AWS 白皮书

Amazon Web Services 上的 HIPAA 安全性和合规性架构

Amazon Web Services 上的 HIPAA 安全性和合规性架构: AWS 白皮书

Table of Contents

Amazon Web Services 上的 HIPAA 安全性和合规性架构

发布日期：2022年9月28日 (文档修订)

本白皮书简要概述了客户如何使用 Amazon Web Services (AWS) 来运行受《美国健康保险流通与责任法案》(HIPAA) 监管的敏感工作负载。我们将重点介绍保护受保护的健康信息 (PHI) 的 HIPAA 隐私和安全规则，如何使用 AWS 加密传输中的数据和静态数据，以及如何使用 AWS 功能来运行包含 PHI 的工作负载。

简介

1996年《健康保险流通与责任法》（HIPAA）适用于 “受保实体” 和 “商业伙伴”。2009 年，《经济和临床健康健康健康信息技术法》（HITECH）对 HIPAA 进行了扩展。

HIPAA 和 HITECH 制定了一套旨在保护 PHI 安全和隐私的联邦标准。HIPAA 和 HITECH 对使用和披露受保护的健康信息 (PHI)、保护 PHI 的适当保障措施、个人权利和管理责任提出了要求。有关 HIPAA 和 HITECH 的更多信息，请访问健康信息隐私主页。

受保实体及其业务伙伴可以使用 Amazon Web Services (AWS) 提供的安全、可扩展、低成本的 IT 组件来架构符合 HIPAA 和 HITECH 合规要求的应用程序。AWS 提供了一个 commercial-off-the-shelf基础设施平台，该平台具有行业认可的认证和审计，例如 ISO 27001、FedRAMP 和服务组织控制报告（SOC1、SOC2 和 SOC3）。AWS 服务和数据中心具有多层运营和物理安全，有助于确保客户数据的完整性和安全性。AWS 没有最低费用、不需要基于期限的合同和 pay-as-you-use 定价，是不断增长的医疗行业应用程序的可靠而有效的解决方案。

AWS 使受 HIPAA 约束的受保实体及其商业伙伴能够安全地处理、存储和传输 PHI。此外，自 2013 年 7 月起，AWS 为此类客户提供了标准化的商业伙伴附录 (BAA)。执行 AWS BAA 的客户可以在指定为 HIPAA 账户的账户中使用任何 AWS 服务，但他们只能使用 AWS BAA 中定义的符合 HIPAA 资格的服务来处理、存储和传输 PHI。有关这些服务的完整列表，请参阅 HIPAA 合格服务参考页面。

AWS 实施基于标准的风险管理计划，确保符合 HIPAA 资格的服务专门支持 HIPAA 的管理、技术和物理保护措施。使用这些服务来存储、处理和传输 PHI 可以帮助我们的客户和 AWS 满足适用于基于 AWS 公用事业的运营模式的 HIPAA 要求。

AWS 的 BAA 要求客户根据卫生与公共服务部长 (HHS) 的指导方针，对存储在符合HIPAA资格的服务中存储或传输的 PHI 进行加密：未经授权的个人无法使用、无法读取或无法破译不安全的受保护健康信息的指南（“指南”）。请参考本网站，因为它可能会更新，并且可能会在 HHS 指定的后续网站（或相关）网站上提供。

AWS 提供了一整套功能和服务，使 PHI 的密钥管理和加密变得易于管理和审计，包括 AWS Key Management Service (AWS KMS)。具有 HIPAA 合规要求的客户在如何满足 PHI 的加密要求方面有很大的灵活性。

在确定如何实施加密时，客户可以评估和利用符合 HIPAA 资格的服务原生的加密功能。或者，客户可以通过符合 HHS 指导的其他方式满足加密要求。

在 AWS 中对 PHI 进行加密和保护

HIPAA 安全规则包括对传输中（“传输中”）和存储（“静态”）的 PHI 进行加密的可寻址实现规范。尽管这是 HIPAA 中可解决的实施规范，但 AWS 要求客户根据卫生与公共服务部长 (HHS) 的指导方针：《使未受保护的健康信息无法使用、无法读取或无法被未经授权的个人理解的指南》（“指南”），对存储在符合HIPAA资格的服务中或使用符合HIPAA资格的服务传输的 PHI 进行加密。请访问本网站，因为它可能会更新，并可能在 HHS 指定的后续站点（或相关网站）上提供。

AWS 提供了一整套功能和服务，使 PHI 的密钥管理和加密变得易于管理和审计，包括 AWS Key Management Service (AWS KMS)。具有 HIPAA 合规要求的客户在如何满足 PHI 的加密要求方面有很大的灵活性。

在确定如何实施加密时，客户可以评估和利用符合 HIPAA 条件的服务所固有的加密功能，也可以通过与 HHS 指导一致的其他方式满足加密要求。以下各节提供了有关在每项符合 HIPAA 条件的服务中使用可用加密功能和其他模式对 PHI 进行加密，以及如何使用 AWS KMS 加密用于在 AWS 上加密 PHI 的密钥的高级细节。

主题

- Amazon API Gateway
- Amazon AppFlow
- 亚马逊 AppStream 2.0
- Amazon Athena
- Amazon Aurora
- Amazon Aurora PostgreSQL
- Amazon CloudFront
- Amazon CloudWatch
- 亚马逊 CloudWatch 活动
- Amazon CloudWatch 日志
- Amazon Comprehend
- Amazon Comprehend Medical
- Amazon Connect
- Amazon DocumentDB（与 MongoDB 兼容）
- Amazon DynamoDB

- Amazon Elastic Block Store
- Amazon Elastic Compute Cloud
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- Amazon Elastic File System (Amazon EFS)
- Amazon Elastic Kubernetes Service(Amazon EKS)
- ElastiCache 适用于 Redis 的 Amazon
- 亚马逊 OpenSearch 服务
- Amazon EMR
- Amazon EventBridge
- Amazon Forecast
- Amazon FSx
- Amazon GuardDuty
- Amazon HealthLake
- Amazon Inspector
- 适用于 Apache Flink 的亚马逊托管服务
- Amazon Data Firehose
- Amazon Kinesis Streams
- Amazon Kinesis Video Streams
- Amazon Lex
- Amazon Managed Streaming for Apache Kafka (Amazon MSK)
- Amazon MQ
- Amazon Neptune
- AWS 网络防火墙
- Amazon Pinpoint
- Amazon Polly
- Amazon Quantum Ledger Database (Amazon QLDB)
- Amazon QuickSight
- Amazon RDS for MariaDB
- Amazon RDS for MySQL

- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL
- Amazon RDS for SQL Server
- Amazon Redshift
- Amazon Rekognition
- Amazon Route 53
- Simple Storage Service (Amazon S3) Glacier
- Amazon S3 Transfer Acceleration
- Amazon SageMaker
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Email Service（Amazon SES）
- Amazon Simple Queue Service(Amazon SQS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Simple Workflow Service
- Amazon Textract
- Amazon Transcribe
- Amazon Translate
- Amazon Virtual Private Cloud
- Amazon WorkDocs
- Amazon WorkSpaces
- AWS App Mesh
- AWS 应用程序迁移服务
- AWS Auto Scaling
- AWS Backup
- AWS Batch
- AWS Certificate Manager
- AWS Cloud Map
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail

- AWS CodeBuild
- AWS CodeDeploy
- AWS CodeCommit
- AWS CodePipeline
- AWS Config
- AWS Data Exchange
- AWS Database Migration Service
- AWS DataSync
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS 弹性灾难恢复
- AWS Fargate
- AWS Firewall Manager
- AWS Global Accelerator
- AWS Glue
- AWS Glue DataBrew
- AWS IoT 核心和 AWS IoT Device Management
- AWS IoT Greengrass
- AWS Lambda
- AWS Managed Services
- AWS OpsWorks 适用于厨师自动化
- AWS OpsWorks 适用于木偶企业
- AWS OpsWorks 堆栈
- AWS Organizations
- AWS RoboMaker
- AWS 开发工具包指标
- AWS Secrets Manager
- AWS Security Hub CSPM
- AWS 服务器迁移服务
- AWS Serverless Application Repository

- 服务目录
- AWS Shield
- AWS Snowball Edge
- AWS Snowball Edge 边缘
- AWS Step Functions
- AWS Storage Gateway
- AWS Systems Manager
- AWS Transfer for SFTP
- AWS WAF — Web 应用程序防火墙
- AWS X-Ray
- Elastic Load Balancing
- FreeRTOS
- AWS KMS 用于对 PHI 进行加密
- VM Import/Export

Amazon API Gateway

客户可以使用 Amazon API Gateway 来处理和传输受保护的健康信息 (PHI)。虽然 Amazon API Gateway 会自动使用 HTTPS 终端节点进行动态加密，但客户也可以选择在客户端加密有效负载。API Gateway 通过内存传递所有非缓存数据，不会将其写入磁盘。客户可以使用 AWS 签名版本 4 通过 API Gateway 进行授权。有关更多信息，请参阅下列内容：

- Amazon API Gateway 常见问题：安全和授权
- 在 API Gateway 中控制和管理对 REST API 的访问权限

客户可以与任何连接到 API Gateway 的服务集成，前提是当涉及 PHI 时，服务的配置必须与《指南》和 BAA 一致。有关将 API Gateway 与后端服务集成的信息，请参阅在 API Gate way 中设置 REST API 方法。

客户可以使用 AWS CloudTrail 和 Amazon CloudWatch 启用符合其日志要求的日志记录。确保通过 API Gateway 发送的任何 PHI（例如标头、网址和请求/响应中）只能被配置为与指南一致的符合 HIPAA 资格的服务捕获。有关使用 API Gateway 进行日志记录的更多信息，请参阅如何启用 CloudWatch 日志以对我的 API Gateway REST API 或 WebSocket API 进行故障排除？

Amazon AppFlow

亚马逊 AppFlow 是一项完全托管的集成服务，它使客户能够在诸如Salesforce、Marketo、Slack和之类的SaaS应用程序与AWS oftware-as-a 服务（例如Amazon S3 ServiceNow 和Amazon Redshift）之间安全地传输数据。 AppFlow 可以按客户选择的频率运行数据流 — 按计划、响应业务事件或按需运行。客户还可以配置诸如筛选和验证之类的数据转换功能，以生成作为流程本身一部分的丰富 ready-to-use 数据，而无需执行其他步骤。

Amazon AppFlow 可用于处理和传输包含 PHI 的数据。默认情况下，使用 TLS 1.2 或更高版本对 AppFlow 与配置的源/目的地之间传输的数据进行加密。静态存储在 S3 中的数据使用客户指定的 AWS KMS 密钥（以前称为 CMK）自动加密。对于传输到非 S3 目标的 PHI 数据，客户必须确保所选目的地的静态存储满足其安全需求。 AppFlow 通过与集成 AWS CloudTrail 来记录 API 调用，Amazon 可以发出流程执行事件 EventBridge ，从而实现应用程序监控。

亚马逊 AppStream 2.0

Amazon AppStream 2.0 是一项完全托管的应用程序流媒体服务。客户拥有自己的数据，必须以符合其监管要求的方式配置必要的 Windows 应用程序。客户可以通过主文件夹配置永久存储。使用 Amazon S3 的 SSL 端点对文件和文件夹进行传输中加密。使用 Amazon S3 托管的加密密钥对文件和文件夹进行静态加密。有关更多信息，请参阅为您的 AppStream 2.0 用户启用和管理永久存储如果客户选择使用第三方存储解决方案，则他们有责任确保该解决方案的配置与指南一致。与 Amazon AppStream 2.0 的所有公共 API 通信均使用 TLS 进行加密。有关更多信息，请参阅 Amazon AppStream 2.0 文档。

Amazon AppStream 2.0 与一项服务集成 AWS CloudTrail，该服务可在客户的 AWS 账户中记录由亚马逊 AppStream 2.0 或代表其进行的 API 调用，并将日志文件传输到指定的 Amazon S3 存储桶。CloudTrail 捕获从亚马逊 AppStream 2.0 控制台或亚马逊 2.0 API 发出的 API 调用。 AppStream 客户还可以使用 Amazon CloudWatch 记录资源使用量指标。有关更多信息，请参阅监控 Amazon AppStream 2.0 资源和使用记录 AppStream 2.0 API 调用 AWS CloudTrail。

Amazon Athena

Amazon Athena 是一种交互式查询服务，让您能够轻松使用标准 SQL 直接分析 Amazon Simple Storage Service（Amazon S3）中的数据。Athena 帮助客户分析存储在 Amazon S3 中的非结构化、半结构化和结构化数据。示例包括 CSV、JSON 或列式数据格式，如 Apache Parquet 和 Apache ORC。客户可以使用 Athena 通过 ANSI SQL 运行即席查询，而无需将数据聚合或加载到 Athena 中。

Amazon Athena 现在可用于处理包含 PHI 的数据。默认情况下，使用 SSL/TLS 对在 Amazon Athena 和 S3 之间传输的数据进行加密。在 S3 上处于静止状态时，应按照 S3 部分中提供的指导对 PHI 进行

加密。应使用使用 Amazon S3 托管密钥 (SSE-S3)、托管密钥 (SSE-KMS) 的服务器端加密或使用托管密钥的客户端加密 (CSE-KMS) AWS KMS来启用对来自 Amazon Athena 和内部的查询结果（包括暂存结果）的加密。 AWS KMS亚马逊 Athena AWS CloudTrail 使用记录所有 API 调用。

Amazon Aurora

Amazon Aurora 允许客户使用他们管理的密钥对静态的 Aurora 数据库集群和快照进行加密 AWS KMS。在使用 Amazon Aurora 加密运行的数据库实例上，静态存储在底层存储中的数据会被加密，自动备份、只读副本和快照也是如此。

由于指南可能会更新，因此客户应继续评估和确定 Amazon Aurora 加密是否满足其合规和监管要求。有关使用 Amazon Aurora 进行静态加密的更多信息，请参阅使用加密保护数据。

与运行 Aurora MySQL 的数据库集群的连接必须使用传输加密，使用安全套接字层 (SSL) 或传输层安全 (TLS)。有关实现 SSL/TLS 的更多信息，请参阅在 Aurora MySQL 数据库集群中使用 SSL/TLS。

Amazon Aurora PostgreSQL

Amazon Aurora 允许客户使用他们管理的密钥对静态的 Aurora 数据库集群和快照进行加密 AWS KMS。在使用 Amazon Aurora 加密运行的数据库实例上，静态存储在底层存储中的数据会被加密，自动备份、只读副本和快照也是如此。

由于指南可能会更新，因此客户应继续评估和确定 Amazon Aurora 加密是否满足其合规和监管要求。有关使用 Amazon Aurora 进行静态加密的更多信息，请参阅使用加密保护数据。

与运行 Aurora PostgreSQL 的数据库集群的连接必须使用传输加密，使用安全套接字层 (SSL) 或传输层安全 (TLS)。有关实现 SSL/TLS 的更多信息，请参阅使用 SSL 保护 Aurora PostgreSQL 数据。

Amazon CloudFront

Amazon CloudFront 是一项全球内容分发网络 (CDN) 服务，可加速客户网站、API、视频内容或其他网络资产的交付。它与其他 Amazon Web Services 产品集成，为开发人员和企业提供了一种简便的方式，可以加速向最终用户提供内容，而无需最低使用量承诺。为确保在传输过程中对 PHI 进行加密 CloudFront，客户必须配置 CloudFront 为使用 end-to-end 从源站到查看器的 HTTPS。

这包括与查看者 CloudFront 之间的流量、来自自定义来源的 CloudFront 重新 CloudFront 分配以及从 Amazon S3 源进行分发。 客户还应确保在源站对数据进行加密，以确保数据在 CloudFront缓存时保持静态加密状态。如果使用 Amazon S3 作为来源，则客户可以使用 S3 服务器端加密功能。如果客户从自定义来源进行分发，则必须确保在源站对数据进行加密。

Lambda@Edge

Lambda @Edge 是一项计算服务，允许在 AWS 边缘站点执行 Lambda 函数。Lambda @Edge 可用于自定义通过传送的内容。 CloudFront将 Lambda @Edge 与 PHI 配合使用时，客户应遵循使用指南。 CloudFront所有进出 Lambda @Edge 的连接都应使用 HTTPS 或 SSL/TLS 进行加密。

Amazon CloudWatch

Amazon CloudWatch 是一项监控 AWS 云资源和客户在 AWS 上运行的应用程序的服务。客户可以使用 Amazon CloudWatch 收集和跟踪指标、收集和监控日志文件以及设置警报。亚马逊 CloudWatch 本身并不生产、存储或传输 PHI。客户可以使用监控 CloudWatch API 调用 AWS CloudTrail。有关更多信息，请参阅使用记录 Amazon CloudWatch API 调用 AWS CloudTrail。

有关配置要求的更多详细信息，请参阅 Amazon CloudWatch 日志部分。

亚马逊 CloudWatch 活动

Amazon CloudWatch Ev near-real-time ents 提供了一系列描述了 AWS 资源变化的系统事件。客户应确保 PHI 不会流入 CloudWatch 事件，并且任何发出存储、处理或传输 PHI CloudWatch 的事件的 AWS 资源均按照指南进行配置。

客户可以将 Amazon E CloudWatch vents 配置为注册为 AWS API 调用 CloudTrail。有关更多信息，请参阅使用创建在 AWS API 调用时触发 CloudWatch 的事件规则 AWS CloudTrail。

Amazon CloudWatch 日志

客户可以使用 Amazon Lo CloudWatch gs 监控、存储和访问来自亚马逊弹性计算云 (Amazon EC2) 实例 AWS CloudTrail、亚马逊 Route 53 和其他来源的日志文件。然后，他们可以从 Logs 中检索相关的 CloudWatch 日志数据。日志数据在传输过程中和静止状态时都经过加密。因此，无需重新加密任何其他服务发出并传送到 CloudWatch 日志的 PHI。

Amazon Comprehend

Amazon Comprehend 使用自然语言处理来提取有关文档内容的见解。Amazon Comprehend 可以处理 UTF-8 格式的任何文本文件。它可以通过识别文档中的实体、关键短语、语言、情绪和其他常见元素生成见解。Amazon Comprehend 可用于处理包含 PHI 的数据。Amazon Comprehend 不保留或存

