Architecting for HIPAA Security and Compliance on Amazon Web Services

January 2020

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

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided "as is" without warranties, representations, or conditions of any kind, whether express or implied. 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 healthcare providers engaged in certain electronic transactions, health plans, and healthcare 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 healthcare 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

aws

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 using 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 open standard transport encryption mechanisms such as Transport Layer Security (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.

AWS Systems Manager

AWS Systems Manager Console and Resource Groups are not in scope for the HIPAA BAA.

AWS Systems Manager (previously Amazon EC2 Systems Manager) is a unified interface that allows customers to easily centralize operational data, automate tasks across their AWS resources, and shortens the time to detect and resolve operational problems in their infrastructure. Systems Manager provides a complete view of a customer's infrastructure performance and configuration, simplifies resource and application management, and makes it easy to operate and manage their infrastructure at scale.

When outputting data that may contain PHI to other services such as Amazon 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. Additionally, customers should not use Resource Groups or the AWS Systems Manager console, although they may use the EC2 Systems Manager console.

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud (Amazon 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

aws

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 Redshift Spectrum enables customers to run Amazon Redshift SQL
queries against exabytes of data in Amazon S3. Redshift Spectrum is a feature
of Amazon Redshift, and thus is also in scope for the HIPAA BAA.

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 uses 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.

aws

- Amazon SQS supports server-side encryption integrated with the 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 before 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 uses 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 S3 Glacier

Amazon S3 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 S3 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 S3 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.Encryptio n.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.SS L.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.Encryptio
n.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.Or
  acle.Options.AdvSecurity.html.

- Using AWS CloudHSM to store Amazon RDS Oracle TDE keys:
  http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.Or
  acleCloudHSM.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.O
ptions.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.Encryptio
n.html.

aws

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

aws

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 Amazon S3 origin.

Customers should also ensure that the data is encrypted at the origin to ensure it remains encrypted at rest while cached in CloudFront. If using Amazon 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 that the data is encrypted at the origin.

aws

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 backend instances. Sessions containing PHI must encrypt both front-end and backend 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 backend 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 Elastic Container Service (Amazon 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 (for example, 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.

Amazon DynamoDB offers DynamoDB encryption, which allows customers to encrypt databases using keys that customers manage through AWS KMS. On a database instance running with Amazon DynamoDB 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 DynamoDB encryption satisfies their compliance and regulatory requirements. For more information on encryption at rest using Amazon DynamoDB, see https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/EncryptionAtRest.html

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 backend 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

aws

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 open 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 TLS 1.2 to secure PHI in transport.

Tape Gateway

Tape gateway provides a VTL (virtual tape library) interface to third-party backup applications running on-premises. Customers should enable encryption for PHI within the third-party backup application when setting up a tape backup job. Communication between the Tape Gateway VM and AWS is encrypted using 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 use 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 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 IoT 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

AWS 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 SSL/TLS. 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 SSL/TLS. AWS web and mobile applications, and desktop sync clients, transmit files directly to Amazon WorkDocs using SSL/TLS. 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 file names 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 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 (that is, 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 Lambda 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 Amazon 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 in S3, the object name that 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 Amazon 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 open 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 AWS CloudHSM 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.

Amazon ElastiCache for Redis

Amazon ElastiCache for Redis is a Redis-compatible in-memory data structure service that can be used as a data store or cache.

In order to store PHI, customers must ensure that they are running the latest HIPAA-eligible ElastiCache for Redis engine version and current generation node types. Amazon ElastiCache for Redis supports storing PHI for the following node types and Redis engine version:

- Node Types: current generation only (for example, as of the time of publication of this whitepaper, M4, M5, R4, R5, T2, T3)

- ElastiCache for Redis engine version: 3.2.6 and 4.0.10 onwards

For more information about choosing current generation nodes, see https://aws.amazon.com/elasticache/pricing/. For more information about choosing an ElastiCache for Redis engine, see http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/SelectEngine.Uses.html

Customers must also ensure that the cluster and nodes within the cluster are configured to encrypt data at rest, enable transport encryption and enable authentication of Redis commands. In addition, customers must also ensure that their Redis clusters are updated with the latest 'Security' type service updates on or before the 'Recommended Apply by Date' (the date by which it is recommended the update be applied) at all times. For more information, see the sections below.

Encryption at Rest

Amazon ElastiCache for Redis provides data encryption for its cluster to help protect the data at rest. When customers enable encryption at rest for a cluster at the time of creation, Amazon ElastiCache for Redis encrypts data on disk and automated Redis backups. Customer data on disk is encrypted using hardware accelerated Advanced Encryption Standard (AES)-512 symmetric keys. Redis backups are encrypted through Amazon S3-managed encryption keys (SSE-S3). A S3 bucket with server-side encryption enabled will encrypt the data using hardware-accelerated Advanced Encryption Standard (AES)-256 symmetric keys before saving it in the bucket. For more details on Amazon S3-managed encryption keys (SSE-S3), see http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html. On an ElastiCache Redis cluster (single or multi-node) running with encryption, data stored at rest is encrypted consistent with the Guidance in effect at the time of publication of this whitepaper. This includes data on disk and automated backups in S3 bucket. Because the Guidance might be

updated, customers should continue to evaluate and determine whether Amazon ElastiCache for Redis encryption satisfies their compliance and regulatory requirements. For more information about encryption at rest using Amazon ElastiCache for Redis, see http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/at-rest-encryption.html.

