



SUMMARY Of HIPAA Enforcement On Covered Entities - 1st Qtr - 2008

(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.)

HIPAA Solutions, LC has conducted an analysis of trends of enforcement activities and court rulings related to HIPAA which indicates that every organization subject to HIPAA should evaluate its current level of compliance and take steps to address any areas of non-compliance to avoid potential litigation, prosecution, disruption of operations and the associated costs of dealing with a data breach or the improper use of PHI. The following information clearly shows a pattern of stronger enforcement and risks of non-compliance.

1) EMPLOYEE DISMISSALS FOR VIOLATING HIPAA – One of the costs to an organization for inadequate training or improper procedures related to PHI used by the organization is the necessity for terminating skilled employees who violate HIPAA regulations. This means dealing with potential EEOC activity, negative public relations, hiring and training replacements for former employees. Much of this disruption could be eliminated with proper training and assessments to ensure that adequate safeguards were in place to ensure compliance.

2) CRIMINAL PROSECUTION FOR VIOLATING HIPAA – One of the most recent criminal prosecutions has just resulted in an indictment of a worker in a counseling environment where PHI was used in an identity theft scheme.

3) HIPAA “DERIVATIVE LAWSUITS” ALLOWS INDIVIDUALS TO SUE USING HIPAA

(UPDATE March 17, 2008) – “HIPAA Derivative Litigation” is a new concept that has developed through court rulings related to misuse of PHI. The information in this analysis provides a quick reference guide on “HIPAA derivative” civil lawsuits.

The case information that follows below involves breaches of HIPAA that resulted in individuals suing under negligence and other theories to sustain personal lawsuits. In sum, the results of the court rulings represent a method of using HIPAA to sustain individual lawsuit which dramatically expands the risk to organizations for non-compliance.

HOSPITALS & OTHER HEALTHCARE PROVIDERS GENERALLY

TRANSUNION CASE: STATUS AS OF March 17, 2008: ONGOING (HOWEVER A SETTLEMENT AGREEMENT HAS BEEN REACHED WITH ONE ORGANIZATION FOR AN “UNDISCLOSED FINANACIAL SUM.”) This case involved the first prosecution under HIPAA involving Eric Drew. Drew’s identity was stolen by a hospital employee that eventually went to jail under HIPAA for committing ID theft. Drew sued 6 financial institution including TransUnion, Equifax, Chase bank, Citibank and Experian. The TransUnion settlement was the first.

PUNO V. MOUNT DESSERT ISLAND HOSPITAL: STATUS AS OF March 17, 2008 A SETTLEMENT AGREEMENT WAS REACHED (THE TERMS ARE “UNDISCLOSED.”) The HIPAA violation in this case resulted in a federal lawsuit for employment discrimination based on race and gender, retaliatory



discharge, and a whistleblower's claim under state law. Please note settlements of this type usually involve money among other types of compensation going to the plaintiff. This does not include the litigation costs to the hospital.

SORENSEN V. BARBUTO: STATUS AS OF March 17, 2008 AFTER YEARS OF LITIGATION, THE DEFENDANT DOCTOR FAILED TO PREVENT THIS TORT CASE FROM GOING TO TRIAL.

THE UTAH STATE SUPREME COURT ALLOWED THE PLAINTIFF TO SUSTAIN AN INDIVIDUAL TORT LAWSUIT STEMING FROM A HIPAA BREACH. THE CASE WAS "REMANDED" OR SENT BACK TO THE TRIAL COURT FOR ADDITIONAL LITIGATION. THE DEFENDANT MUST EITHER CONTINUE TO PAY FOR LITIGATION, OR REACH A SETTLEMENT AGREEMENT. In this case the plaintiff sued his treating physician for negligence based on a HIPAA violation and breach of confidentiality. After years of litigation costs the defendant lost in his attempt to prevent this type of lawsuit from reaching a jury. The defendant is left with no recourse other than to continue paying litigation costs or settle the case with the plaintiff.

