



Encrypt and secure patient data across multiple, diverse platforms from a single console
Create automatic audit trails that offer proof of end-to-end data security
Comply with HIPAA and HITECH and federal EHR requirements

With CREDANT, healthcare organizations can:

- › **Ensure security for protected health information** and prevent data storage in unencrypted devices.
- › **Provide confidentiality, privacy and auditing** of data on any endpoint.
- › **Reduce risk of internal breaches** with tamper-proof security and enforceable and auditable data protection that cannot be disabled by the end-user.

Regulations Demand New Approaches to Protecting Patient Information

A hospital can manage more data on a person than almost any other kind of organization—and, as a matter of course, hospital employees must routinely access protected health information (PHI). Yet this access comes at a price: analysts report that more than 1.5 million patient names have been exposed by data breaches in recent years.

Today, controlling access and storage of patient data is more challenging than ever before, due to:

- › More geographically dispersed delivery of care
- › Increasing use of specialists and sophisticated diagnostic and treatment technology

- › A need for immediate access to patient and disease data and automated decision support tools
- › Increasingly mobile medical personnel and patient care in remote locations

Rely on CREDANT to Meet Current and Future Mandates

The PHI landscape is changing. With the advent of a new electronic health records (EHR) network established by The American Recovery and Reinvestment Act of 2009, mobile devices such as smartphones, laptops, and tablets will increasingly be tied into hospital and clinical IT infrastructures. Left unsecured, patient health information puts hospitals, physicians, insurance providers, healthcare clearinghouses, IT professionals and others at risk of fines and damaged reputations—and worse—it puts patients at risk of misdiagnosis and even death.

Meet HITECH and HIPAA Compliance Requirements—and Prove It

Healthcare organizations rely on CREDANT data encryption solutions to protect sensitive patient health information wherever it resides, to meet compliance mandates and prove compliance through advanced auditing and reporting features.

CREDANT Mobile Guardian (CMG) can help healthcare organizations and their business associates address:

- › **Healthcare Insurance Portability and Accountability Act (HIPAA) requirements**, including access control rules and unique user identifiers that must be addressed through a combination of encryption, port and application controls, backed by strong audit trails and access controls.
- › **Health Information Technology for Economic and Clinical Health (HITECH) Act requirements**, which amends HIPAA to include improved security and enforcement provisions, including public breach notifications.

“Meaningful Use” of EHR System Translates to Meaningful Dollars for Healthcare

Under the new Recovery Act guidelines, healthcare providers will be eligible for up to \$44,000 in premium reimbursements from Medicaid and Medicare between 2011 and 2014 if they meet the government’s criteria for meaningful use. By choosing the right solutions now, healthcare organizations and their business associates can establish a thorough and cost-effective strategy to ensure the right infrastructure and capabilities are in place before 2011. By choosing CREDANT solutions to protect patient data, healthcare organizations will not only meet EHR “meaningful use” criteria — they will also become eligible to collect those reimbursements.

Prepare for New HITECH Regulations Now

Introduced in 2009 and expanding through 2014, new regulations governing the U.S. health information technology infrastructure will change the way healthcare organizations work, interact, share protected health and financial information and enable delivery of quality care. Prepare now to ensure your organization can:

- › Comply with HIPAA and HITECH mandates
- › Process and share electronic records as part of the nation’s new EHR network
- › Receive available premium incentives between 2011 and 2014, and avoid discounted reimbursements after 2014

Healthcare Organizations Choose CREDANT Mobile Guardian (CMG) to:

- › Securely access and share patient health records
- › Encrypt and secure data across multiple diverse platforms from a single console
- › Provide a transparent end-user interface that supports user productivity while securing data
- › Protect sensitive PHI even on multi-user devices, without impacting ease-of-access for appropriate personnel (e.g. Shared desktops/laptops in hospital wards)
- › Ensure security for PHI by preventing users from storing data in unencrypted locations
- › Provide confidentiality, privacy and auditing of data residing on any endpoint
- › Protect sensitive data from unwarranted access, reducing risk of internal breaches
- › Encrypt data using FIPS 140 2-compliant algorithms
- › Provide audit reports required by HIPAA and HITECH
- › Deliver quality of care to an increasingly mobile network of healthcare providers

The time to prepare is now. CREDANT can help.

Learn more

With nearly 800 global customers, including some of the world’s most respected healthcare providers, CREDANT solutions protect patient health information no matter where it resides. Download a demonstration of CMG in action at www.credant.com/demo. For more information about CREDANT solutions for healthcare, email sales@credant.com, or visit www.credant.com.