储任何数据，对 API 的所有调用均使用 SSL/TLS 加密。Amazon Comp CloudTrail rehend 用于记录所有 API 调用。

AWS Identity and Access Management

访问 Amazon Comprehend 需要安全访问功能，例如身份验证和授权，这些功能可以通过 (IAM) 进行AWS Identity and Access Management控制，并且可以使用证书来访问 IAM。有关更多信息，请参阅《亚马逊 Comprehend 用户指南》中的 Amazon Comprehend 身份验证和访问控制。

账户管理

默认情况下，IAM 用户无权创建或修改 Amazon Comprehend 资源，也无权使用 Amazon Comprehend API 执行任务。为了允许用户创建或修改资源并执行任务，客户有责任利用 IAM 策略向用户授予用户需要使用的特定资源（例如 Amazon Comprehend 和 API 操作）的权限，然后将策略附加到需要特定权限的用户或群组。

借助 Amazon Comprehend， AWS Identity and Access Management 您可以使用 (IAM) 创建具有附加策略的用户，以启用 Amazon Comprehend 权限。或者，您可以选择创建要附加到角色的自定义策略。然后，您可以为该角色添加管理员，使其能够根据组织定义的基于角色的访问权限和最低权限原则调用 Amazon Comprehend 管理的 API。

身份和访问权限

借助 Amazon Comprehend，您可以要求用户根据其组织对 AWS 身份验证的要求使用多重身份验证进行身份验证。

使用 AWS 管理控制台，IAM 管理员可以创建客户托管策略，该策略拒绝除用户管理自己的证书和 MFA 设备所需的权限之外的所有权限。JSON 策略模板可在 IAM 控制台的 “我的安全凭证” 页面上找到。

或者，您可以利用与 IAM 合作伙伴兼容的第三方 MFA 功能。有关更多信息，请参阅 IAM 合作伙伴。

管理

我们建议您 Amazon Comprehend 选择基于身份的策略，在该策略中，账户管理员可以向 IAM 身份（用户、群组和角色）附加权限策略，从而授予对 Amazon Comprehend 资源执行操作的权限。

Amazon Comprehend 的 API 操作列表可在 API 参考指南中找到。您还应考虑根据用户或角色的最低权限和基于角色的组织要求，向他们授予对预定义的 IAM 策略、客户 IAM 策略和 API 操作的访问权限。有关更多信息，请参阅开发者指南中的使用亚马逊 Comp rehend API。

外部身份验证

Amazon Comprehend 与使用 IAM 角色的联合身份验证兼容。这样，Amazon Comprehend 您的用户就可以通过扮演管理员 AWS 配置的角色进行身份验证。 AWS 使用来自其组织或第三方的凭据进行访问的用户间接扮演角色。

AWS 对 Kerberos 和 Active Directory 的支持提供了对数据库用户进行单点登录和集中身份验证的好处。 AWS 用户可以选择在 Microsoft Active Directory 中 AWS Directory Service 或客户本地 Active Directory 中管理和存储用户凭据。

强制执行数据流

AWS 作为数据控制者或数据处理者的客户和 APN 合作伙伴应对他们在 AWS 云 和 Amazon Comprehend 中输入的任何个人数据负责。您负责使用 IAM 策略控制 Amazon Comprehend 的数据输入和输出的流程。

数据保护和机密管理

责任 AWS 共担模式适用于亚马逊 Comprehend 中的数据保护。如本模型所述 AWS ，负责保护运行所有 AWS 云的全球基础架构。您负责维护对托管在此基础设施上的内容的控制。此内容包括您使用的 AWS 服务的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。

《Amazon Comprehend 开发者指南》中的 “Amazon Comprehend 中的数据保护” 部分提供了在保护数据时应考虑的提示，例如使用 TLS 进行传输以及避免将敏感信息放入标签或自由格式字段中。

的加密 data-at-rest

Amazon Comprehend 与 AWS Key Management Service (AWS KMS) 配合使用，为您的数据提供增强的加密。亚马逊简单存储服务 (Amazon S3) 已经允许您在创建文本分析、主题建模或自定义 Amazon Comprehend 任务时对输入文档进行加密。 AWS KMS 通过与集成，您可以加密存储卷中的数据以启动*和创建* 作业，并使用您自己的密钥对启动* 作业的输出结果进行加密。 AWS KMS

Amazon Comprehend 用户的最佳做法是，根据其组织政策，使用可用的 S3 加密解决方案对用于输入文档的 Amazon S3 存储桶进行加密。

使用自己的 AWS 管理控制台密钥对 Amazon Comprehend 定制模型进行加密。 AWS KMS 对于 AWS CLI，Amazon Comprehend 可以使用 AWS KMS 自己的密钥或提供的客户托管密钥 (CMK) 对自定义模型进行加密。

如果在使用时选择加密 AWS 管理控制台，则可以选择以下一种或两种可选方法：

- 卷加密-确保 Comprehend 使用的 EBS 卷上的数据在训练/推理期间经过加密（数据在训练/推理后刷新，因此此密钥仅在作业进行时才相关）。
- 输出结果加密-用于使用客户提供的密钥对 comprehend 存储在客户存储桶中的输出进行加密。 AWS KMS

有关加密类型（例如批量加密）的更多信息，请参阅 Amazon Comprehend 中的AWS KMS 加密。

个人身份信息

您可以使用 Amazon Comprehend 控制台或 API 来检测英文文本文档中的个人身份信息 (PII)。有关检测和标记 PII 实体以及操作各种 PII 分析任务的更多信息，请参阅 Amazon Comp rehend 开发者指南中的个人身份信息部分。

数据删除

如果您是使用 Amazon S3 并选择 AWS KMS 管理自己的密钥的 Amazon Comprehend 客户，则 AWS KMS 应考虑根据他们的组织要求撤销密钥并定义这样做的程序理由。撤销 Amazon S3 的 AWS KMS 密钥会导致任何数据不可用/不可读。

网络分段和强化

作为一项托管服务，Amazon Comprehend 遵守AWS 安全、身份和合规的最佳实践。

有关推荐的网络安全保护措施，请参阅《亚马逊 Comprehend 开发者指南》中的 Amazon Comprehend 中的基础设施安全。

使用亚马逊虚拟私有云（亚马逊 VPC）保护作业

Amazon Comprehend 使用多种安全措施来确保您的数据在 Amazon Comprehend 使用期间存储在我们的作业容器中的安全。但是，任务容器会通过 Interne AWS t 访问资源，例如用于存储数据和模型工件的 Amazon S3 存储桶。

要控制对您的模型容器和数据的访问，我们建议您创建一个虚拟私有云 VPC，并配置该 VPC 以便无法通过互联网进行访问。有关创建和配置 VPC 的信息，请参阅《Amazon VPC 用户指南》中的 Amazon VPC 入门。使用 VPC 有助于保护您的数据，因为您可以配置 VPC 以使其不连接到互联网。使用 VPC，您还可以通过 VPC 流日志来监控进出作业容器的所有网络流量。有关更多信息，请参阅《Amazon VPC 用户指南》中的 VPC 流日志。

创建作业时，您通过指定子网和安全组来指定 VPC 配置。当您指定子网和安全组时，Amazon Comprehend 会创建与其中一个子网中的安全组关联的弹性网络接口 (ENI)。ENI 可将您的作业容器连接到 VPC 中的资源。有关 ENI 的信息，请参阅《Amazon VPC 用户指南》中的弹性网络接口。

> **Note**
>
> 对于作业，只能使用默认的租赁 VPC 配置子网，其中实例在共享硬件上运行。有关 VPC 租赁属性的更多信息，请参阅《适用于 Linux 实例的 Amazon EC2 用户指南》中的专用实例。

您可以通过创建接口 VPC 终端节点在 VPC 和 Amazon Comprehend 之间建立私有连接。有关更多信息，请参阅 Amazon Comprehend 和接口 VPC 终端节点 ()。AWS PrivateLink

主机和映像强化

根据责任 AWS 共担模型，Amazon Comprehend AWS 环境的主机和映像强化由 AWS 作为一项提供的服务进行管理。

多租户

为了使您的建议更加安全，我们建议您实施以下多租户安全建议：

- 仅使用经过验证的电子邮件地址，根据域匹配授权用户访问租户。仅信任经过您的应用程序验证或者或者外部 IdP 提供了验证证明的电子邮件地址和电话号码。有关设置这些权限的更多详细信息，请参阅属性权限和范围。
- 对标识租户的用户配置文件属性使用不可变或可变属性。管理员必须能够更改这些属性。此外，向应用程序客户端授予对属性的只读访问权。
- 在外部 IdP 与应用程序客户端之间使用 1:1 映射，以防止未经授权的跨租户访问。已通过外部 IdP 身份验证且具有有效 Amazon Cognito 会话 Cookie 的用户，可以访问信任相同 IdP 的其他租户应用程序。
- 在应用程序中实施与租户匹配的授权逻辑时，请限制用户，使他们不能修改用于授权用户访问租户的条件。此外，如果使用外部 IdP 进行联合身份验证，请限制租户身份提供商管理员，使其无法修改用户访问权限。

防止跨服务混淆代理

令人困惑的副手问题是一个多租户安全问题，即无权执行操作的实体可以强迫特权更高的实体执行操作。在中 AWS，跨服务模仿可能会导致混乱的副手问题。一个服务（调用服务）调用另一项服务（被

调用服务)时，可能会发生跨服务模拟。可以操纵调用服务以使用其权限对另一个客户的资源进行操作，否则该服务不应有访问权限。为了防止这种情况，我们 AWS 提供了一些工具，这些工具可以帮助您保护所有服务的数据，这些服务委托人已被授予对您账户中资源的访问权限。有关更多信息，包括解决此安全问题时应考虑的保障措施，请参阅 Amazon Comprehend 开发者指南中的跨服务混乱副手预防。

Amazon Comprehend Medical

有关指导，请参阅上一Amazon Comprehend节。

Amazon Connect

Amazon Connect 是一项基于云的自助式联络中心服务，可实现任何规模的动态、个性化和自然的客户互动。客户不应在 Amazon Connect 中与管理用户、安全资料和联系流程相关的任何字段中包含任何 PHI。

Amazon Connect 客户档案是 Amazon Connect 的一项功能，它为联络中心代理提供了更统一的客户资料视图，其中包含最新信息，从而提供更加个性化的客户服务。Customer Profiles 旨在自动将来自多个应用程序的客户信息整合到一个统一的客户档案中，在支持电话或互动开始后立即将档案直接提供给客服。客户应避免使用 PHI 数据命名域或对象密钥。域和对象的内容经过加密和保护，但密钥标识符不是。

Amazon DocumentDB（与 MongoDB 兼容）

Amazon DocumentDB（兼容 MongoDB）（Amazon DocumentDB）通过集群创建期间提供静态加密，允许客户使用 AWS 或客户管理 AWS KMS的密钥对数据库进行加密。在启用加密的情况下运行的数据库实例上，静态存储的数据将按照本白皮书发布时有效的指南进行加密，自动备份、只读副本和快照也是如此。由于指南可能会更新，因此客户应继续评估和确定 Amazon DocumentDB 加密是否满足其合规和监管要求。有关使用 Amazon DocumentDB 进行静态加密的更多信息，请参阅加密亚马逊文档数据库的静态数据。

与包含 PHI 的亚马逊 DocumentDB 的连接必须使用接受加密传输 (HTTPS) 的终端节点。默认情况下，新创建的 Amazon DocumentDB 集群仅接受使用传输层安全 (TLS) 的安全连接。有关更多信息，请参阅加密传输中的数据。亚马逊 DocumentDB AWS CloudTrail 用于记录所有 API 调用。有关更多信息，请参阅 Amazon DocumentDB 中的日志和监控。

对于某些管理功能，Amazon DocumentDB 使用与 Amazon RDS 共享的操作技术。亚马逊 DocumentDB 控制台、AWS CLI 和 API 调用记录为对亚马逊 RDS API 的调用。

Amazon DynamoDB

与包含 PHI 的亚马逊 DynamoDB 的连接必须使用接受加密传输 (HTTPS) 的终端节点。有关区域终端节点的列表，请参阅 AWS 服务终端节点。

亚马逊 DynamoDB 提供 DynamoDB 加密，允许客户使用客户管理的密钥对数据库进行加密。 AWS KMS在使用 Amazon DynamoDB 加密运行的数据库实例上，静态存储在底层存储中的数据将按照本白皮书发布时有效的指南进行加密，自动备份、只读副本和快照也是如此。

由于指南可能会更新，因此客户应继续评估和确定 Amazon DynamoDB 加密是否满足其合规和监管要求。有关使用 Amazon DynamoDB 进行静态加密的更多信息，请参阅 DynamoDB 静态加密。

Amazon Elastic Block Store

Amazon EBS 静态加密与本白皮书发布时有效的指南一致。由于指南可能会更新，因此客户应继续评估和确定 Amazon EBS 加密是否满足其合规和监管要求。使用 Amazon EBS 加密，将为每个 EBS 卷生成一个唯一的卷加密密钥。客户可以灵活地选择使用 AWS Key Management Service 哪个 KMS 密钥来加密每个卷密钥。有关更多信息，请参阅 Amazon EBS 加密。

Amazon Elastic Compute Cloud

Amazon EC2 是一项可扩展、用户可配置的计算服务，支持多种加密静态数据的方法。例如，当在 Amazon EC2 实例中托管的应用程序或数据库平台中处理时，客户可能会选择对 PHI 执行应用程序级或字段级加密。方法包括使用应用程序框架（例如Java或.NET）中的标准库对数据进行加密；利用Microsoft SQL或Oracle中的透明数据加密功能；或者将其他第三方和基于软件即服务 (SaaS) 的解决方案集成到其应用程序中。

客户可以选择将其在 Amazon EC2 中运行的应用程序与 AWS KMS 软件开发工具包集成，从而简化密钥管理和存储过程。客户还可以使用AWS Marketplace 合作伙伴提供的第三方软件或本机文件系统加密工具（例如 dm-crypt、LUKS 等），使用文件级或全盘加密 (FDE) 对静态数据进行加密。

包含 PHI 的网络流量必须对传输中的数据进行加密。对于外部来源（例如互联网或传统 IT 环境）与 Amazon EC2 之间的流量，客户应使用开放标准的传输加密机制，例如传输层安全 (TLS) 或 IPsec 虚拟专用网络 (VPN)，这与《指南》一致。在 Amazon Virtual Private Cloud (VPC) 内部，对于在 Amazon EC2 实例之间传输的数据，还必须对包含 PHI 的网络流量进行加密；大多数应用程序都支持 TLS 或其他提供传输中加密的协议，可以将其配置为与指南保持一致。对于不支持加密的应用程序和协议，可以在实例之间使用 IPsec 或类似的实现通过加密隧道发送传输 PHI 的会话。

Amazon Elastic Container Registry

Amazon Elastic Container Registry (Amazon ECR) 与亚马逊弹性容器服务 (Amazon ECS) 集成，允许客户轻松存储、运行和管理在亚马逊 ECS 上运行的应用程序的容器映像。客户在任务定义中指定 Amazon ECR 存储库后，Amazon ECS 将为其应用程序检索相应的映像。

使用包含 PHI 的容器映像的 Amazon ECR 无需特殊步骤。容器映像在传输过程中进行加密，在静止状态下使用 Amazon S3 服务器端加密 (SSE-S3) 进行加密存储。

Amazon Elastic Container Service

Amazon Elastic Container Service (Amazon ECS) 是一项高度可扩展、高性能的容器管理服务，它支持 Docker 容器，并允许客户在由 Amazon EC2 实例组成的托管集群上轻松运行应用程序。Amazon ECS 使客户无需安装、操作和扩展自己的集群管理基础设施。

通过简单的 API 调用，客户可以启动和停止支持 Docker 的应用程序，查询其集群的完整状态，并访问许多熟悉的功能，例如安全组、Elastic Load Balancing、EBS 卷和 IAM 角色。客户可以使用 Amazon ECS 根据其资源需求和可用性要求在其集群中安排容器的放置。

将 ECS 与处理 PHI 的工作负载一起使用，无需额外配置。ECS 充当协调服务，用于协调 EC2 上容器（映像存储在 S3 中）的启动，它不对正在编排的工作负载中的数据进行操作，也不会对正在编排的工作负载中的数据进行操作。根据 HIPAA 法规和 AWS 商业伙伴附录，使用 ECS 启动的容器访问时，PHI 应在传输和静态时进行加密。每个 AWS 存储选项（例如 S3、EBS 和 KMS）都有多种静态加密机制。确保对容器之间发送的 PHI 进行完全加密还可能导致客户部署覆盖网络（例如 VNS3、Weave Net 或类似网络），以提供冗余的加密层。但是，还应启用完整的日志记录（例如，通过 CloudTrail），并且所有容器实例日志都应定向到 CloudWatch。

使用 Firelens 和 f AWS or Fluent Bit 处理处理 PHI 的工作负载无需额外配置，除非日志包含 PHI。如果日志包含 PHI，则除非启用了磁盘加密，否则不应将其发送到日志文件中。取而代之的是，将您的应用程序配置为将日志发送到标准输出/错误，这些日志将由自动收集。 FireLens同样，除非还启用了磁盘加密，否则不要为 Fluent Bit 启用文件缓冲。最后，日志目标必须支持 encryption-in-transit；AWS for Fluent Bit 中的所有 AWS 服务输出插件都将始终使用 TLS 加密来导出日志。

Amazon Elastic File System (Amazon EFS)

Amazon Elastic File System (Amazon EFS) 提供简单、可扩展的弹性文件存储，用于 AWS 云服务和本地资源。它易于使用，界面简单，允许客户快速轻松地创建和配置文件系统。Amazon EFS 旨在在不中断应用程序的情况下按需弹性扩展，并且会随着客户添加和删除文件而自动增长和缩小。

为了满足 PHI 在静态时加密的要求，EFS 上有两条路径可用。创建新文件系统时，EFS 支持静态加密。在创建过程中，应选择 “启用静态数据加密” 选项。选择此选项可确保使用 AES-256 加密和 AWS KMS托管密钥对放置在 EFS 文件系统上的所有数据进行加密。客户也可以选择在将数据放入 EFS 之前对其进行加密，但随后他们将负责管理加密过程和密钥管理。

