

Meet HIPAA requirements established by the HITECH Act while increasing data security internally & externally with business associates

Technology has enabled the healthcare industry to be 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. Information handled by doctors, insurance providers, and their business associates must remain protected at all times.

HITECH Act overview

In February of 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act applies to "HIPAA covered entities and their business associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured protected health information..." The Act (section 13402) mandates the issue of regulations to covered entities under the Health Insurance Portability Act of 1996 (HIPAA) and their business associates to provide for notification in the case of breaches of unsecured protected health information. Covered entities included a "health plan, health plan clearinghouse, or health care provider that transmits any health information electronically in connection with a covered transaction, such as submitting health care claims to a health plan..."¹

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.

Non-compliance

The HITECH Act provides a system for assessing the penalties associated with each non-compliance violation. 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 limits of fines in place. Those organizations who are not in compliance with the established regulations face fines up to \$50,000 per violation and \$1.5 million for the calendar year.

¹<http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>



HITECH Act requirement: data in transit

"Valid encryption processes for data in motion are those that comply with the requirements of Federal Information Processing Standards (FIPS) 140-2."¹

SecureZIP is the industry-leading, FIPS 140-2 compliant security and compression utility that encrypts and decrypts using X.509 digital certificates, passphrases, or both. Using data-centric technology, protection remains with the data wherever it is, wherever it goes, however it gets there. In addition, portability and seamless exchange of secured data is ensured since SecureZIP leverages the ubiquitous .zip container and is supported on all major platforms including mainframe, midrange, server, and desktop systems.



HITECH Act requirement: data at rest

"Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices."¹

Utilizing a data-centric approach to protect the data, SecureZIP allows employees the flexibility to choose the storage medium: CD/DVD, Hard disk, USB Drives, etc. SecureZIP is a secure container which not only protects the data and helps maintain compliance, but compresses the data to save on storage space and increase operational efficiencies.

Extend security policies to protect data outside your enterprise

Business Associates (BAs) who provide transmission of protected health information and/or require access to that information are required to comply with regulations established by the HITECH Act. In addition, Personal Health Record (PHR) vendors who have contracts with entities covered by the HITECH Act are also required to meet compliance requirements. Examples of BAs include:

- ✔ Transcriptionists
- ✔ Contracted lab & radiology departments
- ✔ Third-party billing agencies
- ✔ Hospital couriers
- ✔ Collection agencies
- ✔ Pharmacies with hospital contracts
- ✔ Consultants
- ✔ Off-site storage facilities

SecureZIP'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.

SecureZIP PartnerLink, a special deployment of SecureZIP, 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, SecureZIP PartnerLink requires minimal time and resource investments for you and your partners.

About PKWARE

As the inventor and continuing innovator of the ZIP standard, PKWARE, Inc. (www.pkware.com) is a global technology leader known around the world as the expert in data compression and file management. With the launch of SecureZIP in 2005, PKWARE successfully entered the data security marketplace, combining ZIP compression and strong encryption to deliver a data-centric security solution. Today, SecureZIP is used by over 200 government agencies and 30,000 corporate entities, including 90% of the Fortune 100. Organizations in financial services, banking, healthcare, government and retail use PKWARE products daily to avoid the costs, legal penalties and damaged reputations caused by data that is compromised. SecureZIP provides a data-centric security solution that ensures information remains protected across the enterprise on all major computing platforms, while still enabling appropriate organizational security controls. PKZIP is the industry-leading file management and compression utility that greatly improves data processing efficiencies by reducing transmission times and required storage space. PKWARE, a privately held company, was founded in 1986 and is based in Milwaukee, Wisconsin; additional offices are located in New York, Ohio and the United Kingdom.

“Our gap analysis of the data protection aspects of the HITECH Act shows that our largest cost associated with becoming compliant lies with our business partners. Once we inform our business partners of their new requirements, we are going to need to amend many of our contracts; and those amendments will open the door for price negotiations.”

Director of Information Security,
Major Health Insurance Provider