

## CREDANT Solutions for HIPAA Compliance

Electronic data stored in hospitals and healthcare facilities is extremely valuable and vulnerable.



### CREDANT SOLUTION

*CREDANT Mobile Guardian (CMG) ensures that HIPAA encryption and security requirements are consistently and efficiently enforced – regardless of where the data resides.*

#### Only CMG enables organizations to:

- › Encrypt and secure data across multiple, diverse platforms from a single console.
- › Create automatic audit trails that offer proof of end-to-end data security.
- › Provide a transparent end-user interface that supports user productivity while keeping data safe.

*CMG's Intelligent Encryption provides centrally managed, highly scalable and architecturally flexible security to manage all data endpoints. With CRE DANT, organizations can:*

- › Provide all the necessary audit reports required by HIPAA policies.
- › Protect patient data from leaving the organization unprotected on USB flash drives or other forms of removable media.
- › Protect data from unwarranted access, thus reducing risk of internal breaches.

### Regulatory overview

The Health Insurance Portability and Accountability Act (HIPAA) was passed by Congress in 1996 to safeguard patient identities, medical records, health insurance activities and other protected health information (PHI). The regulation mandates that healthcare plans, clearinghouses and providers take steps to ensure the standardization of electronic patient data, assign unique health identifiers to patients and others, and implement security standards regarding the confidentiality and integrity of patient data.

More specifically, HIPAA Security Standard and Implementation Specifications require that access control rules and unique user identifiers must be addressed through a combination of encryption, port and application controls, backed by strong access controls.

### The compliance challenge

A single hospital can have more data on an individual than almost any other organization. Data can include a patient's name, Social Security number, date of birth, healthcare records, insurance information, phone number and mailing address, as well as financially sensitive information such as credit card and checking account numbers.

Unfortunately, this highly sensitive data is accessed, generated and shared by doctors, technicians and other specialists who often use their own PCs, laptops and mobile devices to communicate across unsecured networks without encryption or other safeguards. Along with the possible theft or accidental loss of data from these devices, networks can be vulnerable to attacks and malicious activities by hackers, third-party service providers, technology vendors or healthcare employees.

As a result, security has become a critical and growing issue in the healthcare industry. Over 1.5 million names were exposed in data breaches occurring in hospitals in 2006 and 2007, according to analysts. HIPAA mandates a number of ways to improve data security, but what is the best technology solution for demonstrating HIPAA compliance?

### CREDANT

More than 700 enterprises and government agencies -- including 50 of the Global 500 -- rely on CRE DANT to ensure security compliance, protect their brand and enhance IT and end-user productivity.