不应将 PHI 用作任何文件名或文件夹名称的全部或一部分。Amazon EFS 传输过程中的 PHI 加密由 EFS 服务和装载文件系统的实例之间的传输层安全 (TLS) 提供。EFS 提供了挂载帮助程序，便于使用 TLS 连接到文件系统。默认情况下，不使用 TLS，使用 EFS 挂载帮助程序挂载文件系统时必须启用 TLS。确保挂载命令包含 “-o tls” 选项以启用 TLS 加密。或者，选择不使用 EFS 挂载帮助程序的客户可以按照 EFS 文档中的说明将其 NFS 客户端配置为通过 TLS 隧道进行连接。

Amazon Elastic Kubernetes Service(Amazon EKS)

Amazon Elastic Kubernetes Service（Amazon EKS）是一项托管服务，可让客户轻松地在 AWS 上运行 Kubernetes，而无需站起来或维护自己的 Kubernetes 控制平面。Kubernetes 是一个用于实现容器化应用程序的部署、扩缩和管理自动化的开源系统。有关其他安全与合规性信息，请参阅 A mazon EKS 上的 HIPAA 安全与合规架构白皮书。

ElastiCache 适用于 Redis 的 Amazon

Amazon ElastiCache for Redis 是一项与 Redis 兼容的内存数据结构服务，可用作数据存储或缓存。为了存储 PHI，客户必须确保他们运行的是符合 HIPAA ElastiCache 要求的最新 Redis 引擎版本和当前一代节点类型。Amazon ElastiCache for Redis 支持存储以下节点类型和 Redis 引擎版本的 PHI：

- 节点类型：仅限当前一代（例如，截至本白皮书发布时，M4、M5、R4、R5、T2、T3）
- ElastiCache 适用于 Redis 引擎版本：3.2.6 和 4.0.10 及更高版本

有关选择当前一代节点的更多信息，请参阅 Amazon ElastiCache 定价。有关选择适用于 Redis ElastiCache 的引擎的更多信息，请参阅 R edis ElastiCache 的亚马逊是什么？

客户还必须确保将集群和集群中的节点配置为加密静态数据、启用传输加密和启用 Redis 命令的身份验证。此外，客户还必须确保在 “建议应用截止日期”（建议应用更新的截止日期）当天或之前，使用最新的 “安全” 类型服务更新来更新他们的 Redis 集群。有关更多信息，请参阅以下部分。

主题

- 静态加密
- 传输加密

- 身份验证
- 应用 ElastiCache 服务更新

静态加密

Amazon for Redis ElastiCache 为其集群提供数据加密，以帮助保护静态数据。当客户在集群创建时启用静态加密时，Amazon for Redis 会加密磁盘上的数据并自动 ElastiCache 备份 Redis。磁盘上的客户数据使用硬件加速的高级加密标准 (AES) -512 对称密钥进行加密。Redis 备份通过亚马逊 S3 托管的加密密钥 (SSE-S3) 进行加密。启用服务器端加密的 S3 存储桶将使用硬件加速的高级加密标准 (AES) -256 对称密钥对数据进行加密，然后再将其保存在存储桶中。

有关亚马逊 S3 托管的加密密钥 (SSE-S3) 的更多详细信息，请参阅使用带有亚马逊 S3 托管加密密钥的服务器端加密来保护数据 (SSE-S3)。在运行加密 ElastiCache 的 Redis 集群（单节点或多节点）上，静态存储的数据将按照本白皮书发布时有效的指南进行加密。这包括磁盘上的数据和 S3 存储桶中的自动备份。由于指南可能会更新，因此客户应继续评估和确定 Amazon ElastiCache for Redis 加密是否满足其合规和监管要求。有关使用 Amazon for Redis 进行静态加密 ElastiCache 的更多信息，请参阅 Redis ElastiCache 的亚马逊是什么？

传输加密

Amazon ElastiCache for Redis 使用 TLS 对传输中的数据进行加密。与包含 PHI ElastiCache 的 Redis 的连接必须使用传输加密，并评估配置是否与指南一致。有关更多信息，请参阅CreateReplicationGroup。有关启用传输加密的更多信息，ElastiCache 请参阅 Redis 传输中加密 (TLS)。

身份验证

包含 PHI ElastiCache 的 Amazon for Redis 集群（单/多节点）必须提供 Redis 身份验证令牌才能启用 Redis 命令的身份验证。当同时启用静态加密和传输中加密时，Redis AUTH 才可用。客户应为 Redis AUTH 提供强有力的代币，但有以下限制：

- 只能是可打印的 ASCII 字符
- 必须至少为 16 个字符且长度不超过 128 个字符
- 不能包含以下任何字符：'/'、"" 或 “@”

此令牌必须在创建 Redis 复制组（单/多节点）时从请求参数中进行设置，并且可以在以后使用新值进行更新。AWS 使用 AWS Key Management Service (AWS KMS) 加密此令牌。有关 Redis 身份验证的更多信息，ElastiCache 请参阅 Redis 传输中加密 (TL S)。

应用 ElastiCache 服务更新

包含 PHI 的 Amazon ElastiCache for Redis 集群（单/多节点）必须在 “建议申请截止日期” 当天或之前使用最新的 “安全” 类型服务更新进行更新。 ElastiCache 将其作为自助服务功能提供，客户可以使用该功能随时按需实时应用更新。每个服务更新都带有 “严重性” 和 “建议按日期申请”，并且仅适用于适用的 Redis 复制组。

服务更新功能中的 “SLA Met” 字段将说明更新是在 “推荐申请截止日期” 还是之前应用。如果客户选择在 “建议应用截止日期” 之前不将更新应用于适用的 Redis 复制组，则 ElastiCache 不会采取任何措施来应用这些更新。客户可以使用服务更新历史记录仪表板来查看一段时间内更新对其 Redis 复制组的应用情况。有关如何使用此功能的更多信息，请参阅 Amazon 中的自助服务更新 ElastiCache。

亚马逊 OpenSearch 服务

亚马逊 OpenSearch 服务使客户能够在专用的亚马逊虚拟私有云（亚马逊 VPC）中运行托管 OpenSearch 或传统的 Elasticsearch OSS 集群。在 PHI 中使用 OpenSearch 服务时，客户应使用 OpenSearch 或 Elasticsearch 6.0 或更高版本。买家应确保在 Ama OpenSearch zon 服务中对静态和传输中的 PHI 进行加密。客户可以使用 AWS KMS 密钥加密来加密其 OpenSearch 服务域中的静态数据，这仅适用于 Elasticsearch 5.1 或更高版本。 OpenSearch 有关如何加密静态数据的更多信息，请参阅 Amazon S OpenSearch ervice 的静态数据加密。

每个 OpenSearch 服务域都在自己的 VPC 中运行。客户应启用 node-to-node 加密，该功能适用于所有 OpenSearch 版本以及 Elasticsearch 6.0 或更高版本。如果客户通过 HTTPS 向 OpenSearch 服务发送数据，则 node-to-node 加密有助于确保其数据在整个集群中 OpenSearch 分发（和重新分发）时保持加密状态。如果数据通过 HTTP 未加密到达，则 OpenSearch 服务会在数据到达集群后对其进行加密。因此，任何进入亚马逊 OpenSearch 服务集群的 PHI 都应通过 HTTPS 发送。有关更多信息，请参阅 Amazon OpenSearch 服务的 N ode-to-node 加密。

可以在中捕获来自 OpenSearch 服务配置 API 的日志 AWS CloudTrail。有关更多信息，请参阅使用监控亚马逊 OpenSearch 服务 API 调用 AWS CloudTrail。

Amazon EMR

Amazon EMR 在客户的账户中部署和管理一组 Amazon EC2 实例。有关使用 Amazon EMR 进行加密的信息，请参阅加密选项。

Amazon EventBridge

Amazon EventBridge （前身为 Amazon CloudWatch Events）是一种无服务器事件总线，可让您创建可扩展的事件驱动应用程序。 EventBridge 提供来自事件源（例如 Zendesk、Datadog 或 Pagerduty）的实时数据流，并将这些数据路由到诸如此类的目标。 AWS Lambda

默认情况下，使用 AW EventBridge S 拥有的 CMK 下的 256 位高级加密标准 (AES-256) 对数据进行加密，这有助于保护客户数据免遭未经授权的访问。客户应确保任何触发存储、处理或传输 PHI 的事件的 AWS 资源都按照最佳实践进行配置。

Amazon EventBridge 已与 AWS CloudTrail Amazon 集成，客户可以在 CloudTrail 控制台的 “事件历史记录” 中查看最新事件。有关更多信息，请参阅中的EventBridge 信息 CloudTrail。

Amazon Forecast

Amazon Forecast 是一项完全托管的服务，它使用机器学习来提供高度准确的预测。基于与 Amazon.com 相同的机器学习预测技术。客户与 Amazon Forecast 的每一次互动都受到加密保护。Amazon Forecast 处理的任何内容均通过亚马逊密钥管理服务使用客户密钥进行加密，并在客户使用该服务的 AWS 地区进行静态加密。

Amazon Forec AWS CloudTrail ast 与一项服务集成，该服务提供用户、角色或 AWS 服务在 Amazon Forecast 中采取的操作的记录。 CloudTrail 将 Amazon Forecast 的所有 API 调用作为事件捕获。捕获的调用包括来自 Amazon Forecast 控制台的调用和对 Amazon Forecast API 操作的代码调用。如果客户创建了跟踪，则客户可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括 Amazon Forecast 的事件。有关更多信息，请参阅使用记录 Forecast API 调用 AWS CloudTrail。

默认情况下，传送 CloudTrail 到其存储桶的日志文件由亚马逊服务器端加密，使用 Amazon S3 托管的加密密钥 (SSE-S3) 进行加密。为了提供可直接管理的安全层，客户可以改为使用带有 AWS KMS托管密钥 (SSE-KMS) 的服务器端加密来处理日志文件。 CloudTrail 启用服务器端加密将使用 SSE-KMS 加密日志文件而不加密摘要文件。摘要文件使用 Simple Storage Service（Amazon S3）托管加密密钥（SSE-S3）加密。

AWS Forecast 从 S3 存储桶导入和导出数据。从 Amazon S3 导入和导出数据时，客户应确保以与指南一致的方式配置 S3 存储桶。有关更多信息，请参阅 入门。

Amazon FSx

Amazon FSx 是一项完全托管的服务，提供功能丰富且高性能的文件系统。适用于 Windows File Server 的 Amazon FSx 提供高度可靠和可扩展的文件存储，可通过服务器消息块 (SMB) 协议进行访

问。Amazon FSx for Lustre 为计算工作负载提供高性能存储，并由世界上最受欢迎的高性能文件系统 Lustre 提供支持。

Amazon FSx 支持两种形式的文件系统加密：传输中的数据加密和静态加密。适用于 Windows File Server 的 Amazon FsX 还支持使用记录所有 API 调用 AWS CloudTrail。

在支持 SMB 协议 3.0 或更高版本的计算实例上，适用于 Windows File Server 的 Amazon FSx 支持对传输中的数据进行加密；在支持传输中加密的亚马逊 EC2 实例上，亚马逊 FSx for Lustre 支持对传输中的数据进行加密。或者，客户可以在将数据存储到 Amazon FSx 之前对其进行加密，但随后需要负责加密过程和密钥管理。

使用 AES-256 加密算法和托管密钥创建 Amazon FSx 文件系统时，会自动启用静 AWS KMS态数据加密。数据和元数据在写入文件系统之前会自动加密，并在呈现给应用程序之前自动解密。不应在任何文件或文件夹名称中使用 PHI。

Amazon GuardDuty

Amazon GuardDuty 是一项托管威胁检测服务，可持续监控恶意或未经授权的行为，以帮助客户保护其 AWS 账户和工作负载。它会监控各种活动，例如异常 API 调用或可能未经授权的部署，这些活动表明账户可能遭到入侵。Amazon GuardDuty 还会检测可能遭到入侵的实例或攻击者的侦测。

Amazon GuardDuty 持续监控和分析以下数据源：VPC 流日志、 AWS CloudTrail 事件日志和 DNS 日志。它使用威胁情报源（例如恶意 IP 和域名列表）以及机器学习来识别 AWS 环境中意外且可能未经授权的恶意活动。因此，Amazon GuardDuty 不应遇到任何 PHI，因为这些数据不会存储在上面列出的任何基于 AWS 的数据源中。

Amazon HealthLake

Amazon HealthLake 使医疗保健和生命科学行业的客户能够存储、转换、查询和分析 PB 级的健康数据。买家可以使用 Amazon HealthLake 传输、处理和存储 PHI。默认情况下，Amazon 会 HealthLake 加密客户数据存储中的静态数据。所有服务数据和元数据均使用服务拥有的 KMS 密钥进行加密。根据 Fast Healthcare 互操作性资源 (FHIR) 规范，如果客户删除 FHIR 资源，则只能将其隐藏起来，无法检索，并将由服务保留以进行版本控制。当客户使用 StartFHir ImportJob API 时，亚马逊 HealthLake 将强制要求将数据导出到加密的 Amazon S3 存储桶。

Amazon HealthLake 对传输中的数据和静态数据进行加密。要对传输中的数据进行加密，您可以使用 AWS 发布的 API 调用 HealthLake 通过网络进行访问。客户端必须支持传输层安全性 (TLS) 1.0 或更高版本。我们要求使用 TLS 1.2，建议使用 TLS 1.3。客户端还必须支持具有完全向前保密

（PFS）的密码套件，例如 Ephemeral Diffie-Hellman（DHE）或 Elliptic Curve Ephemeral Diffie-Hellman（ECDHE）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。此外，必须使用访问密钥 ID 和与 IAM 主体关联的秘密访问密钥来对请求进行签名。或者，客户可以使用 AWS Security Token Service (AWS STS) 生成临时安全证书来签署请求。为了加密静态数据，默认情况下，Amazon HealthLake 使用客户拥有的 AWS KMS 密钥或服务拥有的 AWS KMS 密钥对客户数据存储中的数据进行加密。所有服务数据和元数据均使用服务拥有的 AWS KMS 密钥进行静态加密。

亚马逊 HealthLake 与集成 AWS CloudTrail。 CloudTrail 将对 Amazon 的所有 API 调用 HealthLake 作为事件捕获，包括与 AWS 管理控制台命令行接口 (CLI) 交互而进行的调用，以及使用软件开发套件 (SDK) 以编程方式进行的调用。

Amazon Inspector

Amazon Inspector 是一项自动安全评估服务，面向寻求提高部署在 AWS 上的应用程序的安全性和合规性的客户。Amazon Inspector 会自动评估应用程序的漏洞以及偏离最佳实践的情况。执行评估后，Amazon Inspector 会生成一份按严重程度排列优先顺序的安全调查结果的详细列表。客户可以在包含 PHI 的 EC2 实例上运行 Amazon Inspector。Amazon Inspector 对通过网络传输的所有数据以及静态存储的所有遥测数据进行加密。

适用于 Apache Flink 的亚马逊托管服务

Amazon Apache Flink 托管服务使客户能够快速编写 SQL 代码，以近乎实时的方式持续读取、处理和存储数据。使用对流数据的标准 SQL 查询，客户可以构建能够转换数据并提供对数据的见解的应用程序。适用于 Apache Flink 的托管服务支持来自 Kinesis Data Streams 和 Firehose 交付流的输入作为分析应用程序的来源。如果数据流已加密，则适用于 Apache Flink 的托管服务无需进一步配置即可无缝访问加密流中的数据。适用于 Apache Flink 的托管服务不存储从 Kinesis Data Streams 读取的未加密数据。有关更多信息，请参阅配置应用程序输入。

适用于 Apache Flink 的托管服务与两者和 AWS CloudTrail Amazon Logs 集成 CloudWatch ，用于应用程序监控。有关更多信息，请参阅监控工具和使用 Amazon CloudWatch 日志。

Amazon Data Firehose

当客户将数据从其数据生成者发送到他们的 Kinesis 数据流时，Amazon Kinesis Data Streams 会使用 AWS KMS 密钥对数据进行加密，然后再将其存储在静态状态。当 Firehose 传输流从 Kinesis 流中读取数据时，Kinesis Data Streams 会首先解密数据，然后将其发送到 Firehose。Firehose 根据客户指定的缓冲提示将数据缓冲到内存中。

然后，它将数据传送到目的地，而不存储未加密的静态数据。有关使用 Firehose 进行加密的更多信息，请参阅亚马逊数据 Firehose 中的数据保护。

AWS 提供各种工具供客户用来监控 Amazon Data Firehose，包括亚马逊 CloudWatch 指标、亚马逊 CloudWatch 日志、Kinesis 代理以及 API 日志和历史记录。有关更多信息，请参阅监控亚马逊数据 Firehose。

Amazon Kinesis Streams

Amazon Kinesis Streams 使客户能够构建自定义应用程序，这些应用程序可以根据特殊需求处理或分析流数据。服务器端加密功能允许客户对静态数据进行加密。启用服务器端加密后，Kinesis Streams 将使用密钥 AWS KMS 对数据进行加密，然后再将其存储在磁盘上。有关更多信息，请参阅 Amazon Kinesis Data Streams 数据保护。与包含 PHI 的 Amazon S3 的连接必须使用接受加密传输（即 HTTPS）的终端节点。有关区域终端节点的列表，请参阅 AWS 服务终端节点。

Amazon Kinesis Video Streams

Amazon Kinesis Video Streams 是一项完全托管的 AWS 服务，客户可以使用它来将直播视频从设备流式传输到 AWS 云，或者构建用于实时视频处理或批处理视频分析的应用程序。服务器端加密是 Kinesis Video Streams 中的 AWS KMS 一项功能，它使用客户指定的密钥（以前称为 CMK）自动加密静态数据。数据在写入 Kinesis Video Streams 流存储层之前会对其进行加密，从存储中检索数据后会被解密。

亚马逊 Kinesis Video Streams SDK 可用于传输包含 PHI 的流媒体视频数据。默认情况下，SDK 使用 TLS 对安装它的硬件设备生成的帧和片段进行加密。SDK 不管理也不影响静态存储的数据。亚马逊 Kinesis Video Streams AWS CloudTrail 使用记录所有 API 调用。

Amazon Lex

Amazon Lex 是一项 AWS 服务，用于使用语音和文本来为应用程序构建对话界面。借助 Amazon Lex，任何开发者都可以使用支持 Amazon Alexa 的对话引擎，使客户能够在新的和现有的应用程序中构建复杂的自然语言聊天机器人。Amazon Lex 提供自然语言理解 (NLU) 和自动语音识别 (ASR) 的深度功能和灵活性，因此客户可以通过逼真的对话互动来打造极具吸引力的用户体验，并创建新的产品类别。

