Architecting for HIPAA Security and Compliance on Amazon Web Services

October 2017

We welcome your feedback. Please share your thoughts at this link.

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract

This paper briefly outlines how companies can use Amazon Web Services (AWS) to create HIPAA (Health Insurance Portability and Accountability Act)-compliant applications. We will focus on the HIPAA Privacy and Security Rules for protecting Protected Health Information (PHI), how to use AWS to encrypt data in transit and at rest, and how AWS features can be used to meet HIPAA requirements for auditing, back-ups, and disaster recovery.

Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) applies to "covered entities" and "business associates." Covered entities include health care providers engaged in certain electronic transactions, health plans, and health care clearinghouses. Business associates are entities that provide services to a covered entity that involve access by the business associate to Protected Health Information (PHI), as well as entities that create, receive, maintain, or transmit PHI on behalf of another business associate. HIPAA was expanded in 2009 by the Health Information Technology for Economic and Clinical Health (HITECH) Act. HIPAA and HITECH establish a set of federal standards intended to protect the security and privacy of PHI. HIPAA and HITECH impose requirements related to the use and disclosure of PHI, appropriate safeguards to protect PHI, individual rights, and administrative responsibilities. For additional information on HIPAA and HITECH, visit http://www.hhs.gov/ocr/privacy/.

Covered entities and their business associates can use the secure, scalable, low-cost IT components provided by Amazon Web Services (AWS) to architect applications in alignment with HIPAA and HITECH compliance requirements. AWS offers a commercial-off-the-shelf infrastructure platform with industry-recognized certifications and audits such as ISO 27001, FedRAMP, and the Service Organization Control Reports (SOC1, SOC2, and SOC3). AWS services and data centers have multiple layers of operational and physical security to help ensure the integrity and safety of customer data. With no minimum fees, no term-based contracts required, and pay-as-you-use pricing, AWS is a reliable and effective solution for growing health care industry applications.

AWS enables covered entities and their business associates subject to HIPAA to securely process, store, and transmit PHI. Additionally, AWS, as of July 2013, offers a standardized Business Associate Addendum (BAA) for such customers.

Customers who execute an AWS BAA may use any AWS service in an account designated as a HIPAA Account, but they may only process, store and transmit PHI using the HIPAA-eligible services defined in the AWS BAA. For a complete list of these services, see the HIPAA Eligible Services Reference page (https://aws.amazon.com/compliance/hipaa-eligible-services-reference/).

AWS maintains a standards-based risk management program to ensure that the HIPAA-eligible services specifically support the administrative, technical, and physical safeguards required under HIPAA. Using these services to store, process, and transmit PHI allows our customers and AWS to address the HIPAA requirements applicable to the AWS utility-based operating model.

Encryption and Protection of PHI in AWS

The HIPAA Security Rule includes addressable implementation specifications for the encryption of PHI in transmission ("in transit") and in storage ("at rest"). Although this is an addressable implementation specification in HIPAA, AWS requires customers to encrypt PHI stored in or transmitted using HIPAA-eligible services in accordance with guidance from the Secretary of Health and Human Services (HHS): Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals ("Guidance"). Please refer to this site because it may be updated, and may be made available on a successor (or related site) designated by HHS.

AWS offers a comprehensive set of features and services to make key management and encryption of PHI easy to manage and simpler to audit, including the AWS Key Management Service (AWS KMS). Customers with HIPAA compliance requirements have a great deal of flexibility in how they meet encryption requirements for PHI.

When determining how to implement encryption, customers may evaluate and take advantage of the encryption features native to the HIPAA-eligible services, or they can satisfy the encryption requirements through other means consistent with the guidance from HHS. The following sections provide high-level details about using available encryption features in each of the HIPAA-eligible services and other patterns for encrypting PHI, and how AWS KMS can be used to encrypt the keys used for encryption of PHI on AWS.

Amazon EC2

Amazon EC2 is a scalable, user-configurable compute service that supports multiple methods for encrypting data at rest. For example, customers might elect to perform application- or field-level encryption of PHI as it is processed within an application or database platform hosted in an Amazon EC2 instance. Approaches range from encrypting data using standard libraries in an

application framework such as Java or .NET; leveraging Transparent Data Encryption features in Microsoft SQL or Oracle; or by integrating other third-party and software as a service (SaaS)-based solutions into their applications. Customers can choose to integrate their applications running in Amazon EC2 with AWS KMS SDKs, simplifying the process of key management and storage. Customers can also implement encryption of data at rest using file-level or full disk encryption (FDE) by utilizing third-party software from AWS Marketplace Partners or native file system encryption tools (such as dm-crypt, LUKS, etc.).

Network traffic containing PHI must encrypt data in transit. For traffic between external sources (such as the Internet or a traditional IT environment) and Amazon EC2, customers should use industry-standard transport encryption mechanisms such as TLS or IPsec virtual private networks (VPNs), consistent with the Guidance. Internal to an Amazon Virtual Private Cloud (VPC) for data traveling between Amazon EC2 instances, network traffic containing PHI must also be encrypted; most applications support TLS or other protocols providing in transit encryption that can be configured to be consistent with the Guidance. For applications and protocols that do not support encryption, sessions transmitting PHI can be sent through encrypted tunnels using IPsec or similar implementations between instances.

