NCIPHER

www.ncipher.com

Securing Patient Data

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

Helping healthcare organizations improve their data security and compliance postures

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.

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

Helping healthcare organizations improve their data security and compliance postures

NCIPHER SECURITY DATA PROTECTION SOLUTIONS FOR HEALTHCARE ENTERPRISES

nCipher 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 & KEY PROTECTION

Database Encryption

Databases are treasure troves of sensitive information. They often contain customers' personal data, confidential competitive information, and intellectual property. Lost or stolen data, especially customer data, can result in brand damage, competitive disadvantage, and serious fines—even lawsuits.

nCipher HSMs add new levels of assurance to database encryption by helping your organization effectively protect and manage encryption keys. With nCipher 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. By storing encryption keys in a protected environment, separate from the database itself, nShield HSMs enforce separation of duties between security staff and DBAs.

LEARN MORE

Visit us at ncipher.com to learn why healthcare organizations trust nCipher to protect their critical data.

Search: nCipherSecurity

www.ncipher.com