Lex 使用 HTTPS 协议与客户以及其他 AWS 服务进行通信。对 Lex 的访问由 API 驱动，可以强制执行适当的 IAM 最低权限。有关更多信息，请参阅 Amazon Lex 中的数据保护。

监控对于维护客户的 Amazon Lex 聊天机器人的可靠性、可用性和性能非常重要。要追踪 Amazon Lex 机器人的运行状况，请使用亚马逊 CloudWatch。借助 CloudWatch，客户可以获取其账户的各个 Amazon Lex 运营或全球 Amazon Lex 运营的指标。客户还可以设置 CloudWatch 警报，以便在一个或多个指标超过客户定义的阈值时收到通知。例如，客户可以监控特定时间段内向机器人发出的请求数量，查看成功请求的延迟，或者在错误超过阈值时发出警报。Lex 还集成到中 AWS CloudTrail 以记录 Lex API 调用。有关更多信息，请参阅 Amazon Lex 中的监控。

Amazon Managed Streaming for Apache Kafka (Amazon MSK)

Amazon MSK 为静态数据和传输中的数据提供加密功能。对于静态数据加密，Amazon MSK 集群使用 Amazon EBS 服务器端加密和 AWS KMS 密钥来加密存储卷。对于传输中的数据，Amazon MSK 集群已通过 TLS 启用加密，用于代理间通信。

创建集群时会启用加密配置设置。此外，默认情况下，对于通过 CLI 或 AWS 控制台创建的集群，传输中加密设置为 TLS。客户端需要进行其他配置才能使用 TLS 加密与集群通信。客户可以通过选择 TLS/PlainText 设置来更改默认加密设置。有关更多信息，请参阅 Amazon MSK 加密。

客户可以使用 Amazon MSK 控制台、Amazon 控制台监控客户集群的性能，或者客户可以使用开源监控解决方案 Prometheus 的开放式监控来访问 JMX 和主机指标。 CloudWatch

专为读取 Prometheus 导出器而设计的工具与 Open Monitoring 兼容，例如：Datadog、Lenses、New Relic、Sumologic或 Prometheus 服务器。有关开放式监控的详细信息，请参阅 Amazon MSK 开放式监控文档。

请注意，与 Apache Kafka 捆绑在一起的 Apache Zookeeper 的默认版本不支持加密。但是，值得注意的是，Apache Zookeeper 和 Apache Kafka 代理之间的通信仅限于代理、主题和分区状态信息。从 Amazon MSK 集群生成和使用数据的唯一方法是通过其 VPC 中的客户端与 Amazon MSK 集群之间的私有连接。Amazon MSK 不支持公共终端节点。

Amazon MQ

Amazon MQ 是一项适用于 Apache ActiveMQ 的托管消息代理服务，可让您在云中轻松设置和操作消息代理。Amazon MQ 无需客户管理、操作或维护自己的消息系统，即可使用现有应用程序和服务。为了在传输过程中对 PHI 数据进行加密，应使用以下启用 TLS 的协议来访问代理：

- AMQP
- MQTT

- MQTT 结束了 WebSocket
- OpenWire
- STOMP
- 大吃一惊 WebSocket

Amazon MQ 使用其安全管理和存储的加密密钥对静态和传输中的消息进行加密。亚马逊 MQ 使用 CloudTrail 记录所有 API 调用。

Amazon Neptune

Amazon Neptune 是一项快速、可靠且完全托管式的图数据库服务，可帮助您轻松构建和运行适用于高度互连数据集的应用程序。Amazon Neptune 的核心是一个专门构建的高性能图形数据库引擎，经过优化，可存储数十亿个关系并以毫秒的延迟查询图表。亚马逊 Neptune 支持流行的图表查询语言 Apache TinkerPop Gremlin 和 W3C 的 SPARQL。

包含 PHI 的数据现在可以保留在 Amazon Neptune 的加密实例中。Amazon Neptune 的加密实例只能在创建时指定，方法是从亚马逊 Neptune 控制台中选择 “启用加密”。Amazon Neptune 加密实例的所有日志、备份和快照都经过加密。Amazon Neptune 加密实例的密钥管理是通过提供的。 AWS KMS传输中的数据通过 SSL/TLS 进行加密。亚马逊 Neptune 使用 CloudTrail 记录所有 API 调用。

AWS 网络防火墙

AWS Network Firewall 是一项托管防火墙服务，可让您轻松地为所有亚马逊虚拟私有云（亚马逊 VPC）部署基本的网络保护。该服务可根据网络流量自动扩展，以提供高可用性保护，而无需设置或维护底层基础架构。客户规则和访问日志都可能包含最终用户 IP 地址，这些地址在 AWS 架构中的静态和传输中都经过加密。此外， AWS Network Firewall 会加密所有静态数据和组件 AWS 服务（亚马逊 S3、亚马逊 DynamoDB、Amazon Logs CloudWatch 、Amazon EBS）之间传输的数据。该服务无需特殊配置即可自动加密数据。

Amazon Pinpoint

Amazon Pinpoint 为开发者提供单个 API 层、CLI 支持和客户端 SDK 支持，以扩展应用程序与用户的通信渠道。符合条件的渠道包括：电子邮件、短信、移动推送通知和自定义渠道。Amazon Pinpoint 还提供了一个分析系统，用于跟踪应用程序用户行为和用户参与度。通过这项服务，开发人员可以了解每个用户偏好的互动方式，并可以个性化用户体验以提高用户满意度。

Amazon Pinpoint 还可以帮助开发者解决多种消息传递用例，例如直接消息或交易消息、定向消息或活动消息以及基于事件的消息传递。通过通过 Amazon Pinpoint 集成和启用所有最终用户参与渠道，开发人员可以创建跨所有客户接触点的 360 度用户参与视图。Amazon Pinpoint 存储用户、终端节点和事件数据，因此客户可以创建区段、向收件人发送消息和捕获参与数据。

Amazon Pinpoint 对静态和传输中的数据进行加密。有关更多信息，请参阅 Amazon Pinpoint 常见问题解答。虽然 Amazon Pinpoint 会对所有静态和传输中的数据进行加密，但最终渠道（例如短信或电子邮件）可能未加密，客户应以符合其要求的方式配置任何渠道。

此外，需要通过短信渠道发送 PHI 的客户应使用专用的短代码（5、6 位数的发起电话号码）来明确用于发送 PHI。有关如何请求短代码的更多信息，请参阅使用 Amazon Pinpoint 请求短信专用短代码。客户也可以选择不通过最终渠道发送 PHI，而是提供一种通过 HTTPS 安全访问 PHI 的机制。

可以使用捕获对 Amazon Pinpoint 的 API 调用。 AWS CloudTrail捕获的调用包括来自亚马逊 Pinpoint 控制台的调用和对亚马逊 Pinpoint API 操作的代码调用。如果客户创建了跟踪，则客户可以允许将 AWS CloudTrail 事件持续传输到 Amazon S3 存储桶，包括 Amazon Pinpoint 的事件。如果客户未配置跟踪，他们仍然可以在 AWS CloudTrail 控制台上使用事件历史记录查看最新事件。通过收集的信息 AWS CloudTrail，买家可以确定请求是向 Amazon Pinpoint 提出的、请求的 IP 地址、谁提出了请求、何时提出请求以及其他详情。有关更多信息，请参阅使用记录亚马逊 Pinpoint API 调用。 AWS CloudTrail

Amazon Polly

Amazon Polly 云服务可以将文本转化为逼真的语音。Amazon Polly 提供简单的 API 操作，客户可以轻松地将其与现有应用程序集成。Amazon Polly 使用 HTTPS 协议与客户通信。对 Amazon Polly 的访问权限由 API 驱动，可以强制执行适当的 IAM 最低权限。有关更多信息，请参阅数据保护。包括 PHI 的一些用例示例：

- Caregiver 将包含 PHI 的文本报告转换为合成语音，这样他们就可以在行走或执行其他任务时收听报告。
- 为视障患者提供医疗指导，并以合成语音的形式接受指导。

Amazon Polly 的最终交付渠道可能会导致在公共场所使用 PHI 播放音频，因此在交付时应采取预防措施，将这一点考虑在内。合成语音输出也可以异步发送到启用加密的 Amazon S3 存储桶。

当 Amazon Polly 中出现支持的事件活动时，该活动会与其他 AWS 服务 AWS CloudTrail 事件一起记录在事件历史记录中。要持续记录客户 AWS 账户中的事件，包括 Amazon Polly 的事件，请创建跟踪。跟踪允许 CloudTrail将日志文件传输到 Amazon S3 存储桶。通过收集的信息 CloudTrail，买家可

以确定向 Amazon Polly 发出的请求、发出请求的 IP 地址、何人提出请求、何时提出请求以及其他详细信息。

Amazon Quantum Ledger Database (Amazon QLDB)

Amazon QLDB 是一个完全托管的分类账数据库，提供了一个透明、不可变、可通过加密方式验证的事务日志，且该事务日志由一家可信的中央机构拥有。Amazon QLDB 会跟踪每一次应用程序数据更改，并维护一段时间内完整且可验证的更改历史记录。包含 PHI 的数据现在可以保留在 QLDB 实例中。默认情况下，所有传输中的和静态的 Amazon QLDB 数据都经过加密。传输中的数据使用 TLS 加密，静态数据使用 AWS 托管密钥进行加密。出于数据保护目的，我们建议客户保护 AWS 账户凭证并使用 AWS Identity and Access Management (IAM) 设置个人用户账户，这样每位用户只能获得履行其工作职责所需的权限。有关更多信息，请参阅 Amazon QLDB 中的数据保护。

Amazon QLDB AWS CloudTrail与一项服务集成，该服务提供用户、角色或 AWS 服务在 QLDB 中采取的操作的记录。 CloudTrail 将 QLDB 的所有控制平面 API 调用捕获为事件。捕获的调用包括来自 QLDB 控制台的调用和对 API 操作的代码调用。如果客户创建了跟踪，则客户可以允许持续向亚马逊简单存储服务 (Amazon S3) Storage Service 存储桶传送 CloudTrail 事件，包括 QLDB 的事件。如果客户未配置跟踪，则客户仍可以在 CloudTrail 控制台上的 “事件历史记录” 中查看最新的事件。 使用收集的信息 CloudTrail，客户可以确定向QLDB发出的请求、发出请求的IP地址、谁提出了请求、何时提出请求以及其他详细信息。

Amazon QuickSight

Amazon QuickSight 是一项业务分析服务，客户可以使用它来构建可视化效果、执行临时分析并从其数据中快速获取业务见解。Amazon QuickSight 发现 AWS 数据源，使组织能够扩展到成千上万的用户，并通过使用强大的内存引擎 (SPICE) 提供响应性能。

客户只能使用亚马逊的企业版 QuickSight 来处理包含 PHI 的数据，因为它支持对静态存储在 SPICE 中的数据进行加密。使用 AWS 托管密钥执行数据加密。

Amazon RDS for MariaDB

适用于 MariaDB 的 Amazon RDS 允许客户使用他们管理的密钥对 MariaDB 数据库进行加密。 AWS KMS在使用 Amazon RDS 加密运行的数据库实例上，静态存储在底层存储中的数据将按照本白皮书发布时有效的指南进行加密，自动备份、只读副本和快照也是如此。

由于指南可能会更新，因此客户应继续评估和确定 Amazon RDS for MariaDB 加密是否满足其合规和监管要求。有关使用 Amazon RDS 进行静态加密的更多信息，请参阅加密 Amazon RDS 资源。

与包含 PHI 的 RDS for MariaDB 的连接必须使用传输加密。有关启用加密连接的更多信息，请参阅使用 SSL/TLS 加密与数据库实例的连接。

Amazon RDS for MySQL

适用于 MySQL 的 Amazon RDS 允许客户使用客户管理的密钥加密 MySQL 数据库 AWS KMS。在使用 Amazon RDS 加密运行的数据库实例上，静态存储在底层存储中的数据将按照本白皮书发布时有效的指南进行加密，自动备份、只读副本和快照也是如此。

由于指南可能会更新，因此客户应继续评估和确定 Amazon RDS for MySQL 加密是否满足其合规和监管要求。有关使用 Amazon RDS 进行静态加密的更多信息，请参阅加密 Amazon RDS 资源。

与包含 PHI 的 RDS for MySQL 的连接必须使用传输加密。有关启用加密连接的更多信息，请参阅使用 SSL/TLS 加密与数据库实例的连接。

Amazon RDS for Oracle

客户有多种选择使用适用于 Oracle 的 Amazon RDS 对静态的 PHI 进行加密。客户可以使用他们管理的密钥加密 Oracle 数据库 AWS KMS。在使用 Amazon RDS 加密运行的数据库实例上，静态存储在底层存储中的数据将按照本白皮书发布时有效的指南进行加密，自动备份、只读副本和快照也是如此。

由于指南可能会更新，因此客户应继续评估和确定 Amazon RDS for Oracle 加密是否满足其合规和监管要求。有关使用 Amazon RDS 进行静态加密的更多信息，请参阅加密 Amazon RDS 资源。

客户还可以使用 Oracle 透明数据加密 (TDE)，他们应评估配置是否与指南一致。Oracle TDE 是 Oracle 企业版中提供的 Oracle 高级安全选项的一项功能。该功能在将数据写入到存储之前自动对数据进行加密，并在从存储读取数据时自动对数据进行解密。客户还可以使用 AWS CloudHSM 来存储 Amazon RDS Oracle TDE 密钥。有关更多信息，请参阅下列内容：

- 适用于 Oracle 的 Amazon RDS 透明数据加密：甲骨文透明数据加密。
- AWS CloudHSM 用于存储 Amazon RDS Oracle TDE 密钥：什么是亚马逊关系数据库服务 (Amazon RDS)？

与包含 PHI 的 Amazon RDS for Oracle 的连接必须使用传输加密，并评估配置是否与指南一致。这是使用 Oracle 原生网络加密实现的，并在 Amazon RDS for Oracle 选项组中启用。有关详细信息，请参阅 Oracle 原生网络加密。

Amazon RDS for PostgreSQL

适用于 PostgreSQL 的 Amazon RDS 允许客户使用客户管理的密钥加密 PostgreSQL 数据库。 AWS KMS在使用 Amazon RDS 加密运行的数据库实例上，静态存储在底层存储中的数据将按照本白皮书发布时有效的指南进行加密，自动备份、只读副本和快照也是如此。

由于指南可能会更新，因此客户应继续评估和确定适用于 PostgreSQL 的 Amazon RDS for PostgreSQL 加密是否满足其合规和监管要求。有关使用 Amazon RDS 进行静态加密的更多信息，请参阅加密 Amazon RDS 资源。

与包含 PHI 的 PostgreSQL 版 RDS 的连接必须使用传输加密。有关启用加密连接的更多信息，请参阅使用 SSL/TLS 加密与数据库实例的连接。

Amazon RDS for SQL Server

RDS for SQL Server 支持存储以下版本和版本组合的 PHI：

- 2008 R2-仅限企业版
- 2012、2014 和 2016 年——网络版、标准版和企业版

重要提示：不支持 SQL Server Express 版本，因此切勿将其用于存储 PHI。

为了存储 PHI，客户必须确保将实例配置为加密静态数据，并启用传输加密和审计，详情如下。

静态加密

客户可以使用他们管理的密钥加密 SQL Server 数据库 AWS KMS。在使用 Amazon RDS 加密运行的数据库实例上，静态存储在底层存储中的数据将按照本白皮书发布时有效的指南进行加密，自动备份和快照也是如此。由于指南可能会更新，因此客户应继续评估和确定 Amazon RDS for SQL Server 加密是否满足其合规和监管要求。有关使用 Amazon RDS 进行静态加密的更多信息，请参阅加密 Amazon RDS 资源。

如果客户使用 SQL Server 企业版，则可以使用服务器透明数据加密 (TDE) 作为替代方案。该功能在将数据写入到存储之前自动对数据进行加密，并在从存储读取数据时自动对数据进行解密。有关 RDS for SQL Server 透明数据加密的更多信息，请参阅支持 SQL Server 中的透明数据加密。

传输加密

与包含 PHI 的 Amazon RDS for SQL Server 的连接必须使用 SQL Server 强制 SSL 提供的传输加密。在参数组中为 Amazon RDS SQL Server 启用了强制 SSL。有关 RDS for SQL Server 强制 SSL 的更多信息，请参阅在微软 SQL Server 数据库实例上使用 SS L。

审核

包含 PHI 的 RDS for SQL Server 实例必须启用审计。在 Amazon RDS SQL Server 的参数组中启用审计。有关 RDS for SQL Server 审计的更多信息，请参阅微软 SQL Server 数据库实例的合规性计划支持。

Amazon Redshift

Amazon Redshift 为其集群提供数据库加密，以帮助保护静态数据。当客户为集群启用加密时，Amazon Redshift 会使用硬件加速的高级加密标准 (AES) -256 个对称密钥对包括备份在内的所有数据进行加密。Amazon Redshift 使用基于密钥的四层架构来进行加密。这些密钥由数据加密密钥、数据库密钥、集群密钥和 KMS 密钥组成。

群集密钥对 Amazon Redshift 群集的数据库密钥进行加密。客户可以使用 AWS KMS 或 AWS CloudHSM （硬件安全模块）来管理集群密钥。Amazon Redshift 静态加密与本白皮书发布时有效的指南一致。由于指南可能会更新，因此客户应继续评估和确定 Amazon Redshift 加密是否满足其合规和监管要求。有关更多信息，请参阅 Amazon Redshift 数据库加密。

与包含 PHI 的 Amazon Redshift 的连接必须使用传输加密，并且客户应评估配置是否与指南一致。有关更多信息，请参阅配置连接的安全选项。Amazon Redshift Spectrum 使客户能够对亚马逊 S3 中的艾字节数据运行亚马逊 Redshift SQL 查询。Redshift Spectrum 是亚马逊 Redshift 的一项功能，因此也在 HIPAA BAA 的范围内。

Amazon Rekognition

Amazon Rekognition 可以轻松地将图像和视频分析添加到客户应用程序中。客户只需向 Amazon Rekognition API 提供图像或视频，该服务就可以识别对象、人物、文本、场景和活动，并检测任何不当内容。Amazon Rekognition 还提供高度准确的面部分析和面部识别。

