This HIPAA Alert summarizes major enforcement changes in the HIPAA laws that were enacted when the economic stimulus bill was signed into law by the President.

The changes in the HIPAA Privacy and Security rules are significant and will have a major impact on healthcare providers as well as "non-covered entities".

There are a wide variety of changes, including increased individual rights, but the focus of this document will be on providing a summary of the impact on enforcement .



**It must be noted that elements of the stimulus bill involve changes in both HIPAA privacy and security rules. The enforcement provisions outlined below indicate that an approach to compliance that uses a strategy of "quick fixes" through technology will not suffice to address the new regulatory requirements.**

Healthcare organizations must become proactive in their compliance efforts and understand that "voluntary compliance" is no longer the state of the regulatory environment. In the future, any organization wishing to comply with HIPAA must approach compliance with specific actions related to comprehensive business processes and the security of technology infrastructure used in managing protected health information.

### **Summary of Changes:**

The new rules **REQUIRE** mandatory audits of Covered Entities (CE's) and Business Associates (BA's) to ensure HIPAA compliance. The rules also require the Secretary of HHS to report to Congress on the number of audits performed and the outcome of these audits. Other enforcement statistics must also be provided to Congress.

**The rules give Attorney Generals in every State the ability to sue (bring a civil action) on behalf of residents of the State against "any person" violating HIPAA in a Federal District court. The rules provide for statutory damages, and State AG's will be able to utilize private law firms to assist in carrying out their obligations under this section of the new rules.**

Under the new regulations, it is very clear that BA's **MUST** follow the same Privacy and Security rules as CE's. The new rules also specifically state that BA's and CE's will be held **EQUALLY** liable in relation to civil and criminal penalties associated with violating HIPAA.

The changes in the HIPAA rules incorporate very strong breach notification requirements. For example, both BA's and CE's **MUST** implement the following breach notification requirements when a breach is discovered under the new rules.

**The CE MUST notify every individual whose "unsecured PHI" information has been breached. In addition, after a breach has been discovered, the CE MUST notify every individual that the CE "reasonably believes" has had their unsecured PHI breached, i.e., accessed, acquired or disclosed as a result of the actual breach itself.**

Following the discovery of a breach by a BA, the BA **MUST** notify the CE of that breach of unsecured PHI. In addition, the "notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during such breach."



A breach is treated as discovered by both the CE or BA on the first day the breach is known to the CE or BA, meaning, "any person, other than the individual committing the breach, that is an employee, officer, other agent" of either the BA or CE, respectively, "or should reasonably have been known to such entity or associate (or

person) to have occurred."

CE's and BA's MUST provide notification as required by law respectively, within 60 calendar days after discovery of a breach. The burden of proof is on the CE or BA with regard to demonstrating that all notification requirements were met.

### **CE's MUST provide notification as follows:**

- To the individual by first class mail or through e-mail as appropriate,
- To the individual through a posting on the home page of the web site of the CE involved for a period of time as determined by the Secretary of the Department of Health and Human Services or through a major media outlet if the breach involved 10 or more individuals "for which there is insufficient or out-of-date contact information,"
- To "prominent media outlets" serving a State or jurisdiction in the case where a breach has been discovered involving more than 500 residents of that State or jurisdiction, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach,
- To the Secretary of Health and Human Services in the case where a breach involves less than 500 individuals annually, during the year when the breaches occurred,
- To the Secretary of Health and Human Services in the case where the breach involves over 500 individuals immediately,  
Posting to the HHS website in the case of a CE and a breach involving more than 500 individuals,

All notices must have specific information that must be included in the notice itself including information on what the CE has done to mitigate the breach as required by the HIPAA Privacy rule, along with other information.

New rules involve the direct application of both civil and criminal penalties to a BA, in the event the BA violates HIPAA.

**The Treatment, Payment and Health Care Operations, or TPO exceptions have been eliminated for Electronic Health Records (EHRs). In certain cases, this will go into effect for some covered entities as early as 2011. In addition, there are significant changes associated with the "minimum necessary rule" and "accounting of disclosures" relating to both BA's and CE's.**

New prohibitions on the sale of EHR's or PHI are established.

New breach notification requirements are established for vendors of personal health records (PHR's). Changes involve enforcement through the Federal Trade Commission, specifically unfair and deceptive acts and practices for vendors of PHRs.



New rules provide clarification on how rules impacting Regional Health Information Organizations, e-Prescribing Gateways and Health Information Exchange Organizations will generally be incorporated into HIPAA.

New rules provide clarification on "**wrongful disclosures**" and make it a criminal offense to violate the Privacy rule's authorization requirements.

Another level of civil liability is added to rules relating to willfully neglecting HIPAA compliance. This includes mandatory investigations and civil or criminal penalties

associated with this type of violation.

New rules utilize fines to further federal enforcement activities.

New rules enable the distribution of fine revenues to harmed individuals.

The new rules significantly increase civil money penalties that eliminate previous defenses for non-compliance. For example, a tiered penalty structure is outlined that enables fines to be levied against "persons" that did not know about the need for compliance, up to \$25,000.00 for one calendar year for one "identical violation." In other words, a specific violation of an "identical requirement or prohibition" may not exceed \$25,000.00 during a calendar year.

**Fines apply to persons that willfully neglect to comply with HIPAA and range from \$10,000.00 per violation to \$50,000.00 per violation, up to \$1.5 million per calendar year for one "identical violation," if corrective action is not taken in the case of willful neglect to comply with HIPAA. In other words, a specific violation of an "identical requirement or prohibition" may not exceed \$1.5 million during a calendar year.**

The rules enable the Office of Civil Rights within the Department of Health and Human Services on the federal level to continue to use "corrective action plans" to enforce HIPAA. Time and costs to implement such plans may prove to be significant.

---

**[HIPAA Solutions, LC](#)** provides comprehensive compliance resources including assessments, remediation, software and consulting.

The HIPAA ComplyPAK is a suite of cost effective software tools that automates the legal/technical compliance activity required by HIPAA.

Contact us Toll Free at (877) 779-3004 or e-mail [info@hipaasolutions.org](mailto:info@hipaasolutions.org).

**The content of this Alert is for informational purposes and not intended as legal advice.**

© 2009 HIPAA Solutions, LC