

*The Source for Comprehensive HIPAA Compliance Resources*

## **Times Are Changing For Healthcare Privacy**

### ***Litigation & Legislative Activity***

Until recently, there has been a lingering question in many healthcare and government organizations, "Will privacy of healthcare information or HIPAA ever really be enforced?"

Another question, linked to privacy enforcement is, "Will the new Obama administration in Washington change the course of HIPAA enforcement and the attitudes towards protecting privacy of health information?"



Recent developments in litigation and legislative initiatives may help in answering these questions.

While HIPAA has been around since 1996, little enforcement has actually occurred, despite a multitude of complaints that have been received by enforcement agencies.

A major settlement has just been reached by the Veteran's Administration where that agency "just decided" to settle class action lawsuits related to a 2006 breach (one of the largest medical privacy breaches to date) for twenty million dollars.

According to a report in "Modern Health Care", "The Veterans Affairs Department has agreed to pay up to \$20 million to veterans for exposing them to possible identity theft in 2006 in what remains the mother of all healthcare security breaches, according to the Associated Press and other reports.

According to court filings Tuesday, lawyers for five veterans groups and the VA reached the settlement in a case filed in U.S. District Court in Washington. Judge James Robertson will have to approve the settlement, however, before it is final, the AP reported.

*The breach occurred when a laptop computer and external hard drive were stolen in the burglary of the Baltimore home of a VA employee and data analyst. The computer storage devices contained data on a reported 26.5 million veterans, data that included their names, Social Security numbers and dates of birth. The equipment was turned over to the FBI anonymously a month later. Forensic analysts with the FBI determined the database had not been accessed since the laptop was stolen. Five VA officials resigned in the wake of the incident, however." [1]*

**This settlement definitely shows that there is a tremendous risk for any organization if personal or health information is handled irresponsibly. Note, while there was no indication that the lost data was actually misused, the potential of damages ended up costing millions of dollars in remediation and jobs were lost.**

*The Source for Comprehensive HIPAA Compliance Resources*



Recent healthcare IT initiatives by the new Obama administration in Washington also reveal a great potential for stronger and more aggressive legislation as well as enforcement of privacy protection for personal health information. According to a recent article in "Modern Health Care", the administration plans significant changes in HIPAA Privacy and Security.

The article states, "A new Congress and a new president could mark a return to healthcare privacy protections rolled back by the Bush administration, with maybe a few new, more stringent federal protections added for good measure."

*The bill contains sections on federal support for the use of healthcare information technology as well as 51 pages on health information privacy.*

*To date, there are at least 43 states that followed the lead set by California that require individuals be notified in the event their personally identifiable information-such as combinations of their name and date of birth, address and Social Security number-are released either by error or a willful breach of record system security, according to a recent report funded by HHS on medical identity theft." [2]*

The Health Information Technology for Economic and Clinical Health Act (HITECH), referred to in the Modern Health Care article, proposes significant changes to "business as usual" relating to HIPAA enforcement.

Among the actions proposed by that bill are the following:

*"Privacy and Security of Personal Health Information*

*This health information technology legislation improves and expands current Federal privacy and security protections for health information. As health care providers move to exchanging large amounts of health information electronically, it is important to ensure that such information remains private and secure. The bill accomplishes this by:*

*Establishing a Federal breach notification requirement for health information that is not encrypted or otherwise made indecipherable. It requires that an individual be notified if there is an unauthorized disclosure or use of their health information.*

*Ensuring that new entities that were not contemplated when the Federal privacy rules were written, as well as those entities that do work on behalf of providers and insurers, are subject to the same privacy and security rules as providers and health insurers.*

*Providing transparency to patients by allowing them to request an audit trail showing all disclosures of*

*The Source for Comprehensive HIPAA Compliance Resources*

*their health information made through an electronic record.*

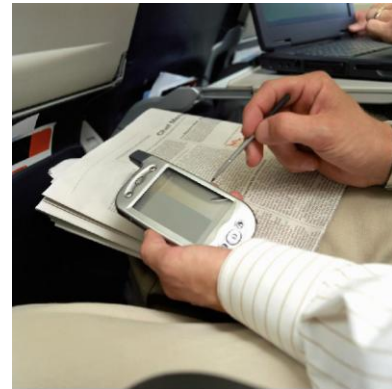
*Shutting down the secondary market that has emerged around the sale and mining of patient health information by prohibiting the sale of an individual's health information without their authorization.*

*Requiring that providers attain authorization from a patient in order to use their health information for marketing and fundraising activities.*

*Strengthening enforcement of Federal privacy and security laws by increasing penalties for violations and providing greater resources for enforcement and oversight activities."*[3]

**The bottom line is that changes in Washington, new health IT initiatives, and escalating privacy breaches have created an environment favoring stronger enforcement of privacy regulations.**

Recent California privacy legislation also dramatically increased the risks for mishandling health information in that state and revealed a growing emphasis on privacy at the state level. Other states may now follow the trend towards tougher regulations on privacy.



Any organization subject to medical privacy laws should clearly understand that times are changing and moving in the direction of more enforcement, not less. The days of "business as usual" and "voluntary compliance" appear to be ending.

**That means it may be a good time for those organizations to conduct assessments of business processes and IT infrastructure to identify potential vulnerabilities and to reduce their vulnerabilities to litigation or prosecution.**

[1] <http://www.modernhealthcare.com/apps/pbcs.dll/article?AID=/20090127/REG/301279953>

[2] <http://www.modernhealthcare.com/apps/pbcs.dll/article?AID=/20090121/REG/301209987/1153&nocache=1>

[3] <http://waysandmeans.house.gov/media/pdf/110/hit2.pdf>



*The Source for Comprehensive HIPAA Compliance Resources*

**HIPAA Solutions, LC provides comprehensive compliance resources including assessments, remediation and consulting.**

**In addition, we offer the HIPAA ComplyPAK suite of software tools that automates the legal/technical compliance activity required by HIPAA. ComplyPAK eliminates much of the need for expensive legal and technical resources while reducing the complexity and cost of compliance.**



**Learn more about the compliance resources from HIPAA Solutions, LC by contacting us Toll Free at (877) 779-3004 or e-mail [info@hipaasolutions.org](mailto:info@hipaasolutions.org). For additional information visit our "Resources" library at: [www.hipaasolutions.org](http://www.hipaasolutions.org) .**

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