Transport Encryption

Amazon ElastiCache for Redis uses TLS to encrypt the data in transit. Connections to ElastiCache for Redis containing PHI must use transport encryption and evaluate the configuration for consistency with the Guidance. For more information, see http://docs.aws.amazon.com/AmazonElastiCache/latest/APIReference/API_CreateReplicationGroup.html. For more information on enabling transport encryption, see http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/in-transit-encryption.html.

Authentication

Amazon ElastiCache for Redis clusters (single/multi node) that contain PHI must provide a Redis AUTH token to enable authentication of Redis commands. Redis AUTH is available when both encryption at-rest and encryption-in transit are enabled. Customers should provide a strong token for Redis AUTH with following constraints:

- Must be only printable ASCII characters

- Must be at least 16 characters and no more than 128 characters in length

- Cannot contain any of the following characters: '/', '"', or "@"

This token must be set from within the Request Parameter at the time of Redis replication group (single/multi node) creation and can be updated later with a new value. AWS encrypts this token using AWS Key Management Service (KMS). For more information on Redis AUTH, see http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/auth.html.

Applying ElastiCache Service Updates

Amazon ElastiCache for Redis clusters (single/multi node) that contain PHI must be updated with the latest 'Security' type service updates on or before the 'Recommended Apply by Date.' ElastiCache offers this as a self-service feature that customers can use to apply the updates anytime on-demand and in real time. Each service update comes with a 'Severity' and 'Recommended Apply by Date' and is available only for the applicable Redis replication groups. The 'SLA Met' field in the service update feature will state whether the update was applied on or before the 'Recommended Apply by Date'. If customers choose to not apply the updates to the applicable Redis replication groups by the 'Recommended Apply by Date,' ElastiCache will not take any action to apply them. Customers can use the service updates history dashboard to review the application of updates to their Redis replication groups over time. For more information on how to use this feature, see https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/Self-Service-Updates.html.

Amazon CloudWatch

Customers can use Amazon CloudWatch Logs to monitor, store, and access their log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, Amazon Route 53, and other sources. They can then retrieve the associated log data from CloudWatch Logs. Log data is encrypted while in transit and while it is at rest. As a result, it is not necessary to re-encrypt PHI emitted by any other service and delivered to CloudWatch Logs.

Amazon Elastic Container Registry

Amazon Elastic Container Registry (Amazon ECR) is integrated with Amazon Elastic Container Service (Amazon ECS) and allows customers to easily store, run, and manage container images for applications running on Amazon ECS. After customers specify the Amazon ECR repository in their Task Definition, Amazon ECS will retrieve the appropriate images for their applications.

No special steps are required to use Amazon ECR with container images that contain PHI. Container images are encrypted while in transit and stored encrypted while at rest using Amazon S3 server-side encryption (SSE-S3).

Amazon Macie

Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Amazon Macie recognizes sensitive data such as PHI or intellectual property, and provides the customer with dashboards and alerts that give visibility into how this data is being accessed or moved. The fully managed service continuously monitors data access activity for anomalies, and generates detailed alerts when it detects risk of unauthorized access or inadvertent data leaks.

Amazon Macie operates only with objects stored in Amazon S3. Customers are not required to enter or store PHI in order to configuration of Amazon Macie. All objects stored within the S3 bucket monitored by Amazon Macie should be encrypted while at rest. However, Amazon Macie cannot read and classify objects that are encrypted using client-side encryption. For the effective monitoring of PHI stored in S3 objects, customers should use server side encryption (SSE-S3) or AWS KMS-managed keys (SSE-KMS).

Amazon QuickSight

Amazon QuickSight is a business analytics service that customers can use to build visualizations, perform ad hoc analysis, and quickly get business insights from their data. Amazon QuickSight discovers AWS data sources, enables organizations to scale to hundreds of thousands of users, and delivers responsive performance by using a robust in-memory engine (SPICE)

Customers can only use the Enterprise edition of Amazon QuickSight to work with data containing PHI as it provides support for encryption of data stored at rest in SPICE. Data encryption is performed using AWS managed keys.

AWS Managed Services

AWS Managed Services provides ongoing management of AWS infrastructures. By implementing best practices to maintain a customer's infrastructure, AWS Managed Services helps to reduce their operational overhead and risk. AWS Managed Services automates common activities such as change requests, monitoring, patch management, security, and backup services, and provides full-lifecycle services to provision, run, and support infrastructures.

Customers can use AWS Managed Services to manage AWS workloads that that operate with data containing PHI. Usage of AWS Managed Services does not alter the AWS Services eligible for the use with PHI. Tooling and automation provided by AWS Managed Services cannot be used for the storage or transmission of PHI.

AWS Fargate

AWS Fargate is a technology that allows customer to run containers without having to manage servers or clusters. With AWS Fargate, customers no longer have to provision, configure, and scale clusters of virtual machines to run containers. This removes the need to choose server types, decide when to scale clusters, or optimize cluster packing. AWS Fargate removes the need for customers to interact with or think about servers or clusters. With Fargate, customers focus on designing and building their applications instead of managing the infrastructure that runs them.

Fargate does not require any additional configuration in order to work with workloads that process PHI. You run your container workloads on Fargate using container orchestration services like Amazon ECS. Fargate only manages the underlying infrastructure and does not operate with or upon data within the workload being orchestrated. In keeping with the requirements for HIPAA, PHI should still be encrypted whenever in transit or at rest when accessed by containers launched with Fargate. Various mechanisms for encrypting at rest are available with each AWS storage option described in this paper.

