AWS 白皮書

Amazon Web Services 上的 HIPAA 安全與合規架構

Amazon Web Services 上的 HIPAA 安全與合規架構: AWS 白皮書

Table of Contents

Amazon Web Services 上的 HIPAA 安全與合規架構

出版日期：二 ○ 二二年九月二十八文件修訂日

本白 paper 簡要概述客戶如何使用 Amazon Web Services (AWS) 執行受美國 Health 保險可攜性與責任法案 (HIPAA) 規範的敏感工作負載。我們將著重於用於保護受保護 Health 資訊 (PHI) 的 HIPAA 隱私權和安全規則、如何使用 AWS 加密傳輸中和靜態資料，以及如何使用 AWS 功能執行包含 PHI 的工作負載。

簡介

1996 年的《Health 保險可攜性和責任法案》（HIPAA）適用於「承保實體」和「商業夥伴」。HIPAA 在 2009 年通過《經濟和臨床 Health 衛生 Health 信息技術（HITECH）法案》進行了擴展。

HIPAA 和 HITECH 制定了一套旨在保護 PHI 安全和隱私的聯邦標準。HIPAA 和 HITECH 施加了與使用和披露受保護的健康信息（PHI）相關的要求，適當的保護措施來保護 PHI，個人權利和行政責任。有關 HIPAA 和 HITECH 的更多信息，請訪問 Health 資訊隱私首頁。

涵蓋的實體及其商業夥伴可以使用 Amazon Web Services (AWS) 提供的安全、可擴展、低成本的 IT 元件來架構符合 HIPAA 和 HITECH 合規要求的應用程式。AWS 提供的 commercial-off-the-shelf基礎設施平台具備業界認可的認證和稽核，例如 ISO 27001、FedRAMP 和服務組織控制報告 (SOC1、SOC2 和 SOC 3)。AWS 服務和資料中心具有多層操作和實體安全性，有助於確保客戶資料的完整性和安全性。AWS 不需要最低費用、不需符合期限的合約和 pay-as-you-use 定價，是適用於不斷成長的醫療保健產業應用程式的可靠且有效的解決方案。

AWS 可讓受 HIPAA 規範的涵蓋實體及其商業夥伴安全地處理、存放和傳輸 PHI。此外，自 2013 年 7 月起，AWS 為此類客戶提供標準化的商業夥伴增補合約 (BAA)。執行 AWS BAA 的客戶可以在指定為 HIPAA 帳戶的帳戶中使用任何 AWS 服務，但只能使用 AWS BAA 中定義的符合 HIPAA 資格的服務來處理、存放和傳輸 PHI。如需這些服務的完整清單，請參閱 HIPAA 合格服務參考頁面。

AWS 維護符合標準的風險管理計劃，以確保符合 HIPAA 資格的服務特別支援 HIPAA 管理、技術和實體保護措施。使用這些服務來存放、處理和傳輸 PHI，可協助我們的客戶和 AWS 解決適用於 AWS 公用程式作業模型的 HIPAA 要求。

AWS 的 BAA 要求客戶根據 Health 與公共服務部長 (HHS) 的指導，將使用符合 HIPAA 資格的服務儲存或傳輸的 PHI 加密：未經授權的個人無法使用、無法讀取或不可辨識 (以下簡稱「指南」)。請參閱本網站，因為它可能會被更新，並且可能在 HHS 指定的繼任者（或相關）網站上提供。

AWS 提供一組全面的功能和服務，可讓 PHI 的金鑰管理和加密變得容易管理，而且更易於稽核，包括 AWS Key Management Service (AWS KMS)。符合 HIPAA 合規要求的客戶在滿足 PHI 加密要求方面具有極大的彈性。

在決定如何實作加密時，客戶可以評估並利用符合 HIPAA 資格服務的原生加密功能。或者，客戶可以通過符合 HHS 指導的其他方式滿足加密要求。

AWS 中 PHI 的加密和保護

HIPAA 安全性規則包含可定址的實作規格，用於在傳輸（「傳輸中」）和儲存（「靜態」）中 PHI 加密。雖然這是 HIPAA 中的可定址實作規格，但 AWS 要求客戶根據衛生與人類服務部長 (HHS) 的指導，加密存放在或使用 HIPAA 合格服務傳輸的 PHI：呈現不安全的受保護 Health 資訊無法使用、無法讀取或無法辨識給未經授權的個人 (以下稱「指導」)。請參閱本網站，因為它可能會被更新，並且可能在 HHS 指定的繼任者（或相關網站）上提供。

AWS 提供一組全面的功能和服務，可讓 PHI 的金鑰管理和加密變得容易管理，而且更易於稽核，包括 AWS Key Management Service (AWS KMS)。符合 HIPAA 合規要求的客戶在滿足 PHI 加密要求方面具有極大的彈性。

在決定如何實作加密時，客戶可以評估並利用符合 HIPAA 資格服務的原生加密功能，或透過符合 HHS 指引的其他方式來滿足加密需求。以下各節提供有關在每個符合 HIPAA 資格的服務中使用可用加密功能以及其他加密 PHI 模式的高階詳細資訊，以及如何使用 AWS KMS 來加密用於 AWS 上 PHI 加密的金鑰。

主題

- Amazon API Gateway
- Amazon AppFlow
- Amazon AppStream 2.0
- Amazon Athena
- Amazon Aurora
- Amazon Aurora PostgreSQL
- Amazon CloudFront
- Amazon CloudWatch
- Amazon CloudWatch 活動
- Amazon CloudWatch 日誌
- Amazon Comprehend
- Amazon Comprehend Medical
- Amazon Connect
- Amazon DocumentDB (with MongoDB compatibility)

- 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)
- Amazon ElastiCache 的雷迪斯
- Amazon OpenSearch 服務
- Amazon EMR
- Amazon EventBridge
- Amazon Forecast
- Amazon FSx
- Amazon GuardDuty
- Amazon HealthLake
- Amazon Inspector
- Amazon Managed Service for Apache Flink
- Amazon 數據 Firehose
- Amazon Kinesis Streams
- Amazon Kinesis Video Streams
- Amazon Lex
- Amazon Managed Streaming for Apache Kafka (Amazon MSK)
- Amazon MQ
- Amazon Neptune
- AWS Network Firewall
- 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
- 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 應用程式遷移
- 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 彈性災難復原
- AWS Fargate
- AWS Firewall Manager
- AWS Global Accelerator
- AWS Glue
- AWS Glue DataBrew
- AWS IoT 核心與 AWS IoT Device Management
- AWS IoT Greengrass
- AWS Lambda
- AWS Managed Services
- AWS OpsWorks 廚師自動化
- AWS OpsWorks 對於木偶企業
- AWS OpsWorks 堆疊

- AWS Organizations
- AWS RoboMaker
- AWS 開發套件指標
- AWS Secrets Manager
- AWS Security Hub
- AWS Server Migration Service
- AWS Serverless Application Repository
- Service Catalog
- AWS Shield
- AWS Snowball
- AWS Snowball 邊
- AWS Step Functions
- AWS Storage Gateway
- AWS Systems Manager
- AWS Transfer for SFTP
- AWS WAF — 網路應用程式防火牆
- AWS X-Ray
- Elastic Load Balancing
- FreeRTOS
- 用 AWS KMS 於 PHI 的加密
- VM Import/Export

Amazon API Gateway

客戶可以使用 Amazon API Gateway 來處理和傳輸受保護的醫療資訊 (PHI)。雖然 Amazon API Gateway 會在執行中自動使用 HTTPS 端點進行加密，但客戶也可以選擇在用戶端加密承載。API Gateway 會透過記憶體傳遞所有非快取資料，而不會將其寫入磁碟。客戶可以透過 API Gateway 使用 AWS 簽名版本 4 進行授權。如需詳細資訊，請參閱下列內容：

- Amazon API Gateway 常見問答集：安全和授權

- 在 API Gateway 中控制和管理對 REST API 的存取

客戶可以與任何連接到 API Gateway 的服務進行整合，前提是在涉及 PHI 時，該服務的配置與指導和 BAA 一致。如需將 API Gateway 與後端服務整合的相關資訊，請參閱在 API Gateway 中設定 REST API 方法。

客戶可以使用 AWS CloudTrail 和 Amazon 啟 CloudWatch 用與其記錄需求一致的記錄功能。確保透過 API Gateway 傳送的任何 PHI (例如在標頭、URL 和要求/回應中) 只能由符合 HIPAA 資格的服務擷取，且已設定為符合指引的服務。如需使用 API Gateway 進行記錄的詳細資訊，請參閱如何啟用記 CloudWatch 錄以疑難排解我的 API Gateway REST API 或 WebSocket API？

Amazon AppFlow

Amazon AppFlow 是一種全受管的整合服務，可讓客戶在 Salesforce、Marketo、Slack 等 S oftware-as-a 服務 (SaaS) 應用程式之間安全地傳輸資料，以及 ServiceNow Amazon S3 和亞馬 Amazon Redshift 等 AWS 服務。 AppFlow 可以按照客戶選擇的頻率執行資料流程 (依排程、回應商務事件或隨需)。客戶還可以設定篩選和驗證等資料轉換功能，以產生豐富的 ready-to-use 資料作為流程本身的一部分，而無需執行其他步驟。

Amazon AppFlow 可用於處理和傳輸包含 PHI 的數據。預設情況下，使用 TLS 1.2 或更新版本提供 AppFlow 與設定來源/目的地之間傳輸時的資料加密。S3 中存放的靜態資料會使用客戶指定的 AWS KMS 金鑰 (先前稱為 CMK) 自動加密。對於傳輸至非 S3 目的地的 PHI 資料，客戶必須確保所選目的地的靜態儲存符合其安全需求。 AppFlow 透過整合 AWS CloudTrail 以記錄 API 呼叫和 Amazon 發出流程執行事件， EventBridge 以啟用應用程式監控。

Amazon AppStream 2.0

Amazon AppStream 2.0 是全受管的應用程式串流服務。客戶擁有自己的資料，並且必須以符合其法規需求的方式設定必要的 Windows 應用程式。客戶可以透過「主資料夾」設定持續性儲存裝置。傳輸中的檔案和資料夾會使用 Amazon S3 的 SSL 端點進行加密。檔案和資料夾使用 Amazon S3 管理的加密金鑰進行靜態加密。如需詳細資訊，請參閱啟用和管理 AppStream 2.0 使用者的持續性儲存體如果客戶選擇使用協力廠商儲存解決方案，他們必須負責確保該解決方案的組態與指導方針一致。所有與 Amazon AppStream 2.0 的公共 API 通信都使用 TLS 進行加密。如需詳細資訊，請參閱 Amazon AppStream 2.0 文件。

Amazon AppStream 2.0 與這項服務整合在一起 AWS CloudTrail，可在客戶的 AWS 帳戶中記錄由 Amazon 2.0 或代表 Amazon AppStream 2.0 發出的 API 呼叫，並將日誌檔交付到指定的 Amazon S3

儲存貯體。 CloudTrail 擷取從 Amazon AppStream 2.0 主控台或 Amazon 2.0 API 進行的 API 呼叫。AppStream 客戶也可以使用 Amazon CloudWatch 記錄資源使用量指標。如需詳細資訊，請參閱使用監控 Amazon AppStream 2.0 資源和記錄 AppStream 2.0 API 呼叫 AWS CloudTrail。

Amazon Athena

Amazon Athena 是一種互動式查詢服務，可在 Amazon Simple Storage Service (Amazon S3) 中使用標準 SQL 輕鬆地直接分析資料。Athena 可協助客戶分析存放在 Amazon S3 中的非結構化、半結構化和結構化資料。範例包括 CSV、JSON 或單欄資料格式，例如 Apache Parquet 和 Apache ORC。客戶可以使用 Athena 使用 ANSI SQL 執行臨機操作查詢，而不需要將資料彙總或載入到 Athena。

Amazon Athena 現在可用於處理包含 PHI 的資料。在 Amazon Athena 和 S3 之間傳輸時，預設使用 SSL/TLS 提供資料加密。應該根據 S3 部分中提供的指導來執行 S3 上靜態時 PHI 的加密。應該使用具有 Amazon S3 受管金鑰 (SSE-S3)、受管金鑰 (SSE-KMS) 的伺服器端加密，或使用受管金鑰 (CSE-KMS) 的用戶端加密來啟用 Amazon Athena 內的查詢結果加密 (包括分段結果)。 AWS KMS AWS KMS Amazon Athena 用 AWS CloudTrail 來記錄所有 API 呼叫。

Amazon Aurora

Amazon Aurora 可讓客戶使用所管理的金鑰來加密 Aurora 資料庫叢集和靜態快照 AWS KMS。在以 Amazon Aurora 加密執行的資料庫執行個體上，存放在基礎儲存體中的靜態資料，以及自動備份、僅供讀取複本和快照都會加密。

由於指引可能會更新，因此客戶應繼續評估並判斷 Amazon Aurora 加密是否符合其合規和法規要求。如需使用 Amazon Aurora 進行靜態加密的詳細資訊，請參閱使用加密保護資料。

與執行 Aurora MySQL 之資料庫叢集的連線必須使用傳輸加密，利用安全通訊端層 (SSL) 或傳輸層安全性 (TLS)。如需有關實作 SSL/TLS 的詳細資訊，請參閱搭配 Aurora MySQL 資料庫叢集使用 SSL/TLS。

Amazon Aurora PostgreSQL

Amazon Aurora 可讓客戶使用所管理的金鑰來加密 Aurora 資料庫叢集和靜態快照 AWS KMS。在以 Amazon Aurora 加密執行的資料庫執行個體上，存放在基礎儲存體中的靜態資料，以及自動備份、僅供讀取複本和快照都會加密。

由於指引可能會更新，因此客戶應繼續評估並判斷 Amazon Aurora 加密是否符合其合規和法規要求。如需使用 Amazon Aurora 進行靜態加密的詳細資訊，請參閱使用加密保護資料。

與執行 Aurora PostgreSQL 之資料庫叢集的連線必須使用傳輸加密，利用安全通訊端層 (SSL) 或傳輸層安全性 (TLS)。如需有關實作 SSL/TLS 的詳細資訊，請參閱使用 SSL 保護 Aurora 資料。

Amazon CloudFront

Amazon CloudFront 是全球內容交付網路 (CDN) 服務，可加速客戶網站、API、影片內容或其他網路資產的交付速度。它與其他 Amazon Web Services 產品整合，讓開發人員和企業能夠輕鬆地將內容加速到最終使用者，而無需最低用量承諾。為了確保在傳輸過程中 PHI 的加密 CloudFront，客戶必須設定 CloudFront 為使用 HTTPS， end-to-end 從原始伺服器到檢視器。

這包括 CloudFront 與檢視器之間的流量、從自訂來源 CloudFront 重新 CloudFront 分配，以及從 Amazon S3 來源分發。 客戶還應確保數據在源頭進行加密，以確保在 CloudFront緩存時保持靜態加密。如果使用 Amazon S3 做為來源，客戶可以使用 S3 伺服器端加密功能。如果客戶從自訂來源散發，則必須確保資料在來源處加密。

Lambda@Edge

Lambda @Edge 是一種運算服務，可讓您在 AWS 節點執行 Lambda 函數。Lambda @Edge 可用來自訂透過 CloudFront. 將 Lambda @Edge 與 PHI 搭配使用時，客戶應遵循使用指南 CloudFront。所有進出 Lambda @Edge 的連線都應該使用 HTTPS 或 SSL/TLS 加密。

Amazon CloudWatch

Amazon CloudWatch 是 AWS 雲端資源和客戶在 AWS 上執行的應用程式的監控服務。客戶可以使 CloudWatch 用 Amazon 收集和追蹤指標、收集和監控日誌檔，以及設定警示。Amazon CloudWatch 本身不生產，存儲或傳輸 PHI。客戶可 CloudWatch 以使用 AWS CloudTrail. 如需詳細資訊，Amazon CloudWatch 參閱使用 AWS CloudTrail.