Amazon EC2 Systems Manager

Amazon EC2 Systems Manager is a management service that helps customers securely and automatically manage their fleet by collecting software inventory, applying OS patches, creating system images, and configuring Windows and Linux operating systems. These capabilities help customers define and track system configurations, prevent drift, and maintain software compliance of their EC2 and on-premises configurations.

EC2 Systems Manager encrypts customer content in transit and at rest. When outputting data that may contain PHI to other services (such as S3), customers must follow the receiving service's guidance for storing PHI. Customers should not include PHI in metadata or identifiers, such as document names and parameter names.

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud (VPC) offers a set of network security features well-aligned to architecting for HIPAA compliance. Features such as stateless network access control lists and dynamic reassignment of instances into stateful security groups afford flexibility in protecting the instances from unauthorized network access. Amazon VPC also allows customers to extend their own network address space into AWS, as well as providing a number of ways to connect their data centers to AWS. VPC Flow Logs provide an audit trail of accepted and rejected connections to instances processing, transmitting or storing PHI. For more information on Amazon VPC, see http://aws.amazon.com/vpc/.

Amazon Elastic Block Store

Amazon EBS encryption at rest is consistent with the Guidance that is in effect at the time of publication of this whitepaper. Because the Guidance might be updated, customers should continue to evaluate and determine whether Amazon EBS encryption satisfies their compliance and regulatory requirements. With Amazon EBS encryption, a unique volume encryption key is generated for each EBS volume; customers have the flexibility to choose which master key from the AWS Key Management Service is used to encrypt each volume key. For more information, see http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html .

Amazon Redshift

Amazon Redshift provides database encryption for its clusters to help protect data at rest. When customers enable encryption for a cluster, Amazon Redshift encrypts all data, including backups, by using hardware-accelerated Advanced Encryption Standard (AES)-256 symmetric keys. Amazon Redshift uses a four-tier, key-based architecture for encryption. These keys consist of data encryption keys, a database key, a cluster key, and a master key. The cluster key encrypts the database key for the Amazon Redshift cluster. Customers can use either AWS KMS or an AWS CloudHSM (Hardware Security Module) to manage the cluster key. Amazon Redshift encryption at rest is consistent with the Guidance that is in effect at the time of publication of this whitepaper. Because the Guidance might be updated, customers should continue to evaluate and

determine whether Amazon Redshift encryption satisfies their compliance and regulatory requirements. For more information see http://docs.aws.amazon.com/redshift/latest/mgmt/working-with-db-encryption.html.

Connections to Amazon Redshift containing PHI must use transport encryption and customers should evaluate the configuration for consistency with the Guidance. For more information, see http://docs.aws.amazon.com/redshift/latest/mgmt/connecting-ssl-support.html.

Amazon S3

Customers have several options for encryption of data at rest when using Amazon S3, including both server-side and client-side encryption and several methods of managing keys. For more information see http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html.

Connections to Amazon S3 containing PHI must use endpoints that accept encrypted transport (HTTPS). For a list of regional endpoints, see http://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region.

Customers should not use PHI in bucket names, object names, or metadata because this data is not encrypted using S3 server-side encryption and is not generally encrypted in client-side encryption architectures.

Amazon S3 Transfer Acceleration

Amazon S3 Transfer Acceleration (S3TA) enables fast, easy, and secure transfers of files over long distances between a customer's client and an S3 bucket. Transfer Acceleration takes advantage of Amazon CloudFront's globally distributed edge locations. As the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path.

Customers should ensure that any data containing PHI transferred using AWS S3TA is encrypted in transit and at rest. Please refer to the guidance for Amazon S3 to understand the available encryption options.

Amazon SNS

Customers should understand the following key encryption requirement in order to use Amazon Simple Notification Service (SNS) with Protected Health Information (PHI). Customers must use the HTTPS API endpoint that SNS provides in each AWS region. The HTTPS endpoint leverages encrypted connections, and protects the privacy and integrity of the data sent to AWS. For a list of all HTTPS API endpoints, see the AWS Documentation at http://docs.aws.amazon.com/general/latest/gr/rande.html#sns_region.

Additionally, Amazon SNS is integrated with CloudTrail, a service that captures API calls made by or on behalf of Amazon SNS in the customer's AWS account and delivers the log files to an Amazon S3 bucket that they specify. CloudTrail captures API calls made from the Amazon SNS console or from the Amazon SNS API. Using the information collected by CloudTrail, customers can determine what request was made to Amazon SNS, the source IP address from which the request was made, who made the request, and when it was made. For more information on logging SNS operations, see http://docs.aws.amazon.com/sns/latest/dg/logging-using-cloudtrail.html.

Amazon SQS

Customers should understand the following key encryption requirements in order to use Amazon SQS with Protected Health Information (PHI).

