



Are Changes On The Way For Healthcare Privacy?

By Brian Gaston, MBA
HIPAA Solutions, LC

Questions on the minds of privacy officers in many healthcare and government organizations are, "Will privacy of healthcare information or HIPAA ever really be enforced?" and, "Will the new Obama administration in Washington change the course of HIPAA enforcement or attitudes towards protecting privacy of health information?"

While HIPAA has been around since 1996, enforcement has not been aggressive despite a multitude of complaints received by enforcement agencies. Recent developments in litigation and legislative initiatives indicate changes in privacy enforcement may be on the way.

First, a major settlement has just been reached by the Veteran's Administration as it settled class action lawsuits related to a 2006 breach 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 The breach occurred when a laptop computer and external hard drive were stolen in the burglary . . . 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. . . . 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

1

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

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

The article stated, *"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."*

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



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 bottom line is that changes in Washington, new health IT initiatives, escalating privacy breaches and more aggressive state laws such as those just passed in California have created an environment favoring stronger enforcement of privacy regulations.

Any public or private organization that is subject to medical privacy laws should clearly understand that times are changing and moving in the direction of stronger enforcement. Voluntary compliance and “business as usual” are no longer the rules of the day. That means it may be a good time for those organizations to take action to identify potential vulnerabilities and reduce their exposure to litigation or prosecution.

Areas that should be addressed include ensuring that . . .

- Business processes, policies, and procedures relate to real compliance activity.
- Disaster recovery procedures and IT infrastructure work as planned.
- Intrusion detection, access controls and sound data storage practices are in place
- Training is updated to address current regulatory developments and court rulings.
- Periodic assessments or audits are conducted on both privacy and security status.

Brian Gaston, MBA is a Principal and consultant with HIPAA Solutions, LC, a nationally recognized HIPAA consulting group with client organizations in healthcare, government and education arenas. His email is brian@hipaasolutions.org and the organization’s web site is www.hipaasolutions.org

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