如需組態需求的詳細資訊，請參閱 Amazon CloudWatch 日誌一節。

Amazon CloudWatch 活動

Amazon CloudWatch 活動提供一系統事件 near-real-time 串流，用來描述 AWS 資源中的變更。客戶應確保 PHI 不會流入 CloudWatch 事件，且任何發出存放、處理或傳輸 PHI 之 CloudWatch 事件的 AWS 資源均根據指導進行設定。

客戶可以將 Amazon CloudWatch 事件設定為註冊為 AWS API 呼叫 CloudTrail。如需詳細資訊，請參閱使用建立在 AWS API 呼叫上觸發的 CloudWatch 事件規則 AWS CloudTrail。

Amazon CloudWatch 日誌

客戶可以使用 Amazon CloudWatch 日誌從 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體、Amazon Route 53 和其他來源監控 AWS CloudTrail、存放和存取其日誌檔。然後，他們可以從日誌中檢索關聯的日 CloudWatch 誌數據。記錄資料在傳輸過程中和靜態時都會加密。因此，不需要重新加密任何其他服務發出的 PHI 並傳送至 CloudWatch 記錄檔。

Amazon Comprehend

Amazon Comprehend 使用自然語言處理來擷取文件內容的洞察。Amazon Comprehend 處理 UTF-8 格式的任何文本文件。它可透過識別文件中的實體、關鍵片語、語言、情感和其他常見元素，以此形成洞見。Amazon Comprehend 可以與包含 PHI 的數據一起使用。亞馬遜不會保留或存放任何資料，所有對 API 的呼叫都會使用 SSL/TLS 進行加密。Amazon Comprehend 用 CloudTrail 於記錄所有 API 調用。

AWS Identity and Access Management

存取 Amazon Comprehend 需要身份驗證和授權等安全存取功能，並且可以使用 AWS Identity and Access Management(IAM) 進行控制，而且可以使用登入資料來存取 IAM。如需詳細資訊，請參閱 Amazon Comprehend 使用者指南中的身份驗證和存取控制。

帳戶管理

根據預設，IAM 使用者沒有使用 Amazon Comprehend API 建立或修改亞馬遜資源或執行任務的權限。為了允許使用者建立或修改資源以及執行任務，客戶應負責利用 IAM 政策，為使用者需要使用的特定資源 (例如 Amazon Comprehend 和 API 動作) 授予使用者許可，然後將政策附加到需要特定許可的使用者或群組。

透過 Amazon Comprehend，您可以使用 AWS Identity and Access Management (IAM) 建立具有連接政策的使用者，以啟用 Amazon Comprehend 許可。或者，您可以選擇建立要附加至角色的自訂策略。然後，您可以根據組織定義的角色型存取和最少權限原則，將管理員新增至角色，以便為 Amazon Comprehend 管理叫用 API。

身分識別與存取

使用 Amazon Comprehend 時，您可以要求使用者根據其組織的身份驗證要求 AWS 使用多因素身份驗證進行身份驗證。

IAM 管理員可以使用建立客戶管理政策 AWS Management Console，拒絕所有許可，使用者管理自己的登入資料和 MFA 裝置所需的權限除外。在 IAM 主控台的「我的安全登入資料」頁面上提供 JSON 政策範本。

或者，您可以透過 IAM 合作夥伴運用相容的第三方 MFA 功能。如需其他資訊，請參閱 IAM 合作夥伴。

管理

我們建議您 Amazon Comprehend 選取以身分為基礎的政策，其中帳戶管理員可以將許可政策附加到 IAM 身分 (使用者、群組和角色)，進而授與在 Amazon Comprehend 資源上執行操作的許可。

您可以在 API 參考指南中找到適用於 Amazon Comprehend 的 API 動作清單。您也應該考慮根據使用者或角色的最低權限和以角色為基礎的組織要求，授權存取預先定義的 IAM 政策、客戶 IAM 政策和 API 動作。如需詳細資訊，請參閱開發人員指南中的使用亞馬遜 API。

外部驗證

Amazon Comprehend 與使用 IAM 角色的聯合身分相容。如此一來，Amazon Comprehend 就能 AWS 透過假設管理員已佈建的角色來驗證您的使用者。 AWS 使用其組織或協力廠商認證存取的使用者會間接擔任角色。

AWS Kerberos 和作用中目錄的支援可提供單一登入和資料庫使用者集中式驗證的優點。 AWS 使用者可以選擇管理和儲存使用者認證，無論是在 AWS Directory Service Microsoft Active Directory 或客戶的內部部署作用中目錄。

資料流程強制

AWS 作為資料控制者或資料處理者的客戶和 APN 合作夥伴負責他們放入 AWS 雲端 和 Amazon Comprehend 中的任何個人資料。您必須負責使用 IAM 政策來控制 Amazon Comprehend 資料輸入和輸出的流程。

資料保護與機密管理

AWS 共同的責任模型適用於 Amazon Comprehend 中的資料保護。如此模型所述， AWS 負責保護執行所有 AWS 雲端的全域基礎結構。您負責維護在此基礎設施上託管內容的控制權。此內容包括您使用之 AWS 服務的安全性設定和管理工作。如需有關資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。

Amazon Comprehend 開發人員指南中的「Amazon Comprehend 中的資料保護」一節提供保護資料時應考慮的提示，例如使用 TLS 進行傳輸，以及避免將敏感資訊放入標籤或任意格式欄位。

的加密 data-at-rest

Amazon Comprehend 可與 AWS Key Management Service(AWS KMS) 搭配使用，為您的資料提供增強的加密功能。亞馬遜簡單儲存服務 (Amazon S3) 已讓您在建立文字分析、主題建模或自訂 Amazon Comprehend 任務時加密輸入文件。與整合 AWS KMS 可讓您加密儲存磁碟區中的資料，以便開始 * 和建立 * 工作，並使用您自己的金鑰加密 start* 工作的輸出結果。 AWS KMS

Amazon Comprehend 使用者最佳做法是根據其組織政策，使用可用的 S3 加密解決方案來加密用於輸入文件的 Amazon S3 儲存貯體。

使用自己的 AWS Management Console金鑰加密 Amazon Comprehend 自訂模型。 AWS KMS 對於 AWS CLI，Amazon Comprehend 可以使用自己的 AWS KMS 金鑰或提供的客戶受管金鑰 (CMK) 來加密自訂模型。

如果在使用時選取加密 AWS Management Console，您可以選擇下列其中一種或兩種選用方法：

- 磁碟區加密-確保 Comprehend 使用的 EBS 磁碟區上的資料會在訓練/推論期間加密 (資料會在訓練/推論後清除，因此此金鑰僅在工作進行中時才相關)。
- 輸出結果加密-用於使用客戶提供的金鑰加密理解在客戶儲存貯體中儲存的輸出。 AWS KMS

如需有關加密類型 (例如磁碟區加密) 的詳細資訊，請參閱 Amazon Comprehend 中的AWS KMS 加密。

個人身份信息

您可以使用 Amazon Comprehend 主控台或 API 來偵測英文文字文件中的個人識別資訊 (PII)。如需有關偵測和標記 PII 實體以及操作各種 PII 分析任務的詳細資訊，請參閱 Amazon Comprehend 開發人員指南中的個人識別資訊一節。

資料刪除

如果您是使用 Amazon S3 的 Amazon Comprehend 客戶，並且選擇管理自己的 AWS KMS 金鑰，則應考慮撤銷 AWS KMS 金鑰並根據其組織要求定義程序合理。撤銷 Amazon S3 的 AWS KMS 金鑰會使任何資料無法使用/無法讀取。

網路分段與強化

作為受管服務，Amazon Comprehend 遵循安全性、身分識別和合規的AWS 最佳實務。

如需建議的網路安全防護措施，請參閱 Amazon Comprehend 開發人員指南中的基礎設施安全性。

使用 Amazon Virtual Private Cloud (Amazon VPC) 保護任務

Amazon Comprehend 使用各種安全措施，透過我們的任務容器在 Amazon Comprehend 正在使用時儲存資料的容器，確保資料的安全性。但是，任務容器會透過網際網路存取 AWS 資源 (例如存放資料和模型人工因素的 Amazon S3 儲存貯體)。

若要控制對資料的存取，我們建議您建立虛擬私有雲 (VPC) 並進行設定，以便無法透過網際網路存取資料和容器。如需 VPC 在建立和設定方面的資訊，請參閱《Amazon VPC 使用者指南》中的 Amazon VPC 入門的相關文章。使用 VPC 有助於保護您的資料，因為您可以設定 VPC，使其未連接到網際網路。使用 VPC 也可讓您使用 VPC 流程記錄來監控工作容器的所有進出網路流量。如需詳細資訊，請參閱 《Amazon VPC 使用者指南》中的 VPC 流量日誌。

您可以在建立工作時指定 VPC 組態，方法是指定子網路和安全群組。當您指定子網路和安全群組時，Amazon Comprehend 會建立與其中一個子網路中的安全群組相關聯的彈性網路界面 (ENI)。ENI 允許我們的工作容器連接到 VPC 中的資源。如需 ENI 的相關資訊，請參閱 Amazon VPC 使用者指南中的彈性網路介面。

> **Note**
>
> 針對工作，您只能使用預設租用 VPC 來設定子網路，而您的執行個體會在共用硬體上執行。如需 VPC 租用屬性的詳細資訊，請參閱 Amazon EC2 Linux 執行個體使用者指南中的專用執行個體。

您可以透過建立介面 VPC 端點，在虛擬私人雲端和 Amazon Comprehend 之間建立私有連線。如需詳細資訊，請參閱 Amazon Comprehend 和介面 VPC 端點 ()。AWS PrivateLink

主機和映像強化

根據 AWS 共同的責任模型，Amazon Comprehend AWS 環境的主機和映像強化是由提供的服務來 AWS 管理。

多租戶

為了協助提高建議的安全性，我們建議您實作下列多租用戶安全性建議：

- 請務必使用已驗證的電子郵件地址，根據網域比對來授權使用者存取租用戶。不要信任電子郵件地址和電話號碼，除非您的應用程式驗證它們，或者外部 IdP 提供驗證證明。如需設定上述許可的詳細資訊，請參閱屬性許可和範圍。

- 針對識別租用户的使用者描述檔屬性，使用不可變或可變屬性。管理員必須能夠變更這些屬性。此外，提供應用程式用戶端對屬性的唯讀存取權。
- 使用 IdP 與應用程式用戶端之間的 1:1 映射，防止未經授權的跨租用戶存取。已經由外部 IdP 進行身分驗證且具有有效 Amazon Cognito 工作階段 Cookie 的使用者，可以存取信任相同 IdP 的其他租用戶應用程式。
- 在應用程式中實作符合租用戶和授權邏輯時，請限制使用者使其無法修改授權使用者存取租用戶的條件。此外，如果外部 IdP 正用於聯合身分，請限制租用者身分提供者管理員，使其無法變更使用者存取權限。

預防跨服務混淆代理人

混淆的副問題是多租戶安全性問題，其中沒有執行動作權限的實體可能會強制更具權限的實體執行動作。在中 AWS，跨服務模擬可能會導致混淆的副問題。在某個服務 (呼叫服務)呼叫另一個服務 (被呼叫服務)時，可能會發生跨服務模擬。可以操縱呼叫服務來使用其許可，以其不應有存取許可的方式對其他客戶的資源採取動作。為了避免這種情況發生， AWS 提供的工具可協助您透過已授予您帳戶中資源存取權的服務主體來保護所有服務的資料。如需包括解決此安全問題時應考慮之保護措施的詳細資訊，請參閱 Amazon Comprehend 開發人員指南中的跨服務混淆副預防。

Amazon Comprehend Medical

如需指引，請參閱前一Amazon Comprehend節。

Amazon Connect

Amazon Connect 是自助式雲端型聯絡中心服務，可實現任何規模的動態、個人化和自然客戶互動。客戶不應在 Amazon Connect 中管理使用者、安全設定檔和聯絡流程相關聯的任何欄位中包含任何 PHI。

Amazon Connect 客戶個人檔案是 Amazon Connect 的一項功能，可讓客服中心代理人更統一地檢視客戶的個人檔案，以及最新資訊，以提供更個人化的客戶服務。客戶個人檔案旨在自動將來自多個應用程式的客戶資訊整合到統一的客戶個人檔案中，在支援呼叫或互動開始時，立即將個人檔案直接傳送給客服人員。客戶應避免使用 PHI 資料來命名網域或物件金鑰。域和對象的內容被加密和保護，但密鑰標識符不是。

Amazon DocumentDB (with MongoDB compatibility)

Amazon DocumentDB (與 MongoDB 相容性) (Amazon DocumentDB) 在叢集建立期間提供靜態加密功能 AWS KMS，可讓客戶使用 AWS 或客戶管理的金鑰加密資料庫。在啟用加密的情況下執行的資料庫執行個體上，靜態儲存的資料會與本白皮書發佈時生效的指引一致，以及自動備份、僅供讀取複本和快照集等資料加密。由於指引可能會更新，因此客戶應繼續評估並判斷 Amazon DocumentDB 加密是否符合其合規和法規要求。如需有關使用 Amazon 文件資料庫靜態加密的詳細資訊，請參閱加密 Amazon 文件資料庫靜態資料。

連線至包含 PHI 的 Amazon DocumentDB 必須使用接受加密傳輸 (HTTPS) 的端點。根據預設，新建立的 Amazon DocumentDB 叢集僅接受使用傳輸層安全性 (TLS) 的安全連線。如需詳細資訊，請參閱加密傳輸中的資料。Amazon DocumentDB 用 AWS CloudTrail 於記錄所有 API 調用。如需詳細資訊，請參閱 Amazon DocumentDB 中的記錄和監控。

對於某些管理功能，Amazon DocumentDB 會使用與 Amazon RDS 共用的操作技術。Amazon DocumentDB 主控台、AWS CLI 和 API 呼叫都會記錄為對 Amazon RDS API 進行的呼叫。

Amazon DynamoDB

與包含 PHI 的 Amazon DynamoDB 連線必須使用接受加密傳輸 (HTTPS) 的端點。如需區域端點的清單，請參閱 AWS 服務端點。

Amazon DynamoDB 提供 DynamoDB 加密功能，可讓客戶使用客戶管理的金鑰來加密資料庫。 AWS KMS在以 Amazon DynamoDB 加密執行的資料庫執行個體上，基礎儲存體中存放的靜態資料會加密，與本白皮書發佈時生效的指導 (自動備份、僅供讀取複本和快照) 一致。

由於指引可能會更新，因此客戶應繼續評估並判斷 Amazon DynamoDB 加密是否符合其合規和法規要求。如需有關使用 Amazon DynamoDB 靜態加密的詳細資訊，請參閱靜態 DynamoDB 加密。

Amazon Elastic Block Store

Amazon EBS 靜態加密與本白皮書發佈時生效的指導一致。由於指引可能會更新，因此客戶應繼續評估並判斷 Amazon EBS 加密是否符合其合規和法規要求。使用 Amazon EBS 加密時，會為每個 EBS 磁碟區產生唯一的磁碟區加密金鑰。客戶可以彈性地選擇要使用哪個 KMS 金鑰來加密每個磁碟區金鑰。 AWS Key Management Service 如需詳細資訊，請參閱 Amazon EBS 加密。

Amazon Elastic Compute Cloud

Amazon EC2 是可擴展、使用者可設定的運算服務，支援多種加密靜態資料的方法。例如，在 Amazon EC2 執行個體託管的應用程式或資料庫平台內處理 PHI 時，客戶可能會選擇執行 PHI 的應用程式或欄位層級加密。方法範圍包括使用 Java 或 .NET 等應用程式架構中的標準程式庫來加密資料；利用 Microsoft SQL 或 Oracle 中的「透明資料加密」功能；或將其他第三方和軟體即服務 (SaaS) 解決方案整合到其應用程式中。

客戶可以選擇將在 Amazon EC2 中執行的應用程式與 AWS KMS SDK 整合，以簡化金鑰管理和儲存程序。客戶也可以使用AWS Marketplace 合作夥伴提供的協力廠商軟體或原生檔案系統加密工具 (例如 dm-crypt、LUKS 等)，使用檔案層級或全磁碟加密 (FDE) 來實作靜態資料加密。

包含 PHI 的網路流量必須加密傳輸中的資料。對於外部來源 (例如網際網路或傳統 IT 環境) 和 Amazon EC2 之間的流量，客戶應使用符合指導的開放標準傳輸加密機制，例如傳輸層安全性 (TLS) 或 IPsec 虛擬私人網路 (VPN)。Amazon Virtual Private Cloud (VPC) 內部對於在 Amazon EC2 執行個體之間傳輸的資料，包含 PHI 的網路流量也必須加密；大多數應用程式支援 TLS 或其他協定，提供傳輸中加密可設定為與指導一致。對於不支援加密的應用程式和通訊協定，可以使用 IPsec 或執行個體之間的類似實作，透過加密通道傳送 PHI 的工作階段。