- Communication with the Amazon SQS Queue via the Query Request must be encrypted with HTTPS. For more information on making SQS requests, see http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/MakingRequests_MakingQueryRequestsArticle.html.
- Amazon SQS supports server-side encryption integrated with the AWS Key Management Service (AWS KMS) to protect data at rest. The addition of server-side encryption allows you to transmit and receive sensitive data with the increased security of using encrypted queues. Amazon SQS server-side encryption uses the 256-bit Advanced Encryption Standard (AES-256 GCM algorithm) to encrypt the body of each message. The integration with AWS KMS allows you to centrally manage the keys that protect Amazon SQS messages along with keys that protect your other AWS resources. AWS KMS logs every use of your

encryption keys to AWS CloudTrail to help meet your regulatory and compliance needs. For more information, and to check your region for the availability for SSE for Amazon SQS, see: http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-server-side-encryption.html.

- If server-side encryption is not used, the message payload itself must be encrypted prior to being sent to SQS. One way to encrypt the message payload is by using the Amazon SQS Extended Client along with the Amazon S3 encryption client. For more information on using client-side encryption, see https://aws.amazon.com/blogs/developer/encrypting-message-payloads-using-the-amazon-sqs-extended-client-and-the-amazon-s3-encryption-client/.

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. You can use the information collected by CloudTrail to determine which requests are made to Amazon SQS, the source IP address from which the request is made, who made the request, when it is made, and so on. For more information on logging SQS operations, see http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/logging-using-cloudtrail.html.

Amazon Glacier

Amazon Glacier automatically encrypts data at rest using AES 256-bit symmetric keys and supports secure transfer of customer data over secure protocols.

Connections to Amazon Glacier containing PHI must use endpoints that accept encrypted transport (HTTPS). For a list of regional endpoints, see http://docs.aws.amazon.com/general/latest/gr/rande.html#glacier_region.

Customers should not use PHI in archive and vault names or metadata because this data is not encrypted using Amazon Glacier server-side encryption and is not generally encrypted in client-side encryption architectures.

Amazon RDS for MySQL

Amazon RDS for MySQL allows customers to encrypt MySQL databases using keys that customers manage through AWS KMS. On a database instance running with Amazon RDS encryption, data stored at rest in the underlying storage is encrypted consistent with the Guidance in effect at the time of publication of this whitepaper, as are automated backups, read replicas, and snapshots. Because the Guidance might be updated, customers should continue to evaluate and determine whether Amazon RDS for MySQL encryption satisfies their compliance and regulatory requirements. For more information on encryption at rest using Amazon RDS, see http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html.

Connections to RDS for MySQL containing PHI must use transport encryption. For more information on enabling encrypted connections, see http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html.

Amazon RDS for Oracle

Customers have several options for encrypting PHI at rest using Amazon RDS for Oracle.

Customers can encrypt Oracle databases using keys that customers manage through AWS KMS. On a database instance running with Amazon RDS encryption, data stored at rest in the underlying storage is encrypted consistent with the Guidance in effect at the time of publication of this whitepaper, as are automated backups, read replicas, and snapshots. Because the Guidance might be updated, customers should continue to evaluate and determine whether Amazon RDS for Oracle encryption satisfies their compliance and regulatory requirements. For more information on encryption at rest using Amazon RDS, see http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html.

Customers can also leverage Oracle Transparent Data Encryption (TDE), and customers should evaluate the configuration for consistency with the Guidance. Oracle TDE is a feature of the Oracle Advanced Security option available in

Oracle Enterprise Edition. This feature automatically encrypts data before it is written to storage and automatically decrypts data when the data is read from storage. Customers can also use AWS CloudHSM to store Amazon RDS Oracle TDE keys. For more information, see the following:

- Amazon RDS for Oracle Transparent Data Encryption: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.Oracle.Options.AdvSecurity.html.
- Using AWS CloudHSM to store Amazon RDS Oracle TDE keys: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.OracleCloudHSM.html.

Connections to Amazon RDS for Oracle containing PHI must use transport encryption and evaluate the configuration for consistency with the Guidance. This is accomplished using Oracle Native Network Encryption and enabled in Amazon RDS for Oracle option groups. For detailed information, see http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.Oracle.Options.NetworkEncryption.html.

Amazon RDS for PostgreSQL

Amazon RDS for PostgreSQL allows customers to encrypt PostgreSQL databases using keys that customers manage through AWS KMS. On a database instance running with Amazon RDS encryption, data stored at rest in the underlying storage is encrypted consistent with the Guidance in effect at the time of publication of this whitepaper, as are automated backups, read replicas, and snapshots. Because the Guidance might be updated, customers should continue to evaluate and determine whether Amazon RDS for PostgreSQL encryption satisfies their compliance and regulatory requirements. For more information on encryption at rest using Amazon RDS, see http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html.

Connections to RDS for PostgreSQL containing PHI must use transport encryption. For more information on enabling encrypted connections, see http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html.

Amazon RDS for SQL Server

RDS for SQL Server supports storing PHI for the following version and edition combinations:

- 2008 R2 - Enterprise Edition only
- 2012, 2014 and 2016 - Web, Standard and Enterprise Editions

> **Important:** SQL Server Express edition is not supported and should never be used for the storage of PHI.

In order to store PHI, customers must ensure that the instance is configured to encrypt data at rest, and enable transport encryption and auditing, as detailed below.

