Helping healthcare organizations improve their data security and compliance posture

Securing patient data

HIGHLIGHTS

- Safeguard medical records by rendering them unusable to attackers
- Facilitate compliance with HIPAA-HITECH and other healthcare data privacy mandates
- Secure the organization's most sensitive keys and business processes in an independently-certified environment
- Protect the organization's reputation and revenue against long-term damage

Securing patient data has become an increasingly difficult task for healthcare organizations, which must strike a balance between user needs and security. With medical records distributed across more databases, applications and devices than ever before, the potential attack surface continues to expand. But clinicians, researchers – and even users themselves – continue to demand access with no slowdown in sight.

LEARN MORE AT ENTRUST.COM/HSM

Improve your data security and compliance posture

Some of the risks facing healthcare enterprises include:

- Reputational and financial damage resulting from a data breach, as future patients will be more likely to seek alternatives
- Highly motivated adversaries seek to exploit vulnerabilities in enterprise networks, as medical records command a premium as compared to stolen credit card numbers and other forms of PII
- Legacy systems and applications complicate security and compliance efforts
- A violation of data privacy mandates could result in fines and increased regulatory scrutiny

Entrust data protection solutions for healthcare enterprises

Entrust and its technology partners help healthcare organizations address their unique challenges. Our data protection solutions help healthcare enterprises reduce risk, demonstrate compliance and enhance agility while pursuing strategic goals around patient outcomes and organizational accountability.

Healthcare data encryption and key protection

Database encryption and strong key protection

Databases are treasure troves of sensitive information. They often contain customers' personal data, confidential competitive information, and intellectual property. Lost or stolen data, especially patient data, can result in reputational damage, public mistrust and serious fines.

Entrust nShield® HSMs add new levels of assurance to database encryption by helping your organization effectively protect and manage encryption keys. With nShield HSMs, you can take full advantage of native database encryption capabilities and still add higher levels of assurance to key management activities, ensuring optimal security, efficiency, and guaranteed accessibility to encrypted data.

nShield HSMs safeguard and manage the cryptographic keys that protect your sensitive data, whether on-premises or in the cloud. nShield HSMs:

- Generate high quality cryptographic keys
- Protect your keys within a FIPS 140-2 certified cryptographic boundary
- Ensure that keys are always available and used only for authorized purposes through robust access control mechanisms and enforced separation of duties

Learn more

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.com**

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com