Automated Safeguards for Athena

- Overview
- Architecture
- Automated Safeguards
  - Compliance Guidance
    - Encrypted Storage
      - Remediation
    - Encrypted Connections
      - Remediation
  - Shared Responsibility
  - Exclusion
- Reference Architecture Diagram
- ClearDATA IAM Group
- RACI

Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run.

Athena is easy to use. Simply point to your data in Amazon S3, define the schema, and start querying using standard SQL. Most results are delivered within seconds. With Athena, there's no need for complex ETL jobs to prepare your data for analysis. This makes it easy for anyone with SQL skills to quickly analyze large-scale datasets.

Pricing Guidelines

Amazon Athena is priced based on the amount of data that is scanned by each query. Please visit the Amazon Athena Pricing page for details and pricing examples.

Amazon Athena is a serverless, interactive service. There is nothing to configure in order to consume the service. Athena connects to S3 buckets, and the ClearDATA Automated Safeguards for S3 ensure those buckets are correctly configured to store sensitive healthcare data.

Amazon Athena must be properly configured to connect to encrypted S3 buckets and the ClearDATA Automated Safeguards ensure that configuration. In addition, the Automated Safeguards also ensure the Athena Query Results are encrypted.

Compliance Guidance

ClearDATA's Automated Safeguards for Athena ensure that the Athena settings are configured to encrypt all query results, and that all S3 data sources are connected over an encrypted connection. See Configuring Encryption Options for details

Encrypted Storage

HIPAA Technical Safeguard 45 CFR 164.312(a)(2)(iv) requires encryption and decryption as an addressable standard and strongly suggests that you implement a mechanism to encrypt and decrypt electronic protected health information (ePHI). ClearDATA's interpretation of this regulation is that all storage must be encrypted. All Athena query results are stored in encrypted S3 buckets.

Remediation

If no encryption option is selected the Safeguards will encrypt the bucket with S3 SSE-KMS.

Encrypted Connections

HIPAA Technical Safeguard 45 CFR 164.312(a)(2)(iv) requires encryption and decryption as an addressable standard and strongly suggests that you implement a mechanism to encrypt and decrypt electronic protected health information (ePHI). ClearDATA's interpretation of this regulation is that all connections to and from data stored in an S3 bucket, including Athena queries, must use encrypted connections.

Remediation

ClearDATA will automatically, and transparently, configure Athena to access all S3 buckets over an encrypted connection.

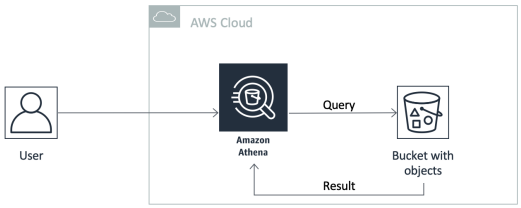
Shared Responsibility

ClearDATA will ensure that all Athena configurations are properly set to encrypt the query results and S3 connections. Customers are responsible for any configuration of a client side query engine via JDBC or ODBC, and ensuring that any PHI or sensitive data that is generated from the client side queries is treated in accordance with their policies and procedures.

Please contact your ClearDATA team for a copy of the Responsibilities Matrix.

Exclusion

Disabling automated remediation at done the Workgroup level. Please contact ClearDATA Support to request that an exclusion be placed to allow for the workgroup to be created.



Users can be added to the **Safeguards-Athena** IAM group to use the Amazon Athena service.

Item	ClearDATA	Customer
Enforcement of Automated Safeguards	RA	IC
Configuration of Athena data structure, tables, and queries	C	RA
Configuration and support of any client side configuration, such as JDBC or ODBC	C	RA