亚马逊 Rekognition 有资格使用包含 PHI 的图片或视频。Amazon Rekognition 作为一项托管服务运行，不提供任何用于处理数据的可配置选项。亚马逊 Rekognition 仅在 BAA 条款允许的情况下使用、披露和维护 PHI。 AWS 所有数据在静态和传输过程中都经过加密，并通过 Amazon Rekognition 进行传输。亚马逊 AWS CloudTrail Rekognition 用于记录所有 API 调用。

Amazon Route 53

Amazon Route 53 是一项托管 DNS 服务，可让客户注册域名、路由互联网流量客户域资源以及检查这些资源的运行状况。虽然 Amazon Route 53 是一项符合 HIPAA 资格的服务，但不应将 PHI 存储在亚马逊 Route 53 中的任何资源名称或标签中，因为不支持对此类数据进行加密。相反，Amazon Route 53 可用于提供对传输或存储 PHI 的客户域资源的访问权限，例如在 Amazon EC2 上运行的网络服务器或存储（例如 Amazon S3）。

Simple Storage Service (Amazon S3) Glacier

Amazon S3 Glacier 使用 AES 256 位对称密钥自动加密静态数据，并支持通过安全协议安全传输客户数据。与包含 PHI 的 Amazon S3 Glacier 连接必须使用接受加密传输 (HTTPS) 的终端节点。有关区域终端节点的列表，请参阅AWS 服务终端节点。

请勿在档案和文件库名称或元数据中使用 PHI，因为这些数据未使用 Amazon S3 Glacier 服务器端加密进行加密，通常也不会在客户端加密架构中进行加密。

Amazon S3 Transfer Acceleration

Amazon S3 Transfer Acceleration (S3TA) 支持在客户的客户端和 S3 存储桶之间进行快速、轻松和安全的长距离文件传输。传输加速利用 CloudFront了 Amazon 全球分布的边缘站点。当数据到达某个边缘站点时，数据会被经过优化的网络路径路由至 Amazon S3。客户应确保使用 AWS S3TA 传输的任何包含 PHI 的数据在传输过程中和静态时都经过加密。要了解可用的加密选项，请参阅 Amazon S3 指南。

Amazon SageMaker

Amazon SageMaker 是一项完全托管的机器学习服务。借助 Amazon SageMaker，数据科学家和开发人员可以快速轻松地构建和训练机器学习模型，然后将其直接部署到可直接用于生产的托管环境中。它提供了一个集成的 Jupyter 创作笔记本实例，便于访问数据源进行探索和分析。Amazon SageMaker 还提供常见的机器学习算法，这些算法经过优化，可在分布式环境中针对极其庞大的数据高效运行。

借助对 bring-your-own-algorithms 框架的原生支持，Amazon SageMaker 提供了灵活的分布式培训选项，可根据客户的特定工作流程进行调整。亚马逊 SageMaker有资格使用包含 PHI 的数据进行运营。传输中数据的加密由 SSL/TLS 提供，用于与亚马逊的前端接口 SageMaker （到笔记本）进行通信，以及当亚马逊与任何其他 AWS 服务 SageMaker 交互时（例如，从 Amazon S3 提取数据）。

为了满足 PHI 在静态状态下加密的要求，在设置终端节点 (DescribeEndpointConfig: KmsKey ID) 时，使用 AWS Key Management Service (KMS) 启用对使用亚马逊 SageMaker 运行模型的实例存储的数据进行加密。使用启用模型训练结果（工件）的加密， AWS KMS 并且应使用 OutputDataConfig描述中的 KmsKey ID 指定密钥。如果未提供 KMS 密钥 ID，则将使用该角色账户的默认 Amazon S3 KMS 密钥。亚马逊 SageMaker AWS CloudTrail 使用记录所有 API 调用。

Amazon Simple Notification Service (Amazon SNS)

要使用带有受保护健康信息 (PHI) 的亚马逊简单通知服务 (SNS) Simple Notification Service (PHI)，客户应了解以下密钥加密要求。客户必须使用 SNS 在每个 AWS 区域提供的 HTTPS API 终端节点。HTTPS 端点利用加密连接，保护发送到 AWS的数据的隐私和完整性。有关所有 HTTPS API 终端节点的列表，请参阅AWS 服务终端节点。

此外，Amazon SNS 还使用 CloudTrail一项服务，它可以捕获客户账户中由亚马逊 SNS 或代表其发出 AWS 的 API 调用，并将日志文件传输到他们指定的亚马逊 S3 存储桶。 CloudTrail 捕获从亚马逊 SNS 控制台或亚马逊 SNS API 发出的 API 调用。通过收集的信息 CloudTrail，买家可以确定向 Amazon SNS 发出了什么请求、发出请求的源 IP 地址、谁提出了请求以及何时提出请求。有关记录 SNS 操作的更多信息，请参阅使用记录 Amazon SNS API 调用。 CloudTrail

Amazon Simple Email Service（Amazon SES）

Amazon Simple Email Service (Amazon SES) 是一项灵活且高度可扩展的电子邮件发送和接收服务。它支持 S/MIME 和 PGP 协议来加密消息以实现完全加 end-to-end 密，并且与 Amazon SES 的所有通信均使用 SSL (TLS 1.2) 进行保护。客户可以选择存储静态加密的消息，方法是将 Amazon SES 配置为接收和加密消息，然后再将其存储在 Amazon S3 存储桶中。有关更多信息，请参阅亚马逊简单电子邮件服务 (Amazon SES) 如何 AWS KMS使用亚马逊简单电子邮件服务 (Amazon SES) 来了解有关加密用于存储的邮件的更多信息。邮件在通过 HTTPS 终端节点或加密的 SMTP 连接传输到 Amazon SES 时受到保护。

对于从 Amazon SES 发送给收件人的邮件，Amazon SES 将首先尝试与接收邮件服务器建立安全连接，但如果无法建立安全连接，它将以未加密的方式发送邮件。要要求加密才能传送给收件人，客户必须在 Amazon SES 中创建配置集，然后使用 AWS CLI 将该 TlsPolicy 属性设置为 “需要”。有关更多信息，请参阅 Amazon SES 和安全协议。Amazon SES 与集成 AWS CloudTrail 以监控所有 API 调用。通过收集的信息 AWS CloudTrail，买家可以确定请求是向 Amazon SES 提出的、请求的 IP 地址、谁提出了请求、何时提出请求以及其他详细信息。有关更多信息，请参阅使用记录 Amazon SES API 调用 AWS CloudTrail。Amazon SES 还提供了监控发送活动的方法，例如发送、拒绝、退回率、交付、打开和点击。有关更多信息，请参阅监控您的 Amazon SES 发送活动。

Amazon Simple Queue Service(Amazon SQS)

要将 Amazon SQS 与 PHI 配合使用，客户应了解以下密钥加密要求。

- 通过查询请求与 Amazon SQS 队列的通信必须使用 HTTPS 进行加密。有关发出 SQS 请求的更多信息，请参阅发出查询 API 请求。
- Amazon SQS 支持与集成的服务器端加密， AWS KMS 以保护静态数据。服务器端加密的增加使客户能够传输和接收敏感数据，同时使用加密队列可以提高安全性。Amazon SQS 服务器端加密使用 256 位高级加密标准（AES-256 GCM 算法）对每条消息的正文进行加密。与的集成 AWS KMS 允许客户集中管理保护 Amazon SQS 消息的密钥以及保护其其他 AWS 资源的密钥。 AWS KMS 记录加密密钥的每一次使用情况 AWS CloudTrail ，以帮助满足监管和合规需求。如需了解更多信息，以及要查看区域以了解适用于 Amazon SQS 的 SSE 的可用性，请参阅静态加密。
- 如果不使用服务器端加密，则必须先对消息负载本身进行加密，然后才能发送到 SQS。加密消息负载的一种方法是使用 Amazon SQS 扩展客户端和 Amazon S3 加密客户端。有关使用客户端加密的更多信息，请参阅使用 Amazon SQS 扩展客户端和 Amazon S3 加密客户端加密消息负载。

Amazon SQS 使用一项服务 CloudTrail，用于记录客户账户中由亚马逊 SQS 或代表其进行的 API 调用，并将日志文件传输到指定 AWS 的 Amazon S3 存储桶。 CloudTrail 捕获从亚马逊 SQS 控制台或亚马逊 SQS API 发出的 API 调用。客户可以使用收集的信息 CloudTrail 来确定向 Amazon SQS 提出了哪些请求、发出请求的源 IP 地址、谁提出了请求、何时发出请求等。有关记录 SQS 操作的更多信息，请参阅使用记录 Amazon SQS API 调用。 AWS CloudTrail

Amazon Simple Storage Service (Amazon S3)

客户在使用 Amazon S3 时有多种方式对静态数据进行加密，包括服务器端和客户端加密，以及多种管理密钥的方法。有关更多信息，请参阅使用加密保护数据。

与包含 PHI 的 Amazon S3 的连接必须使用接受加密传输 (HTTPS) 的终端节点。有关区域终端节点的列表，请参阅AWS 服务终端节点。

请勿在存储桶名称、对象名称或元数据中使用 PHI，因为这些数据未使用 S3 服务器端加密进行加密，通常也不会在客户端加密架构中进行加密。

Amazon Simple Workflow Service

亚马逊简单工作流服务 (Amazon SWF) Simple Workflow Service 可帮助开发人员构建、运行和扩展具有并行或顺序步骤的后台作业。可以将 Amazon SWF 视为云端完全托管的状态跟踪器和任务协调器。

Amazon 简单工作流程服务用于协调工作流程，无法存储或传输数据。不应将 PHI 放在 Amazon SWF 的元数据中或任何任务描述中。Amazon SWF AWS CloudTrail 用于记录所有 API 调用。

Amazon Textract

Amazon Textract 使用机器学习技术自动从扫描的文档中提取文本和数据，这些文本和数据不仅限于简单的光学字符识别 (OCR)，还可以识别、理解和提取表单和表格中的数据。例如，客户可以使用 Amazon Textract 自动提取数据并处理包含受保护健康信息 (PHI) 的表单，无需人为干预即可完成医疗索赔。

Amazon Textract 还可用于维护文档存档的合规性。例如，客户可以使用 Amazon Textract 从保险索赔或医疗处方中提取数据，并自动识别这些文档中的键值对，以便对敏感文档进行编辑。

Amazon Textract 支持对输入文档进行服务器端加密（SSE-S3 和 SSE-KMS），对服务和代理之间传输的数据支持 TLS 加密。客户可以使用亚马逊 CloudWatch来跟踪资源使用情况指标并捕获 AWS CloudTrail 对亚马逊 Textract 的 API 调用。

Amazon Transcribe

Amazon Transcribe 使用先进的机器学习技术来识别音频文件中的语音并将其转录为文本。例如，客户可以使用 Amazon Transcribe 将美国英语和墨西哥西班牙语音频转换为文本，并创建包含音频文件内容的应用程序。Amazon Transcribe 可用于处理包含 PHI 的数据。Amazon Transcribe 不保留或存储任何数据，对 API 的所有调用均使用 SSL/TLS 加密。Amazon Transcribe CloudTrail 用于记录所有 API 调用。

Amazon Translate

Amazon Translate 使用先进的机器学习技术按需提供高质量的翻译。客户可以使用 Amazon Translate 翻译非结构化文本文档或构建支持多种语言的应用程序。包含 PHI 的文档可以使用 Amazon Translate 进行处理。翻译包含 PHI 的文档时，无需进行其他配置。SSL/TLS 对传输中的数据进行加密，Amazon Translate 不会保留任何静态数据。Amazon Translate 使用 CloudTrail 记录所有 API 调用。

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud（亚马逊 VPC）提供了一组网络安全功能，非常适合为 HIPAA 监管的工作负载进行架构。诸如无状态网络访问控制列表和将实例动态重新分配到有状态安全组之类的功能为保护实例免受未经授权的网络访问提供了灵活性。

Amazon VPC 还允许客户将自己的网络地址空间扩展到 AWS，并提供多种连接其数据中心的方式 AWS。VPC Flow Logs 对处理、传输或存储 PHI 的实例的已接受和拒绝连接提供审计跟踪。

AWS Transit Gateway 充当网络中心，可简化 Amazon VPC 与本地网络之间的连接。 AWS Transit Gateway 还为其他公交网关提供区域间对等互连功能，以便使用主 AWS 干网建立全球网络。有关亚马逊 VPC 的更多信息，请参阅亚马逊虚拟私有云。

Amazon WorkDocs

Amazon WorkDocs 是一项完全托管、安全的企业文件存储和共享服务，具有强大的管理控制和反馈功能，可提高用户的工作效率。 Amazon WorkDocs 使用客户通过 AWS Key Management Service (AWS KMS) 管理的密钥对文件进行静态加密。所有传输中的数据均使用 SSL/TLS 进行加密。 AWS Web 和移动应用程序以及桌面同步客户端， Amazon WorkDocs 使用 SSL/TLS 将文件直接传输到。

使用 Amazon WorkDocs 管理控制台， WorkDocs 管理员可以查看审核日志，按时间跟踪文件和用户活动，并选择是否允许用户与组织外部的其他人共享文件。 Amazon WorkDocs 还与 CloudTrail （一种捕获由客户账户或代表客户 AWS 账户发出的 API 调用的服务）集成，并将 CloudTrail 日志文件传输到客户指定的 Amazon S3 存储桶。 Amazon WorkDocs

可以使用 RADIUS 服务器进行多重身份验证 (MFA)，它可以在身份验证过程中为客户提供额外的安全保护。用户通过输入用户名和密码，然后输入硬件或软件令牌提供的 OTP（一次性密码）进行登录。

有关更多信息，请参阅：

- Amazon WorkDocs feature
- 使用记录 Amazon WorkDocs API 调用 AWS CloudTrail

客户不应将 PHI 存储在文件名或目录名中。

Amazon WorkSpaces

Amazon WorkSpaces 是一个完全托管、安全的分布esktop-as-a式服务 (DaaS) 解决方案，可在上运行。 AWS借助亚马逊 WorkSpaces，客户可以轻松地为其用户配置基于云的虚拟 Microsoft Windows 桌面，让他们能够随时随地通过任何支持的设备访问所需的文档、应用程序和资源。

亚马逊 WorkSpaces 将数据存储在亚马逊 Elastic Block Store 卷中。客户可以使用客户管理的密钥对客户的 WorkSpaces存储卷进行加密 AWS Key Management Service。启用加密后 WorkSpace，存储

在底层存储中的静态数据和磁盘存储的自动备份（EBS 快照）都将按照指南进行加密。从 WorkSpace 客户端到的通信使用 SSL/ WorkSpace TLS 进行保护。有关使用 Amazon 进行静态加密的更多信息 WorkSpaces，请参阅已加密 WorkSpaces。

AWS App Mesh

AWS App Mesh 是一种服务网格，它提供应用程序级联网，使您的服务可以轻松地跨多种类型的计算基础设施（例如 Amazon ECS、Amazon EKS 或 Amazon EC2 服务）相互通信。App Mesh 将 Envoy 代理配置为收集可观测性数据并将其传输到您配置的监控集合，从而为您提供可见性。 end-to-end 它可以根据为确保应用程序的高可用性而配置的路由和流量策略来路由流量。可以将应用程序之间的流量配置为使用 TLS。App Mesh 可以使用 AWS 适用于 Kubernetes 的 SDK 或 App Mesh 控制器来使用。虽然 AWS App Mesh 是一项符合 HIPAA 资格的服务，但不应将任何 PHI 存储在里面的任何资源名称/属性中， AWS App Mesh 因为不支持保护此类数据。相反， AWS App Mesh 可以用来监控、控制和保护传输或存储 PHI 的客户域资源。

AWS 应用程序迁移服务

AWS 应用程序迁移服务 (AWS MGN) 允许您快速将服务器和应用程序迁移到 AWS，无需更改且停机时间最短。 AWS MGN 是推荐用于升降和转移迁移的主要迁移服务。 AWS

AWS MGN 使用块级数据复制将源磁盘直接复制到客户账户中的 EBS 卷——数据永远不会通过 AWS MGN 控制的云环境传输。默认情况下，复制的数据在传输过程中会被加密。默认情况下，客户的 EBS 卷中的数据使用客户自己的密钥进行加密。

AWS Auto Scaling

AWS Auto Scaling 使客户能够在几分钟内为作为客户应用程序一部分的 AWS 资源配置自动扩展。客户可以将 A AWS uto Scaling 用于许多涉及 PHI 的服务，例如 Amazon DynamoDB、Amazon ECS、Amazon RDS Aurora 副本和 Auto Scaling 组中的亚马逊 EC2 实例。

AWS Auto Scaling 是一项不直接处理、存储或传输客户内容的编排服务；因此，客户可以将此服务用于加密内容。 AWS 分担责任模型适用于 AWS Auto Scaling 中的数据保护： AWS 负责 AWS 网络安全程序，而客户负责维护对托管在此基础架构上的客户内容的控制。此内容包括客户使用的 AWS 服务的安全配置和管理任务。出于数据保护目的，我们建议客户保护 AWS 账户凭证并使用 AWS Identity and Access Management (IAM) 设置个人用户账户。这仅向每个用户授予履行其工作职责所需的权限。

我们强烈建议客户切勿将敏感的识别信息（例如客户的账号）放入自由格式字段（例如 “姓名” 字段）中。这包括客户使用 AWS 管理控制台、API 或软件开发工具包使用 AWS Auto AWS Scaling 或其他 AWS 服务时。 AWS CLI

客户输入到 AWS Auto Scaling 或其他服务中的任何数据都可能会被提取并包含在诊断日志中。当客户提供外部服务器的 URL 时，他们不应在 URL 中包含凭据信息来验证他们对该服务器的请求。 AWS 还建议客户通过以下方式保护其数据:

- 对每个账户使用多重身份验证 (MFA)。
- 使用 SSL/TLS 与资源通信。 AWS 我们推荐 TLS 1.2 或更高版本
- 使用设置 API 和用户活动日志 AWS CloudTrail。
- 使用 AWS 加密解决方案以及 AWS 服务中的所有默认安全控制。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的个人数据。