AWS CloudFormation

AWS CloudFormation enables customers to create and provision AWS infrastructure deployments predictably and repeatedly. It helps customers leverage AWS products such as Amazon EC2, Amazon Elastic Block Store, Amazon SNS, Elastic Load Balancing, and Auto Scaling to build highly reliable, highly scalable, cost-effective applications in the cloud without worrying about creating and configuring the underlying AWS infrastructure. AWS CloudFormation enables customers to use a template file to create and delete a collection of resources together as a single unit (a stack).

AWS CloudFormation does not itself store, transmit, or process PHI. Instead, it is used to build and deploy architectures that use other AWS services that might store, transmit, and/or process PHI. Only HIPAA Eligible Services should

be used with PHI. Please refer to the entries for those services in this Whitepaper for guidance on use of PHI with those services. AWS CloudFormation uses AWS CloudTrail to log all API calls.

AWS X-Ray

AWS X-Ray is a service that collects data about requests that a customer's application serves, and provides tools that they can use to view, filter, and gain insights into that data to identify issues and opportunities for optimization. For any traced request to a customer's application, they can see detailed information not only about the request and response, but also about calls that their application makes to downstream AWS resources, microservices, databases, and HTTP web APIs.

AWS X-Ray should not be used to store or process PHI. Information transmitted to and from AWS X-Ray is encrypted by default. When using AWS X-Ray, do not place any PHI within segment annotations or segment metadata.

AWS CloudTrail

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of AWS accounts. With CloudTrail, customers can log, continuously monitor, and retain account activity related to actions across their AWS infrastructure. CloudTrail provides event history of their AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.

AWS CloudTrail is enabled for use with all AWS accounts and can be used for audit logging, as required by the AWS BAA. Specific Trails should be created using the CloudTrail console or the AWS Command Line Interface. CloudTrail encrypts all traffic while in transit and at rest when an encrypted Trail is created. An encrypted trail should be created when the potential exists to log PHI. By default an encrypted Trail stores entries in Amazon S3 using Server-Side Encryption with Amazon S3 (SSE-S3) managed keys. If an additional management over keys is desired, it can also be configured with AWS KMS-managed keys (SSE-KMS). As CloudTrail is the final destination for AWS log entries, and thus, a critical component of any architecture that handles PHI, CloudTrail log file integrity validation should be enabled and the associated

CloudTrail digest files should be periodically reviewed. Once enabled, a positive assertion that the log files have not been changed or altered can be established.

AWS CodeBuild

AWS CodeBuild is a fully managed build service in the cloud. AWS CodeBuild compiles source code, runs unit tests, and produces artifacts that are ready to deploy.

AWS CodeBuild uses an AWS KMS customer master key (CMK) to encrypt build output artifacts. A CMK should be created and configured before building artifacts that contain PHI, secrets/passwords, master certificates, etc. AWS CodeBuild uses AWS CloudTrail to log all API calls.

AWS CodeCommit

AWS CodeCommit is a secure, highly scalable, managed source control service that hosts private Git repositories. AWS CodeCommit eliminates the need for customers to manage their own source control system or worry about scaling its infrastructure.

AWS CodeCommit encrypts all traffic and stored information while in transit and at rest. By default, when a repository is created within AWS CodeCommit, an AWS managed key is created with AWS KMS and is used only by that repository to encrypt all data stored at rest. AWS CodeCommit uses AWS CloudTrail to log all API calls.

AWS Config

AWS Config provides a detailed view of the resources associated with a customer's AWS account, including how they are configured, how they are related to one another, and how the configurations and their relationships have changed over time.

AWS Config cannot itself be used to store or transmit PHI. Instead, it can be leveraged to monitor and evaluate architectures built with other AWS services, including architectures that handle PHI, to help determine whether they remain compliant with their intended design goal. Architectures that handle PHI should only be built with HIPAA Eligible Services. AWS Config uses AWS CloudTrail to log all results.

aws

AWS OpsWorks Stack

AWS OpsWorks Stacks provides a simple and flexible way to create and manage stacks and applications. Customers can use AWS OpsWorks Stacks to deploy and monitor applications in their stacks.

AWS OpsWorks Stacks encrypts all traffic while in transit. However, encrypted data bags (a Chef data storage mechanism) are not available and any assets that need to be stored securely, such as PHI, secrets/passwords, master certificates, etc., should be stored in an encrypted bucket in Amazon S3. AWS OpsWorks Stack uses AWS CloudTrail to log all API calls.

Amazon Elastic File System (EFS)

Amazon Elastic File System (Amazon EFS) provides simple, scalable, elastic file storage for use with AWS Cloud services and on-premises resources. It is easy to use and offers a simple interface that allows customers to create and configure file systems quickly and easily. Amazon EFS is built to elastically scale on demand without disrupting applications, growing and shrinking automatically as customers add and remove files.

To satisfy the requirement that PHI be encrypted at rest, two paths are available on EFS. EFS supports encryption at rest when a new file system is created. During creation, the option for "Enable encryption of data at rest" should be selected. Selecting this option will ensure that all data placed on the EFS file system will be encrypted using AES-256 encryption and AWS KMS-managed keys. Customers may alternatively choose to encrypt data before it is placed on EFS, but they are then responsible for managing the encryption process and key management.

PHI should not be used as all or part of any file name or folder name.

Encryption of PHI while in transit for Amazon EFS is provided by Transport Layer Security (TLS) between the EFS service and the instance mounting the file system. EFS offers a mount helper to facilitate connecting to a file system using TLS. By default, TLS is not utilized and must be enabled when mounting the file system using the EFS mount helper. Ensure that the mount command contains the "-o tls" option to enable TLS encryption. Alternatively, customers who choose not to use the EFS mount helper can follow the instructions in the EFS documentation to configure their NFS clients to connect through a TLS tunnel.

