



WWW.HIPAA SOLUTIONS.ORG

"Reliable Resource For Comprehensive HIPAA Compliance"

HIPAA Solutions, LC - Compliance Alert

January 2008

HIPAA Enforcement Heats Up In 2008

CMS Audits, Court Rulings & New Regulations Up The Risks

Since the enactment of the HIPAA Privacy rule over 5 years ago and the enactment of the Security rule over 3 years ago, a great deal of discussion has focused on the topic of "HIPAA enforcement". In fact, the amount of discussion has far outpaced the level of enforcement. There has been so little enforcement (up until now); that even mentioning enforcement in a crowd causes apathetic yawns from some listeners



However, the times are changing and any entity that is subject to HIPAA should take notice. Although there have been numerous HIPAA enforcement warnings, two recent developments should not be ignored.

First, CMS or the Centers for Medicare and Medicaid recently entered into a year long contract with Pricewaterhouse Cooper (PwC) to conduct nationwide security audits of covered entities (CE's).

The CMS contract may allow PwC to audit for the following issues among others:

- Information access management
- Security awareness and training
- Access control
- Workstation use
- Device and media controls

A very important issue related to the CMS action is that the HIPAA Security rule audits also mean that CE's must be compliant with the Privacy rule.

For example, the Security rule states that CE's (healthcare providers,

insurers - including educational institutions, state, local, and federal governmental agencies, that provide healthcare services or health insurance) must "protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part," citing the Privacy rule at 45 CFR § 164.306 (a) (3).

In other words, the Security rule mandates compliance with the Privacy rule! Furthermore, the list of the governmental organizations currently enforcing HIPAA includes:

- **The Office of Inspector General (OIG)** - auditing healthcare providers (Piedmont Hospital in Atlanta was one of the first and more audits are pending)
- **The Department of Justice (DOJ)** - prosecuting and incarcerating non-healthcare providers for violating HIPAA (multiple prosecutions and several incarcerated)
- **The Centers for Medicare and Medicaid (CMS)** - conducting nationwide audits on HIPAA using PwC (first set of target entities has been identified)
- **The Federal Department of Health and Human Services (DHHS)** - currently assembling a Privacy enforcement team.

In another major enforcement development, the civil litigation arena has seen both federal and state level courts allowing individuals to bring **negligence lawsuits by using HIPAA as a "standard of care"** for justifying the lawsuit.

And, as if this increase in enforcement activity is not enough to motivate CE's to begin to take compliance seriously, specific **legislation has been proposed in the U.S. Senate** to strengthen enforcement. The legislation is called "HIPSA" or the Health Information Privacy and Security Act.

HIPSA is focused on the protection of individual privacy rights, national security, intelligence and fighting identity theft related to medical information. The following summary shows how HIPSA would function if it is enacted.

HIPSA would NOT supersede or overturn HIPAA, but would amend and assist in enforcing HIPAA.

HIPSA would mandate internal audits on the Privacy and Security rules and the creation of Risk Management processes and procedures to ensure compliance by all organizations that handle PHI.

HIPSA would re-enforce the application of HIPAA to schools, universities, and governmental organizations while broadening the impact of laws protecting medical information to all types of entities that deal with PHI beyond those to which the federal courts have currently applied HIPAA.

HIPSA would increase the criminal liability, i.e., fines and jail time beyond those found in HIPAA.

HIPSA would provide for the "debarment" of all types of organizations, including governmental, health care providers, insurers, employers, schools, and universities, for criminal violations of laws designed to protect PHI; in other words, organizations will no longer be able to receive any benefits under any Federal health program or other Federal procurement program. Finally, covered entities may also be prohibited from doing business with any organizations that conducts business with the Federal government.

HIPSA would allow individuals to sue directly on the federal level for compensatory and punitive damages for knowing or negligent violations relating to the individual's right to privacy in medical information. In addition, it would make the covered entity or a "principal" jointly and severally liable with the principal's "agent" for these types of damages for any actions of the principal's agent acting within the scope of the agency.

HIPSA would allow for enforcement by State Attorney Generals or local law enforcement agencies able to prosecute consumer protection laws, to bring a civil actions in the Federal District Court to "obtain civil penalties of not more than \$1,000 per day per individual whose personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, up to a maximum of \$50,000 per day".

HIPSA would protect employees against employers that "discharge, demote, suspend, threaten, harass, retaliate against, or in any other manner discriminate or cause any employer to discriminate against an employee," that blows the whistle against the employer for violations of the HIPSA Act.

In summary, HIPAA / HIPSA enforcement is not going away. "Band-Aid compliance" efforts, i.e., using canned policies and procedures without taking any real compliance actions or relying on "inaccurate advice" from naysayers who believe that the privacy regulations are inconsequential may backfire on organizations that don't take steps towards real compliance.



HIPAA Solutions, LC provides reliable resources to assist healthcare providers, government entities, schools & universities and businesses with HIPAA compliance including:

- **Job function specific training** with real world practical application to assist staff in understanding and implementing procedures for their individual requirements with regular updates to ensure that changes in regulations or court rulings are addressed in the organization's

- compliance efforts
- **Auditing and consulting** to analyze an organization's compliance status and vulnerabilities to focus actions on areas for remediation to meet compliance requirements
 - **Products and tools to assist an organization in real compliance activity** across the entire organization. The HIPAA ComplyPAK© provides the ability to address the requirements of both the HIPAA Privacy and Security rules and the PHI Locator© (PHIL) provides a software tool for initial analysis of the use of Protected Health Information or PHI usage in an organization. PHIL also allows the tracking of information use in daily operations and allows the organization to address the legal requirements of Section 514 and "Accounting of Disclosures".

For more information on HIPAA Solutions, LC, visit our web site at www.hipaasolutions.org.

Training
Auditing & Consulting
Compliance Tools & Software

Contact HIPAA Solutions, LC today for your compliance resources. Our comprehensive resources for education & training, auditing & consulting, and compliance software & tools can help your organization reach compliance with HIPAA regulations on Privacy and Security.

Contact us via email at info@hipaasolutions.org or call toll free at 877-779-3004.

HIPAA Solutions, LC
HIPAA Compliance Specialists

© 2008 HIPAA Solutions, LC
Toll Free: 877-779-3004

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