COUNTY, STATE AND LOCAL GOVERNMENT

NELSON V. HENNEPIN COUNTY MEDICAL CENTER: STATUS AS OF March 17, 2008 ONGOING LITIGATION (ALL COSTS HAVE BEEN INCURRED BY THE GOVERNMENTAL ENTITIES and INDIVIDUALS INVOLVED IN THE CASE.) The plaintiff sued Hennepin County Medical Center, two hospitals and the City of North St. Paul for a "HIPAA-Derivative Medical Record Disclosure and Privacy Claims: Negligence, Breach of Contract, Minnesota Human Rights Act, Wrongful Detention, and Deprivation of Freedom." The FEDERAL DISTRICT court made the following recommendation, "the Court strongly believes that it would be in all parties' best interests to engage in good-faith settlement discussions with Magistrate Judge Nelson before they continue their litigation in state court." The District Court made this recommendation based on the costs of litigation and other concerns.

- 4) MEDICAL IDENTITY THEFT RISKS TO PATIENTS AND HEALTHCARE ORGANIZATIONS –** Recent reports indicate that a growing concern in protection of sensitive information, fraud and identity theft involving health information. (MSNBC Report)

The impostor in the ER

Medical identity theft can leave you with hazardous errors in health records

Victims of medical identity theft could face problems such as insurance maxed out to its lifetime limit, years spent untangling paper trails and medical records permanently altered.

<http://www.msnbc.msn.com/id/23392229>

- 5) FEDERAL GOVERNMENT STEPS UP ENFORCEMENT ACTIVITY**

June 15, 2007 (Computerworld) An audit of Atlanta's Piedmont Hospital that was initiated by the U.S. Department of Health and Human Services in March is raising concerns in the health care industry



about the prospect of more enforcement actions related to the data security requirements of the federal HIPAA legislation. . . .

Proposed HIPSA legislation would add urgency to enforcement of HIPAA rules

Memphis Business Journal - by Dwight Flax

The backlash caused by the perceived lackluster enforcement of the HIPAA privacy and security rules has ushered in a new proactive era -- an incremental ramping up that signals a move away from complaint-based voluntary compliance to direct cross-agency audits and the potential for new legislation that increases HIPAA privacy and security enforcement.

. In July, Sen. Edward Kennedy and Sen. Patrick Leahy introduced the Health Information Privacy and Security Act of 2007 that apparently would not supplant HIPAA but require the Department of Health and Human Services to revise HIPAA to be consistent with HIPSA. . . . In mid-April, DHHS delegated to the Director of Office for Civil Rights (the agency within DHHS that enforces the HIPAA Privacy Rule), the authority to issue subpoenas in investigations of alleged violations. . . .
<http://www.bizjournals.com/memphis/stories/2007/10/22/focus4.html>

6) INCREASED RISKS TO HEALTHCARE PROVIDERS FROM CYBER ATTACKS

Are Healthcare Organizations Under Cyberattack?

Healthcare organizations are reporting more Web attacks, disappearing laptops, insider security incidents. What's more, a surprise audit is looming.

Ellen Messmer, Network World
Wednesday, February 27, 2008 04:49 PM PST

. . . . **Healthcare organizations are stepping up efforts to protect electronic patient information as they witness increased attacks against hospital networks, mindful how a data breach could hurt patients and their own reputations.** Besides the loss of confidence such security incidents provoke, the specter of government regulatory probes is looming related to the federal security and privacy rules in the Health Insurance Portability and Accountability Act (HIPAA). **The U.S. Department of Health and Human Services (HHS), which oversees HIPAA compliance, has contracted with the firm PricewaterhouseCoopers (PWC) to conduct surprise audits of hospitals this year, says Gartner analyst Barry Runyon.**

7) SUMMARY

The information in this brief shows a pattern of increased enforcement and clearly indicates that a serious approach to adequate training, accurate assessment of risks and compliance status, along with implementation of comprehensive policies, procedures and a secure



infrastructure are the elements that will reduce risks and allow an organization to avoid disruption of operations and the costs of litigation, prosecution and employee turnover.