HillSouth

iT solutions.

PRODUCT DATASHEET

iT SERVICE BRIEF

Data Encryption in the HillSouth Cloud

Military-grade encryption keeps your organization's data safe

Data Encryption is Mandatory

Many companies that have access to protected health information believe that encryption of the data is optional. Several regulations dictate clearly that encrypting the data is not optional. Fines can be levied should the protected health information be compromised and it is found that all the available safeguards, such as encryption, have not been implemented.

A HIPAA Security Rule dictates PHI be protected by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

Even more important than the requirements to encrypt are the opportunities to avoid breach notification measures. The OCR (federal agency that regulates HIPAA PHI breaches) has safe harbor guidance that an organization losing an encrypted data file but NOT the keys to decrypt said file does NOT have to report the breach publicly according to the widespread breach notification laws that exist at the federal and state levels.

Properly encrypting data wherever it resides and is transmitted to has the potential to function as a "get out of jail free" card for an organization to avoid the embarrassment of putting out public notices of a PHI data breach.

MYTH: Encryption Slows Systems

A well-architected encryption solution can very easily avoid performance degradation with the right components. The challenge for a clinic or small business is clearly how to afford all the numerous components that will allow for high-performance, real-time, data encryption.

Outsourcing your data encryption needs to HillSouth with secure servers located in the HillSouth Cloud is a smart way to meet the data encryption requirements while avoiding the obvious costs of implementing and maintaining a complex encryption system on your organization's premises.

Complements Other Security Measures Already in Place

Common activities that occur every single day in most organizations are encrypting data connections with third parties, typically using a VPN technology. These secure tunnels encrypt PHI and other sensitive business data as it is being transmitted across the Internet to third parties. Data encryption serves a very similar purpose but as the data sits at rest on a server.

Also common in healthcare organizations is email encryption when sending PHI over email. Data encryption is used in those secure email transactions and is a great complementary layer to server data encryption from HillSouth.

PCI Compliance

PCI 3.0 clearly states that card data must be indecipherable wherever it is stored except in the presence of a separately-stored key. Your organization's sensitive card data can be encrypted to meet this requirement.

PROVEN TECHNOLOGY:

- AES 256-BIT encryption for data protection at rest and in-flight
- Data deduplication and caching for increased performance

SERVICE HIGHLIGHTS:

- Meets and exceeds HIPAA Security Rule 45 CFR § 164.312(a)(2)(iv) and (e)(2)(ii) specifying an organization encrypt data
- Works in conjunction with other HillSouth security services to provide additional layer of protection for sensitive data
- Exceeds PCI 3.0 Standards

Get Proactive! Call Us TODAY!

877.292.9070
www.hillsouthcloud.com | info@hillsouth.com

Florence | Columbia | Myrtle Beach, SC