The right healthcare data security prescription

Healthcare organizations constantly face the threat of data breaches. They need encryption dedicated to protecting patient information, but how does it work?

What is encryption?

Encryption
(n.) the process of encoding sensitive information in a way that only authorized personnel can read it.

Here's a simple cipher example:

Protect Patient Information	Original plain text
dkejimaulonpyfxgwcrbtszvhq	Key code
gcxbiebgsgdblifblfxmxcydblxf	Final encryption

Why encrypt healthcare data?

Compliance
All healthcare organizations need to meet compliance mandates to protect personal health information (PHI).

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) protects medical records and PHI through a Privacy Rule that applies to health plans, healthcare clearinghouses and healthcare providers that conduct electronic transactions.

HITECH

The Health Information Technology for Economic and Clinical Health Act (HITECH) enforces the privacy and security rules of HIPAA. It brings additional pressures and incentives to secure PHI, and requires audits to ensure companies are in compliance.

The National Institute of Standards and Technology (NIST) recognizes two encryption processes as rendering protected health information as unusable, unreadable or indecipherable:

1 HIPAA rules state you need to "[i] implement a mechanism to encrypt and decrypt electronic protected health information." [section (a)(2)(iv) of 45 CFR 164]

2 For data at rest, the acceptable processes are those consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.

What risks do they face?

Experian forecasts the growing threat of healthcare breaches as one of the top six data breach trends.

Source: The 2015 Second Annual Data Breach Industry Forecast

HIPAA violations are expensive

Penalties for noncompliance can range from $100 to $50,000 per record.

$1.5M

The maximum penalty is $1.5 million per year with the possibility of jail time.

$5.6 billion

The cost of breaches in the healthcare industry could reach $5.6 billion a year.

The Wall of Shame

HITECH [section 13402(e)(4)] mandates that the Health and Human Services (HHS) Secretary enable public awareness of patient data breaches. Breaches that involve 500+ individuals can be found online on the "Wall of Shame," an extremely public record of healthcare breaches.

- Big Name Pharmacy
- Medical College
- Local Doctor's Office
- Small Town General Hospital
- Big City Hospital

ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Dell Data Protection | Encryption

Dell Data Protection | Encryption (DDP | E) helps covered entities meet HIPAA and HITECH encryption security requirements, regardless of where the data resides.

Why choose DDP | E?

- To secure data across the broadest range of devices and platforms,from iOS and Android mobile devices, cloud, external media, self-encrypting drives, Microsoft BitLocker™, to Dell and non-Dell Windows PCs and Mac.
- To easily generate audit reports required by HIPAA and HITECH mandates.
- To ensure unprotected data does not leave the organization on USB sticks or other removable media.
- To encrypt data using FIPS 140-2 compliant algorithms.

Safe harbor
If PHI is encrypted, a "safe harbor" protects covered entities and business associates. These entities are therefore not required to provide the notification otherwise required by section 13402 in the event of a breach.

Next steps for success

1 Organizations should re-evaluate existing IT security to ensure the prevention of privacy breaches.

2 If anything, encrypt any protected health information on portable drives, laptops, mobile devices or any other data container that might leave the office.

- 10 Free Licenses
- External Media Edition video
- Cloud Edition video

Learn more at Dell.com/dataprotection