Amazon Elastic Container Registry

亞馬遜彈性容器登錄 (Amazon ECR) 與亞馬遜彈性容器服務 (Amazon ECS) 整合，可讓客戶輕鬆存放、執行和管理在 Amazon ECS 上執行的應用程式的容器映像。客戶在其任務定義中指定 Amazon ECR 儲存庫後，Amazon ECS 將擷取其應用程式的適當映像。

不需要特殊步驟即可將 Amazon ECR 與包含 PHI 的容器映像搭配使用。容器映像在傳輸過程中進行加密，並使用 Amazon S3 伺服器端加密 (SSE-S3) 進行靜態存放時進行加密。

Amazon Elastic Container Service

Amazon Elastic Container Service (Amazon ECS) 是可高度擴展的高效能容器管理服務，可支援 Docker 容器，並可讓客戶在 Amazon EC2 執行個體的受管叢集上輕鬆執行應用程式。Amazon ECS 讓客戶無需安裝、操作和擴展自己的叢集管理基礎設施。

透過簡單的 API 呼叫，客戶可以啟動和停止啟用 Docker 的應用程式、查詢叢集的完整狀態，以及存取許多熟悉的功能，例如安全群組、Elastic Load Balancing、EBS 磁碟區和 IAM 角色。客戶可以使用 Amazon ECS，根據其資源需求和可用性需求，在叢集中排定容器的放置。

將 ECS 與處理 PHI 的工作負載搭配使用，不需要額外的設定。ECS 充當協調服務，可協調 EC2 上容器 (存放在 S3 中的映像) 的啟動，而且不會使用正在編排的工作負載內的資料或對資料進行操作。符合 HIPAA 法規和 AWS 商業夥伴增補合約，在使用 ECS 啟動的容器存取時，PHI 應該在傳輸過程中和靜態進行加密。每個 AWS 儲存選項 (例如 S3、EBS 和 KMS) 均提供多種靜態加密機制。確保在容器之間傳送的 PHI 完全加密，也可能導致客戶部署覆蓋網路 (例如 VNS3、Weave Net 或類似的網路)，以提供冗餘的加密層。不過，也應啟用完整的記錄功能 (例如，透過 CloudTrail)，而且所有容器執行個體記錄都應導向至 CloudWatch。

除非日誌包含 PHI，否則在處理 PHI 的工作負載中使用 Firelens 和 AWS 流利位元不需要額外的配置。如果記錄檔包含 PHI，則除非已啟用磁碟加密，否則不應將它們發出到記錄檔。相反，將您的應用程序配置為將日誌發出標準輸出/錯誤，該日誌將由自動收集。 FireLens同樣地，除非同時啟用磁碟加密，否則請勿為 Fluent Bit 啟用檔案緩衝功能。最後，記錄目的地必須支援 encryption-in-transit；AWS 中 Fluent Bit 的所有 AWS 服務輸出外掛程式將一律使用 TLS 加密來匯出日誌。

Amazon Elastic File System (Amazon EFS)

Amazon Elastic File System (Amazon EFS) 提供簡單、可擴展的彈性檔案儲存，可與 AWS 雲端服務和現場部署資源搭配使用。它易於使用，並提供簡單的界面，可讓客戶快速輕鬆地創建和配置文件系統。Amazon EFS 可根據需求彈性擴展而不會中斷應用程式，並在客戶新增和移除檔案時自動擴展和縮減。

為了滿足對 PHI 進行靜態加密的需求，EFS 上有兩個路徑可用。建立新檔案系統時，EFS 支援靜態加密。在創建過程中，應選擇「啟用靜態數據加密」選項。選取此選項可確保放置在 EFS 檔案系統上的所有資料都會使用 AES-256 加密和 AWS KMS管理金鑰加密。客戶也可以選擇在將資料置於 EFS 之前先加密，但隨後他們必須負責管理加密程序和金鑰管理。

PHI 不應作為任何檔案名稱或資料夾名稱的全部或部分使用。Amazon EFS 傳輸中的 PHI 加密由 EFS 服務和掛載檔案系統的執行個體之間的傳輸層安全性 (TLS) 提供。EFS 提供掛載協助程式，可協助您使用 TLS 連線至檔案系統。依預設，不會使用 TLS，而且在使用 EFS 掛載協助程式掛接檔案系統時必須啟用。請確定掛載指令包含「-o tls」選項以啟用 TLS 加密。或者，選擇不使用 EFS 掛載協助程式的客戶可以遵循 EFS 文件中的指示，將其 NFS 用戶端設定為透過 TLS 通道進行連線。

Amazon Elastic Kubernetes Service (Amazon EKS)

Amazon Elastic Kubernetes Service (Amazon EKS) 是一項受管服務，可讓客戶輕鬆在 AWS 上執行 Kubernetes，而不需要站立或維護自己的 Kubernetes 控制平面。Kubernetes 是一套開放原始碼系統，用於容器化應用程式的自動化部署、擴展與管理。如需其他安全性與合規資訊，請參閱 Amazon EKS 上的 HIPAA 安全與合規架構白皮書。

Amazon ElastiCache 的雷迪斯

Amazon ElastiCache for Redis 是一種與 Redis 相容的記憶體內資料結構服務，可用作資料存放區或快取。若要儲存 PHI，客戶必須確保執行符合 Redis 引擎版本和目前一代節點類型 ElastiCache 的最新 HIPAA 資格。 ElastiCache 適用於 Redis 的 Amazon 支持存儲以下節點類型和 Redis 引擎版本的 PHI：

- 節點類型：僅目前一代 (例如，截至本白皮書發佈時，M4、M5、R4、R5、T2、T3)
- ElastiCache 對於雷迪斯引擎版本：3.2.6 和 4.0.10 起

如需有關選擇目前一代節點的詳細資訊，請參閱 Amazon ElastiCache 定價。有關選擇 Redis 引擎的 ElastiCache 更多信息，請參閱什麼是 Amazon ElastiCache 的 Redis？

客戶還必須確保叢集和叢集中的節點設定為加密靜態資料、啟用傳輸加密，以及啟用 Redis 命令的驗證。此外，客戶還必須確保其 Redis 叢集在「建議的日期套用」(建議套用更新的日期) 之前或之前，使用最新的「安全性」類型服務更新進行更新。如需詳細資訊，請參閱「以下各節」。

主題

靜態加密

Amazon ElastiCache for Redis 為其叢集提供資料加密，以協助保護靜態資料。當客戶在建立時為叢集啟用靜態加密時，Amazon ElastiCache for Redis 會加密磁碟上的資料和自動 Redis 備份。磁碟上的客戶資料會使用硬體加速的進階加密標準 (AES) -512 對稱金鑰加密。Redis 備份透過亞馬遜 S3 受管加密金鑰 (SSE-S3) 進行加密。啟用伺服器端加密的 S3 儲存貯體會先使用硬體加速進階加密標準 (AES) -256 對稱金鑰來加密資料，然後再將資料儲存至儲存貯體。

如需有關 Amazon S3 受管加密金鑰 (SSE-S3) 的詳細資訊，請參閱使用具有 Amazon S3 受管加密金鑰的伺服器端加密保護資料 (SSE-S3)。在使用加密執行的 ElastiCache Redis 叢集 (單節點或多節點) 上，靜態儲存的資料會與本白皮書發佈時生效的指引一致進行加密。這包括磁碟上的資料和 S3 儲存貯體中的自動備份。由於指引可能會更新，因此客戶應繼續評估並判斷 Amazon ElastiCache for Redis 加密是否符合其合規和法規要求。有關使用 Amazon 對 Redis 進行靜態加密的 ElastiCache 詳細資訊，請參閱什麼是 Redis ElastiCache 的 Amazon？

傳輸加密

Amazon ElastiCache 版 Redis 使用 TLS 來加密傳輸中的數據。包含 PHI ElastiCache 之 Redis 的連線必須使用傳輸加密，並評估組態是否與指導的一致性。如需詳細資訊，請參閱CreateReplicationGroup。如需啟用傳輸加密的詳細資訊，請參閱 ElastiCache Redis 傳輸中加密 (TLS) 的相關資訊。

身分驗證

Amazon ElastiCache 適用於 Redis 的群集（單個/多節點），包含 PHI 必須提供 Redis AUTH 令牌，以啟用 Redis 命令的身份驗證。當同時啟用靜態加密和傳輸中加密時，Redis AUTH 即可使用。客戶應該為 Redis AUTH 提供強大的令牌，並具有以下約束：

- 必須只能是可列印的 ASCII 字元
- 必須至少 16 個字符，長度不超過 128 個字符
- 不能包含下列任何字元：'/'、"" 或「@」

此權杖必須在 Redis 複寫群組 (單一/多節點) 建立時從「要求參數」中設定，而且稍後可以使用新值進行更新。AWS 使用 AWS Key Management Service （AWS KMS）加密此令牌。如需有關 Redis AUTH 的詳細資訊，請參閱ElastiCache 如需 Redis 傳輸中加密 (TLS) 的相關資訊。

套用 ElastiCache 服務更新

包含 PHI 的 Amazon ElastiCache for Redis 叢集 (單一/多節點) 必須在「建議的按日期套用」之前使用最新的「安全」類型服務更新進行更新。 ElastiCache 提供此自助服務功能，客戶可以隨時隨地即時套用更新。每個服務更新都具有「嚴重性」和「建議按日期套用」，並且僅適用於適用的 Redis 複寫群組可用。

服務更新功能中的「SLA Met' 欄位會說明更新是在「建議的日期套用」或之前套用。如果客戶選擇在「建議的依日期套用」之前不將更新套用至適用的 Redis 複寫群組，則不 ElastiCache 會採取任何動作來套用這些更新。客戶可以使用服務更新歷程記錄儀表板來檢閱一段時間內 Redis 複寫群組的更新應用程式。有關如何使用此功能的詳細資訊，請參閱 Amazon 中的自助服務更新 ElastiCache。

Amazon OpenSearch 服務

Amazon OpenSearch 服務使客戶能夠在專用的 Amazon Virtual Private Cloud（Amazon VPC）中運行受管 OpenSearch 或傳統的 Elasticsearch OSS 叢集。搭配 PHI 使用 OpenSearch 服務時，客戶應使用彈性搜尋 6.0 OpenSearch 或更新版本。客戶應確保 PHI 在 Amazon OpenSearch 服務中進行靜

態和傳輸中加密。客戶可以使用 AWS KMS 金鑰加密來加密其 OpenSearch 服務網域中的靜態資料，該網域僅適用於 OpenSearch 和 Elasticsearch 5.1 或更新版本。如需如何加密靜態資料的詳細資訊，請參閱 Amazon OpenSearch 服務的靜態資料加密。

每個 OpenSearch 服務網域都在其自己的 VPC 中執行。客戶應啟用 node-to-node 加密功能，該加密功能適用於所有 OpenSearch 版本和 Elasticsearch 6.0 或更新版本。如果客戶透過 HTTPS 將資料傳送至 OpenSearch 服務，則 node-to-node 加密有助於確保資料在整個叢集中 OpenSearch 散發 (及再分配) 時，資料會保持加密狀態。如果資料透過 HTTP 未加密到達， OpenSearch Service 會在資料到達叢集之後加密。因此，任何進入 Amazon OpenSearch 服務叢集的 PHI 都應透過 HTTPS 傳送。如需詳細資訊，請參閱 Amazon OpenSearch 服務的 N ode-to-node 加密。

您可以在中擷取來自 OpenSearch 服務設定 API 的記錄 AWS CloudTrail。如需詳細資訊，請參閱使用 AWS CloudTrail. OpenSearch

Amazon EMR

Amazon EMR 會將 Amazon EC2 執行個體叢集部署和管理到客戶的帳戶中。如需使用 Amazon EMR 加密的相關資訊，請參閱加密選項。

Amazon EventBridge

Amazon EventBridge (舊稱為 Amazon Even CloudWatch ts) 是無伺服器事件匯流排，可讓您建立可擴展的事件驅動應用程式。 EventBridge 提供來自事件來源 (例如 Zendesk、Datadog 或 Pageduty) 的即時資料串流，並將該資料路由傳送至類似的目標。 AWS Lambda

根據預設， EventBridge 在 AWS 擁有的 CMK 下，使用 256 位元進階加密標準 (AES-256) 加密資料，有助於保護客戶資料不受未經授權的存取。客戶應確保發出存放、處理或傳輸 PHI 的事件的任何 AWS 資源均按照最佳實務進行設定。

Amazon EventBridge AWS CloudTrail 與整合，客戶可以在事件歷史記錄的 CloudTrail 主控台中檢視最近的事件。如需詳細資訊，請參閱中的EventBridge 資訊 CloudTrail。

Amazon Forecast

Amazon Forecast 是一種全受管服務，使用機器學習來提供高度準確的預測。基於 Amazon.com 使用的相同機器學習預測技術。客戶與 Amazon Forecast 的每次互動都受到加密保護。Amazon Forecast 處理的任何內容都會透過 Amazon 金鑰管理服務使用客戶金鑰加密，並在客戶使用該服務的 AWS 區域中靜態加密。

Amazon 預測與這項服務整合在一起 AWS CloudTrail，該服務可提供使用者、角色或 AWS 服務在 Amazon Forecast 中採取的動作記錄。 CloudTrail 將 Amazon Forecast 的所有 API 呼叫擷取為事件。擷取的呼叫包括來自 Amazon 預測主控台的呼叫，以及對 Amazon Forecast API 操作的程式碼呼叫。如果客戶建立追蹤，客戶可以啟用持續交付 CloudTrail 事件到 Amazon S3 儲存貯體，包括 Amazon 預測的事件。如需詳細資訊，Forecast 參閱使用 AWS CloudTrail.

根據預設，傳送 CloudTrail 到儲存貯體的日誌檔會使用 Amazon 伺服器端加密使用 Amazon S3 受管加密金鑰加密 (SSE-S3)。為了提供可直接管理的安全層，客戶可以改為使用伺服器端加密與 AWS KMS—managed 金鑰 (SSE-KMS) 作為記錄檔。 CloudTrail 啟用伺服器端加密可加密日誌檔案，但未使用 SSE-KMS 加密摘要檔案。摘要檔案是使用 Amazon S3 受管加密金鑰 (SSE-S3) 進行加密。

AWS Forecast 從 S3 儲存貯體匯入和匯出資料。從 Amazon S3 匯入和匯出資料時，客戶應確保 S3 儲存貯體的設定方式符合指導。如需詳細資訊，請參閱 入門。

Amazon FSx

Amazon FSx 是一項全受管服務，提供功能豐富且高效能的檔案系統。適用於 Windows 檔案伺服器的 Amazon FSx 提供高度可靠且可擴展的檔案儲存，並可透過伺服器訊息區 (SMB) 通訊協定存取。Amazon FSx for Lustre 可為運算工作負載提供高效能儲存，並由全球最受歡迎的高效能檔案系統 Lustre 提供支援。

Amazon FSx 支援兩種形式的檔案系統加密：傳輸中的資料加密和靜態加密。視窗版檔案伺服器的 Amazon FSx 也支援使 AWS CloudTrail用.