Amazon Kinesis Video Streams

Amazon Kinesis Video Streams is a fully managed AWS service that customers can use to stream live video from devices to the AWS Cloud, or build applications for real-time video processing or batch-oriented video analytics.

Server-side encryption is a feature in Kinesis Video Streams that automatically encrypts data at rest by using an AWS KMS customer master key (CMK) that is specified by the customer. Data is encrypted before it is written to the Kinesis Video Streams stream storage layer, and it is decrypted after it is retrieved from storage.

The Amazon Kinesis Video Streams SDK can be utilized to transmit streaming video data containing PHI. By default, the SDK uses TLS to encrypt frames and fragments generated by the hardware device on which it is installed. The SDK does not manage or affect data stored at rest.

Amazon Kinesis Video Streams uses AWS CloudTrail to log all API calls.

Amazon Rekognition

Amazon Rekognition makes it easy to add image and video analysis to customer applications. A customer only needs to provide an image or video to the Amazon Rekognition API, and the service can identify the objects, people, text, scenes, and activities, as well as detect any inappropriate content. Amazon Rekognition also provides highly accurate facial analysis and facial recognition.

Amazon Rekognition is eligible to operate with images or video containing PHI. Amazon Rekognition operates as a managed service and does not present any configurable options for the handling of data. Amazon Rekognition only uses, discloses, and maintains PHI as permitted by the terms of the AWS BAA. All data is encrypted at rest and in transit with Amazon Rekognition. Amazon Rekognition uses AWS CloudTrail to log all API calls.

Amazon SageMaker

Amazon SageMaker is a fully managed machine learning service. With Amazon SageMaker, data scientists and developers can quickly and easily build and train machine learning models, and then directly deploy them into a production-ready hosted environment. It provides an integrated Jupyter authoring notebook

aws

instance for easy access to data sources for exploration and analysis. Amazon SageMaker also provides common machine learning algorithms that are optimized to run efficiently against extremely large data in a distributed environment. With native support for bring-your-own-algorithms and frameworks, Amazon SageMaker offers flexible distributed training options that adjust to a customer's specific workflows.

Amazon SageMaker is eligible to operate with data containing PHI. Encryption of data in transit is provided by SSL/TLS and is used when communicating both with the front-end interface of Amazon SageMaker (to the Notebook) and whenever Amazon SageMaker interacts with any other AWS service (for example, pulling data from Amazon S3).

To satisfy the requirement that PHI be encrypted at rest, encryption of data stored with the instance running models with Amazon SageMaker is enabled using AWS Key Management Service (KMS) when setting up the endpoint (DescribeEndpointConfig:KmsKeyID). Encryption of model training results (artifacts) is enabled using AWS KMS and keys should be specified using the KmsKeyID in the OutputDataConfig description. If a KMS Key ID isn't provided, the default Amazon S3 KMS Key for the role's account will be used. Amazon SageMaker uses AWS CloudTrail to log all API calls.

Amazon Simple Workflow Service

Amazon Simple Workflow Service (Amazon SWF) helps developers build, run, and scale background jobs that have parallel or sequential steps. Amazon SWF can be thought of as a fully managed state tracker and task coordinator in the Cloud.

The Amazon Simple Workflow Service is used to orchestrate workflows and is not able to store or transmit data. PHI should not be placed in metadata for Amazon SWF or within any task description. Amazon SWF uses AWS CloudTrail to log all API calls.

AWS Secrets Manager

AWS Secrets Manager is an AWS service that makes it easier for customers to manage "secrets." Secrets can be database credentials, passwords, third-party API keys, and even arbitrary text.

AWS Secrets Manager might be used to store PHI if such information is contained within "secrets". All secrets stored by AWS Secrets Manager are encrypted at rest using the AWS Key Management System (KMS). Users can select the AWS KMS key used when creating a new secret. If no key is selected, the default key for the account will be used. AWS Secrets Manager uses AWS CloudTrail to log all API calls.

AWS Service Catalog

AWS Service Catalog allows IT administrators to create, manage, and distribute portfolios of approved products to end users, who can then access the products they need in a personalized portal.

AWS Service Catalog is used to catalog, share, and deploy self-service solutions on AWS and cannot be used to store, transmit, or process PHI. PHI should not be placed in any metadata for AWS Service Catalog items or within any item description. AWS Service Catalog uses AWS CloudTrail to log all API calls.

AWS Step Functions

AWS Step Functions makes it easy to coordinate the components of distributed applications and microservices using visual workflows.

AWS Step Functions is not able to store, transmit, or process PHI. PHI should not be placed within the metadata for AWS Step Functions or within any task or state machine definition. AWS Step Functions uses AWS CloudTrail to log all API calls.

Amazon Athena

Amazon Athena is an interactive query service that makes it easy to analyze data directly in Amazon Simple Storage Service (Amazon S3) using standard SQL. Athena helps customers analyze unstructured, semistructured, and structured data stored in Amazon S3. Examples include CSV, JSON, or columnar data formats such as Apache Parquet and Apache ORC. Customers can use Athena to run ad hoc queries using ANSI SQL, without the need to aggregate or load the data into Athena.

Amazon Athena can now be used to process data containing PHI. Encryption of data while in transit between Amazon Athena and S3 is provided by default

using SSL/TLS. Encryption of PHI while at rest on S3 should be performed according to the guidance provided in the S3 section. Encryption of query results from and within Amazon Athena, including staged results, should be enabled using server side encryption with Amazon S3 managed keys (SSE-S3), AWS KMS-managed keys (SSE-KMS) or client-side encryption with AWS KMS-managed keys (CSE-KMS). Amazon Athena uses AWS CloudTrail to log all API calls.