Encryption at Rest

Customers can encrypt SQL Server databases using keys that customers manage through AWS KMS. On a database instance running with Amazon RDS encryption, data stored at rest in the underlying storage is encrypted consistent with the Guidance in effect at the time of publication of this whitepaper, as are automated backups, and snapshots. Because the Guidance might be updated, customers should continue to evaluate and determine whether Amazon RDS for SQL Server encryption satisfies their compliance and regulatory requirements. For more information about encryption at rest using Amazon RDS, see http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html.

Customers using SQL Server Enterprise Edition may choose to use Server Transparent Data Encryption (TDE) as an alternative. This feature automatically encrypts data before it is written to storage and automatically decrypts data when the data is read from storage. For more information on RDS for SQL Server Transparent Data Encryption see

http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.SQLServer.Options.TDE.html.

Transport Encryption

Connections to Amazon RDS for SQL Server containing PHI must use transport encryption provided by SQL Server Forced SSL. Forced SSL is enabled from within the parameter group for Amazon RDS SQL Server. For more information on RDS for SQL Server Forced SSL see http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/SQLServer.Concepts.General.SSL.Using.html.

Auditing

RDS for SQL Server instances that contain PHI must have auditing enabled. Auditing is enabled from within the parameter group for Amazon RDS SQL Server. For more information on RDS for SQL Server auditing see http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_SQLServer.html#SQLServer.Concepts.General.Compliance.

Amazon RDS for MariaDB

Amazon RDS for MariaDB allows customers to encrypt MariaDB databases using keys that customers manage through AWS KMS. On a database instance running with Amazon RDS encryption, data stored at rest in the underlying storage is encrypted consistent with the Guidance in effect at the time of publication of this whitepaper, as are automated backups, read replicas, and snapshots. Because the Guidance might be updated, customers should continue to evaluate and determine whether Amazon RDS for MariaDB encryption satisfies their compliance and regulatory requirements. For more information on encryption at rest using Amazon RDS, see http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html.

Connections to RDS for MariaDB containing PHI must use transport encryption. For more information on enabling encrypted connections, see http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html

Amazon Aurora

Amazon Aurora allows customers to encrypt Aurora databases using keys that customers manage through AWS KMS. On a database instance running with Amazon Aurora encryption, data stored at rest in the underlying storage is

encrypted consistent with the Guidance in effect at the time of publication of this whitepaper, as are automated backups, read replicas, and snapshots. Because the Guidance might be updated, customers should continue to evaluate and determine whether Amazon Aurora encryption satisfies their compliance and regulatory requirements. For more information on encryption at rest using Amazon RDS, see http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html.

Customers may use either the MySQL-compatible edition of Amazon Aurora or the PostgreSQL-compatible version as part of our BAA.

Connections to Aurora containing PHI must use transport encryption. For more information on enabling encrypted connections, see http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html.

Amazon CloudFront

Amazon CloudFront is a global content delivery network (CDN) service that accelerates delivery of customer websites, APIs, video content or other web assets. It integrates with other Amazon Web Services products to give developers and businesses an easy way to accelerate content to end users with no minimum usage commitments.

To ensure encryption of PHI while in transit with CloudFront, customers must configure CloudFront to use HTTPS end-to-end from the origin to the viewer. This includes traffic between CloudFront and the viewer, CloudFront re-distributing from a custom origin, and CloudFront distributing from an S3 origin.

Customers should also ensure the data is encrypted at the origin to ensure it remains encrypted at rest while cached in CloudFront. If utilizing S3 as an origin, customers can make use of S3 server-side encryption features. If customers distribute from a custom origin, they need to ensure the data is encrypted at the origin.

Lambda@Edge

Lambda@Edge is a compute service that allows for the execution of Lambda functions at AWS Edge locations. Lambda@Edge can be used to customize content delivered through CloudFront. When using Lambda@Edge with PHI, customers should follow the guidance for the use of CloudFront. All connections into and out of Lambda@Edge should be encrypted using HTTPS or SSL/TLS.

Elastic Load Balancing

Customers may use Elastic Load Balancing to terminate and process sessions containing PHI. Customers may choose either the Classic Load balancer or the Application Load Balancer. Because all network traffic containing PHI must be encrypted in transit end-to-end, customers have the flexibility to implement two different architectures:

Customers can terminate HTTPS, HTTP/2 over TLS (for Application), or SSL/TLS on Elastic Load Balancing by creating a load balancer that uses an encrypted protocol for connections. This feature enables traffic encryption between the customer's load balancer and the clients that initiate HTTPS, HTTP/2 over TLS, or SSL/TLS sessions, and for connections between the load balancer and customer back-end instances. Sessions containing PHI must encrypt both front-end and back-end listeners for transport encryption. Customers should evaluate their certificates and session negotiation policies and maintain them consistent to the Guidance. For more information, see http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-https-load-balancers.html.

Alternatively, customers can configure Amazon ELB in basic TCP-mode (for Classic) or over WebSockets (for Application) and pass-through encrypted sessions to back-end instances where the encrypted session is terminated. In this architecture, customers manage their own certificates and TLS negotiation policies in applications running in their own instances. For more information, see http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-listener-config.html.

