



DECODER

HITECH Compliance

HITECH Summary

The focus of HITECH is to:

- Motivate the healthcare industry to transition from paper health records to electronic health records
- Identify and secure the vulnerabilities associated with electronic PHI transition
- Protect patient health information

HITECH requires any HIPAA-regulated entity and their business partners to protect PHI data when it is in motion, at rest and in use.

If an organization fails to secure PHI and it experiences a breach, strict notification guidelines and large fines ensue.

How CipherOptics Helps

The CipherEngine solution:

- Provides a comprehensive data encryption solution securing PHI in motion for healthcare companies and their business partners
- Renders electronic PHI data unusable, unreadable and indecipherable to all unauthorized parties
- Makes it easy to encrypt data between WANS, servers and PCs
- Ensures electronic PHI will be secured, exempting you from costly breach notifications and HHS fines

We can protect your PHI data in motion, helping you secure electronic PHI and comply with HITECH.

What is HITECH?

The Health Information Technology for Economic and Clinical Health (HITECH) Act was set in motion in 2009 as part of the American Recovery and Reinvestment Act. It provides the healthcare industry over \$31 billion in stimulus funds dedicated to infrastructure improvements, including the adoption of Electronic Health Records (EHR). In addition, HITECH addresses new privacy requirements for patient Protected Health Information (PHI) security, breach notification and penalties for non-compliance.

What are the requirements of HITECH?

HITECH requires any organization that accesses, maintains, retains, or modifies records, or any business that stores, destroys or otherwise holds, uses or discloses PHI to protect that information. The regulation also sets forth the notification requirements for companies that suffer a data breach of unsecured PHI.

How do companies comply with HITECH?

To comply with HITECH, companies must secure PHI data in motion, at rest or in use. According to the Federal Register, the Department of Health and Human Services recommends deploying encryption in order to secure PHI in motion. Data encryption renders “electronic PHI unusable, unreadable or indecipherable to unauthorized persons,” and is therefore an acceptable means of securing PHI.

What are the penalties of HITECH non-compliance?

If an organization is breached and it protected the PHI using authorized methods, it is not subject to the notification requirements. However, if a company is breached and its data was not secured, the company is subject to fines up to \$1.5 million (mandatory for cases of “willful neglect”) and the following notification requirements:

- Written notice by first-class mail to the individual at the last known address.
- If there is insufficient or out-of-date contact information, especially if there are 10 or more individuals with insufficient information for mailed notification, the organization must post notification on their website and/or in major print or broadcast media.
- If the company believes imminent misuse of the unsecured PHI is possible, notice by telephone or other method is permitted in addition to the above methods.
- If more than 500 residents of any given state are affected, then prominent media outlets within the state must be sent notification.
- For any breach of more than 500 individuals, the U.S. Health and Human Services Secretary must be immediately notified. The Secretary must also be notified annually of all other breaches.
- The Secretary will maintain a list on an HHS website that identifies each breach in which the unsecured PHI of more than 500 individuals is compromised.

How does CipherOptics help you comply with HITECH?

CipherOptics CipherEngine provides healthcare organizations and their business partners with a comprehensive data encryption solution that ensures the security of PHI data in motion across any network or infrastructure. Our solution renders your electronic PHI data unusable, unreadable and indecipherable to all unauthorized parties.

The CipherEngine solution allows organizations to easily encrypt data across the network or the entire computing infrastructure using a global policy and key manager along with hardware and software-based encryption enforcement points. Deploying the CipherEngine solution ensures your electronic PHI will be secured, exempting you from costly breach notifications.

