



Securing Public and Private Cloud Databases for .Net or Mono Applications

“Concerns about security are the most prominent reasons that organizations cite for not adopting cloud services.” *—Forrester Research*

CipherDB is the first self-scaling cloud database encryption solution that secures your most sensitive data via military grade encryption and key management. Now you can secure data at-rest in any public or private cloud and comply with strict regulatory requirements like FIPS-140, PCI, HIPAA, and many more. Our solution effortlessly integrates into your .Net or Mono application and eliminates the data privacy, residency, compliance, and security barriers that are holding back your organization from leveraging the benefits of the cloud.

Key Features

AES256-GCM Military Grade Encryption

The encryption is so robust that even the National Security Agency (NSA) recommends it for the protection of government and military classified information.

Automated Key Management

Keys are managed automatically using 4096 bit RSA certificates, and are securely stored separate from the encrypted data in your possession with your complete control.

Self-Scaling Architecture

A stateless, self-scaling security architecture that allows your application and database to scale up or down with negligible performance impact.

Easy Integration

CipherDB understands your application's existing .Net or Mono framework and installs directly into it with no code changes to your application. No gateway solution needed.

Wide Range of Compatibility

CipherDB supports structured and unstructured data in a wide range of databases like Azure SQL, SQL Server, Amazon RDS, MySQL and many more.

Compliance and Audit Ready

Security features and capabilities exceed 3rd party compliance requirements like FIPS-140, PCI, HIPAA, FISMA, EU Data Protection, etc.

Access logs are integrated into CipherDB for forensic and compliance requirements.

Reduce your risk when handling health care data












Our encryption, key management, auditing, and authentication functionality protects your data in the cloud while satisfying compliance requirements. We ensure that requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) are satisfied using our security solutions.





We quickly cover some of the major points of HIPAA and map how Crypteron's security technologies help cover those specific regulatory controls. Please note that full discussion of HIPAA (including HR practices etc.) is beyond the scope of this article - here we focus on Part 164 governing security and privacy requirements within HIPAA. Without Crypteron technology, a very detailed and very expensive audit process is required to prove that data privacy and security is safely contained.

Product Key  *CipherDB*  *CipherStor*  *TotalAuth*


164.306 Security Standard

- ☒ a) General requirements    CipherDB's authentication tags as well as strong encryption bring far reaching, general compliance
- ☒ b) Flexibility of approach    Crypteron technologies are simple to integrate and cloud ready, empowering even the smallest of organizations
- ☒ c) Standards    Enables simpler compliance with sections §164.308, §164.310, §164.312, §164.314, and §164.316








164.308 Administrative Safeguards

- ☒ a-2) Assigned security responsibility  CipherDB enables an identified security officer to easily control encryption keys
- ☒ a-3) Workforce security  DualAuth allows robust user authentication
- ☒ a-4) Information access management   CipherDB/CipherStor only permits authorized access to encrypted data

164.310 Physical Safeguards

- ☒ c) Workstation security  DualAuth brings together a physical device (cellphone) into the authentication process for another layer of protected access

164.312 Technical Safeguards

- ☒ a) Access control   CipherDB/CipherStor use encryption to enforce that only authorized software programs have access rights. DualAuth performs the same job but for users
- ☒ b) Audit control  CipherDB enables logging of access to secured fields and maintains compatibility with traditional SQL monitoring (eg: Azure SQL's sys.event_log etc)
- ☒ c) Integrity  Authenticated encryption with inbuilt checksum tags prevent any form of data tampering. Advanced CipherDB features also prevent several blind cipher text attacks targeting data integrity.
- ☒ d) Person Authentication  DualAuth brings multi-layer authentication for more secure authentication
- ☒ e) Transmission security   CipherDB/CipherStor offer both data-at-rest as well as data-in-transit security via strong military grade (FIPS-140-2/NSA Suite B) encryption.