Data-Centric Security for Healthcare

HIPAA and HITECH technical safeguards specify the use of encryption safeguards for PHI, but many healthcare organizations have fallen into a false sense of security by implementing "checkbox" encryption methods that do nothing to prevent data theft.

Baffle® Data Protection Services helps secure your company's data both on-premise and in the cloud without modifying applications. Data remains encrypted in memory, in use and at-rest without breaking business processes and applications.

Key Benefits

- Mitigates insider threat and data theft risk
- Encrypts data without breaking application functionality
- Ensures compliance with data privacy regulations
- Simplify encryption deployment and reduce development costs

Key Capabilities

Advanced Data Protection
Data is encrypted using AES encryption and protected end-to-end: in memory, in use, in search indices, and at-rest.

Support for Customer Owned Keys
Customers always own the keys and integration with enterprise key management, cloud key management and HSMs is supported.

Comprehensive Application Support
Application functionality is preserved with Baffle's solution and no code modification or rewrites are required.

Secure Compute
Baffle supports wildcard search, mathematical operations, and analytics on AES encrypted data.

Flexible Architecture
The deployment model supports traditional multi-tier applications, microservices architecture, and API-based access models.

Solution Overview

Healthcare compliance regulations such as HIPAA and HITECH require organizations to ensure the confidentiality and data privacy of protected health information (PHI). What many organizations do not know is that commonly used data encryption methods literally donothing to protect data against data theft and hacks.

Baffle Data Protection Services integrates seamlessly with applications to simplify the deployment of encryption, while simultaneously delivering a stronger data protection standard for your organization. Without modifying applications, Baffle can support search and mathematical operations as well as automated workflows and machine-to-machine processing on AES encrypted data to preserve business processes and application functionality.
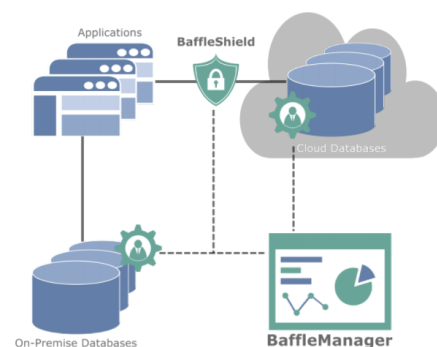
The solution integrates with existing enterprise key management and HSM solutions to support customer-owned keys and can be deployed on-premise or in cloud.

Visit **https://baffle.io/healthcare** for more information.

Key Features and Integrations

Features and Integrations	Status	Description
AES-128 bit encryption	Yes	
AES-256 bit encryption	Yes	
Sort and search on encrypted data	Yes	Wildcard and partial search on AES encrypted data supported
Mathematical operations on encrypted data	Yes	Ability to perform secure computation on encrypted data
Encryption migration utility	Yes	Migration tool to bulk encrypt data
Decryption migration utility	Yes	Migration tool to bulk decrypt data
Live migration supported	Yes	Supports encryption process on production databases
Support for microservices data integrations	Yes	Microservices data access is supported
Support for API-based data integrations	Yes	API-based data access models are supported
Support for customer-owned keys	Yes	Customers own the encryption keys
Integration with Enterprise Key Management	Yes	Supported via KMIP
Integration with HSM	Yes	Supported via PKCS #11 libraries
Integration with AWS KMS	Yes	Supported via REST API
Support for on-premises deployments	Yes	
Support for cloud deployments	Yes	

About Baffle

Baffle Data Protection Services (DPS) provides a transparent "no code" data security layer for distributed data and hybrid cloud environments. Baffle DPS secures data from any source to any destination to ensure data privacy and minimize the risk of data breaches.

Only Baffle supports on-the-fly data de-identification with support for masking, tokenization, field and row level encryption, BYOK/HYOK and privacy preserving analytics for secure data sharing and computation.