Amazon EKS

Amazon Elastic Kubernetes Service (Amazon EKS) is a managed service that makes it easy for customers to run Kubernetes on AWS without needing to stand up or maintain their own Kubernetes control plane. Kubernetes is an open-source system for automating the deployment, scaling, and management of containerized applications.

Using Amazon EKS with workloads that process PHI data requires no additional configuration. Amazon EKS operates as an orchestration service, coordinating the launch of containers (the images for which are stored in S3) on EC2 and does not directly operate with or upon data within the workload being orchestrated. Amazon EKS uses AWS CloudTrail to log all API calls.

AWS IoT Core and AWS IoT Device Management

AWS IoT Core and AWS IoT Device Management provide secure, bidirectional communication between internet-connected devices, such as sensors, actuators, embedded micro-controllers, or smart appliances, and the AWS Cloud.

AWS IoT Core and AWS IoT Device Management can now accommodate devices that transmit data containing PHI. All communication with AWS IoT Core and AWS IoT Device Management is encrypted using TLS. AWS IoT Core and AWS IoT Device Management use AWS CloudTrail to log all API calls.

Amazon FreeRTOS

Amazon FreeRTOS is an operating system for microcontrollers that makes small, low-power edge devices easy to program, deploy, secure, connect, and manage. Amazon FreeRTOS is based on the FreeRTOS kernel, a popular open source operating system for microcontrollers, and extends it with software

libraries that make it easy to securely connect small, low-power devices to AWS Cloud services like AWS IoT Core or to more powerful edge devices running AWS IoT Greengrass.

Data containing PHI can now be encrypted in transit and while at rest when using a qualified device running Amazon FreeRTOS. Amazon FreeRTOS provides two libraries to provide platform security: TLS and PKCS#11. The TLS API should be used to encrypt and authenticate all network traffic that contains PHI. PKCS#11 provides a standard interface for software cryptographic operations and should be used to encrypt any PHI stored on a qualified device running Amazon FreeRTOS.

Amazon GuardDuty

Amazon GuardDuty is a managed threat detection service that continuously monitors for malicious or unauthorized behavior to help customers protect their AWS accounts and workloads. It monitors for activity such as unusual API calls or potentially unauthorized deployments that indicate a possible account compromise. Amazon GuardDuty also detects potentially compromised instances or reconnaissance by attackers.

Amazon GuardDuty continuously monitors and analyzes the following data sources: VPC Flow Logs, AWS CloudTrail event logs, and DNS logs. It uses threat intelligence feeds, such as lists of malicious IPs and domains, and machine learning to identify unexpected and potentially unauthorized and malicious activity within an AWS environment. As such, Amazon GuardDuty should not encounter any PHI as this data is not to be stored in any of the AWS based data sources listed above.

Amazon Neptune

Amazon Neptune is a fast, reliable, fully managed graph database service that makes it easy to build and run applications that work with highly connected datasets. The core of Amazon Neptune is a purpose-built, high-performance graph database engine that is optimized for storing billions of relationships and querying the graph with milliseconds latency. Amazon Neptune supports the popular graph query languages Apache TinkerPop Gremlin and W3C's SPARQL.

Data containing PHI can now be retained in an encrypted instance of Amazon Neptune. An encrypted instance of Amazon Neptune can be specified only at the time of creation by choosing 'Enable Encryption' from the Amazon Neptune console. All logs, backups, and snapshots are encrypted for an Amazon Neptune encrypted instance. Key management for encrypted instances of Amazon Neptune is provided through the AWS KMS. Encryption of data in transit is provided through SSL/TLS. Amazon Neptune uses CloudTrail to log all API calls.

AWS Server Migration Service

AWS Server Migration Service (AWS SMS) automates the migration of on-premises VMware vSphere or Microsoft Hyper-V/SCVMM virtual machines to the AWS Cloud. AWS SMS incrementally replicates server VMs as cloud-hosted Amazon Machine Images (AMIs) ready for deployment on Amazon EC2.

Servers running on-premises and being migrated to the cloud with (AWS SMS) can contain PHI data. AWS SMS encrypts data while in transit and when server VM images are being staged for final placement onto EC2. Refer to the guidance for EC2 and setting up encrypted storage volumes when migrating a server VM containing PHI with AWS SMS. AWS SMS uses CloudTrail to log all API calls.

AWS Database Migration Service

AWS Database Migration Service (AWS DMS) helps customers migrate databases to AWS easily and securely. Customers can migrate their data to and from most widely used commercial and open-source databases, such as Oracle, MySQL, and PostgreSQL. The service supports homogeneous migrations such as Oracle to Oracle, and also heterogeneous migrations between different database platforms, such as Oracle to PostgreSQL or MySQL to Oracle.

Databases running on-premises and being migrated to the cloud with AWS DMS can contain PHI data. AWS DMS encrypts data while in transit and when data is being staged for final migration into the target database on AWS. AWS DMS encrypts the storage used by a replication instance and the endpoint connection information. To encrypt the storage used by a replication instance, AWS DMS uses an AWS KMS key that is unique to the AWS account. Refer to the Guidance for the appropriate target database to ensure that data remains

aws

encrypted once migration is complete. AWS DMS uses CloudTrail to log all API calls.

Amazon MQ

Amazon MQ is a managed message broker service for Apache ActiveMQ that makes it easy to set up and operate message brokers in the cloud. Amazon MQ works with existing applications and services without the need for a customer to manage, operate, or maintain their own messaging system.