In both architectures, customers should implement a level of logging which they determine to be consistent with HIPAA and HITECH requirements.

Amazon ECS

Amazon EC2 Container Service (ECS) is a highly scalable, high performance container management service that supports Docker containers and allows you to easily run applications on a managed cluster of Amazon EC2 instances. Amazon ECS eliminates the need for you to install, operate, and scale your own cluster management infrastructure. With simple API calls, you can launch and stop Docker-enabled applications, query the complete state of your cluster, and access many familiar features like security groups, Elastic Load Balancing, EBS volumes, and IAM roles. You can use Amazon ECS to schedule the placement of containers across your cluster based on your resource needs and availability requirements.

Using ECS with workloads that process PHI requires no additional configuration. ECS acts as an orchestration service that coordinates the launch of containers (images for which are stored in S3) on EC2, and it does not operate with or upon data within the workload being orchestrated. Consistent with HIPAA regulations and the AWS Business Associate Addendum, PHI should be encrypted in transit and at rest when accessed by containers launched with ECS. Various mechanisms for encrypting at rest are available with each AWS storage option (for example, S3, EBS, and KMS). Ensuring complete encryption of PHI sent between containers may also lead a customer to deploy an overlay network (such as VNS3, Weave Net or similar), in order to provide a redundant layer of encryption. Nevertheless, complete logging should also be enabled (e.g. through CloudTrail), and all container instance logs should be directed to CloudWatch.

Amazon EMR

Amazon EMR deploys and manages a cluster of Amazon EC2 instances into a customer's account.

For information on encryption with Amazon EMR, please see https://docs.aws.amazon.com/ElasticMapReduce/latest/ReleaseGuide/emr-data-encryption-options.html.

Amazon DynamoDB

Connections to Amazon DynamoDB containing PHI must use endpoints that accept encrypted transport (HTTPS). For a list of regional endpoints, see http://docs.aws.amazon.com/general/latest/gr/rande.html#ddb_region.

PHI stored in Amazon DynamoDB must be encrypted at rest consistent with the Guidance. Amazon DynamoDB customers can use the application development framework of their choice to encrypt PHI in applications before storing the data in Amazon DynamoDB. Alternatively, a client-side library for encrypting content is available from the AWS Labs GitHub repository. Customers may evaluate this implementation for consistency with the Guidance. For more information, see https://github.com/awslabs/aws-dynamodb-encryption-java. Careful consideration should be taken when selecting primary keys and when creating indexes such that unsecured PHI is not required for queries and scans in Amazon DynamoDB.

Amazon API Gateway

Customers may use Amazon API Gateway to process and transmit PHI. While Amazon API Gateway automatically uses HTTPS endpoints for encryption in-flight, customers may also choose to encrypt payloads client-side. API Gateway passes all non-cached data through memory and does not write it to disk. Customers may use AWS Signature Version 4 for authorization with API Gateway. For more information, see the following:

- https://aws.amazon.com/api-gateway/faqs/#security
- https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-control-access-to-api.html

Customers may integrate with any service that is connected to API Gateway, provided that when PHI is involved, the service is configured consistent with the Guidance and BAA. For information on integrating API Gateway with back end services, see https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-method-settings.html.

Customers can use AWS CloudTrail and Amazon CloudWatch to enable logging that is consistent with their logging requirements. Customers should ensure

that any PHI sent through API Gateway (such as in headers, URLs, and request/response) is only captured by HIPAA-eligible services that have been configured to be consistent with the Guidance. For more information on logging with API Gateway, see https://aws.amazon.com/premiumsupport/knowledge-center/api-gateway-cloudwatch-logs/.

AWS Storage Gateway

AWS Storage Gateway is a hybrid storage service that enables customer's on-premises applications to seamlessly use AWS cloud storage. The gateway uses industry-standard storage protocols to connect existing storage applications and workflows to AWS cloud storage services for minimal process disruption.

File Gateway

File gateway is a type of AWS Storage Gateway that supports a file interface into Amazon S3 and that adds to the current block-based volume and VTL storage. File gateway uses https to communicate with S3 and stores all objects encrypted while on S3 using SSE-S3, by default, or using Client Side Encryption with keys stored in AWS KMS. File metadata, such as file names, remains unencrypted and should not contain any PHI.

Volume Gateway

Volume gateway provides cloud-backed storage volumes that customers can mount as Internet Small Computer System Interface (iSCSI) devices from on-premises application servers. Customers should attach local disks as Upload buffers and Cache to the Volume Gateway VM in accordance with their internal compliance and regulatory requirements. It is recommended that, for PHI, these disks should be capable of providing encryption at rest. Communication between the Volume Gateway VM and AWS is encrypted using SSL (TLS 1.2) to secure PHI in transport.

Tape Gateway

Tape gateway provides a VTL (virtual tape library) interface to 3rd party backup applications running on-premises. Customers should enable encryption for PHI within the 3rd backup application when setting up a tape backup job. Communication between the Tape Gateway VM and AWS is encrypted using SSL (TLS 1.2) to secure PHI in transport.