在支援 SMB 通訊協定 3.0 或更新版本的運算執行個體上的 Amazon FSx for Windows File Server，以及支援傳輸中加密的 Amazon EC2 執行個體上的 Lustre 支援傳輸中資料加密。或者，客戶可以在存放在 Amazon FSx 之前先加密資料，但隨後必須負責加密程序和金鑰管理。

使用 AES-256 加密演算法和 AWS KMS受管金鑰建立 Amazon FSx 檔案系統時，會自動啟用靜態資料加密。資料和中繼資料會在寫入檔案系統之前自動加密，並在呈現給應用程式之前自動解密。PHI 不應用於任何檔案或資料夾名稱。

Amazon GuardDuty

Amazon GuardDuty 是一種受管威脅偵測服務，可持續監控惡意或未經授權的行為，以協助客戶保護其 AWS 帳戶和工作負載。它會監控異常 API 呼叫或可能未經授權的部署等活動，這些活動可能表示帳戶遭到入侵。Amazon GuardDuty 還可偵測潛在遭到入侵的執行個體或攻擊者偵察。

Amazon 會 GuardDuty 持續監控和分析下列資料來源：VPC 人雲端流程日誌、 AWS CloudTrail 事件日誌和 DNS 日誌。它使用威脅情報摘要，例如惡意 IP 和網域清單，以及機器學習來識別 AWS 環境中

的未預期和潛在未經授權和惡意活動。因此，Amazon 不 GuardDuty應該遇到任何 PHI，因為這些資料不會存放在上述任何基於 AWS 的資料來源中。

Amazon HealthLake

Amazon HealthLake 讓醫療保健和生命科學產業的客戶能夠以 PB 規模存放、轉換、查詢和分析醫療資料。客戶可以使用 Amazon HealthLake 來傳輸、處理和存放 PHI。Amazon 預設 HealthLake 會加密客戶資料存放區中的靜態資料。所有服務資料和中繼資料均使用服務擁有的 KMS 金鑰進行加密。根據快速醫療保健互通性資源 (FHIR) 規格，如果客戶刪除 FHIR 資源，該資源只會隱藏無法擷取，並由服務保留以進行版本控制。當客戶使用 StartfHIR ImportJob API 時，亞馬遜 HealthLake 會強制執行將資料匯出到加密的 Amazon S3 儲存貯體的要求。

Amazon HealthLake 會對傳輸中和靜態資料進行加密。對於傳輸中的資料加密，您可以使用 AWS 發佈的 API 呼叫 HealthLake 透過網路進行存取。用戶端必須支援 Transport Layer Security (TLS) 1.0 或更新版本。我們需要 TLS 1.2 並建議使用 TLS 1.3。用戶端也必須支援具備完美轉送私密 (PFS) 的密碼套件，例如臨時 Diffie-Hellman (DHE) 或橢圓曲線臨時 Diffie-Hellman (ECDHE)。現代系統 (如 Java 7 和更新版本) 大多會支援這些模式。此外，請求必須使用存取索引鍵 ID 和與 IAM 主體相關聯的私密存取索引鍵來簽署。或者，客戶也可以使用 AWS Security Token Service (AWS STS) 產生臨時安全登入資料以簽署請求。針對靜態資料加密，Amazon HealthLake 預設會使用客戶擁有的 AWS KMS 金鑰或服務擁有的 AWS KMS 金鑰加密客戶資料存放區中的資料。所有服務資料和中繼資料都會使用服務擁有的 AWS KMS 金鑰在靜態時加密。

Amazon HealthLake 集成 AWS CloudTrail. CloudTrail 擷取所有對 Amazon 的 API 呼叫做 HealthLake 為事件，包括與互動所造成的呼叫 AWS Management Console、命令列界面 (CLI)，以及以程式設計方式使用軟體開發套件 (SDK)。

Amazon Inspector

Amazon Inspector 是一種自動化安全評估服務，適用於尋求改善 AWS 上部署的應用程式安全性和合規性的客戶。Amazon Inspector 會自動評估應用程式是否存在漏洞或與最佳實務偏差。在執行評估之後，Amazon Inspector 會產生一份詳細的安全發現項目清單，並依嚴重程度排列優先順序。客戶可以在包含 PHI 的 EC2 執行個體上執行 Amazon Inspector。Amazon Inspector 會加密透過網路傳輸的所有資料，以及所有靜態存放的遙測資料。

Amazon Managed Service for Apache Flink

適用於 Apache Flink 的 Amazon 受管服務可讓客戶快速編寫 SQL 程式碼，以近乎即時的速度持續讀取、處理和存放資料。對串流資料使用標準 SQL 查詢，客戶可以建構轉換資料並提供深入解析的應用

程式。Apache Flink 的受管理服務支援 Kinesis 資料串流和 Firehose 交付串流的輸入，做為分析應用程式的來源。如果串流已加密，Apache Flink 的受管理服務就能順暢存取加密串流中的資料，無需進一步設定。適用於 Apache Flink 的受管理服務不會儲存從 Kinesis 資料串流讀取的未加密資料。如需詳細資訊，請參閱設定應用程式輸入。

適用於 Apache Flink 的受管服務與 AWS CloudTrail 和 Amazon CloudWatch 日誌整合，以進行應用程式監控。如需詳細資訊，請參閱監控工具和使用 Amazon CloudWatch 日誌。

Amazon 數據 Firehose

當客戶將資料從其資料生產者傳送到 Kinesis 資料串流時，Amazon Kinesis Data Streams 會先使用金 AWS KMS 鑰加密資料，然後再將資料儲存在靜態存放。當 Firehose 傳遞串流從 Kinesis 串流讀取資料時，Kinesis Data Streams 會先將資料解密，然後將資料傳送至 Firehose。Firehose 會根據客戶指定的緩衝提示，緩衝記憶體中的資料。

然後，它將數據傳遞到目的地，而無需存儲靜態未加密的數據。如需使用 Firehose 加密的詳細資訊，請參閱 Amazon 資料防 Firehose 中的資料保護。

AWS 提供客戶可用來監控 Amazon 資料 Firehose 的各種工具，包括 Amazon CloudWatch 指標、Amazon CloudWatch 日誌、Kinesis 代理程式和 API 記錄和歷史記錄。如需詳細資訊，請參閱監控 Amazon 資料 Firehose。

Amazon Kinesis Streams

Amazon Kinesis Streams 可讓客戶建立自訂應用程式，以處理或分析串流資料以滿足特殊需求。伺服器端加密功能可讓客戶加密靜態資料。啟用伺服器端加密後，Kinesis Streams 將使用金 AWS KMS 鑰加密資料，然後再將資料儲存在磁碟上。如需詳細資訊，請參閱 Amazon Kinesis Data Streams 中的資料保護。與包含 PHI 的 Amazon S3 連線必須使用接受加密傳輸 (也就是 HTTPS) 的端點。如需區域端點的清單，請參閱 AWS 服務端點。

Amazon Kinesis Video Streams

Amazon Kinesis Video Streams 是一種全受管 AWS 服務，客戶可以使用它將即時影片從裝置串流到 AWS 雲端，或建立用於即時影片處理或批次導向影片分析的應用程式。伺服器端加密是 Kinesis Video Streams 中的一項功能，可使用客戶指定的金 AWS KMS 鑰 (先前稱為 CMK) 自動加密靜態資料。在將資料寫入 Kinesis Video Streams 儲存層之前，會先加密資料，並在從儲存體擷取資料後解密資料。

Amazon Kinesis Video Streams 開發套件可用於傳輸包含 PHI 的串流影片資料。依預設，SDK 會使用 TLS 來加密安裝它的硬體裝置所產生的框架和片段。SDK 不會管理或影響靜態儲存的資料。Amazon Kinesis Video Streams 用 AWS CloudTrail 於記錄所有 API 呼叫。

Amazon Lex

Amazon Lex 是一種 AWS 服務，可使用語音和文字為應用程式建立交談界面。透過 Amazon Lex，任何開發人員現在都可以使用支援 Amazon Alexa 的相同對話引擎，讓客戶在新的和現有的應用程式中建置複雜的自然語言聊天機器人。Amazon Lex 提供自然語言理解 (NLU) 和自動語音辨識 (ASR) 的深入功能和靈活性，因此客戶可以透過逼真的對話互動建立高度吸引力的使用者體驗，並建立新類別的產品。

Lex 使用 HTTPS 通訊協定與用戶端以及其他 AWS 服務進行通訊。Lex 的存取是 API 驅動的，可以強制執行適當的 IAM 最小特權。如需詳細資訊，請參閱 Amazon Lex 中的資料保護。

監控對於維持客戶 Amazon Lex 聊天機器人的可靠性、可用性和效能非常重要。要跟踪 Amazon Lex 機器人的運行狀況，請使用 Amazon CloudWatch。使用此功能 CloudWatch，客戶可以取得個別 Amazon Lex 作業的指標，或針對其帳戶的全球 Amazon Lex 操作取得指標。客戶也可以設定 CloudWatch 警示，以便在一或多個指標超過客戶定義的閾值時收到通知。例如，客戶可以監控特定時段內對機器人發出的要求數量、檢視成功要求的延遲，或在錯誤超過閾值時發出警示。Lex 還集成 AWS CloudTrail 了記錄 Lex API 調用。如需詳細資訊，請參閱在 Amazon Lex 中進行監控。

Amazon Managed Streaming for Apache Kafka (Amazon MSK)

Amazon MSK 為靜態資料和傳輸中的資料提供加密功能。對於靜態資料加密，Amazon MSK 叢集會使用 Amazon EBS 伺服器端加密和 AWS KMS 金鑰來加密儲存磁碟區。對於傳輸中的資料，Amazon MSK 叢集已透過 TLS 啟用加密，以進行代理程式間通訊。

建立叢集時，會啟用加密組態設定。此外，根據預設，從 CLI 或 AWS 主控台建立的叢集的傳輸中加密設定為 TLS。用戶端需要其他組態才能使用 TLS 加密與叢集進行通訊。客戶可以透過選取 TLS/ 純文字設定來變更預設加密設定。如需詳細資訊，請參閱 Amazon MSK 加密。

客戶可以使用 Amazon MSK 主控台、Amazon 主控台監控客戶叢集的效能，或者客戶也可以使用開放程式碼監 CloudWatch 控解決方案 Prometheus 使用開放式監控來存取 JMX 和託管指標。

旨在從 Prometheus 出口商讀取的工具與開放式監控兼容，例如：數據多，鏡頭，新遺物，Sumologic 或 Prometheus 服務器。如需開放式監控的詳細資訊，請參閱 Amazon MSK 開放監控文件。

請注意，阿帕奇動物園管理員的默認版本捆綁在一起阿帕奇卡夫卡不支持加密。然而，需要注意的是 Apache 動物園管理員和 Apache 卡夫卡經紀人之間的通信僅限於經紀人，主題和分區狀態信息是非常重要的。從 Amazon MSK 叢集產生和使用資料的唯一方法是透過其 VPC 中的用戶端與 Amazon MSK 叢集之間的私有連線。Amazon MSK 不支援公有端點。

Amazon MQ

Amazon MQ 是適用於 Apache ActiveMQ 的受管訊息代理程式服務，可讓您輕鬆地在雲端中設定和操作訊息代理程式。Amazon MQ 可與現有的應用程式和服務搭配使用，無需客戶管理、操作或維護自己的簡訊系統。為了在傳輸過程中對 PHI 資料進行加密，應使用以下啟用 TLS 的通訊協定來存取代理程式：

- AMQP
- MQTT
- MQTT 超過 WebSocket
- OpenWire
- STOMP
- 跺腳過 WebSocket

Amazon MQ 使用安全管理和存放的加密金鑰來加密靜態和傳輸中的訊息。Amazon MQ 用 CloudTrail 於記錄所有 API 呼叫。

Amazon Neptune

Amazon Neptune 是快速、可靠、全受管的圖形資料庫服務，可讓您輕鬆建置和執行搭配高度連線資料集使用的應用程式。Amazon Neptune 的核心是專門打造的高效能圖形資料庫引擎，已針對存放數十億個關係進行最佳化，並以毫秒的延遲查詢圖形。Amazon Neptune 支持流行的圖形查詢語言阿帕奇 TinkerPop 格林和 W3C 的 SPARQL。

包含 PHI 的資料現在可以保留在 Amazon Neptune 的加密執行個體中。只有在建立時，才能透過從 Amazon Neptune 主控台選擇「啟用加密」來指定 Amazon Neptune 的加密執行個體。Amazon Neptune 加密執行個體的所有日誌、備份和快照都會加密。Amazon Neptune 加密執行個體的金鑰管理是透過 AWS KMS. 傳輸中的資料加密是透過 SSL/TLS 提供的。Amazon Neptune 用 CloudTrail 於記錄所有 API 呼叫。

AWS Network Firewall

AWS Network Firewall 是一種受管防火牆服務，可讓您輕鬆為所有 Amazon 虛擬私有雲 (Amazon VPC) 部署基本網路保護。此服務會隨著網路流量自動擴充，以提供高可用性保護，而不需要設定或維護基礎結構。客戶規則和存取記錄都可能包含一般使用者 IP 位址，這些 IP 位址會在 AWS 架構內的靜態和傳輸中進行加密。此外， AWS Network Firewall 會加密元件 AWS 服務 (Amazon S3、Amazon DynamoDB、Amazon CloudWatch 日誌、Amazon EBS) 之間的所有靜態和傳輸中資料。該服務會自動加密數據，而無需特殊配置。

Amazon Pinpoint

Amazon Pinpoint 為開發人員提供單一 API 層、CLI 支援和用戶端開發套件支援，以擴展與使用者之間的應用程式通訊管道。符合資格的通道包括：電子郵件、SMS 簡訊、行動推送通知和自訂管道。Amazon Pinpoint 也提供可追蹤應用程式使用者行為和使用者參與度的分析系統。借助此服務，開發人員可以了解每個用戶喜歡如何參與，並可以個性化用戶體驗以提高用戶滿意度。

Amazon Pinpoint 也可協助開發人員處理多個簡訊使用案例，例如直接或交易簡訊、目標或行銷活動簡訊，以及事件型簡訊。透過 Amazon Pinpoint 整合和啟用所有使用者互動通道，開發人員可以在所有客戶接觸點建立 360 度的使用者互動視圖。Amazon Pinpoint 可存放使用者、端點和事件資料，以便客戶建立細分、傳送訊息給收件人，以及擷取互動資料。

Amazon Pinpoint 會對靜態和傳輸中的資料進行加密。如需詳細資訊，請參閱 Amazon Pinpoint 常見問答集。雖然 Amazon Pinpoint 會加密所有靜態和傳輸中的資料，但最終通道 (例如 SMS 或電子郵件) 可能不會加密，而且客戶應以符合其需求的方式設定任何通道。

此外，需要透過 SMS 通道傳送 PHI 的客戶，應使用專用的短碼（5、6 位數的來源電話號碼），以明確傳送 PHI。如需有關如何請求簡碼的詳細資訊，請參閱使用 Amazon Pinpoint 要求簡訊的專用短碼。客戶也可以選擇不透過最終通道傳送 PHI，而是提供透過 HTTPS 安全存取 PHI 的機制。

可以使用 AWS CloudTrail擷取對 Amazon Pinpoint 的 API 呼叫。擷取的呼叫包括來自 Amazon Pinpoint 主控台的呼叫，以及對 Amazon Pinpoint API 作業進行程式碼呼叫的呼叫。如果客戶建立追蹤，客戶可以啟用持續交付 AWS CloudTrail 事件到 Amazon S3 儲存貯體，包括 Amazon Pinpoint 的事件。如果客戶未設定追蹤，他們仍然可以使用 AWS CloudTrail 主控台上的事件歷史記錄來檢視最近的事件。使用收集的資訊 AWS CloudTrail，客戶可以判斷是否向 Amazon Pinpoint 提出請求、請求的 IP 地址、提出請求的人員、提出請求的時間以及其他詳細資訊。如需詳細資訊，請參閱使用 AWS CloudTrail.