To provide the encryption of PHI data while in transit, the following protocols with TLS enabled should be used to access brokers:

- AMQP
- MQTT
- MQTT over WebSocket
- OpenWire
- STOMP
- STOMP over WebSocket

Amazon MQ encrypts messages at rest and in transit using encryption keys that it manages and stores securely. Amazon MQ uses CloudTrail to log all API calls.

AWS Glue

AWS Glue is a fully managed ETL (extract, transform, and load) service that makes it simple and cost-effective for customers to categorize their data, clean it, enrich it, and move it reliably between various data stores.

In order to ensure the encryption of data containing PHI while in transit, AWS Glue should be configured to use JDBC connections to data stores with SSL/TLS. Additionally, to maintain encryption while in transit, the setting for server-side encryption (SSE-S3) should be passed as a parameter to ETL jobs run with AWS Glue. All data stored at rest within the Data Catalog of AWS Glue is encrypted using keys managed by AWS KMS when encryption is enabled upon creation of a Data Catalog object. AWS Glue uses CloudTrail to log all API calls.

Amazon Comprehend

Amazon Comprehend uses natural language processing to extract insights about the content of documents. Amazon Comprehend processes any text file in UTF-8 format. It develops insights by recognizing the entities, key phrases, language, sentiments, and other common elements in a document.

Amazon Comprehend can be used with data containing PHI. Amazon Comprehend does not retain or store any data and all calls to the API are encrypted with SSL/TLS. Amazon Comprehend uses CloudTrail to log all API calls.

Amazon Transcribe

Amazon Transcribe uses advanced machine learning technologies to recognize speech in audio files and transcribe them into text. For example, customers can use Amazon Transcribe to convert US English and Mexican Spanish audio to text and to create applications that incorporate the content of audio files.

Amazon Transcribe can be used with data containing PHI. Amazon Transcribe does not retain or store any data and all calls to the API are encrypted with SSL/TLS. Amazon Transcribe uses CloudTrail to log all API calls.

Amazon Translate

Amazon Translate uses advanced machine learning technologies to provide high-quality translation on demand. Customers can use Amazon Translate to translate unstructured text documents or to build applications that work in multiple languages.

Documents containing PHI can be processed with Amazon Translate. No additional configuration is required when translating documents that contain PHI. Encryption of data while in transit is provided by SSL/TLS and no data remains at rest with Amazon Translate. Amazon Translate uses CloudTrail to log all API calls.

AWS Certificate Manager

AWS Certificate Manager is a service that lets customers easily provision, manage, and deploy public and private SSL/TLS certificates for use with AWS services and their internal connected resources.

aws

AWS Certificate Manager should not be used to store data containing PHI. AWS Certificate Manager uses CloudTrail to log all API calls.

Amazon CloudWatch

Amazon CloudWatch is a monitoring service for AWS Cloud resources and the applications that customers run on AWS. Customers can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, and set alarms. Amazon CloudWatch itself does not produce, store, or transmit PHI. Customers can monitor CloudWatch API calls with AWS CloudTrail. For more information, see https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/logging_cw_api_calls.html.

For more details on configuration requirements, see the Amazon CloudWatch Logs section.

Amazon CloudWatch Events

Amazon CloudWatch Events delivers a near-real-time stream of system events that describe changes in AWS resources. Customers should ensure that PHI does not flow into CloudWatch Events, and any AWS resource emitting a CloudWatch event that is storing, processing, or transmitting PHI is configured in accordance with the Guidance.

Customers can configure Amazon CloudWatch Events to register as an AWS API call in CloudTrail. For more information, see https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/Create-CloudWatch-Events-CloudTrail-Rule.html.

Amazon Kinesis Data Firehose

When customers send data from their data producers to their Kinesis data stream, Amazon Kinesis Data Streams encrypts data using an AWS KMS key before storing it at rest. When the Kinesis Data Firehose delivery stream reads data from the Kinesis stream, Kinesis Data Streams first decrypts the data and then sends it to Kinesis Data Firehose. Kinesis Data Firehose buffers the data in memory based on the buffering hints specified by the customer. It then delivers the data to the destinations without storing the unencrypted data at

rest. For more information about encryption with Kinesis Data Firehose, see
https://docs.aws.amazon.com/firehose/latest/dev/encryption.html.

AWS provides various tools that you can use to monitor Amazon Kinesis Data
Firehose, including Amazon CloudWatch metrics, Amazon CloudWatch Logs,
Kinesis Agent and API logging and history. For more information, see
https://docs.aws.amazon.com/firehose/latest/dev/monitoring.html.

Amazon Kinesis Data Analytics

Amazon Kinesis Data Analytics enables customers to quickly author SQL code
that continuously reads, processes, and stores data in near real time. Using
standard SQL queries on the streaming data, customers can construct
applications that transform and provide insights into their data. Kinesis Data
Analytics supports inputs from Kinesis Data Streams and Kinesis Data Firehose
delivery streams as sources for analytics application. If the stream is encrypted,
Kinesis Data Analytics accesses the data in the encrypted stream seamlessly
with no further configuration needed. Kinesis Data Analytics does not store
unencrypted data read from Kinesis Data Streams.
https://docs.aws.amazon.com/kinesisanalytics/latest/dev/how-it-works-
input.html

Kinesis Data Analytics integrates with both AWS CloudTrail and Amazon
CloudWatch Logs for application monitoring. For more information, see
https://docs.aws.amazon.com/kinesisanalytics/latest/dev/monitoring-automated-
manual.html and
https://docs.aws.amazon.com/kinesisanalytics/latest/dev/cloudwatch-logs.html.

