Solutions statement
Dell Data Protection | Encryption (DDP | E) enables covered entities and business associates to meet HIPAA-HITECH encryption and security requirements, regardless of where the data resides.

DDP | E is a flexible suite of enhanced security solutions that can help you meet the HIPAA Privacy and Security Rules. This comprehensive suite delivers data security across the broadest range of devices and platforms, from mobile devices, cloud, external media, self-encrypting drives, Microsoft BitLocker™, to Windows PCs and Mac. A single web-based management console helps manage all endpoints, including audit and policy-setting capabilities, without disruption to existing IT processes.

DDP | E’s data-centric, policy-based approach to encryption provides:
• Endpoint data encryption to help avoid breach notification requirements
• Encryption of data using FIPS 140-2 compliant algorithms
• Easy generation of audit reports required by HIPAA and HITECH mandates
• Customizable reporting on all endpoints audit and compliance data, including multi-vendor IT landscapes
• Protection of unprotected patient data from leaving the organization on USB flash drives or other forms of removable media
• Protection of data from unwarranted access, thus reducing risk of internal breaches

Deploying this level of a comprehensive solution can help healthcare entities meet the HIPAA-HITECH security compliance mandates around encryption.

“Our message to covered entities and business associates is simple: encryption is your best defense against these incidents [data breaches] and security is your obligation.”

Susan McAndrew
OCR Deputy Director of Health Information Privacy

Learn more at dell.com/dataprotection
The modern healthcare information environment is complex, with information flowing across numerous interrelated and interdependent institutions, service providers, and other entities. Security professionals in the healthcare industry find themselves facing unprecedented challenges protecting sensitive information as electronic patient information is transferred from laptops to smart phones to specialized handheld medical information devices. Budget and staffing constraints further complicate the matter of safeguarding protected health information (PHI) for many doctors’ offices, clinics, and hospitals.

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule establishes national standards to protect individuals’ medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Health Information Technology for Economic and Clinical Health Act (HITECH) brings additional pressures and incentives into play in its mandate to secure PHI, and puts teeth into the enforcement of the privacy and security rules of HIPAA.

The law

HHS guidance identifies two encryption processes recognized by the National Institute of Standards and Technology (NIST) as rendering protected health information unusable, unreadable, or indecipherable:

- Section (a)(2)(iv) of 45 CFR 164.312, the HIPAA rules clearly say that you need to “[i] implement a mechanism to encrypt and decrypt electronic protected health information.”

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

DDP | E provides non-disruptive encryption by enabling end users to securely access and share data on any device and in the cloud with data-centric encryption. Enforce security across multiple endpoints from one single management console, consistently and efficiently. The solution helps organizations quickly and easily deploys encryption across the entire organization, enforce policies, and audit encryption state.

Encryption provides ‘safe harbor’

The HITECH Act requires that patients be notified of any unauthorized acquisition, access, use, or disclosure of their unsecured PHI that compromises the privacy or security of such information. The HITECH Act defines “unsecured PHI” as any PHI that is not secured by a technology standard that renders it unusable, unreadable, or indecipherable to unauthorized individuals, and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute (ANSI). If PHI is secured, i.e., encrypted, it provides covered entities and business associates a “safe harbor”; and these entities are therefore not required to provide the notification otherwise required by section 13402 in the event of a breach.

DDP | E’s comprehensive solution offers the highest level of Federal Information Processing Standards for all Dell and non-Dell clients, with optional Hardware.

The 2015 Second Annual Data Breach Industry Forecast by Experian forecasts the persistent and growing threat of healthcare breaches as one of the top six data breach trends for 2015. The digitization of records, increased exchange of this information, and the high black market value of medical records makes the healthcare industry an attractive target for cybercriminals.
Encryption Accelerator and Full Volume Encryption on Dell Latitude, OptiPlex and Precision systems. HIPAA-HITECH laws mandate organizations to provide audit-able proof of encryption. DDP | E provides pre-defined templates designed to address specific security goals, or customers can create their own templates to help them meet with regulatory compliances. Having out of the box, pre-set templates helps kick-start companies on the road to compliance and creates the functional equivalent of a ‘safe harbor’ in the event of a breach.