Amazon Polly

Amazon Polly 是一種雲端服務，可將文字轉換為逼真的語音。Amazon Polly 提供簡單的 API 操作，客戶可以輕鬆地與現有的應用程式整合。Amazon Polly 使用 HTTPS 協議與客戶進行通信。Amazon Polly 的存取是 API 驅動的，而且可以強制執行適當的 IAM 最小特權。如需詳細資訊，請參閱資料安全防護。包括 PHI 的一些用例示例：

- 照護者將包含 PHI 的文本報告轉換為綜合語音，以便他們可以在行走或執行其他職責時收聽報告。
- 視障患者被給予醫療指導，並消耗合成語音的形式的指導。

Amazon Polly 的最終交付通道可能會導致在公共場所使用 PHI 播放音訊，並且應採取預防措施，以便交付考慮到這一點。合成語音輸出也可以非同步傳送到啟用加密的 Amazon S3 儲存貯體。

Amazon Polly 中發生受支援的事件活動時，該活動會與事件歷史記錄中的其他 AWS 服務 AWS CloudTrail 事件一起記錄在事件中。如需客戶 AWS 帳戶中持續的事件記錄 (包括 Amazon Polly 的活動)，請建立追蹤。追蹤可 CloudTrail將日誌檔交付到 Amazon S3 儲存貯體。客戶可以使用 CloudTrail 收集的資訊判斷向 Amazon Polly 提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間以及其他詳細資訊。

Amazon Quantum Ledger Database (Amazon QLDB)

Amazon QLDB 是一個全受管分類帳資料庫，提供透明、不可變且以密碼編譯方式驗證的交易日誌，這些交易日誌為集中的受信任授權單位所擁有。Amazon QLDB 會追蹤每個應用程式資料變更，並維護一段時間內完整且可驗證的變更歷史記錄。包含 PHI 的資料現在可以保留在 QLDB 執行個體中。依預設，所有傳輸中和靜態的 Amazon QLDB 資料都會加密。傳輸中的資料會使用 TLS 加密，靜態資料會使用 AWS 受管理金鑰加密。基於資料保護目的，我們建議客戶使用 AWS Identity and Access Management (IAM) 保護帳戶登入資料並設定個別使用者帳 AWS 戶，以便每位使用者僅獲得履行其工作職責所需的權限。如需詳細資訊，請參閱 Amazon QLDB 中的資料保護。

Amazon QLDB 與服務整合在一起 AWS CloudTrail，可提供 QLDB 中使用者、角色或服務所採取的動作記錄的 AWS 服務。 CloudTrail 擷取 QLDB 的所有控制平面 API 呼叫做為事件。擷取的呼叫包括來自 QLDB 主控台的呼叫，以及對 QLDB API 作業的程式碼呼叫。如果客戶建立追蹤，客戶可以啟用持續交付 CloudTrail 事件到 Amazon Simple Storage Service (Amazon S3) 儲存貯體，包括 QLDB 的事件。如果客戶未設定追蹤，客戶仍然可以在 CloudTrail 主控台上檢視事件歷史記錄中最近的事件。 使用收集的資訊 CloudTrail，客戶可以判斷向 QLDB 提出的要求、提出要求的 IP 位址、提出要求的人員、提出要求的時間，以及其他詳細資訊。

Amazon QuickSight

Amazon QuickSight 是一種商業分析服務，客戶可用來建立視覺化、執行臨機操作分析，以及快速從資料中取得商業洞察。Amazon 會 QuickSight 探索 AWS 資料來源，讓組織擴展到數十萬名使用者，並使用強大的記憶體內引擎 (SPICE) 提供回應迅速的效能。

客戶只能使用 Amazon 企業版 QuickSight 來處理包含 PHI 的資料，因為它支援加密 SPICE 中儲存的靜態資料。資料加密是使用 AWS 受管理金鑰執行的。

Amazon RDS for MariaDB

適用 Amazon RDS for MariaDB 可讓客戶使用他們所管理的金鑰來加密 MariaDB 資料庫。 AWS KMS 在以 Amazon RDS 加密執行的資料庫執行個體上，基礎儲存體中存放的靜態資料會與本白皮書發佈時生效的指導一致，以及自動備份、僅供讀取複本和快照等功能一致。

由於指引可能會更新，因此客戶應繼續評估並判斷 Amazon RDS for MariaDB 加密是否符合其合規和法規要求。如需使用 Amazon RDS 進行靜態加密的詳細資訊，請參閱加密 Amazon RDS 資源。

與含有 PHI 之 MariaDB 的 RDS 連線必須使用傳輸加密。如需啟用加密連線的詳細資訊，請參閱 < 使用 SSL/TLS 加密與資料庫執行個體的連線 > 。

Amazon RDS for MySQL

Amazon RDS for MySQL 版 MySQL 允許客戶使用客戶管理的金鑰來加密 MySQL 資料庫 AWS KMS。在以 Amazon RDS 加密執行的資料庫執行個體上，基礎儲存體中存放的靜態資料會與本白皮書發佈時生效的指導一致，以及自動備份、僅供讀取複本和快照等功能一致。

由於指引可能會更新，因此客戶應繼續評估並判斷 Amazon RDS for MySQL 加密是否符合其合規和法規要求。如需使用 Amazon RDS 進行靜態加密的詳細資訊，請參閱加密 Amazon RDS 資源。

與包含 PHI 的適用於 MySQL 的 RDS 連線必須使用傳輸加密。如需啟用加密連線的詳細資訊，請參閱 < 使用 SSL/TLS 加密與資料庫執行個體的連線 > 。

Amazon RDS for Oracle

客戶有多種選擇，可以使用 Amazon RDS for Oracle 文加密靜態 PHI。客戶可以使用他們管理的金鑰來加密 Oracle 資料庫 AWS KMS。在以 Amazon RDS 加密執行的資料庫執行個體上，基礎儲存體中存放的靜態資料會與本白皮書發佈時生效的指導一致，以及自動備份、僅供讀取複本和快照等功能一致。

由於指引可能會更新，因此客戶應繼續評估並判斷適用於 Oracle 加密的 Amazon RDS 是否符合其合規和法規要求。如需使用 Amazon RDS 進行靜態加密的詳細資訊，請參閱加密 Amazon RDS 資源。

客戶也可以使用 Oracle 透明資料加密 (TDE)，並且應該評估組態是否與「指導」的一致性。Oracle TDE 是「Oracle 企業版」中可用的「Oracle 進階安全性」選項的一項功能。此功能會在資料寫入至儲存體之前自動將其加密，並在從儲存體中讀取資料時自動將其解密。客戶也可以使用 AWS CloudHSM 來存放 Amazon RDS 甲骨文 TDE 金鑰。如需詳細資訊，請參閱下列內容：

- 適用於甲骨文通透資料加密的亞馬遜 RDS：Oracle 通透資料加密。
- 用 AWS CloudHSM 於存儲 Amazon RDS 甲骨文 TDE 密鑰：什麼是 Amazon Relational Database Service（Amazon RDS）？

與包含 PHI Amazon RDS for Oracle 連線必須使用傳輸加密，並評估組態是否與指導的一致性。這是使用 Oracle 原生網路加密來完成的，並在適用於 Oracle 選項群組的 Amazon RDS 中啟用。如需詳細資訊，請參閱 Oracle 原生網路加密。

Amazon RDS for PostgreSQL

適用 Amazon RDS for PostgreSQL 可讓客戶使用客戶管理的金鑰來加密 PostgreSQL 資料庫。 AWS KMS在以 Amazon RDS 加密執行的資料庫執行個體上，基礎儲存體中存放的靜態資料會與本白皮書發佈時生效的指導一致，以及自動備份、僅供讀取複本和快照等功能一致。

由於指引可能會更新，因此客戶應繼續評估並判斷 Amazon RDS for PostgreSQL 加密是否符合其合規和法規要求。如需使用 Amazon RDS 進行靜態加密的詳細資訊，請參閱加密 Amazon RDS 資源。

與包含 PHI 的 RDS 連線必須使用傳輸加密。如需啟用加密連線的詳細資訊，請參閱 < 使用 SSL/TLS 加密與資料庫執行個體的連線 >。

Amazon RDS for SQL Server

適用於 SQL 伺服器的 RDS 支援儲存下列版本和版本組合的 PHI：

- 2008 年第二季-僅限企業版
- 2012、2014 及 2016-網頁版、標準版和企業版

重要事項：不支援 SQL 伺服器快速版本，因此絕對不應該用於 PHI 的儲存。

為了儲存 PHI，客戶必須確保執行個體設定為加密靜態資料，並啟用傳輸加密和稽核功能，如下所述。

靜態加密

客戶可以使用他們所管理的金鑰來加密 SQL Server 資料庫 AWS KMS。在以 Amazon RDS 加密執行的資料庫執行個體上，基礎儲存體中存放的靜態資料會與本白皮書發佈時生效的指導 (自動備份和快照) 一致。由於指引可能會更新，因此客戶應繼續評估並判斷 Amazon RDS for SQL Server 加密是否符合其合規和法規要求。如需有關使用 Amazon RDS 進行靜態加密的詳細資訊，請參閱加密 Amazon RDS 資源。

如果客戶使用 SQL Server 企業版，他們可以使用伺服器透明資料加密 (TDE) 作為替代方案。此功能會在資料寫入至儲存體之前自動將其加密，並在從儲存體中讀取資料時自動將其解密。如需有關 SQL Server 通透資料加密的 RDS 的詳細資訊，請參閱 SQL Server 中的通透資料加密 Support。

傳輸加密

與包含 PHI Amazon RDS for SQL Server 連線必須使用 SQL 伺服器強制 SSL 提供的傳輸加密。從 Amazon RDS SQL 伺服器的參數群組內啟用強制 SSL。如需 SQL 伺服器之 RDS 強制 SSL 的詳細資訊，請參閱搭配使用 SSL 與 Microsoft SQL 伺服器資料庫執行個體一起使用。

稽核

包含 PHI 的 SQL 伺服器執行個體 RDS 必須啟用稽核功能。從 Amazon RDS SQL 伺服器的參數群組內啟用稽核功能。如需適用於 SQL 伺服器稽核的 RDS 的詳細資訊，請參閱 < 符合性計畫 Support >。

Amazon Redshift

Amazon Redshift 為其叢集提供資料庫加密，以協助保護靜態資料。當客戶為叢集啟用加密時，Amazon Redshift 會使用硬體加速進階加密標準 (AES) -256 對稱金鑰來加密所有資料 (包括備份)。Amazon Redshift 使用四個階層的金鑰架構來加密。這些金鑰包含資料加密金鑰、資料庫金鑰、叢集金鑰和 KMS 金鑰。

叢集金鑰會加密 Amazon Redshift 叢集的資料庫金鑰。客戶可以使用 AWS KMS 或 AWS CloudHSM (硬體安全模組) 來管理叢集金鑰。Amazon Redshift 靜態加密與本白皮書發佈時生效的指引一致。由於指引可能會更新，因此客戶應繼續評估並判斷 Amazon Redshift 加密是否符合其合規和法規要求。如需詳細資訊，請參閱 Amazon Redshift 資料庫加密。

與包含 PHI 的 Amazon Redshift 連線必須使用傳輸加密，客戶應該評估組態是否與指導的一致性。如需詳細資訊，請參閱設定連線的安全性選項。Amazon Redshift Spectrum 使客戶能夠對 Amazon S3

中的 EB 數據執行亞馬遜紅移 SQL 查詢。Redshift 頻譜是 Amazon Redshift 的一個功能，因此也在 HIPAA BAA 的範圍內。

Amazon Rekognition

Amazon Rekognition 可讓您輕鬆地將影像和視訊分析新增至客戶應用程式。客戶只需要將影像或影片提供給 Amazon Rekognition API，服務就可以識別物件、人員、文字、場景和活動，並偵測任何不適當的內容。Amazon Rekognition 還提供高度準確的臉部分析和臉部識別。

Amazon Rekognition 有資格使用包含 PHI 的圖像或視頻進行操作。Amazon Rekognition 會以受管服務的形式運作，而且不會提供任何可設定的資料處理選項。Amazon Rekognition 僅在 BAA 條款允許的情況下使用、公開和維護 PHI。 AWS 所有資料都會透過 Amazon Rekognition 進行靜態和傳輸中加密。Amazon Rekognition 用 AWS CloudTrail 於記錄所有 API 呼叫。

Amazon Route 53

Amazon Route 53 是一種受管 DNS 服務，可讓客戶註冊網域名稱、路由網際網路流量客戶網域資源，以及檢查這些資源的運作狀態。雖然 Amazon Route 53 是 HIPAA 合格服務，但任何 PHI 都不應該儲存在 Amazon Route 53 內的任何資源名稱或標籤中，因為不支援加密此類資料。相反地，Amazon Route 53 可用來提供對傳輸或存放 PHI 的客戶網域資源的存取權，例如在 Amazon EC2 上執行的網路伺服器或 Amazon S3 等儲存。

Amazon S3 Glacier

Amazon S3 Glacier 會使用 AES 256 位元對稱金鑰自動加密靜態資料，並支援透過安全協定安全傳輸客戶資料。與包含 PHI 的 Amazon S3 冰川連線必須使用接受加密傳輸 (HTTPS) 的端點。如需地區端點的清單，請參閱AWS 服務端點。

請勿在存檔和文件庫名稱或中繼資料中使用 PHI，因為此資料未使用 Amazon S3 Glacier 伺服器端加密進行加密，而且一般不會在用戶端加密架構中加密。

Amazon S3 Transfer Acceleration

Amazon S3 Transfer Acceleration (S3TA) 可在客戶用戶端和 S3 儲存貯體之間長距離快速、輕鬆且安全地傳輸檔案。傳輸加速充分利用 Amazon CloudFront 分佈在全球的節點。當資料到達節點時，資料會經由最佳化的網路路徑而路由至 Amazon S3。客戶應確保使用 AWS S3TA 傳輸的任何含有 PHI 的資料在傳輸和靜態中都經過加密。請參閱 Amazon S3 指南以了解可用的加密選項。

Amazon SageMaker

Amazon SageMaker 是全受管的機器學習服務。透過 Amazon SageMaker，資料科學家和開發人員可以快速輕鬆地建立和訓練機器學習模型，然後將它們直接部署到生產就緒的託管環境中。它提供整合式 Jupyter 撰寫筆記本執行個體，可輕鬆存取資料來源以進行探索和分析。Amazon SageMaker 也提供常見的機器學習演算法，這些演算法經過最佳化，可針對分散式環境中的極大資料有效執行。

透過原生支援 bring-your-own-algorithms 和架構，Amazon SageMaker 提供彈性的分散式訓練選項，可根據客戶的特定工作流程調整。Amazon SageMaker 有資格使用包含 PHI 的數據進行操作。傳輸中的資料加密由 SSL/TLS 提供，並在與 Amazon 的前端介面 SageMaker (與筆記型電腦) 通訊時使用，以及 Amazon 與任何其他 AWS 服務 SageMaker 互動 (例如，從 Amazon S3 提取資料) 時使用。

為了滿足對 PHI 進行靜態加密的要求，在設定端點時 (DescribeEndpointConfig：KmsKeyID) 可以使用 AWS Key Management Service (KMS) SageMaker 對使用 Amazon 執行個體執行模型存放的資料進行加密。使用啟用模型訓練結果 (人工因素) 的加密， AWS KMS 並且應使用 OutputDataConfig說明中的 KmsKey ID 來指定金鑰。如果未提供 KMS 金鑰識別碼，則會使用該角色帳戶的預設 Amazon S3 KMS 金鑰。Amazon SageMaker 用 AWS CloudTrail 來記錄所有 API 調用。

Amazon Simple Notification Service (Amazon SNS)

客戶應瞭解下列金鑰加密要求，才能使用具有受保護 Health 資訊 (PHI) 的 Amazon 簡單通知服務 (SNS)。客戶必須使用 SNS 在每個 AWS 區域中提供的 HTTPS API 端點。HTTPS 端點利用加密的連線，並保護傳送至 AWS的資料的隱私權和完整性。如需所有 HTTPS API 端點的清單，請參閱AWS 服務端點。

此外，Amazon SNS 還使用這項服務 CloudTrail，可擷取客戶 AWS 帳戶中 Amazon SNS 發出或代表 Amazon SNS 發出的 API 呼叫，並將日誌檔傳送到他們指定的 Amazon S3 儲存貯體。 CloudTrail 擷取從 Amazon SNS 主控台或 Amazon SNS API 進行的 API 呼叫。使用收集的資訊 CloudTrail，客戶可以判斷向 Amazon SNS 發出的請求、提出請求的來源 IP 地址、提出請求的人員以及提出請求的時間。如需記錄 SNS 操作的詳細資訊，請參閱使用記錄 Amazon SNS API 呼叫 CloudTrail。

Amazon Simple Email Service (Amazon SES)

Amazon Simple Email Service (Amazon SES) 是一種靈活且可高度擴展的電子郵件傳送和接收服務。它同時支援 S/MIME 和 PGP 通訊協定來加密訊息以進行完整 end-to-end 加密，而且所有與 Amazon SES 的通訊均使用 SSL (TLS 1.2) 進行保護。客戶可以選擇將 Amazon SES 設定為在將訊息存放在 Amazon S3 儲存貯體之前接收和加密訊息，以存放靜態加密的訊息。如需詳細資訊，請參閱 Amazon

Simple Email Service (Amazon SES) 如何用 AWS KMS來瞭解有關加密訊息以進行儲存的詳細資訊。訊息會透過 HTTPS 端點或加密的 SMTP 連線，在傳輸至 Amazon SES 的過程中得到保護。