Amazon Elasticsearch Service

Amazon Elasticsearch Service (Amazon ES) enables customers to run a
managed Elasticsearch cluster in a dedicated Amazon Virtual Private Cloud
(Amazon VPC). When using Amazon ES with PHI, customers should use
Elasticsearch 6.0 or later. All PHI should be encrypted at-rest and in-transit
within Amazon Elasticsearch Service. Customers may use AWS KMS key
encryption to encrypt data at rest in their Elasticsearch domains, which is only
available for Elasticsearch 5.1 or later. For more information about how to
encrypt data at-rest, see https://docs.aws.amazon.com/elasticsearch-
service/latest/developerguide/encryption-at-rest.html.

Each Amazon ES domain runs in its own VPC. Customers should enable node-to-node encryption, which is available in Elasticsearch 6.0 or later. If you send data to Amazon ES over HTTPS, node-to-node encryption helps ensure that your data remains encrypted as Elasticsearch distributes (and redistributes) it throughout the cluster. If data arrives unencrypted over HTTP, Amazon ES encrypts the data after it reaches the cluster. Therefore, any PHI that enters an Amazon Elasticsearch Service cluster should be sent over HTTPS. For more information, see https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/ntn.html.

Logs from the Amazon ES configuration API can be captured in AWS CloudTrail. For more information, see https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-managedomains.html#es-managedomains-cloudtrailauditing.

Amazon DocumentDB (with MongoDB compatibility)

Amazon DocumentDB (with MongoDB compatibility) (Amazon DocumentDB) offers encryption at rest during cluster creation via AWS KMS, which allows customers to encrypt databases using AWS or customer-managed keys. On a database instance running with encryption enabled, data stored at rest 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 DocumentDB encryption satisfies their compliance and regulatory requirements. For more information on encryption at rest using Amazon DocumentDB, see http://russherm.aka.corp.amazon.com/0c19998524313a62be89fa71faea655f024503458b4ed59c/APIReference/encryption-at-rest.html.

Connections to Amazon DocumentDB containing PHI must use endpoints that accept encrypted transport (HTTPS). By default, a newly created Amazon DocumentDB cluster only accepts secure connections using Transport Layer Security (TLS). For more information, see http://russherm.aka.corp.amazon.com/0c19998524313a62be89fa71faea655f024503458b4ed59c/APIReference/security.encryption.ssl.html.

Amazon DocumentDB uses AWS CloudTrail to log all API calls. For more information, see http://russherm.aka.corp.amazon.com/0c19998524313a62be89fa71faea655f024503458b4ed59c/APIReference/logging-with-cloudtrail.html.

For certain management features, Amazon DocumentDB uses operational technology that is shared with Amazon RDS. Amazon DocumentDB console, AWS CLI, and API calls are logged as calls made to the Amazon RDS API.

AWS Mobile Hub

AWS Mobile Hub provides a set of tools that enable you to quickly configure AWS services and integrate them into your mobile app. AWS Mobile Hub itself does not store or transmit PHI. Instead, it is used to administer and orchestrate mobile architectures built with other AWS services, including architectures that handle PHI. Architectures that handle PHI should only be built with HIPAA eligible services, and PHI should not be placed in metadata for AWS Mobile Hub. AWS Mobile Hub uses AWS CloudTrail to log all actions. For more information, see https://docs.aws.amazon.com/aws-mobile/latest/developerguide/aws-mobile-cli-cloudtrail-logging.html.

AWS IoT Greengrass

AWS IoT Greengrass lets you run local compute, messaging, data caching, sync, and ML inference capabilities for connected devices in a secure way. AWS IoT Greengrass uses X.509 certificates, managed subscriptions, AWS IoT policies, and IAM policies and roles to ensure that your Greengrass applications are secure. AWS IoT Greengrass uses the AWS IoT transport security model to encrypt communication with the cloud using TLS. In addition, AWS IoT Greengrass data is encrypted when at rest (in the cloud). For more information on Greengrass security, see https://docs.aws.amazon.com/greengrass/latest/developerguide/gg-sec.html.

Customers can log AWS IoT Greengrass API actions using AWS CloudTrail. For more information, see https://docs.aws.amazon.com/greengrass/latest/developerguide/logging-using-cloudtrail.html.

AWS OpsWorks for Chef Automate

AWS OpsWorks for Chef Automate is a fully managed configuration management service that hosts Chef Automate, a set of automation tools from Chef for infrastructure and application management. The service itself does not contain, transmit, or handle any PHI or sensitive information, but customers should ensure that any resources configured by OpsWorks for Chef Automate is configured consistent with the Guidance. API calls are captured with AWS CloudTrail. For more information, see https://docs.aws.amazon.com/opsworks/latest/userguide/monitoring-cloudtrail.html.

AWS OpsWorks for Puppet Enterprise

AWS OpsWorks for Puppet Enterprise is a fully managed configuration management service that hosts Puppet Enterprise, a set of automation tools from Puppet for infrastructure and application management. The service itself does not contain, transmit, or handle any PHI or sensitive information, but customers should ensure that any resource configured by OpsWorks for Puppet Enterprise is configured consistent with the Guidance. API calls are captured with AWS CloudTrail. For more information, see https://docs.aws.amazon.com/opsworks/latest/userguide/monitoring-cloudtrail.html.

