

*HIPAA and HITECH Regulations
Have Evolved – Has Your
Encryption Solution?*

Data Breaches: A Growing Problem for the Healthcare Community

The electronic exchange of health information is improving patient care and safety while providing increased efficiencies for hospitals, insurers and pharmaceutical companies. A young girl in California can be diagnosed with a rare type of cancer and, within hours, the experts at Dana–Farber in Boston are developing her aggressive treatment regimen. Also, while the pros of Electronic Medical Records (EMR) and online Healthcare Portals greatly outweigh the cons, their introduction comes at a price — an increased risk of both accidental and intentional data loss.

A well-organized and sophisticated network of cyber criminals that first targeted the financial services and retail industries has the healthcare industry squarely in its sights. Almost one out of every six data breaches in 2009 came from the healthcare industry, with that number rising to almost one in four in 2010.

The government has responded to this alarming threat by issuing recent updates to both the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. Consider the key revisions to the right:

HIPAA and HITECH Key Revisions

Notice of Breach

Health plans, healthcare clearinghouses and providers are now required to notify affected individuals following a detected breach of unsecured Protected Health Information (PHI). Entities not covered under HIPAA are now required to file breach notifications with the U.S. Federal Trade Commission (FTC).

HIPAA Applies to Business Associates

The full set of HIPAA security requirements have been extended to cover business associates. Business associates can include consultants, pharmacies, payers (i.e., health insurance providers), laboratories, e-health record software vendors, Regional Health Information Organizations (RHIOs) and Health Information Exchanges (HIEs).

Penalties and Enforcement

HITECH extends various HIPAA security and privacy requirements, thus providing a foundation for increased compliance auditing and enforcement. Criminal and increased civil monetary noncompliance penalties now apply to business associates. Civil monies obtained by the Federal Government are used to fund enforcement action by state attorneys general.

Data Disposal

Under HITECH breach notification requirements, Electronic PHI must be purged before disposal consistent with the US National Institute of Standards and Technology Guidelines for Media Sanitization — NIST 800–88.

Self-Encrypting Drives and Wave's EMBASSY® Software: Keeping EPHI Safe

With the move toward exchanging medical information electronically, it's no wonder that protecting a patient's medical history, prescription drug use or payment/billing details is a high priority for healthcare IT professionals. Also, given the fact that lost and stolen laptops are a leading cause of data breaches, securing information on these devices is a critical part of any healthcare provider's or payer's security and compliance strategy.

There are numerous security options available for protecting EPHI, from strong authentication technologies, such as one-time password tokens, to data loss prevention (DLP) solutions that include port protection. Also, while many of these offerings provide good value within a layered security model, encryption is the only HIPAA and HITECH sanctioned way for avoiding the high costs and damaging publicity associated with notifying individuals in the event of a data breach.

Wave Systems, a pioneer in hardware-based laptop security, has partnered with leading hard drive manufacturers Hitachi, Samsung and Seagate to provide enterprise security management for self-encrypting hard drives — hard disk and solid state drives with encryption built into the drive itself. These standards-based

drives provide security and performance far superior to software encryption and can be added to most new laptop purchases for a nominal cost over an ordinary drive. However, a data protection solution requires more than just encryption. To comply with the recent HIPAA and HITECH revisions, organizations that handle EPHI must employ a managed encryption environment — one that centrally provisions security policies, limits access to only authorized users and, perhaps, most importantly, proves whether or not EPHI, stored on a laptop, was encrypted at the time it went missing. Wave's EMBASSY® software provides these essential capabilities and more.

While self-encrypting drives are superior to software-based encryption in the market, Wave understands that many healthcare organizations must protect information on PCs that do not have self-encrypting hard drives. In support of these mixed environments, Wave's EMBASSY software offers a complete range of security management capabilities for Microsoft BitLocker — software encryption that comes with select versions of Windows, including Win 7. For legacy systems, Wave provides full management for SafeNet's ProtectDrive software as well. Whatever type of full disk encryption is needed — we've got your data covered.

