Automated Safeguards for Simple Queuing Service (SQS)

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available.

SQS is priced based on the number of requests made on a queue. Please see Amazon Simple Queue Service Pricing for details.

SQS offers queues for multiple use cases, with standard queues supporting nearly unlimited transactions per second and FIFO queues built for more reliable delivery. Queues can process an unlimited number of messages, and can be used in conjunction with many other AWS services. Please see Amazon Simple Queue Service Features for details.

ClearDATA Automated Safeguards for SQS ensure that all queues have server-side encryption enabled, ensuring that messages containing ePHI and other sensitive healthcare information are encrypted as they are processed by the SQS service.

Compliance Guidance

Encrypted Storage

HIPAA Technical Safeguard 45 CFR 164.312(a)(2)(iv) requires encryption and decryption addressable standard 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, and as a result the Automated Safeguards for SQS configure server-side encryption for all queues.

Remediation

ClearDATA automatically, and transparently, enables server-side encryption of the queue.

Audit Logging

HIPAA Technical Safeguard 45 CFR § 164.312(b) requires a Covered Entity to “Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.” Amazon SQS is integrated with CloudTrail, a service that logs API calls made by or on behalf of Amazon SQS in your AWS account and delivers the log files to the specified Amazon S3 bucket. CloudTrail captures API calls made from the Amazon SQS console or from the Amazon SQS API.

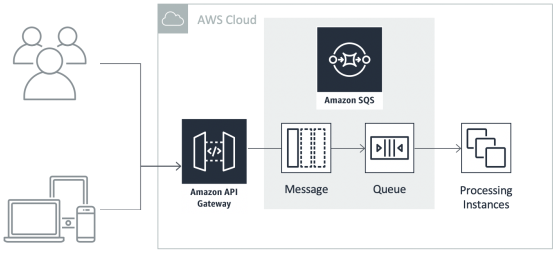
Shared Responsibility

ClearDATA will ensure that all queues have server-side encryption enabled. Customers are responsible for ensuring that connections made to a queue from an application or client uses a secure HTTPS connection. For more information about making SQS requests see Making Query API Requests for details.

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

Exclusion

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



Users can be added to the **Safeguards-SQS** group to gain access to create and manage RDS instances.

Item	**ClearDATA**	**Custom er**
Enforce Automated Safeguards	RA	IC
Ensure all connections made to and from SQS queues use a HTTPS endpoint	C	RA
Ensure any service excluded from automated remediation does not contain any PHI/PII	IC	RA