Customers using any of the Storage Gateway configurations with PHI should enable full logging. For more information, see http://docs.aws.amazon.com/storagegateway/latest/userguide/logging-using-cloudtrail-common.html

Using AWS KMS for Encryption of PHI

Master keys in AWS KMS can be used to encrypt/decrypt data encryption keys used to encrypt PHI in customer applications or in AWS services that are integrated with AWS KMS. AWS KMS can be used in conjunction with a HIPAA account, but PHI may only be processed, stored, or transmitted in HIPAA Eligible Services. AWS KMS is normally used to generate and manage keys for applications running in other HIPAA Eligible Services. For example, an application processing PHI in Amazon EC2 could use the GenerateDataKey API call to generate data encryption keys for encrypting and decrypting PHI in the application. The data encryption keys would be protected by customer master keys stored in AWS KMS, creating a highly auditable key hierarchy as API calls to AWS KMS are logged in AWS CloudTrail. PHI should not be stored in the Tags (metadata) for any keys stored in AWS KMS.

AWS Shield

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards web applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection.

AWS Shield cannot be used to store or transmit PHI, but instead can be used to safeguard web applications that do operate with PHI. As such, no special configuration is needed when engaging AWS Shield.

All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge. AWS Shield Standard defends against most common, frequently-occurring network and transport layer DDoS attacks that target your website or applications. For higher levels of protection against attacks targeting your web applications running on Elastic Load Balancing (ELB), Amazon CloudFront, and Amazon Route 53 resources, you can subscribe to AWS Shield Advanced.

AWS Snowball

With AWS Snowball (Snowball), customers can transfer hundreds of terabytes or petabytes of data between their on-premises data centers and Amazon Simple Storage Service (Amazon S3).

PHI stored in AWS Snowball must be encrypted at rest consistent with the Guidance. When creating an import job, customers will need to specify the ARN for the AWS Key Management Service (AWS KMS) master key to be used to protect data within the Snowball. In addition, during the creation of the import job, customers should choose a destination S3 bucket that meets the encryption standards set by the Guidance. While Snowball does not currently support server-side encryption with AWS KMS-managed keys (SSE-KMS) or server-side encryption with customer provided keys (SSE-C), Snowball does support server-side encryption with Amazon S3-managed encryption keys (SSE-S3). For more information see Protecting Data Using Server-Side Encryption with Amazon S3-Managed Encryption Keys (SSE-S3).

Alternatively, customers can use the encryption methodology of their choice to encrypt PHI before storing the data in AWS Snowball.

Currently, customers may use the standard AWS Snowball appliance or AWS Snowmobile as part of our BAA.

AWS Snowball Edge

AWS Snowball Edge connects to existing customer applications and infrastructure using standard storage interfaces, streamlining the data transfer process and minimizing setup and integration. Snowball Edge can cluster together to form a local storage tier and process customer data on-site, helping customers ensure that their applications continue to run even when they are not able to access the cloud.

To ensure that PHI remains encrypted while using Snowball Edge, customers should make sure to use an encrypted connection protocol such as HTTPS or SSL/TLS when using AWS Lambda procedures powered by AWS Greengrass to transmit PHI to/from resources external to Snowball Edge. Additionally, PHI should be encrypted while stored on the local volumes of Snowball Edge, either through local access or via NFS. Encryption is automatically applied to data

placed into Snowball Edge using the Snowball Management Console and API for bulk transport into S3. For more information on data transport into S3, see the related guidance for AWS Snowball above.

AWS Snowmobile

Snowmobile is operated by AWS as a managed service. As such, AWS will contact the customer to determine requirements for deployment and arrange for network connectivity as well as provide assistance moving data. Data stored on Snowmobile is encrypted using the same guidance provided for AWS Snowball.

AWS WAF – Web Application Firewall

AWS WAF is a web application firewall that helps protect customer web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.

Customers may place AWS WAF between their web applications hosted on AWS that operate with or exchange PHI, and their end users. As with the transmission of any PHI while on AWS, data containing PHI must be encrypted while in transit. Refer to the guidance for Amazon EC2 to better understand the available encryption options.

AWS Directory Service

AWS Directory Service for Microsoft AD

AWS Directory Service for Microsoft Active Directory (Enterprise Edition), also known as AWS Microsoft AD, enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud. AWS Microsoft AD stores directory content (including content containing PHI) in encrypted Amazon Elastic Block Store volumes using encryption keys that AWS manages. For more information, see Amazon EBS Encryption. Data in transit to and from Active Directory clients is encrypted when it travels through Lightweight Directory Access Protocol (LDAP) over your Amazon Virtual Private Cloud (VPC) network. If an Active Directory client resides in an on-premises network, the traffic travels to your VPC by a virtual private network link or an AWS Direct Connect link.

Amazon Cloud Directory

Amazon Cloud Directory enables you to build flexible cloud-native directories for organizing hierarchies of data along multiple dimensions. You also can create directories for a variety of use cases, such as organizational charts, course catalogs, and device registries. For example, you can create an organizational chart that can be navigated through separate hierarchies for reporting structure, location, and cost center. Amazon Cloud Directory automatically encrypts data at rest and in transit by using 256-bit encryption keys that are managed by the AWS Key Management Service (KMS).

