# Channel Partner Battlecard – Healthcare

## The Challenge

Healthcare organizations face significant pressure to protect patient records, as data breaches lead to reputational damage, lost revenue and compliance violations. The adversary is highly motivated, however, as medical records fetch a premium among cyber-criminal networks. As attackers increase their sophistication and data environments expand, healthcare organizations must bolster their security and compliance efforts.

Medical records are also now shared at unprecedented levels across applications, devices and facilities, expanding the potential surface attack area.

Health Care SecurityThis is why Boards and C-suites are demanding data protection that goes beyond compliance to true security. For many healthcare organizations, however, the budget and resources available for data security is more limited as compared to other industries

## Benefits

- Safeguard medical records by rendering them unusable to attackers.
- Increase compliance with HIPAA-HITECH and other healthcare data privacy mandates.
- Secure the most sensitive keys and business processes in the organization in an independently-certified, tamper-resistant environment.
- Protect the organization's reputation and revenue against long-term damage.
- Encrypt sensitive data efficiently, with little to no system degradation.
- Establish a root of trust for medical devices added to the healthcare enterprise's network.

## Opportunities

Healthcare organizations place their highest priorities around serving the needs of patients and the delivery of the care that they need. But at the same time, they operate within the limitations of a maze of regulatory and compliance requirements:

• **HIPAA/HITECH**: Meeting US Health Insurance Portability and Accountability Act (HIPAA) as well as Health Information Technology for Economic and Clinical Health Act (HITECH) requirements for safeguarding electronic Personal Healthcare Information (ePHI)

• **Data Breaches:** Protecting their organizations from a violation of State, Federal and Local data breach statutes

• **EPCS:** Meet US Drug Enforcement Agency's (DEA) requirements for Electronic Prescriptions of Controlled Substances (EPCS)

• **PCI DSS:** Ensuring the security of payment transactions as required under the Payment Card Industry Data Security Standard (PCI DSS)

• **FDA:** Meeting US Food and Drug Administration (FDA) requirements for ensuring the trustworthiness and reliability of electronic records and signatures

## Key Attributes

### Qualifying Questions

1. Do you have HIPAA/HITEC data you need to protect?
2. Where does HIPAA data reside?
3. How are you protecting cloud data?
4. By taking payments, you may be obligated to comply with PCI regulations. How are you protecting the data today?
5. Do you have HIPAA data in any big data/no SQL environment?
6. Is the insider threat a concern?
7. How are you managing your encryption keys?
8. How are you protecting end-point devices such as MRIs where applying security patches may invalidate a manufacturer warranty?

## Thales Data Protection Solutions for Healthcare

Our data protection solutions help healthcare enterprises reduce risk, demonstrate compliance and enhance agility while pursuing strategic goals around patient outcomes and organizational accountability.
The Vormetric Data Security Platform is the only solution with a single extensible framework for protecting both structured and unstructured data-at-rest under the diverse requirements of healthcare institutions, across the broadest range of OS platforms, databases, cloud environments and big data implementations.

**Vormetric Transparent Encryption** - provides file and volume level data-at-rest encryption, secure key management and access controls required by regulation and compliance regimes. Deployment is simple, scalable and fast.

**Vormetric Application Encryption-** enables healthcare enterprises that require field-level encryption for database, big data, PaaS or other applications to easily build encryption capabilities into internal applications at the field and column level.

**Vormetric Cloud Encryption Gateway** - encrypts data before it is saved to cloud storage, while keeping encryption keys and access policies under enterprise control. This enables healthcare security teams to establish the visibility and control they need over sensitive patient records.

**Vormetric Key Management** - enables centralized management third-party encryption keys and stores certificates securely. It also provides high availability, standards-based enterprise encryption key management for Transparent Database Encryption (TDE), KMIP compliant devices, and offers vaulting and inventory of certificates.

**Thales nShield HSMs** also offer tamper-resistant, FIPS-certified encryption key protection and management6 that meets the highest security and compliance standards.

THALES

Please visit the Channel Partner Portal and download the Sales Enablement Kit