What is the HITECH Act?

The Health Information Technology for Economic and Clinical Health (HITECH) Act requires health providers, health insurance companies, and other organizations to issue notifications when unsecured protected health information is breached. The requirements apply to organizations that are considered "covered entities" under the Health Insurance Portability and Accountability Act (HIPAA).

The information security segments of the HITECH Act were developed to help organizations that handle PHI prevent fraud, hacking, and other security threats by leveraging technologies and methodologies that can be used to render PHI unusable, unreadable, or indecipherable to unauthorized individuals.

How Does HITECH Affect My Organization?

Technology has enabled the healthcare industry to become more efficient and cost-effective with medical documentation and has allowed patients to be more proactive in their personal healthcare. Medical records and health concerns can be documented electronically from the exam room, patients can correspond with their doctors via email, and health records can be accessed online. With increased accessibility to medical and health insurance data, the need for increased data security has become imperative. HIPAA and HITECH require that Information handled by doctors, insurance providers, and their business associates must remain protected at all times.

The HITECH Act provides a system for assessing penalties for non-compliance. The Centers for Medicare & Medicaid (CMS), which enforces the HIPAA security rule, and the Office for Civil Rights, which enforces the HIPAA privacy rule, dictate the fines that may be applied. Organizations that are not in compliance with the established regulations face fines up to $50,000 per violation and $1.5 million for the calendar year.

How Does Smartcrypt Help Meet HITECH Act Requirements?

PKWARE’s Smartcrypt is an industry-leading, FIPS 140-2 compliant security and compression solution that encrypts and decrypts using X.509 digital certificates, passphrases, or a combination of the two. Smartcrypt allows organizations to meet all HITECH Act requirements for data at rest and data in motion.
With Smartcrypt, protection remains with the data wherever it is used, shared, or stored. This helps ensure HITECH compliance on the part of Business Associates (BAs) who transmit access sensitive information, and by Personal Health Record (PHR) vendors who have contracts with entities covered by the HITECH Act.

Smartcrypt also ensures portability and seamless exchange of secured data, as it leverages the ubiquitous .zip container and is supported on all major platforms including mainframe, midrange, server, and desktop systems.

**Extend Security Policies to Protect Data Outside the Enterprise**

Smartcrypt’s data-centric approach means that even the most sensitive data can be sent via open, public networks, without additional protection or secure tunnels, yet still meet the HITECH Act requirements. You can even extend your organization’s security policies to external partners, at no cost to them, for data that is exchanged outside of your enterprise.

Smartcrypt enables secure bi-directional exchange of information with external partners. It allows organizations to mitigate the risk inherent to the exchange of sensitive data, without requiring them to invest in a complex solution.

- Single solution for secure bi-directional data-exchange with partners—enables the secure exchange of PHI between an enterprise and its customers, server providers, and suppliers.
- Integrates with existing IT infrastructures—Ensures rapid installation and easy adoption by partners.
- Eliminates administrative overhead—Easy to deploy and maintain, and requires minimal time and resource investments for you and your partners.