



## IMPORTANT CHANGES IN HIPAA REGULATIONS ENACTED

**Peter MacKoul, JD**

**February 16, 2009**

*(A Note to the Reader - The information contained in this document is meant for informational purposes only and not intended to act as a substitute for the advice of an attorney. Please contact appropriate legal counsel before acting on any of the information contained in this document.)*

The material in this document summarizes major enforcement changes in the HIPAA laws as a result of the stimulus bill that has been passed by Congress and has been sent to the President for his signature.

The changes in the HIPAA Privacy and Security rule are *significant* and will have a major impact on healthcare providers as well as "non-covered entities". Although there are a wide variety of changes including increased individual rights, the focus of this document will be on providing a summary of the changes involving enforcement.

It must be noted that elements of the stimulus bill involve **changes in both HIPAA privacy and security rules**. Consequently, compliance efforts must be undertaken that involve taking specific actions and documenting those actions as required by law.

In addition, 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. Specific actions involving comprehensive business process and technology efforts must be undertaken to achieve and maintain compliance in the future.

Summary of Changes:

1. 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.



2. 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.
3. 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.
4. 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.
  - a. 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.
  - b. 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."
  - c. **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."
  - d. 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.
  - e. **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.
5. New rules involve the direct application of **both civil and criminal penalties** to a BA, in the event the BA violates HIPAA.
  6. 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.
  7. **New prohibitions** on the sale of EHR’s or PHI are established.
  8. 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.

9. 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.
10. New rules provide clarification on “wrongful disclosures” and make it a **criminal offense** to violate the Privacy rule’s authorization requirements,
11. 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.
12. New rules utilize fines to further federal enforcement activities.
13. New rules enable the distribution of fine revenues to harmed individuals.
14. 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.
15. 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.
16. 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.

**Please contact HIPAA Solutions, LC toll free at (877) 779-3004 or email [info@hipaasolutions.org](mailto:info@hipaasolutions.org) with questions or to discuss compliance resources.**