Architecting for HIPAA in the cloud

You can use AWS to run sensitive workloads regulated under the U.S. Health Insurance Portability and Accountability Act (HIPAA). If you plan to include Protected Health Information (as defined by HIPAA) on AWS services, you must first accept the AWS Business Associate Addendum (AWS BAA). You can review, accept, and check the status of your AWS BAA through a self-service portal available in AWS Artifact.

Any AWS service can be used with a healthcare application, but only services covered by the AWS BAA can be used to store, process, and transmit Protected Health Information under HIPAA.

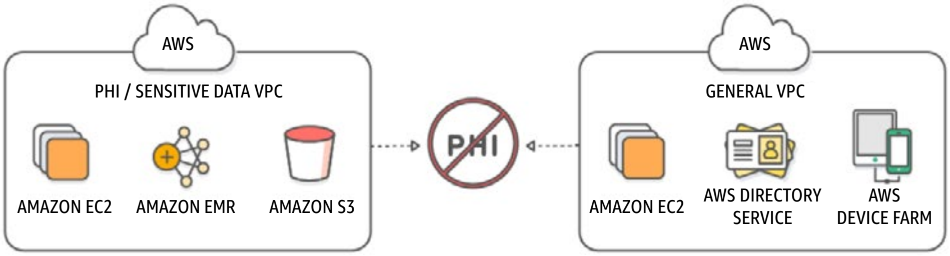
View the current list of services covered by the AWS BAA »

Architecture Strategies

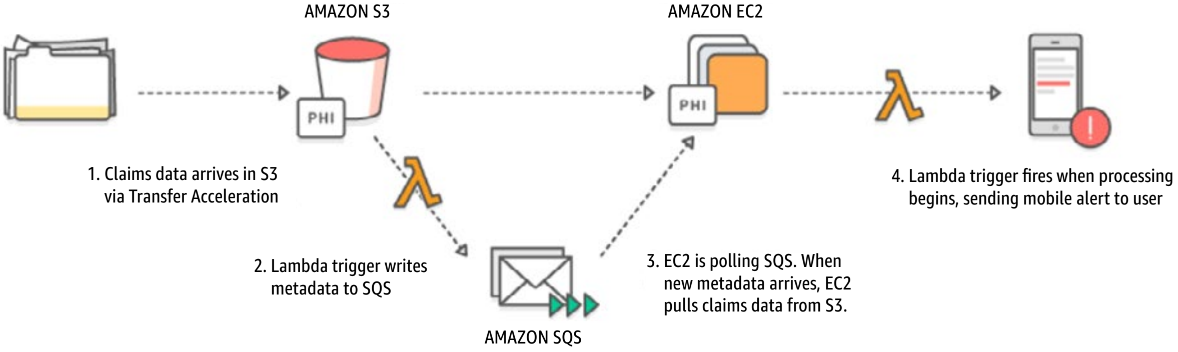
Using AWS for HIPAA applications means following some general strategies, such as:

- Decoupling protected data from processing/orchestration
- Tracking where data flows using automation
- Have logical boundaries between protected and general workflows

Example 1: Separate Amazon Virtual Private Clouds (VPC) for PHI and non-PHI data. The right hand VPC is used to test a mobile app, while the left-hand VPC stores and processes PHI. PHI does not flow from the left-hand to the right-hand VPC. Note: Left-hand VPC must be architected to be consistent with our HIPAA guidance.



Example 2: Indirection strategy. When a new object containing PHI is written to S3 via S3 Transfer Acceleration, an S3 trigger signals AWS Lambda to write the appropriate metadata to an Amazon SQS queue. A service running on Amazon EC2 polls the SQS queue, and if new data is available, pulls the PHI data from S3. A second Lambda function triggers a mobile alert, notifying that processing of data has begun. In this example only S3 and EC2 are used to store, process, and transmit all PHI data; Lambda and SQS are only used to orchestrate services or notify when jobs should begin.


AMAZON S3
AMAZON EC2
PHI
PHI
1. Claims data arrives in S3 via Transfer Acceleration
2. Lambda trigger writes metadata to SQS
AMAZON SQS
3. EC2 is polling SQS. When new metadata arrives, EC2 pulls claims data from S3.
4. Lambda trigger fires when processing begins, sending mobile alert to user

Examples of common architecture patterns are shown below. It is recommended that you do your due diligence, and consult AWS or your internal compliance department before implementing. Learn more at https://aws.amazon.com/health/healthcare-compliance/