AWS Transfer for SFTP

AWS Transfer for SFTP provides Secure File Transfer Protocol (SFTP) access to a customer's S3 resources. Customers are presented with a virtual server, which is accessed using the standard SFTP protocol at a regional service endpoint. From the point of view of the AWS customer and the SFTP client, the SFTP gateway looks like a standard, highly available SFTP server. Although the service itself does not store, process, or transmit PHI, the resources that the customer is accessing on Amazon S3 should be configured in a manner that is consistent with the Guidance. Customers can also use AWS CloudTrail to log API calls made to AWS Transfer for SFTP.

AWS DataSync

AWS DataSync is an online transfer service that simplifies, automates, and accelerates moving data between on-premises storage and AWS. Customers

aws

can use AWS DataSync to connect their data sources to either Amazon S3 or Amazon EFS. Customers should ensure that Amazon S3 and Amazon EFS are configured in a manner consistent with the Guidance. By default, customer data is encrypted in transit using TLS 1.2. For more information about encryption and AWS DataSync, see https://aws.amazon.com/datasync/features/.

Customers can monitor DataSync activity using AWS CloudTrail. For more information on logging with CloudTrail, see https://aws.amazon.com/datasync/features/.

AWS Global Accelerator

AWS Global Accelerator is a global load balancing service that improves the availability and latency of multi-region applications. To ensure that PHI remains encrypted in transit and at rest while using AWS Global Accelerator, architectures being load balanced by Global Accelerator should use an encrypted protocol, such as HTTPS or SSL/TLS. Refer to the guidance for Amazon EC2, Elastic Load Balancing, and other AWS services to better understand the available encryption options for backend resources. AWS Global Accelerator uses AWS CloudTrail to log all API calls.

Amazon Comprehend Medical

For guidance, see the previous Amazon Comprehend section.

AWS RoboMaker

AWS RoboMaker enables customers to execute code in the cloud for application development and provides a robotics simulation service to accelerate application testing. AWS RoboMaker also provides a robotics fleet management service for remote application deployment, update, and management.

Network traffic containing PHI must encrypt data in transit. All management communication with the simulation server is over TLS, and customers should use open standard transport encryption mechanisms for connections to other AWS services. AWS RoboMaker also integrates with CloudTrail to log all API calls to a specific Amazon S3 bucket.

AWS RoboMaker logs do not contain PHI, and the EBS volumes used by the simulation server are encrypted. When transferring data that may contain PHI to

other services, such as Amazon S3, customers must follow the receiving service's guidance for storing PHI. For deployments to robots, customers must ensure that encryption of data in transit and at rest is consistent with their interpretation of the Guidance.

Alexa for Business

Alexa for Business makes it easy to configure, install, and manage fleets of Alexa-enabled devices in the enterprise. Alexa for Business allows the enterprise to control which skills (Alexa apps) are available to its users, and which corporate resources (email, calendar, directories, etc.) designated Alexa skills have access to. Through this access, it extends Alexa's capabilities with new enterprise-specific skills, such as starting meetings and checking if conference rooms are booked.

The Alexa for Business system consists of two components. First is the Alexa for Business management console, an AWS service that configures and monitors the Alexa-enabled hardware and allows configuration of the system. It also provides the hooks so that designated Alexa skills can access corporate resources. The second is the Alexa system, which processes end-user queries and commands, takes action, and provides responses. The Alexa system is not an AWS service.

The Alexa for Business management console does not process or store any PHI. Therefore, Alexa for Business can be used in conjunction with Alexa skills that do not process PHI, such as starting meetings, checking on conference rooms, or using any Alexa skill that also does not process PHI.

If you want to process PHI with Alexa and Alexa for Business, you must use a HIPAA-eligible Alexa skill and sign a BAA with the Alexa organization. You can find out more about building HIPAA-eligible Alexa skills at https://developer.amazon.com/en-US/alexa/alexa-skills-kit/healthcare-skills.

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 are stored automatically 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

aws

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
January 2020	Added sections on Amazon CloudWatch, Amazon CloudWatch Events, Amazon Kinesis Data Firehose, Amazon Kinesis Data Analytics, Amazon Elasticsearch Service, Amazon DocumentDB (with MongoDB compatibility), AWS Mobile Hub, AWS IoT Greengrass, AWS OpsWorks for Chef Automate, AWS OpsWorks for Puppet Enterprise, AWS Transfer for SFTP, AWS DataSync, AWS Global Accelerator, Amazon Comprehend Medical, AWS RoboMaker, and Alexa for Business.
January 2019	Added sections on Amazon Comprehend, Amazon Transcribe, Amazon Translate, and AWS Certificate Manager.
November 2018	Added sections on Amazon Athena, Amazon EKS, AWS IoT Core and AWS IoT Device Management, Amazon FreeRTOS, Amazon GuardDuty, Amazon Neptune, AWS Server Migration Service, AWS Database Migration Service, Amazon MQ, and AWS Glue.
June 2018	Added sections on Amazon Elastic File System (EFS), Amazon Kinesis Video Streams, Amazon Rekognition, Amazon SageMaker, Amazon Simple Workflow, AWS Secrets Manage, AWS Service Catalog, and AWS Step Functions.
April 2018	Added sections on AWS CloudFormation, AWS X-Ray, AWS CloudTrail, AWS CodeBuild, AWS CodeCommit, AWS Config, and AWS OpsWorks Stack.
January 2018	Added section on AWS Fargate.
November 2017	Added sections on Amazon EC2 Container Registry, Amazon Macie, Amazon QuickSight, and AWS Managed Services.

Date	Description
November 2017	Added sections on Amazon ElastiCache for Redis and Amazon CloudWatch.
October 2017	Added sections on Amazon SNS, Amazon Route 53, 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.
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