Amazon WorkSpaces

Amazon WorkSpaces is a fully managed, secure Desktop-as-a-Service (DaaS) solution that runs on AWS. With Amazon WorkSpaces, you can easily provision virtual, cloud-based Microsoft Windows desktops for your users, providing them access to the documents, applications, and resources they need, anywhere, anytime, from any supported device.

Amazon WorkSpaces stores data in Amazon Elastic Block Store volumes. You can encrypt your WorkSpaces storage volumes using keys that you manage through AWS Key Management Service. When encryption is enabled on a WorkSpace, both the data stored at rest in the underlying storage and the automated backups (EBS Snapshots) of the disk storage are encrypted consistent with the Guidance. Communication from the WorkSpace clients to WorkSpace is secured using industry-standard SSL. For more information on encryption at rest using Amazon WorkSpaces, see http://docs.aws.amazon.com/workspaces/latest/adminguide/encrypt-workspaces.html.

Amazon WorkDocs

Amazon WorkDocs is a fully managed, secure enterprise file storage and sharing service with strong administrative controls and feedback capabilities that improve user productivity.

Amazon WorkDocs files are encrypted at rest using keys that you manage through AWS Key Management Service (KMS). All data in transit is encrypted using industry-standard SSL. AWS web and mobile applications, and desktop sync clients, transmit files directly to Amazon WorkDocs using SSL. Using the

Amazon WorkDocs Management Console, WorkDocs administrators can view audit logs to track file and user activity by time, and choose whether to allow users to share files with others outside their organization. Amazon WorkDocs is also integrated with CloudTrail (a service that captures API calls made by or on behalf of Amazon WorkDocs in your AWS account), and delivers CloudTrail log files to an Amazon S3 bucket that you specify.

Multi-factor authentication (MFA) using a RADIUS server is available and can provide you with an additional layer of security during the authentication process. Users log in by entering their user name and password followed by an OTP (One-Time Passcode) supplied by a hardware or a software token.

For more information, see:

- https://aws.amazon.com/workdocs/details/#secure
- http://docs.aws.amazon.com/workdocs/latest/adminguide/cloudtrail_logging.html

Customers should not store PHI in filenames or directory names.

Amazon Inspector

Amazon Inspector is an automated security assessment service for customers seeking to improve their security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity.

Customers may run Amazon Inspector on EC2 instances that contain PHI. Amazon Inspector encrypts all data transmitted over the network as well as all telemetry data stored at rest.

Amazon Kinesis Streams

Amazon Kinesis Streams enables customers to build custom applications that process or analyze streaming data for specialized needs. The server-side encryption feature allows customers to encrypt data at rest. When server-side encryption is enabled, Kinesis Streams will use an AWS Key Management

Service (AWS KMS) key to encrypt the data before storing it on disks. For more information, see http://docs.aws.amazon.com/streams/latest/dev/server-side-encryption.html.

Connections to Amazon S3 containing PHI must use endpoints that accept encrypted transport (i.e., HTTPS). For a list of regional endpoints, see http://docs.aws.amazon.com/general/latest/gr/rande.html#ak_region.

AWS Lambda

AWS Lambda lets customers run code without provisioning or managing servers on their own. AWS Lamba uses a compute fleet of Amazon Elastic Compute Cloud (Amazon EC2) instances across multiple Availability Zones in a region, which provides the high availability, security, performance, and scalability of the AWS infrastructure.

To ensure that PHI remains encrypted while using AWS Lambda, connections to external resources should use an encrypted protocol such as HTTPS or SSL/TLS. For example, when S3 is accessed from a Lambda procedure, it should be addressed with https://bucket.s3-aws-region.amazonaws.com. If any PHI is placed at rest or idled within a running procedure, it should be encrypted client-side or server-side with keys obtained from AWS KMS or AWS CloudHSM. Follow the related guidance for AWS API Gateway when triggering AWS Lambda functions through the service. When using events from other AWS services to trigger AWS Lambda functions, the event data should not contain (in and of itself) PHI. For example, when a Lambda procedure is triggered from an S3 event, such as the arrival of an object on S3, the object name which is relayed to Lambda should not have any PHI, although the object itself can contain such data.

AWS Batch

AWS Batch enables developers, scientists, and engineers to easily and efficiently run hundreds of thousands of batch computing jobs on AWS. AWS Batch dynamically provisions the optimal quantity and type of compute resources (such as CPU or memory optimized instances) based on the volume and specific resource requirements of the batch jobs submitted. AWS Batch plans, schedules, and executes your batch computing workloads across the full range of AWS compute services and features.

Similar to guidance for AWS ECS, PHI should not be placed directly into the job definition, the job queue or the tags for AWS Batch. Instead, jobs scheduled and executed with AWS Batch may operate on encrypted PHI. Any information returned by stages of a job to AWS Batch should also not contain any PHI. Whenever jobs being executed by AWS Batch need to transmit or receive PHI, that connection should be encrypted using HTTPS or SSL/TLS.

Amazon Connect

Amazon Connect is a self-service, cloud-based contact center service that enables dynamic, personal, and natural customer engagement at any scale.

