



## Risks Rise In 2007 For HIPAA Non-Compliance

### Litigation & Enforcement Actions Expand

A recent article in "The National Law Journal" analyzing the latest developments in enforcement and litigation related to the protection of health information covered under the Federal Health Insurance Portability and Accountability Act (HIPAA) concluded that any entity that falls under HIPAA regulations should understand that enforcement and litigation activity is rapidly expanding.

The article stated, "The Health Insurance Portability and Accountability Act is raising new legal fears for health care providers in light of tougher government enforcement and recent court rulings that could trigger private lawsuits.

Labor and employment attorneys who represent health care providers are especially concerned about the prospect of private HIPAA litigation because the law does not currently provide a private right of action. But plaintiffs appear to be getting around that. They say that courts in recent years have begun letting plaintiffs use HIPAA standards to prove liability in privacy lawsuits alleging that their sensitive medical records were inadequately protected."

In two recent and similar cases, *Sorensen v. Barbuto*, 143 P.3d 295 (Utah Ct. App. 2006) and *Acosta v. Byrum*, 638 S.E.2d 246 (N.C. Ct. App. 2006), courts rulings allowed individual causes of action related to privacy claims based on "the standard of care HIPAA establishes for protection of patient medical records."

This basically circumvented the idea that only class action litigation is allowed under HIPAA and could open up a broad exposure for litigation if an entity has not adequately addressed required compliance activity.

In addition, the level of Federal enforcement activity has noticeably accelerated in the first half of 2007. The Fed's have initiated audits through the Office of Inspector General, expanded subpoena authority from HHS to the Office of Civil Rights and created a web site to assist citizens in filing complaints. State Attorney Generals have also been directed to create enforcement departments to assist in addressing healthcare fraud with a strong emphasis on privacy.

Attorney Joseph Lazzarotti of Jackson Lewis in White Plains, whose clients include sponsors of health care plans and health care providers, gave his strategy in advising clients about HIPAA in the Law Journal article.

"I want them to know that HIPAA does really mean something and the government is going to do something about it. What that is, well, it's more than they were doing yesterday," he said. He tells clients they should, ". . . know exactly what information is on hand and who has access to it. And then document everything . . ."

He admitted that clients questioned why they needed to comply and said, "One of the things that clients have objected about HIPAA is, 'Why do we have all these policies and procedures?' It's because if you get an audit, you're going to need to point to something tangible that says, 'Here's what we did,'" Lazzarotti said. "You can't just say, 'We don't do that.'"

School districts are specifically designated in the HIPAA regulations, along with

healthcare providers, as organizations that are covered by HIPAA. However, many districts have been mistakenly led to believe that their only vulnerability is in the area of group health plans and benefits.

In reality, there are many areas in school districts that may fall under HIPAA including Special Education, Nursing, Counselors, Public Safety, Athletics and benefits/Group Health Plans. Many of these areas utilize sensitive health information of students or employees on a regular basis and much of that information falls specifically under HIPAA. Employee records in health plans are often only a small part of the potential exposure to privacy and security violations.

In light of the current emphasis on privacy and security and the increases in litigation and government enforcement activity, districts may want to examine their compliance status and take steps quickly to address vulnerabilities.

(This article includes references from The National Law Journal June 1, 2007 edition)

### ***Technical Snafu's Put Schools At Risk Of Privacy Violations***



Recent headlines describing a major security breach could be the type of legal and public relations nightmare any school district might face because of a procedural or technical slip up that results in a security breach which exposes protected information of students or employees. The following excerpts are from [eschoolnews.com](http://eschoolnews.com) and the Indianapolis Star in May of 2007.

#### ***District posts confidential data online***

*Unsecured servers expose information for some 7,500 Indianapolis students*

*From eSchool News staff and wire service reports*

*May 21, 2007--In one of the worst security breaches ever in a public K-12 school system, confidential data for thousands of Indianapolis Public Schools (IPS) students--including, in some cases, medical information and Social Security numbers--were accidentally posted online.*

*The Indianapolis Star, which discovered the error and reported it May 16 to the district, said it appeared the problem had been going on for at least two years.*

*The Star reported that at least 7,500 students were affected. The nature of the information posted to the internet varied.*

*Among the files that were accessible were special-education diagnoses, students' names and addresses, and essays in which some students revealed personal details such as experiences with abuse.*

*Details about the IPS computer system, employee job reviews, and other personnel files also were posted.*

*Beth Givens, an identity-theft expert with the Privacy Rights Clearinghouse, said the most dangerous data consisted of Social Security numbers for about 20 students and five staff members.*

*"That's horrendous--the entire family has been victimized," she said.*

*Internet security expert Roger Thompson, who reviewed the IPS web site at the Star's request, said the error appeared to have resulted from improper settings on the district's server or from a software flaw . . . .*

The ultimate damage to the school district has yet to be determined since the situation is still evolving. But, in addition to the public relations damage, there is a serious possibility of litigation. And, since medical data may have been included in the information that was released, HIPAA violations could become part of the scenario.

A key component of the HIPAA regulations is the Security component, which requires any organization that is covered by HIPAA to take specific actions to protect networks and storage of Protected Health Information (PHI) and to document those specific actions in the event an incident occurs or an audit is conducted on the organization. Often, districts may actually take some required actions but, do not properly document them so they may still be exposed to non-compliance risks.

Conducting a thorough audit of technology and business practices related to the daily handling of sensitive information in special education, counseling, nursing, athletics, benefits and IT departments, among other areas, is an important part of protecting the security of employee or student information and will also reduce the risks to districts of mishandling information.

## Proper Procedures Are Important Part Of Privacy

HIPAA requires that any organization that utilizes "Protected Health Information" (PHI) as defined by HIPAA take specific actions to protect that information, which can include physical or mental health information and billing information.



But, almost as important as taking the actions required by HIPAA is the DOCUMENTATION of actions as required by the law. In the event of an incident which may expose an organization to litigation or prosecution, documentation can make the difference between serious damages and inconvenience.

However, documentation without taking required actions could cause even more serious problems if an incident occurs because of the appearance of deliberately ignoring the regulatory requirements. The best strategy is to take steps to protect information as required and make sure that documentation and training of staff in proper procedures is accomplished.

---

### HIPAA Solutions, LC Announces the HIPAA ComplyPAK®

[www.hipaasolutions.org](http://www.hipaasolutions.org)

*Compliance for Education, Government, Business & Healthcare*

HIPAA Solutions, LC offers comprehensive and affordable compliance resources through the HIPAA ComplyPAK®, a suite of products and tools that can be implemented by clients to manage Privacy and Security elements of HIPAA. ComplyPAK basically automates the legal and technical compliance efforts for HIPAA Privacy and Security.

ComplyPAK also addresses group health plan requirements of HIPAA and provides automation for tracking Protected Health Information (PHI) uses within an organization.

Contact HIPAA Solutions, LC today to schedule a demonstration or webinar briefing on the HIPAA ComplyPAK® or to discuss compliance consulting needs. Email [info@hipaasolutions.org](mailto:info@hipaasolutions.org) or call Toll Free at 877-779-3004.

---

**"HIPAA & ISD's - TRENDS IN ENFORCEMENT"**

**SIGN UP FOR A FREE WEBINAR TODAY**

**Email [info@hipaasolutions.org](mailto:info@hipaasolutions.org) to schedule a Webinar**

---

**HIPAA Solutions, LC**  
*HIPAA Compliance Specialists*

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