AWS Backup

AWS Backup 提供集中式、完全托管且基于策略的服务，以保护客户数据并确保各项 AWS 服务的合规性，从而实现业务连续性。借助 AWS Backup，客户可以集中配置数据保护（备份）策略并监控客户 AWS 资源的备份活动，包括亚马逊 EBS 卷、亚马逊关系数据库服务 (Amazon RDS) 数据库（包括 Aurora 集群）、亚马逊 DynamoDB 表、亚马逊弹性文件系统 (Amazon EFS)、亚马逊 FSx 文件系统、亚马逊 EC2 实例和卷。 AWS Storage Gateway

AWS Backup 对传输中的和静态的客户数据进行加密。来自具有现有快照功能的服务的备份使用源服务的快照加密方法进行加密。例如，使用创建快照的卷的加密密钥对 EBS 快照进行加密。

来自引入内置备份功能的新 AWS 服务（例如 Amazon EFS）的备份在 AWS Backup传输中和静态时都独立于源服务进行加密，从而为客户备份提供了额外的保护层。加密是在 Backup Vault 级别配置的。默认保管库已加密。客户创建新保管库时，必须选择加密密钥。

AWS Batch

AWS Batch 使开发人员、科学家和工程师能够轻松高效地运行成千上万的批量计算作业 AWS。 AWS Batch 根据提交的批处理作业的数量和特定资源需求，动态配置计算资源的最佳数量和类型（例如 CPU 或内存优化型实例）。 AWS Batch 规划、安排和执行各种计算服务和功能的批量 AWS 计算工作负载。

与 Amazon ECS 指南类似，不应将 PHI 直接放入任务定义、任务队列或标签中 AWS Batch。相反，使用调度和执行的作业 AWS Batch 可以在加密的 PHI 上运行。任务各阶段返回给的任何信息也不 AWS Batch 应包含任何 PHI。每当执行的任务 AWS Batch 必须传输或接收 PHI 时，都应使用 HTTPS 或 SSL/TLS 对连接进行加密。

AWS Certificate Manager

AWS Certificate Manager 是一项服务，可让客户轻松预置、管理和部署公共和私有 SSL/TLS 证书，以用于 AWS 服务及其内部连接的资源。 AWS Certificate Manager CloudTrail 用于记录所有 API 调用。

如果用户想在 AWS 外部进行交互，则需要编程访问权限 AWS 管理控制台。授予编程访问权限的方式取决于正在访问的用户类型 AWS。

要向用户授予编程式访问权限，请选择以下选项之一。

哪个用户需要编程式访问权限？	目的	方式
人力身份 （在 IAM Identity Center 中管理的用户）	使用临时证书签署向 AWS CLI、 AWS 软件开发工具包或 AWS API 发出的编程请求。	按照您希望使用的界面的说明进行操作。 • 有关的 AWS CLI，请参阅《AWS Command Line Interface 用户指南》 AWS IAM Identity Center中的配置 AWS CLI 以使用。 • 有关 AWS 软件开发工具包、工具和 AWS API，请参阅《软件开发工具包和AWS 工具参考指南》中的 IAM 身份中心身份验证。
IAM	使用临时证书签署向 AWS CLI、 AWS 软件开发工具包或 AWS API 发出的编程请求。	按照 IAM 用户指南中的将临时证书与 AWS 资源配合使用中的说明进行操作。

哪个用户需要编程式访问权限？	目的	方式
IAM	（不推荐使用） 使用长期凭证签署向 AWS CLI、 AWS 软件开发工具包或 AWS API 发出的编程请求。	按照您希望使用的界面的说明进行操作。 • 有关信息 AWS CLI，请参阅用户指南中的使用 IAM 用户证书进行身份验证。AWS Command Line Interface • 有关 AWS SDK 和工具，请参阅 S AWS DK 和工具参考指南中的使用长期凭证进行身份验证。 • 有关 AWS API，请参阅 IAM 用户指南中的管理 IAM 用户的访问密钥。

AWS Cloud Map

AWS 云地图是一项云资源发现服务。借助 AWS Cloud Map，客户可以为应用程序资源定义自定义名称，例如亚马逊 ECS 任务、亚马逊 EC2 实例、亚马逊 S3 存储桶、亚马逊 DynamoDB 表、亚马逊 SQS 队列或任何其他云资源。然后，客户可以使用这些自定义名称，通过 AWS SDK 和经过身份验证的 API 查询从其应用程序中发现云资源的位置和元数据。虽然 AWS 云地图是一项符合 HIPAA 资格的服务，但不应将 PHI 存储在 AWS 云地图中的任何资源名称/属性中，因为不支持保护此类数据。相反，AWS Cloud Map 可用于发现传输或存储 PHI 的客户域资源。

AWS CloudFormation

AWS CloudFormation 使客户能够以可预测的方式重复创建和配置 AWS 基础设施部署。它可以帮助客户利用 AWS 产品，例如 Amazon EC2、Amazon Elastic Block Store、Amazon SNS、Elastic Load Balancing 和 Auto Scaling，在云中构建高度可靠、高度可扩展、经济实惠的应用程序，而不必担心创建和配置底层 AWS 基础设施。 AWS CloudFormation 使客户能够使用模板文件将资源集合作为一个单元（堆栈）一起创建和删除。

AWS CloudFormation 本身不存储、传输或处理 PHI。相反，它用于构建和部署使用其他 AWS 服务的架构，这些服务可能存储、传输和/或处理 PHI。只有符合 HIPAA 资格的服务才能与 PHI 一起使用。请参阅本白皮书中这些服务的条目，以获取有关在这些服务中使用 PHI 的指导。 AWS CloudFormation AWS CloudTrail 用于记录所有 API 调用。

AWS CloudHSM

AWS CloudHSM 是一个基于云的硬件安全模块 (HSM)，可让客户在 AWS 云上轻松生成和使用自己的加密密钥。借助 CloudHSM，客户可以使用经过 FIPS 140-2 3 级验证的 HSM 来管理自己的加密密钥。CloudHSM 让客户能够灵活地使用开放标准 API 与其应用程序集成，例如 PKCS #11、Java 密码学扩展 (JCE) 和微软 Cryptong (CNG) 库。

CloudHSM 还符合标准，允许客户将其所有密钥导出到大多数其他市售的 HSM。与硬件设备密钥管理服务一样 AWS CloudHSM ，它无法存储或传输 PHI。客户不应将 PHI 存储在标签（元数据）中。无需其他特殊指导。

AWS CloudTrail

AWS CloudTrail 是一项支持 AWS 账户的治理、合规、运营审计和风险审计的服务。借助 CloudTrail，客户可以记录、持续监控和保留与其 AWS 基础设施中的操作相关的账户活动。CloudTrail 提供其 AWS 账户活动的事件历史记录，包括通过、AWS 软件开发工具包 AWS 管理控制台、命令行工具和其他 AWS 服务执行的操作。此事件历史记录简化了安全分析、资源变更跟踪和故障排除。

AWS CloudTrail 已启用适用于所有 AWS 账户，并且可以按照 AWS BAA 的要求用于审计日志。应使用 CloudTrail 控制台或 AWS 命令行界面创建特定的跟踪。 CloudTrail 在创建加密的 Trail 时，对传输中的所有流量和静态流量进行加密。当有可能记录 PHI 时，应创建加密跟踪。

默认情况下，加密的跟踪使用服务器端加密和 Amazon S3 (SSE-S3) 托管密钥将条目存储在 Amazon S3 中。如果需要对密钥进行额外管理，也可以使用 AWS KMS托管密钥 (SSE-KMS) 进行配置。AWS 日志条目的最终目的地，因此，作为 CloudTrail 任何处理 PHI 的架构的关键组成部分，都应启用 CloudTrail 日志文件完整性验证，并应定期检查相关的 CloudTrail 摘要文件。启用后，可以肯定地断言日志文件未被更改或更改。

AWS CodeBuild

AWS CodeBuild 是云端完全托管的生成服务。 AWS CodeBuild 编译源代码、运行单元测试并生成准备部署的工件。 AWS CodeBuild 使用 AWS KMS 密钥对构建输出工件进行加密。在构建 AWS

CodeBuild 用于 AWS CloudTrail 记录所有 API 调用的包含 PHI、密钥/密码、证书等的项目之前，应创建和配置 KMS 密钥。

AWS CodeDeploy

AWS CodeDeploy 是一项完全托管的部署服务，可自动将软件部署到各种计算服务，包括 Amazon EC2 AWS Fargate、 AWS Lambda、和本地服务器。客户习惯 AWS CodeDeploy 于快速发布容器化工作负载的新功能，并处理更新应用程序的复杂性。

AWS CodeDeploy 支持对部署工件进行服务器端加密 (SSE-S3)，为在服务和代理之间传输的数据支持 TLS 加密。客户可以使用 Amazon E CloudWatch vents 来跟踪部署并捕获 AWS CloudTrail 对的 API 调用 AWS CodeDeploy。

AWS CodeCommit

AWS CodeCommit 是一项安全、高度可扩展的托管源代码控制服务，用于托管私有 Git 存储库。AWS CodeCommit 客户无需管理自己的源代码控制系统，也不必担心扩展其基础架构。

AWS CodeCommit 在传输和静止时对所有流量和存储的信息进行加密。默认情况下，在其中创建存储库时 AWS CodeCommit，会使用该存储库创建 AWS 托管密钥， AWS KMS 并且该密钥只能由该存储库用于加密所有静态存储的数据。 AWS CodeCommit AWS CloudTrail 用于记录所有 API 调用。

AWS CodePipeline

AWS CodePipeline 是一项完全托管的持续交付服务，可帮助客户实现客户发布渠道的自动化，从而实现快速可靠的应用程序和基础架构更新。客户过去 AWS CodePipeline 允许研究人员自动处理临床试验数据、实验室结果和基因组数据，这只是客户使用的工作流程的几个例子。

AWS CodePipeline 支持对代码工件进行服务器端加密（SSE-S3 和 SSE-KMS），对服务和代理之间传输的数据支持 TLS 加密。客户可以使用 Amazon E CloudWatch vents 来跟踪渠道变更并捕获 AWS CloudTrail 对的 API 调用 AWS CodePipeline。

AWS Config

AWS Config 提供了与客户的 AWS 账户关联的资源的详细视图，包括这些资源的配置方式、它们之间的关系以及配置及其关系如何随着时间的推移而发生变化。

AWS Config 本身不能用于存储或传输 PHI。

相反，可以利用它来监控和评估使用其他 AWS 服务构建的架构，包括处理 PHI 的架构，以帮助确定它们是否符合预期的设计目标。处理 PHI 的架构只能使用符合 HIPAA 条件的服务构建。 AWS Config AWS CloudTrail 用于记录所有结果。

AWS Data Exchange

AWS Data Exchange 让您可以轻松地在云中查找、订阅和使用第三方数据。订阅数据产品后，客户可以使用 AWS Data Exchange API 将数据直接加载到 A mazon S3 中，然后使用各种 AWS 分析和机器学习服务对其进行分析。对于数据提供商而言，AWS Data Exchange 无需构建和维护用于数据存储、交付、计费和授权的基础设施，从而轻松接触迁移到云端的数百万个 AWS 客户。

AWS Data Exchange 始终对存储在静态服务中的所有数据产品进行加密，而无需进行任何其他配置。这种加密是通过服务托管的 KMS 密钥自动完成的。AWS Data Exchange 使用传输层安全 (TLS) 和客户端加密在传输过程中进行加密。与 AWS Data Exchange 的通信始终通过 HTTPS 完成，因此客户的数据在传输过程中始终处于加密状态。当客户使用 AWS Data Exchange 时，系统会默认配置此加密。有关更多信息，请参阅 AWS Data Exchange 中的数据保护。

AWS Data Exchange 已与集成 AWS CloudTrail。 AWS CloudTrail 将对 AWS Data Exchange API 的所有调用作为事件捕获，包括来自 AWS Data Exchange 控制台的调用和对 AWS Data Exchange API 操作的代码调用。客户可以采取的某些操作仅限控制台操作。AWS 开发工具包或 AWS CLI 中没有相应的 API。这些操作依赖于 AWS Marketplace 功能，例如发布或订阅产品。AWS Data Exchange 为这些仅限控制台操作的子集提供 CloudTrail 日志。有关更多信息，请参阅使用记录 AWS Data Exchange API 调用 AWS CloudTrail。

请注意，所有使用 AWS Data Exchange 的列表都必须遵守 AWS Data Exchange 的发布指南和针对 AWS Marketplace 提供商的 AWS Data Exchange 常见问题解答，这些指南限制了某些类别的数据。有关更多信息，请参阅 AWS Data Exchange 常见问题解答。

AWS Database Migration Service

AWS Database Migration Service (AWS DMS) 可帮助客户轻松安全地将数据库迁移到 AWS。客户可以将其数据迁移到最广泛使用的商业和开源数据库，例如 Oracle、MySQL 和 PostgreSQL。该服务支持同构迁移 (如 Oracle 到 Oracle)，也支持不同数据库平台之间的异构迁移 (如 Oracle 到 PostgreSQL 或 MySQL 到 Oracle)。

在本地运行并通过 AWS DMS 迁移到云端的数据库可以包含 PHI 数据。AWS DMS 会在传输过程中以及暂存数据以便最终迁移到 AWS 上的目标数据库时对数据进行加密。AWS DMS 对复制实例使用的存储和终端节点连接信息进行加密。为了加密复制实例使用的存储，AWS DMS 使用 AWS 账户独有的

AWS KMS 密钥。请参阅相应目标数据库的指南，以确保迁移完成后数据保持加密状态。AWS DMS CloudTrail 用于记录所有 API 调用。

AWS DataSync

AWS DataSync 是一项在线传输服务，可简化、自动化和加速本地存储与 AWS 之间的数据移动。客户可以使用 AWS 将其数据源连接 DataSync 到 Amazon S3 或 Amazon EFS。客户应确保 Amazon S3 和 Amazon EFS 的配置方式与指南一致。默认情况下，客户数据在传输过程中使用 TLS 1.2 进行加密。有关加密和 AWS 的更多信息 DataSync，请参阅 AWS DataSync 功能。客户可以使用监控 DataSync 活动 AWS CloudTrail。有关使用登录的更多信息 CloudTrail，请参阅使用记录 AWS DataSync API 调用 AWS CloudTrail。

AWS Directory Service

适用于微软 AD 的 AWS Directory Service

适用于微软的 AWS Directory Service（企业版）（也称为 AWS Microsoft AD）允许目录感知型工作负载和 AWS 资源使用 AWS 云中的托管活动目录。AWS Microsoft AD 使用 AWS 管理的加密密钥将目录内容（包括包含 PHI 的内容）存储在加密的 Amazon Elastic Block Store 卷中。有关更多信息，请参阅 Amazon EBS 加密。

传入和传出 Active Directory 客户端的数据通过轻量级目录访问协议 (LDAP) 通过客户的亚马逊虚拟私有云 (VPC) 网络传输时，会被加密。如果 Active Directory 客户端位于本地网络中，则流量将通过虚拟专用网络链接或链接传输到客户的 VPC。 AWS Direct Connect

Amazon Cloud Directory

Amazon Cloud Directory 使客户能够构建灵活的云原生目录，用于按多个维度组织数据层次结构。客户还可以为各种用例创建目录，例如组织结构图、课程目录和设备注册表。例如，客户可以创建组织结构图，该图表可以在不同的层次结构中导航，用于报告结构、位置和成本中心。Amazon Cloud Directory 使用由 () 管理的 256 位加密密钥自动加密静态和传输中的数据。 AWS Key Management Service AWS KMS

AWS Elastic Beanstalk

借助 AWS Elastic Beanstalk，客户可以在 AWS 云中快速部署和管理应用程序，而不必了解运行这些应用程序的基础设施。客户只需上传代码并 AWS Elastic Beanstalk 自动处理部署，从容量配置、负载

平衡、自动扩展到应用程序运行状况监控。同时，客户可以完全控制为其应用程序提供支持的 AWS 资源，并且可以随时访问底层资源。

AWS Elastic Beanstalk 本身不存储、传输或处理 PHI。相反，客户可以使用它来构建和部署可能存储、传输和/或处理 PHI 的其他 AWS 服务的架构。客户在选择部署的服务时，应确保仅在 PHI AWS Elastic Beanstalk 中使用符合 HIPAA 条件的服务。有关在这些服务中使用 PHI 的指南，请参阅本白皮书中这些服务的条目。

客户不应在其中的任何自由格式字段（ AWS Elastic Beanstalk 例如 “名称” 字段）中包含 PHI。 AWS Elastic Beanstalk AWS CloudTrail 用于记录所有 API 调用。

AWS 弹性灾难恢复

AWS Elastic 灾难恢复 (AWS DRS) 使用经济实惠的存储、最少的计算和恢复，快速、可靠地 point-in-time 恢复本地和基于云的应用程序，最大限度地减少停机时间和数据丢失。

客户可以在源服务器上设置 AWS Elastic 灾难恢复，以启动安全的数据复制。他们的数据将复制到您的 AWS 账户中他们选择的 AWS 区域的暂存区域子网中。暂存区域的设计通过使用经济实惠的存储和最少的计算资源来维持持续的复制，从而降低了成本。AWS Elastic 灾难恢复复制的客户数据在传输过程中使用 TLS 1.2 进行加密，并直接从其源服务器传输到其 VPC。客户可以利用私有连接（例如 AWS Direct Connect 或 VPN）来配置复制路由。也可以使用 Amazon EBS 加密在 AWS 上对客户数据进行静态加密。

客户可以执行无中断测试以确认实施已完成。在正常操作期间，通过监控复制并定期执行无中断恢复和故障恢复演练，保持就绪状态。如果客户需要恢复应用程序，他们可以在几分钟内在 AWS 上启动恢复实例，使用最多的 up-to-date 服务器状态或之前的时间点。客户应用程序在 AWS 上运行后，他们可以选择将其保留在那里，也可以在问题解决后启动数据复制回主站点。客户可以在准备就绪时回切到其主站点。

AWS Fargate

AWS Fargate 是一种允许客户无需管理服务器或集群即可运行容器的技术。有了 AWS Fargate它，客户不再需要预置、配置和扩展虚拟机集群来运行容器。这样就无需选择服务器类型、决定何时扩展集群或优化集群打包。 AWS Fargate 客户无需与服务器或群集交互或思考服务器或群集。借助 Fargate，客户可以专注于设计和构建应用程序，而不是管理运行应用程序的基础架构。