對於從 Amazon SES 傳送至接收者的訊息，Amazon SES 會先嘗試與接收郵件伺服器建立安全連線，但如果無法建立安全連線，則會以未加密的方式傳送訊息。若要要求加密才能交付給接收者，客戶必須在 Amazon SES 中建立組態集，並使用 AWS CLI 將 TlsPolicy 屬性設定為「需要」。如需詳細資訊，請參閱 Amazon SES 和安全協定。Amazon SES 與整合 AWS CloudTrail 以監控所有 API 呼叫。使用收集的資訊 AWS CloudTrail，客戶可以判斷要求是否向 Amazon SES、請求的 IP 地址、提出請求的人員、提出請求的時間以及其他詳細資訊。如需詳細資訊，請參閱使用 AWS CloudTrail. Amazon SES 也提供監控傳送活動的方法，例如傳送、拒絕、退回率、交付、開啟和點按。如需詳細資訊，請參閱監控您的 Amazon SES 傳送活動。

Amazon Simple Queue Service (Amazon SQS)

客戶應瞭解下列金鑰加密要求，才能搭配 PHI 使用 Amazon SQS。

- 透過查詢請求與 Amazon SQS 佇列的通訊必須使用 HTTPS 加密。如需提出 SQS 要求的詳細資訊，請參閱發出查詢 API 要求。
- Amazon SQS 支援與整合的伺服器端加密， AWS KMS 以保護靜態資料。新增伺服器端加密功能可讓客戶透過加密佇列的安全性提升，傳輸和接收敏感資料。Amazon SQS 伺服器端加密使用 256 位元進階加密標準 (AES-256 GCM 演算法) 來加密每則訊息的內文。與整合 AWS KMS 可讓客戶集中管理保護 Amazon SQS 訊息的金鑰，以及保護其他 AWS 資源的金鑰。 AWS KMS 記錄每次使用加密金鑰， AWS CloudTrail 以協助滿足法規和合規性需求。如需詳細資訊，並查看區域以瞭解適用於 Amazon SQS SSE 的可用性，請參閱靜態加密。
- 如果未使用伺服器端加密，則必須先加密訊息承載本身，才能傳送至 SQS。加密訊息承載的一種方法是使用 Amazon SQS 擴充用戶端以及 Amazon S3 加密用戶端。如需使用用戶端加密的詳細資訊，請參閱使用 Amazon SQS 擴充用戶端和 Amazon S3 加密用戶端加密訊息承載。

Amazon SQS 使用這項服務 CloudTrail，可記錄客戶 AWS 帳戶中 Amazon SQS 所發出或代表 Amazon SQS 發出的 API 呼叫，並將日誌檔傳送到指定的 Amazon S3 儲存貯體。 CloudTrail 擷取從 Amazon SQS 主控台或 Amazon SQS API 進行的 API 呼叫。客戶可以使用收集 CloudTrail 到的資訊來判斷向 Amazon SQS 發出哪些請求、發出請求的來源 IP 地址、提出請求的人員、提出請求的時間等。如需記錄 SQS 作業的詳細資訊，請參閱使用記錄 Amazon SQS API 呼叫。 AWS CloudTrail

Amazon Simple Storage Service (Amazon S3)

客戶在使用 Amazon S3 時可以選擇加密靜態資料，包括伺服器端和用戶端加密，以及多種管理金鑰的方法。如需詳細資訊，請參閱使用加密保護資料。

與包含 PHI 的 Amazon S3 連線必須使用接受加密傳輸 (HTTPS) 的端點。如需地區端點的清單，請參閱AWS 服務端點。

請勿在儲存貯體名稱、物件名稱或中繼資料中使用 PHI，因為這些資料未使用 S3 伺服器端加密進行加密，而且通常不會在用戶端加密架構中加密。

Amazon Simple Workflow Service

Amazon 簡單工作流程服務 (Amazon SWF) 可協助開發人員建置、執行和擴展具有 parallel 或連續步驟的背景任務。Amazon SWF 可以被視為雲端中的全受管狀態追蹤器和任務協調器。

Amazon 簡單工作流程服務用於協調工作流程，無法存放或傳輸資料。PHI 不應放置在 Amazon SWF 的元數據中或任何任務描述中。Amazon SWF 用 AWS CloudTrail 於記錄所有 API 調用。

Amazon Textract

Amazon Textract 使用機器學習技術，從掃描的文件中自動擷取文字和資料，這些文件超越了簡單的光學字元辨識 (OCR)，以識別、理解和擷取表單和表格中的資料。例如，客戶可以使用 Amazon Textract 自動擷取具有受保護健康資訊 (PHI) 的資料和處理表單，而無需人工干預來完成醫療索賠。

Amazon Textract 也可用來維護文件存檔中的合規性。例如，客戶可以使用 Amazon Textract 從保險索賠或醫療處方擷取資料，並自動識別這些文件中的鍵值對，以便編輯敏感的金鑰值組。

Amazon Textract 支援輸入文件的伺服器端加密 (SSE-S3 和 SSE-KMS)，並針對服務和代理程式之間傳輸中的資料進行 TLS 加密。客戶可以使用 Amazon CloudWatch 追蹤資源使用量指標， AWS CloudTrail 以及擷取傳送給 Amazon Textract 的 API 呼叫。

Amazon Transcribe

Amazon Transcribe 使用先進的機器學習技術來辨識音訊檔案中的語音，並將其轉錄為文字。例如，客戶可以使用 Amazon Transcribe 將美國英文和墨西哥西班牙文音訊轉換為文字，並建立包含音訊檔案內容的應用程式。Amazon Transcribe 可以與包含 PHI 的數據一起使用。Amazon Transcribe 不會保留或存放任何資料，所有對 API 的呼叫都會使用 SSL/TLS 進行加密。Amazon Transcribe 用 CloudTrail 於記錄所有 API 呼叫。

Amazon Translate

Amazon Translate 使用先進的機器學習技術，隨需提供高品質的翻譯。客戶可以使用 Amazon Translate 翻譯非結構化文字文件，或建置以多種語言運作的應用程式。包含 PHI 的文件可以使用 Amazon Translate 進行處理。翻譯包含 PHI 的文件時，不需要額外的組態。傳輸中的資料加密由 SSL/TLS 提供，而且 Amazon Translate 不會保留任何靜態資料。Amazon Translate 用 CloudTrail 於記錄所有 API 呼叫。

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud (Amazon VPC) 提供一組網路安全功能，與 HIPAA 受管制工作負載的架構完全一致。無狀態網路存取控制清單，以及將執行個體動態重新指派至可狀態安全群組等功能，提供彈性保護執行個體免於未經授權的網路存取。

Amazon VPC 還允許客戶將自己的網路地址空間擴展到 AWS，並提供多種將資料中心連接到的方式。AWS VPC 流程記錄會針對執行個體處理、傳輸或儲存 PHI 的已接受和拒絕連線提供稽核追蹤。

AWS Transit Gateway 充當網路中樞，並簡化 Amazon VPC 與現場部署網路之間的連線。 AWS Transit Gateway 還為其他傳輸閘道提供區域間對等功能，以使用骨幹建立全球網路。 AWS 如需 Amazon VPC 的詳細資訊，請參閱 Amazon Virtual Private Cloud。

Amazon WorkDocs

Amazon WorkDocs 是一項完全受管、安全的企業檔案儲存與共用服務，具備強大的管理控制和回饋功能，可提升使用者生產力。 Amazon WorkDocs 使用客戶透過 AWS Key Management Service (AWS KMS) 管理的金鑰靜態加密檔案。所有傳輸中的資料均使用 SSL/TLS 加密。 AWS Web 和行動應用程式，以及桌面同步用戶端，可直接 Amazon WorkDocs 使用 SSL/TLS 傳輸檔案。

管理 WorkDocs 員可以使用 Amazon WorkDocs 管理主控台檢視稽核記錄，依時間追蹤檔案和使用者活動，並選擇是否允許使用者與組織外的其他人共用檔案。 Amazon WorkDocs 也與 CloudTrail (擷取客戶帳戶 Amazon WorkDocs 中代表或代表客戶 AWS 帳戶發出的 API 呼叫的服務) 整合，並將 CloudTrail 日誌檔交付到客戶指定的 Amazon S3 儲存貯體。

使用 RADIUS 伺服器的多重要素驗證 (MFA) 可供客戶在驗證程序期間提供額外的安全性。使用者透過輸入其使用者名稱和密碼，然後輸入由硬體或軟體權杖提供的 OTP (一次性密碼) 來登入。

如需詳細資訊，請參閱：

- Amazon WorkDocs 特徵

- 使用記錄 Amazon WorkDocs API 呼叫 AWS CloudTrail

客戶不應以檔案名稱或目錄名稱儲存 PHI。

Amazon WorkSpaces

Amazon WorkSpaces 是在上運行的全受管，安全的 D esktop-as-a 服務（DaaS）解決方案。 AWS透過 Amazon WorkSpaces，客戶可以輕鬆地為使用者佈建虛擬的雲端型 Microsoft Windows 桌面，讓他們隨時隨地透過任何支援的裝置存取所需的文件、應用程式和資源。

Amazon 將數據 WorkSpaces 存儲在 Amazon 彈性塊存儲卷中。客戶可以使用客戶管理的金鑰來加密客戶的 WorkSpaces儲存磁碟區 AWS Key Management Service。在上啟用加密時 WorkSpace，儲存在基礎儲存體中的靜態資料和磁碟儲存體的自動備份 (EBS 快照) 都會根據指導進行加密。來自用 WorkSpace 戶端的通訊 WorkSpace 是使用 SSL/TLS 來保護的。如需有關使用 Amazon 靜態加密的詳細資訊 WorkSpaces，請參閱加密 WorkSpaces。

AWS App Mesh

AWS App Mesh 是一種服務網格，可提供應用程式層級聯網，讓您的服務能夠輕鬆地跨多種類型的運算基礎設施彼此通訊，例如 Amazon ECS、Amazon EKS 或 Amazon EC2 服務。App Mesh 配置 Envoy 代理以收集觀察性數據並將其傳輸到您配置的監控集惡習，從而為您提供可見性。 end-to-end 它可以根據設定的路由和流量原則來路由流量，以確保應用程式的高可用性。應用程式之間的流量可設定為使用 TLS。App Mesh 可以使用 AWS SDK 或 App Mesh 控制器為 Kubernetes 使用。雖然屬於 HIPAA 合格服務，但由於不支援保護 AWS App Mesh 此類資料， AWS App Mesh 因此不應將 PHI 儲存在任何資源名稱/屬性中。相反， AWS App Mesh 可用於監視、控制和保護傳輸或儲存 PHI 的客戶網域資源。

AWS 應用程式遷移

AWS 應用程式遷移服務 (AWS MGN) 可讓您快速地將伺服器和應用程式移轉至中，而不需要變更 AWS，而且將停機時間降至最低。 AWS MGN 是建議用於升降機和輪班移轉至的主要移轉 AWS服務。

AWS MGN 使用區塊層級資料複寫將來源磁碟直接複製到客戶帳戶中的 EBS 磁碟區-資料永遠不會透過 AWS MGN 控制的雲端環境傳輸。依預設，複製的資料會在傳輸過程中加密。依預設，客戶 EBS 磁碟區中的資料會使用客戶自己的金鑰加密。

AWS Auto Scaling

AWS Auto Scaling 可讓客戶在幾分鐘內為屬於客戶應用程式一部分的 AWS 資源設定自動調整規模。客戶可以將 AWS Auto Scaling 用於一些涉及 PHI 的服務，例如 Auto Scaling 動擴展群組中的 Amazon DynamoDB、Amazon ECS、亞馬遜 RDS Aurora 複本和 Amazon EC2 執行個體。

AWS Auto Scaling 是一種協調服務，不會直接處理、儲存或傳輸客戶內容；因此，客戶可以將此服務與加密內容搭配使用。 AWS 共同責任模型適用於 AWS Auto Scaling 中的資料保護： AWS 負責 AWS 網路安全性程序，而客戶則負責維持對此基礎架構上託管之客戶內容的控制權。此內容包括客戶使用之 AWS 服務的安全性設定和管理工作。基於資料保護目的，我們建議客戶使用 AWS Identity and Access Management (IAM) 保護 AWS 帳戶登入資料，並設定個別使用者帳戶。如此一來，每個使用者都只會獲得授予完成其任務所必須的許可。

我們強烈建議客戶不要將敏感的識別資訊 (例如客戶帳號) 放入任意格式欄位 (例如「名稱」欄位) 中。這包括當客戶使用 AWS Management Console、API 或 AWS SDK 使用 AWS Auto Scaling 或其他 AWS 服務時。 AWS CLI

客戶在 AWS Auto Scaling 或其他服務中輸入的任何資料都可能會被拾取以包含在診斷記錄中。當客戶向外部伺服器提供 URL 時，不應在 URL 中包含認證資訊，以驗證其對該伺服器的要求。 AWS 同時建議客戶以下列方式保護其資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源進行通訊。我們建議使用 TLS 1.2 或更新版本
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案，以及 AWS 服務中的所有預設安全性控制。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Simple Storage Service (Amazon Simple Storage Service (Amazon S3)) 的個人資料。

AWS Backup

AWS Backup 提供集中式、全受管且以政策為基礎的服務，以保護客戶資料並確保各項服務的合規性，以達成業 AWS 務持續性。使用此功能 AWS Backup，客戶可以集中設定資料保護 (備份) 政策，並監控跨客戶 AWS 資源的備份活動，包括 Amazon EBS 磁碟區、Amazon Relational Database Service 服務 (Amazon RDS) 資料庫 (包括 Aurora 叢集)、Amazon DynamoDB 表、Amazon 彈性檔案系統 (Amazon EFS)、Amazon FSx 檔案系統、Amazon EC2 執行個體和磁碟區。 AWS Storage Gateway

AWS Backup 加密傳輸中和靜態的客戶資料。使用來源服務的快照加密方法，使用現有快照功能的服務備份進行加密。例如，EBS 快照會使用建立快照之磁碟區的加密金鑰加密。

來自引入建置備份功能 (例如 Amazon EFS) 的較新 AWS 服務備份，會獨立於 AWS Backup來源服務的傳輸中和靜態加密，為客戶提供額外的備份保護。加密是在「Backup 保存庫」層級設定的。預設保管庫已加密。當客戶建立新的儲存庫時，必須選取加密金鑰。

AWS Batch

AWS Batch 讓開發人員、科學家和工程師能夠輕鬆有效率地執行數十萬個批次運算工作 AWS。 AWS Batch 根據提交的批次工作的數量和特定資源需求，動態佈建運算資源的最佳數量和類型 (例如 CPU 或記憶體最佳化執行個體)。 AWS Batch 針對所有運算服務和功能規劃、排程和執行批次運 AWS 算工作負載。

與 Amazon ECS 的指引類似，PHI 不應直接放置在任務定義、任務佇列或的標籤中。 AWS Batch相反地，排程和執行的工作 AWS Batch 可能會在加密的 PHI 上運作。工作階段傳回的任何資訊也不 AWS Batch 應包含任何 PHI。每當正在執行的作業 AWS Batch 必須傳輸或接收 PHI 時，該連線應該使用 HTTPS 或 SSL/TLS 加密。

AWS Certificate Manager

AWS Certificate Manager 這項服務可讓客戶輕鬆佈建、管理及部署公用和私有 SSL/TLS 憑證，以搭配 AWS 服務及其內部連線資源使用。 AWS Certificate Manager 用 CloudTrail 於記錄所有 API 呼叫。

如果使用者想要與 AWS 之外的 AWS Management Console. 授與程式設計存 AWS取權的方式取決於正在存取的使用者類型。

若要授與使用者程式設計存取權，請選擇下列其中一個選項。

哪個使用者需要程式設計存取權？	到	By
人力身分 (IAM Identity Center 中管理的使用者)	使用臨時登入資料來簽署對 AWS CLI、 AWS SDK 或 AWS API 的程式設計要求。	請依照您要使用的介面所提供的指示操作。 • 如需詳細資訊 AWS CLI，請參閱《使 AWS CLI 用AWS Command Line Interface者

