



How to Secure Health Care Data to Meet HITECH Act Compliance

By: Gretchen Hellman, Vice President of Security Solutions at Vormetric

The Health Information Technology for Economic and Clinical Health Act was enacted as part of the American Recovery and Reinvestment Act of 2009. The HITECH Act imposes certain requirements on vendors of personal health records (and other related entities) in the event of certain security breaches relating to protected health information. Here, Knowledge Center contributor Gretchen Hellman explains the new HITECH Act compliance requirements, their implications and some best practices for meeting HITECH Act compliance.

In February 2009, President Obama signed the Health Information Technology for Economic and Clinical Health (HITECH) Act as part of his overall economic stimulus plan. The HITECH Act continues the effort of the Health Insurance Portability and Accountability Act (HIPAA) to encourage movement to electronic patient records and to deliver stricter data protection regulations for more secure patient privacy.

Among the most important of the new HITECH Act mandates is a federal breach notification requirement for stored health information that is not encrypted or otherwise made indecipherable, as well as increasing penalties for violations. Until this law was passed, only two of the 48 states with data breach notification requirements included health information

as a specified data type. Now with the HITECH Act, the entire United States health industry and their business partners must quickly understand and get ready for these new data breach notification requirements.

With HITECH Act data breach disclosure requirements already in effect, the problem is imminent and unsolved. Most health organizations are currently not encrypting their patient health data stores. The HIPAA Security Rule, finalized in 2003, defines encryption as “addressable,” which required HIPAA-regulated entities to evaluate and document whether or not they were going to use encryption based on viability and organizational risk—but did not mandate encryption.

Now with the HITECH Act, thousands of

healthcare-related businesses are finding themselves struggling to understand not only the HITECH Act's breach notification requirements, but also what it means to encrypt their data. In addition to data breach notification requirements for all HIPAA-covered entities, the HITECH Act also extended HIPAA requirements beyond the traditionally covered entities of "payors, providers and clearinghouses" to include their business partners.

In light of the new demands and requirements that the HITECH Act has put on healthcare organizations, as well as the introduction of more severe penalties, organizations need to get started with a strategy immediately.

Encryption or destruction

In August 2009, the Department of Health and Human Services (HHS) issued a statement specifying only "encryption and destruction as the technologies and methodologies that render protected health information unusable, unreadable or indecipherable to unauthorized individuals."

Encryption or destruction are, therefore, the only two means to protect patient health data, thereby eliminating breach notification requirements. That really only leaves encryption as the method to secure data that will be used.

Due to the complexities of managing public-key infrastructure (PKI) and attempts at implementing invasive approaches, encryption has gained a bit of a negative reputation over the past decade. However, this negative association is no longer warranted based on advances in the market. Healthcare organizations should quickly update their encryption knowledge.

Enterprise-grade encryption has experienced significant technical evolution since HIPAA was finalized in 2003. Today, companies can secure information without performance degradation, rewriting applications, or management costs. For HIPAA-covered entities and their business

partners who haven't started, immediate focus should be placed on understanding the benefits and challenges of different encryption approaches.

These entities and business partners should be getting updated on the state of the art of encryption today, as well as understand the difference between the management requirements of point (self-contained) encryption solutions versus centrally-managed solutions.

Evaluate your risk

During 2008 and 2009, there were numerous and widespread data breaches of patients' protected health information (PHI)—with the largest security breaches resulting from both internal and external attacks on database and file servers. This means that companies need to ensure that their encryption strategy protects information resting in the data center and distributed environments.

Prior to the HITECH Act, only California and Arkansas included patient health data in data breach requirements, but the results of their laws demand attention. For example, California reported 800 PHI breaches in the first five months after the requirement. This is a strong indicator of heavy risks to patient data. It's also a strong indicator that there's a high probability that organizations will experience a breach and have to notify if they do not encrypt.

The cost of data breach disclosure extends beyond notification to include lost customers, class action lawsuits and brand damage. Companies need to consider these costs combined with the risk when determining the investment that should be placed in encryption.

Re-evaluate your stance on encryption

When HIPAA was enacted in 2003 after years of debate, data encryption was an "addressable" requirement. Addressable HIPAA requirements gave companies leeway to decide if they should

meet the requirement, make a determination, document the determination and implement the decision. Most organizations chose not to encrypt since HIPAA was not heavily regulated and encryption seemed unmanageable in 2003.

But today, organizations should immediately implement projects to revisit encryption because of the technical advancements, the demonstrated risk of public data breaches, and the impending HITECH Act compliance requirements.

Gretchen Hellman is Vice President of Security Solutions at Vormetric. Gretchen has broad experience in helping companies of all industries meet their security management and regulatory compliance objectives. After gaining direct experience as a consultant specializing in security management and regulatory compliance, Gretchen worked with technology vendors and their customers to deliver practical solutions for the complex security and compliance problems facing the enterprise. She can be reached at ghellman@vormetric.com.



VORMETRIC