Fargate 不需要任何其他配置即可处理处理 PHI 的工作负载。客户可以使用 Amazon ECS 等容器编排服务在 Fargate 上运行容器工作负载。Fargate 仅管理底层基础架构，不对正在编排的工作负载中的

数据进行操作。为了符合 HIPAA 的要求，无论何时通过 Fargate 启动的容器访问，PHI 仍应在传输或静止状态下进行加密。本 paper 中描述的每个 AWS 存储选项都提供了多种静态加密机制。有关其他 HIPAA 安全和配置信息，请参阅 Amazon EKS 上的 HIPAA 安全与合规架构白皮书。

AWS Firewall Manager

AWS Firewall Manager 是一项安全管理服务，允许客户在中的客户帐户和应用程序中集中配置和管理防火墙规则 AWS Organizations。随着新应用程序的创建，Firewall Manager 通过强制执行一组通用的安全规则，可以轻松地使新的应用程序和资源合规。现在，客户只需一个中央管理员帐户即可通过单一服务来构建防火墙规则、创建安全策略并以一致的分层方式在整个基础架构中强制执行这些规则。

AWS Firewall Manager 是一种不直接处理、存储或传输用户数据的编排服务。该服务不加密客户内容，但 AWS Firewall Manager 使用的底层服务（例如 DynamoDB）会加密用户数据。

AWS Global Accelerator

AWS Global Accelerator 是一项全球负载平衡服务，可改善多区域应用程序的可用性和延迟。为确保 PHI 在传输过程中和使用时处于静态状态 AWS Global Accelerator，由全球加速器进行负载平衡的架构应使用加密协议，例如 HTTPS 或 SSL/TLS。请参阅 Amazon EC2、Elastic Load Balancing 和其他 AWS 服务的指南，以更好地了解后端资源的可用加密选项。 AWS Global Accelerator AWS CloudTrail 用于记录所有 API 调用。

AWS Glue

AWS Glue 是一项完全托管的 ETL（提取、转换和加载）服务，它使客户可以简单且经济高效地对数据进行分类、清理、丰富数据并在各种数据存储之间可靠地移动数据。为了确保在传输过程中对包含 PHI 的数据进行加密， AWS Glue 应配置为使用 JDBC 连接到具有 SSL/TLS 的数据存储区。此外，为了在传输过程中保持加密，应将服务器端加密 (SSE-S3) 的设置作为参数传递给运行时使用的 ETL 作业。 AWS Glue数据目录中所有静态存储的数据 AWS Glue 都使用在创建数据目录对象 AWS KMS 时启用加密时管理的密钥进行加密。 AWS Glue CloudTrail 用于记录所有 API 调用。

AWS Glue DataBrew

AWS Glue DataBrew 是一项完全托管的可视化数据准备服务，可让数据分析师和数据科学家轻松清理和标准化数据，为分析和机器学习做好准备。为了确保在传输过程中对包含 PHI 的数据进行加密， DataBrew 应配置为使用 JDBC 连接到具有 SSL/TLS 的数据存储区。连接到 JDBC 数据源时，DataBrew 使用您的 AWS Glue 连接上的设置，包括 “需要 SSL 连接” 选项。此外，为了在 S3 存

储桶中保持静态加密，应将服务器端加密（SSE-S3 或 SSE-KMS）的设置作为参数传递给作业。
DataBrew

AWS IoT 核心和 AWS IoT Device Management

AWS IoT 核心并 AWS IoT Device Management 提供联网设备（例如传感器、执行器、嵌入式微控制器或智能设备）与 AWS 云之间的安全双向通信。 AWS IoT Core，现在 AWS IoT Device Management 可以容纳传输包含 PHI 的数据的设备。所有与 AWS IoT Core 的通信均使用 TLS 进行加密。 AWS IoT Device Management AWS IoT 核心并 AWS IoT Device Management AWS CloudTrail 用于记录所有 API 调用。

AWS IoT Greengrass

AWS IoT Greengrass 允许客户以安全的方式为联网设备运行本地计算、消息传递、数据缓存、同步和机器学习推理功能。 AWS IoT Greengrass 使用 X.509 证书、托管订阅、 AWS IoT 策略以及 IAM 策略和角色来确保客户的 Greengrass 应用程序的安全。 AWS IoT Greengrass 使用 AWS IoT 传输安全模型通过 TLS 加密与云的通信。此外， AWS IoT Greengrass 数据在静止时会被加密（在云中）。有关 Greengrass 安全的更多信息，请参阅安全概述。 AWS IoT Greengrass

客户可以使用记录 AWS IoT Greengrass API 操作 AWS CloudTrail。有关更多信息，请参阅使用记录 AWS IoT Greengrass API 调用 AWS CloudTrail。

AWS Lambda

AWS Lambda 让客户无需自行配置或管理服务器即可运行代码。 AWS Lambda 使用由跨区域多个可用区的亚马逊弹性计算云 (Amazon EC2) 实例组成的计算队列，从而提供 AWS 基础设施的高可用性、安全性、性能和可扩展性。

为确保 PHI 在使用时保持加密状态 AWS Lambda，与外部资源的连接应使用加密协议，例如 HTTPS 或 SSL/TLS。例如，当通过 Lambda 过程访问 S3 时，应使用 https://bucket.s3-aws-region.amazonaws.com 进行寻址。

如果任何 PHI 处于静止状态或在运行过程中处于空闲状态，则应使用从或获取的密钥在客户端或服务器端对其进行加密。 AWS KMS AWS CloudHSM通过该服务触发 AWS Lambda 函数时，请按照 Amazon API Gateway 的相关指南进行操作。使用来自其他 AWS 服务的事件触发 AWS Lambda 函数时，事件数据（本身不应包含）PHI。例如，当 Lambda 过程从 S3 事件（例如对象到达 S3）触发时，中继到 Lambda 的对象名称不应包含任何 PHI，尽管该对象本身可以包含此类数据。

AWS Managed Services

AWS Managed Services 提供对 AWS 基础设施的持续管理。通过实施最佳实践来维护客户的基础架构， AWS Managed Services 有助于降低他们的运营开销和风险。 AWS Managed Services 自动执行变更请求、监控、补丁管理、安全和备份服务等常见活动，并为配置、运行和支持基础架构提供完整的生命周期服务。

客户可以使用 AWS Managed Services 来管理使用包含 PHI 的数据运行的 AWS 工作负载。的使用 AWS Managed Services 不会改变有资格与 PHI 一起使用的 AWS 服务。提供的工具和自动化 AWS Managed Services 不能用于 PHI 的存储或传输。

AWS OpsWorks 适用于厨师自动化

AWS OpsWorks for Chef Automate 是一项完全托管的配置管理服务，它托管 Chef Automate，这是一套来自 Chef 的用于基础设施和应用程序管理的自动化工具。该服务本身不包含、传输或处理任何 PHI 或敏感信息，但客户应确保为 Chef Automate 配置的任何资源都与指南保持一致。 OpsWorks API 调用是用捕获的 AWS CloudTrail。有关更多信息，请参阅使用记录 AWS OpsWorks 堆栈 API 调用 AWS CloudTrail。

AWS OpsWorks 适用于木偶企业

AWS OpsWorks for Puppet Enterprise 是一项完全托管的配置管理服务，它托管 Puppet Enterprise，这是一套来自 Puppet 的用于基础设施和应用程序管理的自动化工具。该服务本身不包含、传输或处理任何 PHI 或敏感信息，但客户应确保为 Puppet Enterprise 配置的任何资源都与指南保持一致。 OpsWorksAPI 调用是用捕获的 AWS CloudTrail。有关更多信息，请参阅使用记录 AWS OpsWorks 堆栈 API 调用 AWS CloudTrail。

AWS OpsWorks 堆栈

AWS OpsWorks Stacks 提供了一种简单而灵活的方式来创建和管理堆栈和应用程序。客户可以使用 AWS OpsWorks Stacks 来部署和监控堆栈中的应用程序。

AWS OpsWorks Stacks 会在传输过程中对所有流量进行加密。但是，加密的数据袋（Chef 数据存储机制）不可用，任何必须安全存储的资产，例如 PHI、机密/密码、证书等，都应存储在 Amazon S3 的加密存储桶中。AWS OpsWorks Stack AWS CloudTrail 用于记录所有 API 调用。

AWS Organizations

AWS Organizations 帮助客户在增长和扩展 AWS 资源时集中管理和治理其环境。使用 AWS Organizations，他们可以编程方式创建新的 AWS 账户并分配资源，对账户进行分组以组织其工作流程，将策略应用于账户或群组进行管理，并通过对所有账户使用单一付款方式来简化账单。

此外， AWS Organizations 还与其他 AWS 服务集成，因此客户可以定义中心配置、安全机制、审计要求以及组织内账户间的资源共享。 AWS Organizations 向所有 AWS 客户提供，无需支付额外费用。

AWS Organizations 是一种不直接处理、存储或传输用户数据的编排服务。该服务不加密客户内容，但是在其中启动的底层服务会加密用户数据。 AWS Organizations AWS Organizations 与一项服务集成 AWS CloudTrail，该服务提供用户、角色或 AWS 服务在中执行的操作的记录 AWS Organizations。

AWS RoboMaker

AWS RoboMaker 使客户能够在云中执行用于应用程序开发的代码，并提供机器人仿真服务以加快应用程序测试。AWS RoboMaker 还提供机器人队列管理服务，用于远程应用程序部署、更新和管理。

包含 PHI 的网络流量必须对传输中的数据进行加密。与模拟服务器的所有管理通信均通过 TLS 进行，客户应使用开放标准传输加密机制连接其他 AWS 服务。AWS RoboMaker 还与集成，可将所有 API 调用记录 CloudTrail 到特定的 Amazon S3 存储桶。

AWS RoboMaker 日志不包含 PHI，并且模拟服务器使用的 EBS 卷已加密。将可能包含 PHI 的数据传输到其他服务（例如 Amazon S3）时，客户必须遵循接收服务机构关于存储 PHI 的指导方针。要部署到机器人，客户必须确保传输中和静态数据的加密与他们对指南的解释一致。

AWS 开发工具包指标

企业客户可以使用带有适用于企业支持的 AWS 软件开发工具包指标（SDK 指标）的 AWS CloudWatch 代理，从其主机和客户端上的 AWS 开发工具包中收集指标。这些指标与 AWS Enterprise Support 共享。SDK Metrics 可以帮助客户收集有关其应用程序与 AWS 服务连接的相关指标和诊断数据，而无需在代码中添加自定义工具，并减少与之共享日志和数据所需的手动工作 AWS 支持。

请注意，软件开发工具包指标仅适用于订阅 Enterprise Support 的 AWS 客户。客户可以将软件开发工具包指标用于任何直接调用 AWS 服务且使用 AWS 开发工具包构建的应用程序，该软件开发工具包指标是 AWS 指标文档中列出的版本之一。

SDK Metrics 监控由 AWS 开发工具包发出的调用，并使用与客户端应用程序在相同环境中运行的 CloudWatch 代理。

CloudWatch 代理对从本地计算机传输到目标日志组中的数据进行加密。可以按照使用加密日志中的日志数据中的 CloudWatch 说明将日志组配置为加密 AWS KMS。

AWS Secrets Manager

AWS Secrets Manager 是一项 AWS 服务，可让客户更轻松地管理 “机密”。密钥可以是数据库凭证、密码、第三方 API 密钥，甚至是任意文本。 AWS 如果此类信息包含在 “机密” 中，则可以使用 Secrets Manager 来存储 PHI。Secrets Manager 存储的所有 AWS 密钥均使用 AWS 密钥管理系统 (KMS) 进行静态加密。用户可以选择创建新 AWS KMS 密钥时使用的密钥。如果未选择任何密钥，则将使用账户的默认密钥。 AWS Secrets Manager 用于 AWS CloudTrail 记录所有 API 调用。

AWS Security Hub CSPM

AWS Security Hub CSPM 收集并整合客户环境中启用的 AWS 安全服务的调查结果，例如来自亚马逊的入侵检测结果、Amazon Inspector 的漏洞扫描 GuardDuty、Amazon Macie 的 Amazon S3 存储桶策略发现、IAM Access Analyzer 提供的可公开访问的跨账户资源，以及缺少 WAF 覆盖的资源。AWS Firewall Manager AWS Security Hub CSPM 还整合了集成 AWS 合作伙伴网络 (APN) 安全解决方案的发现。

AWS Security Hub CSPM 与 Amazon E CloudWatch vents 集成，使客户能够创建自定义的响应和补救工作流程。客户可以轻松地将调查结果发送到 SIEM、聊天工具、票务系统、安全编排自动化和响应 (SOAR) 工具以及待命管理平台。响应和补救操作可以完全自动化，也可以在控制台中手动触发。客户还可以使用 AWS Systems Manager Automation 文档和 AWS Lambda 函数来构建可从中启动的自动修复工作流程 AWS Security Hub CSPM。 AWS Step Functions

为确保数据保护， AWS Security Hub CSPM 对静态数据和组件服务之间传输的数据进行加密。 AWS Security Hub CSPM 作为多个 AWS 合规计划的一部分，第三方审计师会评估其安全性和合规性。AWS Security Hub CSPM 是 AWS 的 SOC、ISO、PCI 和 HIPAA 合规计划的一部分。

AWS 服务器迁移服务

AWS 服务器迁移服务 (AWS SMS) Migration 可自动将本地 VMware vSphere 或微软 Hyper-v/SCVMM 虚拟机迁移到 AWS 云。AWS SMS 以增量方式将服务器虚拟机复制为云托管的亚马逊系统映像 (AMI)，准备在 Amazon EC2 上部署。

在本地运行并通过 (AWS SMS) 迁移到云端的服务器可以包含 PHI 数据。AWS SMS 会在传输过程中以及暂存服务器 VM 映像以便最终放置到 EC2 上时对数据进行加密。使用 AWS SMS 迁移包含 PHI 的服务器虚拟机时，请参阅 EC2 指南和设置加密存储卷。AWS SMS CloudTrail 用于记录所有 API 调用。

AWS Serverless Application Repository

AWS Serverless Application Repository (SAR) 是用于无服务器应用程序的托管存储库。它使团队、组织和个人开发人员能够存储和共享可重复使用的应用程序，并以强大的新方式轻松组装和部署无服务器架构。应用程序是 CloudFormation 模板，其中包含应用程序基础架构的定义和应用程序 AWS Lambda 功能代码的编译二进制文件。

尽管处于 PHI 中的应用程序可以处理 PHI，但它们只有在部署到客户账户后才会执行此操作，而不是作为 SAR 本身的一部分。 AWS Serverless Application Repository AWS Serverless Application Repository 加密客户上传的文件，包括部署包和图层存档。对于传输中的数据， AWS Serverless Application Repository 使用 TLS 对服务和代理之间的数据进行加密。 AWS Serverless Application Repository 与集成 AWS CloudTrail，后者是一项服务，用于记录用户、角色或 AWS 服务在中执行的操作 AWS Serverless Application Repository。

服务目录

Service Catalog 允许 IT 管理员创建、管理和向最终用户分发经批准的产品组合，然后最终用户可以在个性化门户中访问所需的产品。Service Catalog 用于在 AWS 上编目、共享和部署自助服务解决方案，不能用于存储、传输或处理 PHI。不应将 PHI 放在 Service Catalog 项目的任何元数据中或任何项目描述中。Service Catalog 用于 AWS CloudTrail 记录所有 API 调用。

AWS Shield

AWS Shield 是一项托管分布式拒绝服务 (DDoS) 保护服务，可保护在 AWS 上运行的 Web 应用程序。AWS Shield 提供始终在线检测和自动内联缓解措施，可最大限度地减少应用程序停机时间和延迟，因此无需参与即可从 DDoS 保护中 AWS 支持 受益。

AWS Shield 不能用于存储或传输 PHI，但可以用来保护使用 PHI 运行的 Web 应用程序。因此，在接合时无需进行特殊配置 AWS Shield。

所有 AWS 客户均可享受自动保护 AWS Shield Standard，无需支付额外费用。 AWS Shield Standard 防御针对其网站或应用程序的最常见、最常见的网络和传输层 DDoS 攻击。要获得更高级别的保护，

抵御针对在 Elastic Load Balancing (ELB) CloudFront、Amazon 和 Amazon Route 53 资源上运行的 Web 应用程序的攻击，客户可以订阅。 AWS Shield Advanced

AWS Snowball Edge

借助 AWS Snowball Edge (Snowball)，客户可以在本地数据中心和亚马逊简单存储服务 (Amazon S3) 之间传输数百 TB 或 PB 的数据。存储在中的 PHI AWS Snowball Edge 必须按照《指南》进行静态加密。创建导入任务时，客户必须为用于保护 Snowball 中数据的 AWS KMS 密钥指定 ARN。此外，在创建导入任务期间，客户应选择符合指南设定的加密标准的目标 S3 存储桶。

虽然 Snowball 目前不支持使用 AWS KMS托管密钥进行服务器端加密 (SSE-KMS) 或使用客户提供的密钥进行服务器端加密 (SSE-C)，但 Snowball 确实支持使用亚马逊 S3 托管的加密密钥进行服务器端加密 (SSE-S3)。有关更多信息，请参阅使用服务器端加密与 Amazon S3 托管加密密钥 (SSE-S3) 保护数据。

或者，客户可以在将数据存储到之前使用自己选择的加密方法对 PHI 进行加密 AWS Snowball Edge。

目前，客户可以将标准 AWS Snowball Edge 设备作为我们的 BAA 的一部分使用。

AWS Snowball Edge 边缘

AWS Snowball Edge Edge 使用标准存储接口连接到现有的客户应用程序和基础架构，从而简化了数据传输过程并最大限度地减少了设置和集成。Snowball Edge 可以聚集在一起形成本地存储层并在现场处理客户数据，从而帮助客户确保即使无法访问云，他们的应用程序也能继续运行。

为确保 PHI 在使用 Snowball Edge 时保持加密状态，客户在使用由 AWS IoT Greengrass 支持的 AWS Lambda 程序与 Snowball Edge 外部资源之间传输 PHI 时，应确保使用加密的连接协议，例如 HTTPS 或 SSL/TLS。此外，PHI 存储在 Snowball Edge 的本地卷上时，应通过本地访问或通过 NFS 进行加密。使用 Snowball 管理控制台和 API 将加密自动应用于放入 Snowball Edge 的数据，以便批量传输到 Snowball Edge 中。有关将数据传输到 S3 的更多信息，请参阅的相关指南the section called “AWS Snowball Edge”。

