

Fed's Conduct HIPAA Audits In Surprise Move

Office of Inspector General Begins HIPAA Audits

In an unexpected move that could impact any organization that is subject to HIPAA, the Federal Department of HHS and the Office of Inspector General (OIG) announced the start of government conducted HIPAA security compliance audits on organizations that are subject to HIPAA. The OIG initiated the first audit activity of this kind on March 5, 2007 at Piedmont hospital in Atlanta.



The OIG's action was described in a recent report from the March 8, 2007 issue of Medicare Advantage News, which also reported that the OIG is expanding its audit resources and plans to perform audits on a national basis in the future.

Government audits should serve as a red flag to every organization that is covered by HIPAA. Organizations may want to thoroughly review their compliance activities and any gaps in compliance should be addressed as quickly as possible to reduce the risk of non-compliance penalties.

It is important that Privacy and Security Officers understand that "boilerplate" policies and procedures that are not supported by real compliance actions may not sufficiently protect an organization if an audit occurs.

HIPAA LAWSUIT RISKS EXPAND

Appellate Court Rules On Right of Individual Action Related to HIPAA

An appeals court ruling in the Acosta v. Byrum case (Court of Appeals of North Carolina) has opened the potential for a new avenue of exposure to litigation for organizations that are subject to HIPAA if they have not adequately addressed HIPAA compliance issues.



In this case, the plaintiff filed an individual lawsuit for the negligent infliction of emotional distress. The plaintiff's allegation was that her doctor was negligent and violated HIPAA by allowing his office manager to use his medical record access number, which the office manager used to retrieve the patient's confidential psychiatric and medical records which were then disclosed to third parties without the patient's consent.

While HIPAA does not allow for an individual cause of action, the use of HIPAA privacy violations as a standard of care for negligence liability may be used by other individuals whose health information is disclosed, inadvertently or deliberately.

This ruling may be used by plaintiff's attorneys in the future as leverage in lawsuits involving disclosure of medical information or Individually Identifiable Health Information. It would be a good idea for any organization to take a new look at the level of compliance if they are subject to HIPAA.

Criminal Conviction For HIPAA Violation



A criminal case in Florida involving HIPAA has resulted in the conviction for criminal violations including computer fraud, identity theft, Medicare fraud and HIPAA violations for disclosure of individually identifiable health information.

The case involved the theft of Social Security Numbers, Medicare numbers and names by an employee and his relative from a medical clinic that were then used to file over \$7 million dollars in false Medicare claims. One of the defendants, Fernando Ferrer, Jr. faces up to 30 years in prison and \$1,750,000 in fines, including 10 years and \$250,000 for HIPAA violations.

HIPAA Impact On Technology In ISD's

Courts have applied HIPAA to schools and universities along with FERPA. Educational associations such as the National School Board Association and Texas Association of School Boards recommend that school districts take steps to ensure compliance with HIPAA. If information qualifies as "Protected Health Information" (PHI), as regulated by the Health Insurance Portability and Accountability Act (HIPAA), used on a daily basis in Nursing, Counseling, Special Education, Public Health, Athletics, Safety, Human Resource or IT departments, it is important to reduce compliance risks.

HIPAA Solutions, LC Announces the HIPAA ComplyPAK®

Compliance for Government, Education, 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.

The **Strategic Compliance Solution Security Module (SCS)** of ComplyPAK allows IT Departments to assess vulnerabilities related to HIPAA and is based on the standards of **ISO** (International Standards Organization), **NIST** (National Institute of Standards & Technology), **FIPS** (Federal Information Processing Standards) and the **CFR** (Code of Federal regulations).

The SCS Security module includes several critical tools that provide for proper assessment and remediation of vulnerabilities including the **Initial Security Assessment for Risk Analysis** which is designed to model the current Information Security Architecture for an organization and perform a basic gap analysis as it compares to HIPAA. Other tools in SCS then assist in remediation vulnerabilities that may be revealed by the Risk Analysis.

If you wish to contact HIPAA Solutions, LC to schedule a demonstration or webinar briefing on the HIPAA ComplyPAK® or to discuss compliance consulting requirements, email 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 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.