哪個使用者需要程式設計存取權？	到	By
		指南》 AWS IAM Identity Center中的〈配置使用〉。 • 如需 AWS SDK、工具和 AWS API，請參閱 AWS SDK 和工具參考指南中的 IAM 身分中心身分驗證。
IAM	使用臨時登入資料來簽署對 AWS CLI、 AWS SDK 或 AWS API 的程式設計要求。	遵循《IAM 使用者指南》中的〈將臨時登入資料搭配 AWS 資源使用〉中的指示
IAM	(不建議使用) 使用長期認證來簽署對 AWS CLI、 AWS SDK 或 AWS API 的程式設計要求。	請依照您要使用的介面所提供的指示操作。 • 如需相關資訊 AWS CLI，請參閱使用指南中的使用 IAM 使用者登入資料進行驗證。AWS Command Line Interface • 對於 AWS SDK 和工具，請參閱 AWS SDK 和工具參考指南中的使用長期憑據進行身份驗證。 • 如需 AWS API，請參閱 IAM 使用者指南中的管理 IAM 使用者的存取金鑰。

AWS Cloud Map

AWS 雲端地圖是雲端資源探索服務。使用 AWS 雲端地圖，客戶可以為應用程式資源定義自訂名稱，例如 Amazon ECS 任務、Amazon EC2 執行個體、Amazon S3 儲存貯體、Amazon DynamoDB 表格、Amazon SQS 佇列或任何其他雲端資源。然後，客戶可以使用這些自訂名稱，使用 AWS SDK 和經過驗證的 API 查詢，從應用程式中探索雲端資源的位置和中繼資料。雖然 AWS 雲端地圖是 HIPAA

合格服務，但由於不支援保護此類資料，因此不應將 PHI 存放在 AWS 雲端對應內的任何資源名稱/屬性中。相反地，AWS 雲端對應可用於探索傳輸或存放 PHI 的客戶網域資源。

AWS CloudFormation

AWS CloudFormation 讓客戶能夠以預測和重複的方式建立和佈建 AWS 基礎設施部署。它可協助客戶利用 Amazon EC2、Amazon 彈性區塊存放區、Amazon SNS、Elastic Load Balancing 和自動擴展等 AWS 產品，在雲端建置高度可靠、可高度擴展且具成本效益的應用程式，而不必擔心建立和設定基礎 AWS 基礎設施。 AWS CloudFormation 可讓客戶使用範本檔案，以單一單元 (堆疊) 的形式一起建立和刪除資源集合。

AWS CloudFormation 本身並不儲存、傳輸或處理 PHI。相反地，它是用來建置和部署使用其他 AWS 服務的架構，這些服務可能會存放、傳輸和/或處理 PHI。只有 HIPAA 合格的服務應與 PHI 一起使用。請參閱本白皮書中這些服務的項目，以取得在這些服務中使用 PHI 的指引。 AWS CloudFormation 用 AWS CloudTrail 於記錄所有 API 呼叫。

AWS CloudHSM

AWS CloudHSM 是雲端硬體安全模組 (HSM)，可讓客戶在 AWS 雲端輕鬆產生和使用自己的加密金鑰。透過 CloudHSM，客戶可以使用 FIPS 140-2 第 3 級驗證的 HSM 來管理自己的加密金鑰。CloudHSM 為客戶提供使用開放標準 API (例如 PKCS #11、Java 加密延伸模組 (JCE) 和 Microsoft 加密 (CNG) 程式庫與應用程式整合的彈性。

CloudHSM 也符合標準，可讓客戶將所有金鑰匯出至大多數其他市售 HSM。硬體應用裝置金鑰管理服務也無法儲存或傳輸 PHI。 AWS CloudHSM 客戶不應將 PHI 儲存在標籤 (中繼資料) 中。不需要其他特別指導。

AWS CloudTrail

AWS CloudTrail 是一項可對 AWS 帳戶進行管理、合規、操作稽核和風險稽核的服務。使用此功能 CloudTrail，客戶可以記錄、持續監控和保留與 AWS 基礎設施中動作相關的帳戶活動。 CloudTrail 提供 AWS 帳戶活動的事件歷史記錄，包括透過 AWS 開發套件 AWS Management Console、命令列工具和其他 AWS 服務執行的動作。此事件歷史記錄可簡化安全分析、資源變更追蹤及疑難排解。

AWS CloudTrail 已啟用可用於所有 AWS 帳戶，並可根據 AWS BAA 的要求用於稽核記錄。應使用 CloudTrail 主控台或 AWS 命令列界面建立特定追蹤。 CloudTrail 在建立加密的 Trail 時，加密傳輸中和靜態的所有流量。當可能存在記錄 PHI 時，應建立加密的追蹤。

根據預設，加密的追蹤會使用伺服器端加密搭配 Amazon S3 (SSE-S3) 受管金鑰，將項目存放在 Amazon S3 中。如果需要對金鑰進行其他管理，也可以使用 AWS KMS受管理的金鑰 (SSE-KMS) 來設定。 CloudTrail 就像 AWS 日誌項目的最終目的地一樣，因此，處理 PHI 之任何架構的關鍵元件都應該啟用 CloudTrail 日誌檔完整性驗證，並定期檢閱相關聯的 CloudTrail 摘要檔。一旦啟用，就可以建立記錄檔尚未變更或變更的正面宣告。

AWS CodeBuild

AWS CodeBuild 是雲端中完全受控的建置服務。 AWS CodeBuild 編譯原始程式碼、執行單元測試，以及產生準備好部署的成品。 AWS CodeBuild 使用密 AWS KMS 鑰來加密構建輸出成品。建置包含 PHI、密碼/密碼、憑證等 AWS CodeBuild 用 AWS CloudTrail 來記錄所有 API 呼叫的成品之前，應先建立和設定 KMS 金鑰。

AWS CodeDeploy

AWS CodeDeploy 是一種全受管部署服務，可將軟體部署自動化到各種運算服務，包括 Amazon EC2、 AWS Fargate AWS Lambda、和現場部署伺服器。客戶用 AWS CodeDeploy 來快速發行容器化工作負載的新功能，並處理更新應用程式的複雜性。

AWS CodeDeploy 支援用於部署人工因素的伺服器端加密 (SSE-S3)，並支援 TLS 加密服務與代理程式之間傳輸中的資料。客戶可以使用 Amazon CloudWatch 事件追蹤部署並擷 AWS CloudTrail 取對其的 API 呼叫 AWS CodeDeploy。

AWS CodeCommit

AWS CodeCommit 是一種安全、可高度擴充的受管原始檔控制服務，可託管私有 Git 儲存庫。 AWS CodeCommit 客戶無需管理自己的原始檔控制系統，也不必擔心擴充其基礎架構。

AWS CodeCommit 加密傳輸和靜態中的所有流量和存儲的信息。根據預設，當在中建立儲存庫時 AWS CodeCommit，會使用建立 AWS 受管金鑰， AWS KMS 且僅由該儲存庫使用來加密儲存的所有靜態資料。 AWS CodeCommit 用 AWS CloudTrail 於記錄所有 API 呼叫。

AWS CodePipeline

AWS CodePipeline 是一項全受管的持續交付服務，可協助客戶自動化客戶發行管道，進行快速可靠的應用程式和基礎架構更新 客戶用 AWS CodePipeline 來允許研究人員自動處理臨床試驗數據，實驗室結果和基因組數據是客戶使用的工作流程管道的幾個例子。

AWS CodePipeline 支援用於程式碼人工因素的伺服器端加密 (SSE-S3 和 SSE-KMS)，並針對服務與代理程式之間傳輸中的資料進行 TLS 加密。客戶可以使用 Amazon CloudWatch 事件追蹤管道變更並擷 AWS CloudTrail 取對其的 API 呼叫 AWS CodePipeline。

AWS Config

AWS Config 提供與客戶 AWS 帳戶相關聯的資源的詳細檢視，包括如何設定這些資源、彼此之間的關聯性，以及組態及其關係在一段時間內如何變更。

AWS Config 本身不能用於存儲或傳輸 PHI。

相反，它可以用來監控和評估使用其他 AWS 服務建立的架構 (包括處理 PHI 的架構)，以協助判斷它們是否符合預期的設計目標。處理 PHI 的架構只能使用 HIPAA 合格的服務來建立。 AWS Config 用 AWS CloudTrail 於記錄所有結果。

AWS Data Exchange

AWS Data Exchange 可讓您輕鬆在雲端中尋找、訂閱和使用第三方資料。訂閱資料產品後，客戶可以使用 AWS Data Exchange API 將資料直接載入 Amazon S3，然後使用各種 AWS 分析和機器學習服務進行分析。對於資料供應商而言，AWS Data Exchange 不需要為資料儲存、交付、計費和授權建立和維護基礎設施，輕鬆觸及數百萬移轉到雲端的 AWS 客戶。

AWS Data Exchange 一律會加密存放在靜態服務中的所有資料產品，而不需要任何其他設定。此加密會透過服務受管理的 KMS 金鑰自動完成。AWS Data Exchange 使用傳輸層安全性 (TLS) 和用戶端加密來進行傳輸中的加密。與 AWS Data Exchange 的通訊一律會透過 HTTPS 完成，因此客戶的資料在傳輸過程中一律會加密。客戶使用 AWS Data Exchange 時，預設會設定此加密。如需詳細資訊，請參閱 AWS Data Exchange 中的資料保護。

AWS Data Exchange 已與 AWS CloudTrail. AWS CloudTrail 以事件形式擷取對 AWS Data Exchange API 的所有呼叫，包括來自 AWS Data Exchange 主控台的呼叫，以及從程式碼呼叫到 AWS Data Exchange API 操作。客戶可以採取的某些動作是僅限主機的動作。AWS 開發套件或 AWS CLI 中沒有對應的 API。這些是依賴 AWS Marketplace 功能的動作，例如發佈或訂閱產品。AWS Data Exchange 會為這些僅限主控台動作的子集提供 CloudTrail 記錄。如需詳細資訊，請參閱使用記錄 AWS Data Exchange API 呼叫 AWS CloudTrail。

請注意，所有使用 AWS Data Exchange 的清單都必須遵守 AWS 資料交換指南和 AWS Marketplace 供應商適用的 AWS Data Exchange 常見問答集，這些問題會限制特定類別的資料。如需詳細資訊，請參閱 AWS Data Exchange 常見問答集。

AWS Database Migration Service

AWS Database Migration Service (AWS DMS) 協助客戶輕鬆安全地將資料庫遷移到 AWS。客戶可以在最廣泛使用的商業和開放原始碼資料庫 (例如甲骨文、MySQL 和 PostgreSQL) 之間移轉資料。此服務支援同質遷移 (例如 Oracle 至 Oracle) 以及不同資料庫平台之間的異質遷移 (例如 Oracle 至 PostgreSQL 或 MySQL 至 Oracle)。

在現場部署執行並透過 AWS DMS 遷移到雲端的資料庫可以包含 PHI 資料。AWS DMS 會在傳輸過程中和資料暫存時加密資料，以便最終遷移到 AWS 上的目標資料庫。AWS DMS 會加密複寫執行個體使用的儲存和端點連線資訊。為了加密複寫執行個體使用的儲存，AWS DMS 會使用 AWS 帳戶唯一的 AWS KMS 金鑰。請參閱適當目標資料庫的指引，以確保資料在移轉完成後仍保持加密狀態。AWS DMS 用 CloudTrail 於記錄所有 API 呼叫。

AWS DataSync

AWS DataSync 是一種線上傳輸服務，可簡化、自動化和加速現場部署儲存與 AWS 之間的資料移動。客戶可以使 DataSync 用 AWS 將其資料來源連接到 Amazon S3 或 Amazon EFS。客戶應確保 Amazon S3 和 Amazon EFS 的設定方式與指導一致。根據預設，客戶資料會在傳輸過程中使用 TLS 1.2 加密。如需有關加密和 AWS 的詳細資訊 DataSync，請參閱 AWS DataSync 功能。客戶可以 DataSync 使用 AWS CloudTrail. 如需使用記錄的詳細資訊 CloudTrail，請參閱使用 AWS CloudTrail. DataSync

AWS Directory Service

適用於 Microsoft AD 的 AWS Directory Service

適用於 Microsoft 活動目錄（企業版）的 AWS Directory Service，也稱為 AWS Microsoft AD，可讓目錄感知工作負載和 AWS 資源在 AWS 雲端中使用受管的活動目錄。AWS Microsoft AD 會使用 AWS 管理的加密金鑰，將目錄內容 (包括含有 PHI 的內容) 存放在加密的 Amazon 彈性區塊存放區磁碟區中。如需詳細資訊，請參閱 Amazon EBS 加密。

透過客戶的亞馬遜虛擬私人雲端 (VPC) 網路透過輕量型目錄存取通訊協定 (LDAP) 傳輸至 Active Directory 用戶端和傳出 Active Directory 用戶端的傳輸中資料會加密。如果 Active Directory 用戶端位於內部部署網路中，則流量會透過虛擬私人網路連結或連結傳送至客戶的虛擬私人雲端。 AWS Direct Connect

Amazon 雲端目錄

Amazon Cloud Directory 可讓客戶建立彈性的雲端原生目錄，以便在多個維度上組織資料階層。客戶也可以為各種使用案例建立目錄，例如組織圖、課程目錄和裝置登錄。例如，客戶可以建立組織圖，以便在報告結構、地點和成本中心的不同階層中導覽。Amazon Cloud Directory 會使用由 () 管理的 256 位元加密金鑰，自動加密靜態和傳輸中的資料。 AWS Key Management Service AWS KMS

AWS Elastic Beanstalk

有了 AWS Elastic Beanstalk，客戶可以在 AWS 雲端快速部署和管理應用程式，而不必了解執行這些應用程式的基礎設施。客戶只需上傳程式碼並 AWS Elastic Beanstalk 自動處理部署作業，從容量佈建、負載平衡、自動調整規模到應用程式健康狀態監控。同時，客戶保留對支援應用程式的 AWS 資源的完整控制權，並可隨時存取基礎資源。

AWS Elastic Beanstalk 本身並不儲存、傳輸或處理 PHI。相反地，客戶可以使用它來建立和部署架構，搭配其他可能存放、傳輸和/或處理 PHI 的 AWS 服務。客戶在選擇部署的服務時，應確保僅 AWS Elastic Beanstalk 將 HIPAA 合格服務與 PHI 搭配使用。如需將 PHI 與這些服務搭配使用的指引，請參閱本白皮書中這些服務的項目。

客戶不應在任何自由格式欄位 AWS Elastic Beanstalk (例如「名稱」欄位) 中包含 PHI。 AWS Elastic Beanstalk 用 AWS CloudTrail 於記錄所有 API 呼叫。

AWS 彈性災難復原

AWS 彈性災難復原 (AWS DRS) 使用經濟實惠的儲存裝置、最少運算和復原，快速可靠地復原現場部署和雲端應用程式，將停機時間和 point-in-time 資料遺失降到最低。

客戶可以在其來源伺服器上設定 AWS 彈性災難復原，以啟動安全的資料複寫。他們的資料會複寫到 AWS 帳戶中所選 AWS 區域的暫存區子網路。暫存區設計透過使用經濟實惠的儲存裝置和最少的運算資源來維護持續複寫，降低成本。AWS 彈性災難復原複寫的客戶資料會在傳輸過程中使用 TLS 1.2 加密，並直接從其來源伺服器傳輸到 VPC。客戶可以利用私有連線 (例如 AWS Direct Connect 或 VPN) 來設定複寫路由。客戶資料也可以在 AWS 上使用 Amazon EBS 加密進行靜態加密。

客戶可以執行不中斷的測試，以確認實作已完成。在正常作業期間，監控複寫並定期執行不中斷的復原與容錯回復演練，以維持準備狀態。如果客戶需要復原應用程式，他們可以使用最多的 up-to-date 伺服器狀態或先前的時間點，在幾分鐘內在 AWS 上啟動復原執行個體。客戶應用程式在 AWS 上執行之後，可以選擇將應用程式保留在該處，或者在問題解決後啟動資料複寫回其主要站台。客戶可能會在準備就緒時失敗回到其主要站台。

AWS Fargate

AWS Fargate 這項技術可讓客戶執行容器，而不必管理伺服器或叢集。有了 AWS Fargate，客戶不再需要佈建、設定和擴展虛擬機器叢集來執行容器。這樣就不需要選擇伺服器類型、決定何時擴展叢集或最佳化叢集封裝。 AWS Fargate 無需客戶與伺服器或叢集互動或考慮伺服器或叢集。借助 Fargate，客戶專注於設計和構建應用程序，而不是管理運行應用程序的基礎架構。