Customers should not include any PHI in any fields associated with managing users, security profiles, and contact flows within Amazon Connect.

Amazon Route 53

Amazon Route 53 is a managed DNS service that provides customers the ability to register domain names, route internet traffic customer domain resources and check the health of those resources. While Amazon Route 53 is a HIPAA Eligible Service, no PHI should be stored in any resource names or tags within Amazon Route 53 as there is no support for encrypting such data. Instead, Amazon Route 53 can be used to provide access to customer domain resources that transmit or store PHI such as web servers running on Amazon EC2 or storage such as Amazon S3.

AWS CloudHSM

AWS CloudHSM is a cloud-based hardware security module (HSM) that enables customers to easily generate and use their own encryption keys on the AWS Cloud. With CloudHSM, customers can manage their own encryption keys using FIPS 140-2 Level 3 validated HSMs. CloudHSM offers customers the flexibility to integrate with their applications using industry-standard APIs, such as PKCS#11, Java Cryptography Extensions (JCE), and Microsoft CryptoNG (CNG) libraries. CloudHSM is also standards-compliant and enables customers to export all of their keys to most other commercially-available HSMs.

As Cloud HSM is a hardware appliance key management service, it is unable to store or transmit PHI. Customers should not store PHI in Tags (metadata). No other special guidance is required.

Auditing, Back-Ups, and Disaster Recovery

HIPAA's Security Rule also requires in-depth auditing capabilities, data back-up procedures, and disaster recovery mechanisms. The services in AWS contain many features that help customers address these requirements.

In designing an information system that is consistent with HIPAA and HITECH requirements, customers should put auditing capabilities in place to allow security analysts to examine detailed activity logs or reports to see who had access, IP address entry, what data was accessed, etc. This data should be tracked, logged, and stored in a central location for extended periods of time, in case of an audit. Using Amazon EC2, customers can run activity log files and audits down to the packet layer on their virtual servers, just as they do on traditional hardware. They also can track any IP traffic that reaches their virtual server instance. A customer's administrators can back up the log files into Amazon S3 for long-term reliable storage.

Under HIPAA, covered entities must have a contingency plan to protect data in case of an emergency and must create and maintain retrievable exact copies of electronic PHI. To implement a data back-up plan on AWS, Amazon EBS offers persistent storage for Amazon EC2 virtual server instances. These volumes can be exposed as standard block devices, and they offer off-instance storage that persists independently from the life of an instance. To align with HIPAA guidelines, customers can create point-in-time snapshots of Amazon EBS volumes that automatically are stored in Amazon S3 and are replicated across multiple Availability Zones, which are distinct locations engineered to be insulated from failures in other Availability Zones. These snapshots can be accessed at any time and can protect data for long-term durability. Amazon S3 also provides a highly available solution for data storage and automated back-ups. By simply loading a file or image into Amazon S3, multiple redundant copies are automatically created and stored in separate data centers. These files can be accessed at any time, from anywhere (based on permissions), and are stored until intentionally deleted.

Disaster recovery, the process of protecting an organization's data and IT infrastructure in times of disaster, is typically one of the more expensive HIPAA requirements to comply with. This involves maintaining highly available systems, keeping both the data and system replicated off-site, and enabling continuous access to both. AWS inherently offers a variety of disaster recovery mechanisms.

With Amazon EC2, administrators can start server instances very quickly and can use an Elastic IP address (a static IP address for the cloud computing environment) for graceful failover from one machine to another. Amazon EC2 also offers Availability Zones. Administrators can launch Amazon EC2 instances in multiple Availability Zones to create geographically diverse, fault tolerant systems that are highly resilient in the event of network failures, natural disasters, and most other probable sources of downtime. Using Amazon S3, a customer's data is replicated and automatically stored in separate data centers to provide reliable data storage designed to provide 99.99% availability.

For more information on disaster recovery, see the AWS Disaster Recovery whitepaper available at http://aws.amazon.com/disaster-recovery/.

Document Revisions

Date	Description
October 2017	Added sections on Amazon SNS, Amazon Route53, AWS Storage Gateway, AWS Snowmobile, and AWS CloudHSM. Updated section on AWS Key Management Service.
September 2017	Added sections on Amazon Connect, Amazon Kinesis Streams, Amazon RDS (Maria) DB, Amazon RDS SQL Server, AWS Batch, AWS Lambda, AWS Snowball Edge, and the Lambda@Edge feature of Amazon CloudFront.
August 2017	Added sections on Amazon EC2 Systems Manager and Amazon Inspector.
July 2017	Added sections on Amazon WorkSpaces, Amazon WorkDocs, AWS Directory Service, and Amazon ECS.
June 2017	Added sections on Amazon CloudFront, AWS WAF, AWS Shield, and Amazon S3 Transfer Acceleration.
May 2017	Removed requirement for Dedicated Instances or Dedicated Hosts for processing PHI in EC2 and EMR.

Date	Description
March 2017	Updated list of services to point to AWS Services in Scope by Compliance Program page. Added description for Amazon API Gateway.
January 2017	Updated to newest template.
October 2016	First publication