Auditing and reporting
The HITECH Act requires periodic audits to ensure that covered entities and business associates are in compliance. However, the increasingly important task of monitoring audit logs for unauthorized or inappropriate activity has languished due to the time-consuming, resource-intensive nature of the task. This is despite numerous examples where such monitoring would have greatly reduced or even prevented unauthorized disclosure of sensitive information.

- Multi-vendor IT landscapes should support audit and report capability for data access, user, and asset access activity, and provisioning and de-provisioning in a restrictive timeframe should a breach occur.

With DDP | E organizations can easily create and produce automatic audit trails that offer proof end-to-end data security, across a multi-vendor landscape. DDP | E includes software-based, data-centric encryption that protects your data without disrupting IT processes or end user productivity. It allows IT to enforce encryption polici-ies easily, whether the data resides on the system drive or external media, and doesn’t require end user intervention.

Violations are costly
Businesses dealing with PHI are responsible under the HIPAA law to protect that data from unauthorized access. That reason alone should make the criticality of PHI encryption self-evident. In addition, however, costs can quickly escalate if due diligence is lacking and a data breach occurs.

- HIPAA violations are expensive; Penalties for noncompliance can range from $100 to $50,000 per record breached based on the level of negligence, and, with a maximum penalty of $1.5 million per year for violations of an identical provision. Violations can also carry criminal charges that may result in jail time.
- The potential cost of breaches for the healthcare industry could be as much as $5.6 Billion annually.³

DDP | E’s flexible encryption policies enable access to data, based on end user profile, data sensitivity or compliance needs. Encrypting data on external media, disabling ports altogether, while allowing non-storage devices to function; quickly detecting new devices to enforce and audit encryption through remote manage-ment and quick system recovery make it easy for organizations to stay ahead of a costly violation should a breach occur.

And finally, the HHS Wall of Shame
Since 2009, the HHS Office for Civil Rights (OCR) has posted all large data breaches – those that involve 500 or more individuals – online on its so-called “Wall of Shame.” With an average of 1.5 million unique visitors per month, it is an extremely public record of healthcare organizations with PHI breaches of 500 records or more. HITECH [section 13402(e)(4)] mandates that the HHS Secretary enable public awareness of patient data breaches.

However, OCR now requires the same level of specific HHS reporting detail for small breaches as for large breaches. For breaches involving less than 500 individuals, the Breach Notification Rule requires a covered entity to maintain a log or other documenta-tion of such breaches, in addition to annual submission of details to HHS for breaches occurring during the preceding calendar year. Covered entities must report such inci-dents no later than 60 days after the end of each calendar year. As with notification of larger breaches, the rule further requires that the notifications to the government be provided through the HHS website.

³ Fourth Annual Benchmark Study on Patient Privacy & Data Security,” Ponemon Institute, March 2014
Next steps for organizations

Although attacks targeting sensitive information may grab the headlines, it is the day-to-day challenges of ensuring the right people have access to critical information when they need it, and that potentially highly sensitive, protected information is secure, that remains among the top concerns of security professionals.

Every organization must address compliance requirements in terms of their unique business goals and technical environment. As next steps, organizations should re-evaluate existing IT security to ensure measures are in place to prevent privacy breaches. How you store, manage and secure data is going to be trickier to manage, including data stored in the cloud. This is especially important for small businesses that oftentimes lack robust IT resources.

Half of all records exposed in reported data breaches involve information on laptops, other electronic portable devices, and removable media. If you only do one thing to increase your adherence to the HIPAA Security Rule, it is this: Encrypt any protected health information on portable drives, laptops, mobile devices or any other data container that leaves the office—or that might leave the office.

Stolen data that has been encrypted in accordance with HIPAA Omnibus Final Rule has no value to a data thief. Encryption protects your patients’ information and provides safe harbor against penalties and patient-notification rules.

Barely 75 percent of providers⁴ use any form of encryption, despite the fact that it confers immunity under HIPAA regulations from the requirement to report ePHI breaches. In sum, encryption helps protect both against the likelihood of a security breach arising in the first place, and the adverse consequences of a breach – both for the individuals whose data are compromised and also for the business in terms of mitigating its liabilities following the breach.


Learn more at dell.com/dataprotection