AWS Step Functions

AWS Step Functions 使用可视化工作流可以轻松协调分布式应用程序和微服务的组件。 AWS Step Functions 无法存储、传输或处理 PHI。不应将 PHI 放在任何任务 AWS Step Functions 或状态机定义的元数据中或之内。 AWS Step Functions AWS CloudTrail 用于记录所有 API 调用。

AWS Storage Gateway

AWS Storage Gateway 是一项混合存储服务，可让客户的本地应用程序无缝使用 AWS 云存储。该网关使用开放标准存储协议将现有存储应用程序和工作流程连接到 AWS 云存储服务，从而最大限度地减少流程中断。

文件网关

文件网关 AWS Storage Gateway 是一种支持 Amazon S3 文件接口的类型，它可以添加到当前基于块的卷和 VTL 存储空间中。文件网关使用 HTTPS 与 S3 通信，并存储在 S3 上加密的所有对象，默认情况下使用 SSE-S3，或者使用客户端加密（密钥存储在中 AWS KMS）。文件元数据（例如文件名）仍未加密，不应包含任何 PHI。

卷网关

Volume gateway 提供支持云的存储卷，客户可以将其作为互联网小型计算机系统接口 (iSCSI) 设备从本地应用程序服务器进行安装。客户应根据其内部合规性和监管要求将本地磁盘作为上传缓冲区和缓存连接到 Volume Gateway 虚拟机。建议对于 PHI，这些磁盘应能够提供静态加密。Volume Gateway VM 和 AWS 之间的通信使用 TLS 1.2 进行加密，以保护传输中的 PHI。

磁带网关

磁带网关为本地运行的第三方备份应用程序提供了 VTL（虚拟磁带库）接口。设置磁带备份任务时，客户应在第三方备份应用程序中启用对 PHI 的加密。Tape Gateway VM 和 AWS 之间的通信使用 TLS 1.2 进行加密，以保护传输中的 PHI。在 PHI 中使用任何 Storage Gateway 配置的客户都应启用完整日志记录。有关更多信息，请参阅什么是 AWS Storage Gateway？。

AWS Systems Manager

AWS Systems Manager 是一个统一的界面，允许客户轻松地集中运营数据，自动执行其 AWS 资源中的任务，并缩短检测和解决基础设施中操作问题的时间。Systems Manager 提供了客户基础架构性能和配置的完整视图，简化了资源和应用程序管理，并使其易于大规模操作和管理其基础架构。

将可能包含 PHI 的数据输出到其他服务（例如 Amazon S3）时，客户必须遵循接收服务机构关于存储 PHI 的指导方针。客户不应在元数据或标识符（例如文档名称和参数名称）中包含 PHI。

AWS Transfer for SFTP

AWS Transfer for SFTP 提供对客户的 S3 资源的安全文件传输协议 (SFTP) 访问权限。客户将看到一台虚拟服务器，可在区域服务端点使用标准 SFTP 协议访问该服务器。从 AWS 客户和 SFTP 客户端的角度来看，SFTP 网关看起来像一台标准的、高度可用的 SFTP 服务器。尽管服务本身并不存储、处理或传输 PHI，但客户在 Amazon S3 上访问的资源应按照与指南一致的方式进行配置。客户还可以使用记录向 AWS T AWS CloudTrail ransfer for SFTP 发出的 API 调用。

AWS WAF — Web 应用程序防火墙

AWS WAF 是一款 Web 应用程序防火墙，可帮助保护客户的 Web 应用程序免受常见 Web 漏洞的侵害，这些漏洞可能会影响应用程序可用性、危及安全性或消耗过多资源。客户可以将 AWS WAF 放在 AWS 上托管的、与 PHI 一起运行或交换 PHI 的 Web 应用程序与其最终用户之间。与在 AWS 上传输任何 PHI 一样，包含 PHI 的数据在传输过程中必须进行加密。请参阅 Amazon EC2 指南，以更好地了解可用的加密选项。

AWS X-Ray

AWS X-Ray 是一项服务，它收集有关客户应用程序所服务的请求的数据，并提供工具，供他们查看、筛选和深入了解这些数据，以识别问题和优化机会。对于对客户应用程序的任何追踪请求，他们不仅可以查看有关请求和响应的详细信息，还可以查看其应用程序对下游 AWS 资源、微服务、数据库和 HTTP Web API 的调用的详细信息。 AWS X-Ray 不应用于存储或处理 PHI。默认情况下，传入和传出的信息 AWS X-Ray 是加密的。使用时 AWS X-Ray，请勿在区段注释或区段元数据中放置任何 PHI。

Elastic Load Balancing

客户可以使用 Elastic Load Balancing 来终止和处理包含 PHI 的会话。客户可以选择 Classic Load Balancer 或 Application 负载均衡器。由于所有包含 PHI 的网络流量在传输过程中都必须进行加密 end-to-end，因此客户可以灵活地实施两种不同的架构：

通过创建使用加密连接协议的负载均衡器，客户可以在 Elastic Load Balancing 上终止 HTTPS、通过 TLS 的 HTTP/2（适用于应用程序）或 SSL/TLS。此功能支持负载均衡器与启动 HTTPS、通过 TLS 的 HTTP/2 或 SSL/TLS 会话的客户端之间的流量加密，以及对负载均衡器与客户后端实例之间的连接进行流量加密。包含 PHI 的会话必须加密前端和后端侦听器才能进行传输加密。客户应评估其证书和会话谈判政策，并使其与指南保持一致。有关更多信息，请参阅 C lassic Load Balancer 的 HTTPS 侦听器。

或者，客户可以将 Amazon ELB 配置为基本 TCP 模式（适用于经典）或更高模式 WebSockets （适用于应用程序），并将加密会话传递到终止加密会话的后端实例。在此架构中，客户在自己的实例中运行的应用程序中管理自己的证书和 TLS 协商策略。有关更多信息，请参阅 C lassic Load Balancer 的监听器。在这两种架构中，客户都应实现他们认为符合 HIPAA 和 HITECH 要求的日志级别。

FreeRTOS

FreeRTOS 是一款适用于微控制器的操作系统，它使小型低功耗边缘设备易于编程、部署、保护、连接和管理。FreeRTOS 基于 FreeRTOS 内核，这是一种流行的微控制器开源操作系统，并通过软件库对其进行了扩展，可以轻松地将小型低功耗设备安全地连接到 Core 等 AWS 云服务 AWS IoT 或运行的更强大的边缘设备。 AWS IoT Greengrass

现在，当使用运行 FreeRTOS 的合格设备时，包含 PHI 的数据可以在传输过程中和静态时进行加密。FreeRTOS 提供了两个库来提供平台安全：TLS 和 PKCS #11. 应使用 TLS API 对包含 PHI 的所有网络流量进行加密和身份验证。PKCS #11 为软件加密操作提供了标准接口，应用于加密运行 FreeRTOS 的合格设备上存储的任何 PHI。

AWS KMS 用于对 PHI 进行加密

KMS 密钥可用于加密/解密用于在客户应用程序或使用的 AWS 服务中加密 PHI 的数据加密密钥。AWS KMS AWS KMS 可以与 HIPAA 账户一起使用，但是 PHI 只能在符合 HIPAA 条件的服务中处理、存储或传输。 AWS KMS 通常用于为在其他 HIPAA 合格服务中运行的应用程序生成和管理密钥。

例如，在 Amazon EC2 中处理 PHI 的应用程序可以使用 GenerateDataKey API 调用生成数据加密密钥，用于在应用程序中加密和解密 PHI。数据加密密钥将受到存储在中的客户的 KMS 密钥的保护 AWS KMS，从而在 API 调用登录时创建高度可审计的密钥层次结构。 AWS KMS AWS CloudTrail PHI 不应存储在中存储的任何密钥的标签（元数据）中 AWS KMS。

VM Import/Export

VM Import/Export 使客户能够轻松地将虚拟机映像从现有环境导入到 Amazon EC2 实例，然后将其导出回您的本地环境。该产品允许客户利用您为满足 iRIT 安全、配置管理和合规要求而构建的虚拟机的现有投资，将这些虚拟机作为 ready-to-use 实例引入 Amazon EC2。客户还可以将导入的实例导回其本地虚拟化基础架构，从而允许他们在您的 IT 基础架构中部署工作负载。

除了 Amazon EC2 和 Amazon S3 的标准使用费外，虚拟机导入/导出无需支付额外费用。

要导入客户映像，客户可以使用 AWS CLI 或其他开发人员工具从其 VMware 环境中导入虚拟机 (VM) 映像。如果客户使用 VMware vSphere 虚拟化平台，他们还可以使用适用于 vCenter 的

AWS 管理门户网站来导入虚拟机。作为导入过程的一部分，VM Import 会将客户的虚拟机转换为 Amazon EC2 AMI，他们可以用它来运行亚马逊 EC2 实例。导入虚拟机后，他们就可以通过 Auto Scaling、Elastic Load Balancing 等产品利用 Amazon 的弹性、可扩展性和监控功能，并支持导入的映像。 CloudWatch

客户可以使用亚马逊 EC2 API 工具导出之前导入的亚马逊 EC2 实例。只需指定目标实例、虚拟机文件格式和目标 Amazon S3 存储桶，VM Import/Export 就会自动将该实例导出到 Amazon S3 存储桶，并提供加密选项，以保护其虚拟机映像的传输和存储。然后，客户可以在本地虚拟化基础架构中下载并启动导出的虚拟机。

客户可以导入使用 VMware ESX 或 Workstation、Microsoft Hyper-V 和 Citrix Xen 虚拟化格式的 Windows 和 Linux 虚拟机。客户可以将之前导入的亚马逊 EC2 实例导出为 VMware ESX、Microsoft Hyper-V 或 Citrix Xen 格式。有关支持的操作系统、版本和格式的完整列表，请参阅虚拟机导入/导出要求。AWS 计划将来增加对其他操作系统、版本和格式的支持。

审计、备份和灾难恢复

HIPAA 的《安全规则》对深入的审计能力、数据备份程序和灾难恢复机制有详细的要求。AWS 中的服务包含许多功能，可帮助客户满足其需求。例如，客户应考虑建立审计功能，允许安全分析师检查详细的活动日志或报告，以了解谁有权访问、IP 地址输入、访问了哪些数据等。

在进行审计时，应长时间跟踪和记录这些数据，并将其存储在中央位置。使用 Amazon EC2，客户可以在虚拟服务器上运行活动日志文件并向下审核到数据包层，就像在传统硬件上一样。他们还可以跟踪到达其虚拟服务器实例的任何 IP 流量。客户的管理员可以将日志文件备份到 Amazon S3 中，以实现长期可靠的存储。

HIPAA 还对维护应急计划以在紧急情况下保护数据有详细要求，并且必须创建和维护可检索的电子 PHI 的精确副本。为了在 AWS 上实施数据备份计划，Amazon EBS 为 Amazon EC2 虚拟服务器实例提供了永久存储。这些卷可以作为标准块设备公开，它们提供独立于实例生命周期的非实例存储。为了符合 HIPAA 指南，客户可以创建 Amazon EBS 卷的 point-in-time快照，这些快照会自动存储在 Amazon S3 中，并在多个可用区之间进行复制，这些可用区是为防止其他可用区出现故障而设计的不同位置。

这些快照可以随时访问，并且可以保护数据以实现长期持久性。Amazon S3 还为数据存储和自动备份提供了高度可用的解决方案。只需将文件或图像加载到 Amazon S3 中，即可自动创建多个冗余副本并将其存储在不同的数据中心中。这些文件可以随时随地访问（视权限而定），并且会一直存储到故意删除为止。

此外，AWS 本质上提供了各种灾难恢复机制。灾难恢复是在灾难发生时保护组织数据和IT基础设施的过程，它涉及维护高度可用的系统，将数据和系统复制到异地，以及实现对两者的持续访问。

借助 Amazon EC2，管理员可以非常快速地启动服务器实例，并且可以使用弹性 IP 地址（云计算环境的静态 IP 地址）实现从一台机器到另一台机器的平滑故障转移。亚马逊 EC2 还提供可用区。管理员可以在多个可用区启动 Amazon EC2 实例，以创建地理位置多样的容错系统，这些系统在出现网络故障、自然灾害和大多数其他可能的停机源时具有很强的弹性。

使用 Amazon S3，客户的数据会被复制并自动存储在不同的数据中心中，以提供可靠的数据存储，旨在提供 99.99% 的可用性。

使用 AWS Elastic 灾难恢复 (AWS DRS)，客户可以快速恢复 AWS 上的应用程序，无论是在应用程序的最高 up-to-date 状态下，还是从较早的时间点恢复。

文档修订

如需获取有关该白皮书更新的通知，请订阅 RSS 信息源。

变更	说明	日期
次要更新	次要更新	2023 年 5 月 12 日
次要更新	更新了白皮书，扩展了有关服务的可用内容。	2022 年 9 月 28 日
次要更新	修复非包容性语言。	2022 年 4 月 6 日
已更新白皮书	添加了有关 AWS 应用程序迁移服务的信息，并更新了 Amazon ECS 的信息	2021 年 12 月 6 日
已更新白皮书	亚马逊 Healthlake 和 Amazon VPC 部分中的更新信息	2021 年 11 月 9 日
已更新白皮书	添加了有关 AWS Network Firewall 的信息	2021 年 9 月 9 日
已更新白皮书	有关 Amazon Connect 客户资料的更新信息	2021 年 8 月 26 日
已更新白皮书	添加了 “亚马逊” AppFlow 和 “AWS Glue” 章节 DataBrew	2021 年 7 月 22 日
已更新白皮书	更新了导航和组织结构。	2021 年 4 月 26 日
已更新白皮书	添加了以下章节： AWS CodeDeploy、、亚马逊 Aurora AWS CodePipel ine、Aurora PostgreSQL、亚马逊 Textract、Amazon Polly、亚马逊 FSx、AWS A AWS Backup AWS Elastic Beanstalk uto Scaling、、	2021 年 3 月 31 日

	、、、、、、、、、VM 导入/导 AWS Firewall Manager出 AWS Organizations、亚马逊 AWS Security Hub CSPM AWS Serverless Application Repository、亚马逊。HealthLake EventBridge更新了亚马逊 Aurora 版块。	
已更新白皮书	添加了有关 AWS App Mesh 的章节，并更新了 AWS 系统管理器内容	2020 年 8 月 25 日
已更新白皮书	增加了亚马逊 Appstream 2.0、AWS SDK 指标、AWS Data Exchange、亚马逊 MSK、亚马逊 Pinpoint、Amazon Lex、Amazon SES 和亚马逊预测、亚马逊量子账本数据库 (QLDB) 等章节。AWS Cloud Map	2020 年 5 月 7 日

已更新白皮书	增加了关于亚马逊 CloudWatch、亚马逊 CloudWatch 活动、亚马逊 Data Firehose、适用于 Apache Flink 的亚马逊托管服务、亚马逊服务、亚马 OpenSearch 逊 DocumentDB（兼容 MongoDB）、AWS Mobile Hub、 AWS OpsWorks Chef Automate、Puppet Enterprise、AWS AWS IoT Greengrass Transfer、AWS、AWS、Amazon Comprehend Medical 的章节 AWS DataSync。AWS OpsWorks AWS Global Accelerator RoboMaker	2020 年 1 月 1 日
已更新白皮书	增加了关于亚马逊 Comprehend、Amazon Transcribe、Amazon Translate 和 AWS Certificate Manager 的章节。	2019年1月1日
已更新白皮书	增加了关于亚马逊 Athena、亚马逊 AWS IoT EKS、 AWS IoT Device Management Core 和 Amazon FreeRTOS、亚马逊、 GuardDuty亚马逊 Neptune、AWS 服务器迁移 AWS Database Migration Service服务、亚马逊 MQ 和的章节。 AWS Glue	2018 年 11 月 1 日

已更新白皮书	添加了有关亚马逊 Elastic File System (EFS)、亚马逊 Kinesis Video Streams、亚马逊 Rekognition、 SageMaker 亚马逊、亚马逊简单工作流程、AWS 机密管理、服务目录和的章节。 AWS Step Functions	2018 年 6 月 1 日
已更新白皮书	添加了有关 AWS CloudFormation、、、 AWS X-Ray、AWS CloudTrail AWS CodeBuild AWS CodeCommit AWS Config、和 AWS OpsWorks Stack 的章节。	2018年4月1日
已更新白皮书	添加了关于的章节 AWS Fargate。	2018年1月1日

2018 年之前的更新：

Date	描述
2017 年 11 月	添加了有关亚马逊 EC2 容器注册表、亚马逊 Macie QuickSight、亚马逊和的章节。 AWS Managed Services
2017 年 11 月	在亚马逊上添加了 ElastiCache 适用于 Redis 和亚马逊 CloudWatch的章节。
2017 年 10 月 日	添加了有关亚马逊 SNS、 AWS Storage Gateway亚马逊 Route 53 和的章节。 AWS CloudHSM更新了关于的章节 AWS Key Management Service。
2017 年 9 月	添加了有关 Amazon Connect、Amazon Kinesis Streams、亚马逊 RDS (Maria) 数据库、亚

Date	描述
	马逊 RDS SQL Server AWS Batch、 AWS Lambda、 AWS Snowball Edge 、Edge 和亚马逊的 Lambda @Edge 功能的章节。 CloudFront
2017 年 8 月	添加了有关亚马逊 EC2 Systems Manager 和亚马逊 Inspector 的章节。
2017 年 7 月	增加了关于亚马逊 WorkSpaces、亚马逊 WorkDocs、AWS Directory Service 和亚马逊 ECS 的章节。
2017 年 6 月	添加了有关亚马逊 CloudFront、AWS WAF 和亚马逊 S3 Transfer A AWS Shield cceleration 的章节。
2017 年 5 月 日	删除了在 EC2 和 EMR 中处理 PHI 时对专用实例或专用主机的要求。
2017 年 3 月 日	更新了服务列表，指向按合规性计划划分的范围内的 AWS 服务页面。添加了亚马逊 API Gateway 的描述。
2017 年 1 月	已更新为最新模板。
2016 年 10 月 日	首次发布

版权声明

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。