Fargate 不需要任何其他配置即可處理 PHI 的工作負載。客戶可以使用 Amazon ECS 等容器協調服務，在 Fargate 上執行容器工作負載。Fargate 僅管理基礎架構，不會使用正在協調的工作負載中的資料或對資料進行操作。為了符合 HIPAA 的要求，無論何時傳輸中或靜態，當使用 Fargate 啟動的容器存取 PHI 時，仍應加密 PHI。本 paper 皮書所述的每個 AWS 儲存選項均提供多種靜態加密機制。如需其他 HIPAA 安全性和組態資訊，請參閱 Amazon EKS 上的 HIPAA 安全與合規架構白皮書。

AWS Firewall Manager

AWS Firewall Manager 是一項安全管理服務，允許客戶集中配置和管理中客戶帳戶和應用程序的防火牆規則 AWS Organizations。建立新應用程式時，Firewall Manager 可透過強制執行一組通用的安全規則，輕鬆將新的應用程式和資源納入法規遵循。現在，客戶可以透過單一服務來建置防火牆規則、建立安全性原則，並以一致、階層式的方式在整個基礎架構中強制執行這些規則，從中央系統管理員帳戶。

AWS Firewall Manager 是一種協調服務，不會直接處理、儲存或傳輸使用者資料。此服務不會加密客戶內容，但 AWS Firewall Manager 使用的基礎服務 (例如 DynamoDB) 會加密使用者資料。

AWS Global Accelerator

AWS Global Accelerator 是一項全域負載平衡服務，可改善多區域應用程式的可用性和延遲時間。為了確保 PHI 在傳輸和靜態使用時保持加密狀態 AWS Global Accelerator，由全域加速器負載平衡的架構應該使用加密的通訊協定，例如 HTTPS 或 SSL/TLS。請參閱 Amazon EC2、Elastic Load Balancing 和其他 AWS 服務的指導，以進一步了解後端資源的可用加密選項。 AWS Global Accelerator 用 AWS CloudTrail 於記錄所有 API 呼叫。

AWS Glue

AWS Glue 是完全受控的 ETL (擷取、轉換和載入) 服務，可讓客戶輕鬆分類資料、清理資料、豐富資料，以及在各種資料存放區之間可靠地移動資料，並且符合成本效益。為了確保在傳輸過程中包含 PHI 的數據的加密， AWS Glue 應配置為使用 JDBC 連接到具有 SSL/TLS 的數據存儲。此外，為了在傳

輸中保持加密，伺服器端加密 (SSE-S3) 的設定應當作參數傳遞給使用執行的 ETL 工作。 AWS Glue 在建立資料目錄物件 AWS KMS 時啟用加密時，會使用所管理的 AWS Glue 金鑰加密儲存在「資料目錄」中的所有靜態資料。 AWS Glue 用 CloudTrail 於記錄所有 API 呼叫。

AWS Glue DataBrew

AWS Glue DataBrew 是全受管的視覺化資料準備服務，可讓資料分析師和資料科學家輕鬆清理和標準化資料，為分析和機器學習做好準備。為了確保在傳輸過程中包含 PHI 的數據的加密， DataBrew 應配置為使用 JDBC 連接到具有 SSL/TLS 的數據存儲。連線至 JDBC 資料來源時，請 DataBrew 使用 AWS Glue 連線上的設定，包括「需要 SSL 連線」選項。此外，若要在 S3 儲存貯體中靜態時保持加密，伺服器端加密 (SSE-S3 或 SSE-KMS) 的設定應當做參數傳遞給任務。 DataBrew

AWS IoT 核心與 AWS IoT Device Management

AWS IoT 在連接網際網路的裝置 (例如感應器、致動器、嵌入式微控制器或智慧設備以及 AWS 雲端) 之間進行核心，並 AWS IoT Device Management 提供安全的雙向通訊。 AWS IoT 核心並且現在 AWS IoT Device Management 可以容納傳輸包含 PHI 資料的裝置。與 AWS IoT 核心的所有通信 AWS IoT Device Management ，並使用 TLS 加密。 AWS IoT 核心並 AWS IoT Device Management 用 AWS CloudTrail 於記錄所有 API 呼叫。

AWS IoT Greengrass

AWS IoT Greengrass 可讓客戶以安全的方式執行連線裝置的本機運算、訊息、資料快取、同步和 ML 推論功能。 AWS IoT Greengrass 使用 X.509 憑證、受管訂閱、 AWS IoT 政策以及 IAM 政策和角色來確保客戶的 Greengrass 應用程式安全無虞。 AWS IoT Greengrass 使用傳 AWS IoT 輸安全性模型來加密使用 TLS 與雲端的通訊。此外，靜態 (在雲端) 時， AWS IoT Greengrass 資料也會加密。如需 Greengrass 安全性的詳細資訊，請參閱安全性概觀。 AWS IoT Greengrass

客戶可 AWS IoT Greengrass 以使用 AWS CloudTrail. 如需詳細資訊，請 AWS IoT Greengrass 參閱使用 AWS CloudTrail.

AWS Lambda

AWS Lambda 可讓客戶執行程式碼，而不需要自行佈建或管理伺服器。 AWS Lambda 在一個區域的多個可用區域中使用 Amazon 彈性運算雲端 (Amazon EC2) 執行個體的運算叢集，以提供 AWS 基礎設施的高可用性、安全性、效能和可擴展性。

為了確保 PHI 在使用時保持加密狀態 AWS Lambda，與外部資源的連線應該使用加密的通訊協定，例如 HTTPS 或 SSL/TLS。例如，從 Lambda 程序存取 S3 時，應透過以下方式解決此問題：https://bucket.s3-aws-region.amazonaws.com。

如果有任何 PHI 在執行中 AWS KMS 的程序中放置或閒置，則應使用從或取得的金鑰對其進行加密用戶端或伺服器端。 AWS CloudHSM透過服務觸發 AWS Lambda 功能時，請遵循 Amazon API Gateway 的相關指引。使用來自其他 AWS 服務的事件觸發 AWS Lambda 函數時，事件資料不應包含 (本身) PHI。例如，當從 S3 事件 (例如 S3 中的物件到達) 觸發 Lambda 程序時，轉送至 Lambda 的物件名稱不應該有任何 PHI，儘管物件本身可以包含此類資料。

AWS Managed Services

AWS Managed Services 提供 AWS 基礎架構的持續管理。透過實施最佳實務來維護客戶的基礎架構，AWS Managed Services 有助於降低營運開銷和風險。 AWS Managed Services 自動執行變更要求、監控、修補程式管理、安全性和備份服務等常見活動，並提供佈建、執行和支援基礎架構的完整生命週期服務。

客戶可以用 AWS Managed Services 來管理使用包含 PHI 之資料運作的 AWS 工作負載。的使用 AWS Managed Services 不會改變符合 PHI 使用資格的 AWS 服務。提供的工具和自動化 AWS Managed Services 不能用於 PHI 的存儲或傳輸。

AWS OpsWorks 廚師自動化

AWS OpsWorks Chef Automation 是一項全受管的組態管理服務，可託管 Chef Automation，這是 Chef 提供的一組用於基礎架構和應用程式管理的自動化工具 該服務本身不包含，傳輸或處理任何 PHI 或敏感信息，但客戶應確保 OpsWorks 為 Chef Automatic 配置的任何資源配置與指南一致。使用擷取 API 呼叫 AWS CloudTrail。如需詳細資訊，AWS OpsWorks 請參閱使用 AWS CloudTrail.

AWS OpsWorks 對於木偶企業

AWS OpsWorks Puppet 企業版是一項完全受控的組態管理服務，主控 Puppet 企業，這是 Puppet 提供的一組自動化工具，用於基礎結構和應用程式管理。服務本身不包含、傳輸或處理任何 PHI 或敏感資訊，但客戶應確保 OpsWorks針對 Puppet Enterprise 設定的任何資源設定均符合指引。使用擷取 API 呼叫 AWS CloudTrail。如需詳細資訊，AWS OpsWorks 請參閱使用 AWS CloudTrail.

AWS OpsWorks 堆疊

AWS OpsWorks Stacks 提供了一種簡單而靈活的方式來建立和管理堆疊和應用程式。客戶可以使用 AWS OpsWorks Stack 來部署和監控堆疊中的應用程式。

AWS OpsWorks 堆疊會在傳輸過程中加密所有流量。但是，無法使用加密的資料包 (Chef 資料儲存機制)，且必須安全存放的任何資產 (例如 PHI、秘密/密碼、憑證等) 都應存放在 Amazon S3 的加密儲存貯體中。AWS OpsWorks 堆疊用 AWS CloudTrail 來記錄所有 API 呼叫。

AWS Organizations

AWS Organizations 協助客戶集中管理和控管其 AWS 資源的成長和擴展環境。他們可以使用 AWS Organizations程式設計方式建立新的 AWS 帳戶和分配資源、將帳戶分組以組織工作流程、將政策套用至帳戶或群組以進行管理，以及針對所有帳戶使用單一付款方式簡化帳單。

此外， AWS Organizations 還與其他 AWS 服務整合，因此客戶可以定義組織中的帳戶之間的中央組態、安全機制、稽核需求和資源共用。 AWS Organizations 所有 AWS 客戶均可使用，不收取額外費用。

AWS Organizations 是一種協調服務，不會直接處理、儲存或傳輸使用者資料。該服務不會加密客戶內容，但在其中 AWS Organizations啟動的基礎服務會對用戶數據進行加密。 AWS Organizations 與中提供使用者 AWS CloudTrail、角色或 AWS 服務所採取動作記錄的服務整合 AWS Organizations。

AWS RoboMaker

AWS RoboMaker 可讓客戶在雲端執行程式碼以進行應用程式開發，並提供機器人模擬服務以加速應用程式測試。AWS RoboMaker 也為遠端應用程式部署、更新和管理提供機器人叢集管理服務。

包含 PHI 的網路流量必須加密傳輸中的資料。與模擬伺服器的所有管理通訊均透過 TLS 進行，客戶應使用開放標準傳輸加密機制連線至其他 AWS 服務。AWS RoboMaker 也與整合，可 CloudTrail 將所有 API 呼叫記錄到特定的 Amazon S3 儲存貯體。

AWS RoboMaker 日誌不包含 PHI，模擬伺服器使用的 EBS 磁碟區也會加密。將可能包含 PHI 的資料傳輸到其他服務 (例如 Amazon S3) 時，客戶必須遵循接收服務的指導來存放 PHI。對於機器人的部署，客戶必須確保傳輸中和靜態資料的加密與他們對指南的解釋一致。

AWS 開發套件指標

企業客戶可以使用 AWS CloudWatch 代理程式搭配適用於企業 Support 的 AWS 開發套件指標 (SDK 指標)，從其主機和用戶端上的 AWS 開發套件收集指標。這些指標與 AWS 企業 Support 共用。SDK 指標可協助客戶收集應用程式與 AWS 服務連線的相關指標和診斷資料，而無需在程式碼中新增自訂檢測，並減少與其共用日誌和資料所需的手動工作 AWS Support。

請注意，SDK 指標僅適用於擁有企業 Support 訂閱的 AWS 客戶。客戶可以將 SDK 指標與任何直接呼叫 AWS 服務的應用程式搭配使用，而這些應用程式是使用 AWS 指標文件中列出的其中一個版本所建立的 AWS 開發套件。

SDK 指標會監控 AWS 開發套件所進行的呼叫，並使用在與用戶端應用程 CloudWatch 式相同環境中執行的代理程式。

CloudWatch 代理程式會將從本機電腦傳輸中的資料加密到目的地記錄群組中的傳送。您可以將記錄群組設定為依照使用加密記錄檔中的 CloudWatch 記錄資料中的指示進行加密 AWS KMS。

AWS Secrets Manager

AWS Secrets Manager 是一項 AWS 服務，可讓客戶更輕鬆地管理「機密」。密碼可以是資料庫認證、密碼、協力廠商 API 金鑰，甚至是任意文字。 AWS 如果這些信息包含在「秘密」中，則秘密管理器可能用於存儲 PHI。秘密管理 Secre AWS ts Manager 存放的所有密碼都會使用 AWS 金鑰管理系統 (KMS) 進行靜態加密。使用者可以選取建立新密碼時使用的 AWS KMS 金鑰。如果未選取金鑰，則會使用帳戶的預設金鑰。 AWS Secrets Manager 用 AWS CloudTrail 來記錄所有 API 呼叫。

AWS Security Hub

AWS Security Hub 從客戶環境中啟用的 AWS 安全服務收集並整合發現的結果，例如 Amazon 的入侵偵測發現項目 GuardDuty、Amazon Inspector 的漏洞掃描、Amazon Macie 發現的 Amazon S3 儲存貯體政策、IAM 存取分析器可公開存取的跨帳戶資源，以及缺少 WAF 涵蓋範圍的資源。 AWS Firewall Manager AWS Security Hub 還整合了整合 AWS 合作夥伴網路 (APN) 安全解決方案的發現結果。

AWS Security Hub 與 Amazon E CloudWatch vents 整合，讓客戶能夠建立自訂回應和修復工作流程。客戶可以輕鬆地將調查結果發送到 SIIM，聊天工具，票務系統，安全協調自動化和響應（SOAR）工具以及隨時召集管理平台。回應和補救動作可以完全自動化，也可以在主控台中手動觸發。客戶還可以使用自動 AWS Systems Manager 化文件和 AWS Lambda 功能來建立可從中啟動的自動補救工作流程 AWS Security Hub。 AWS Step Functions

為了確保資料保護，請在元件服務之間 AWS Security Hub 加密靜態資料和傳輸中的資料。 AWS Security Hub 作為多個 AWS 合規計劃的一部分，第三方稽核員會評估其安全性和合規性。 AWS Security Hub 是 AWS SOC、ISO、PCI 和 HIPAA 合規計劃的一部分。

AWS Server Migration Service

AWS Server Migration Service (AWS SMS) (AWS SMS) 可自動將現場部署 VMware vSphere 或 Microsoft 超 V/SCVMM 虛擬機器遷移到 AWS 雲端。AWS SMS 會以增量方式將伺服器虛擬機器複寫為雲端託管的 Amazon 機器映像 (AMI)，可在 Amazon EC2 上進行部署。

在現場部署執行並透過 (AWS SMS) 遷移到雲端的伺服器可以包含 PHI 資料。AWS SMS 會在傳輸中以及伺服器虛擬機器映像檔暫存，以便最終放置到 EC2 時加密資料。使用 AWS SMS 遷移含有 PHI 的伺服器虛擬機器時，請參閱 EC2 指南和設定加密儲存磁碟區。AWS 簡訊用 CloudTrail 於記錄所有 API 呼叫。

AWS Serverless Application Repository

AWS Serverless Application Repository (SAR) 是無伺服器應用程式的受管理儲存庫。它可讓團隊、組織和個別開發人員儲存和共用可重複使用的應用程式，並以強大的新方式輕鬆組合和部署無伺服器架構。這些應用程序是 AWS CloudFormation 模板，其中包含應用程序基礎結構的定義和應用程序 AWS Lambda 函數代碼的編譯二進製文件。

雖然可以處理 PHI 的應用程式，但只有在部署 AWS Serverless Application Repository 到客戶帳戶後才會執行此操作，而不是 SAR 本身的一部分。 AWS Serverless Application Repository 會加密客戶上傳的檔案，包括部署套件和層壓縮檔。對於傳輸中的資料，會 AWS Serverless Application Repository 使用 TLS 加密服務與代理程式之間的資料。 AWS Serverless Application Repository 與整合 AWS CloudTrail，這是一項服務，可提供使用者、角色或 AWS 服務在 AWS Serverless Application Repository.

Service Catalog

Service Catalog 可讓 IT 管理員建立、管理及分發已核准產品的產品組合給使用者，使用者隨後可以在個人化入口網站中存取所需的產品。Service Catalog 用於在 AWS 上編目、共用和部署自助解決方案，無法用於存放、傳輸或處理 PHI。PHI 不應放置在 Service Catalog 項目的任何中繼資料或任何項目說明中。Service Catalog 用 AWS CloudTrail 來記錄所有 API 呼叫。

AWS Shield

AWS Shield 是受管的分散式拒絕服務 (DDoS) 保護服務，可保護在 AWS 上執行的 Web 應用程式。AWS Shield 提供永遠在線的偵測和自動內嵌緩解措施，可將應用程式停機時間和延遲降至最低，因此無需參與即可受益 AWS Support 於 DDoS 保護。

AWS Shield 不能用於存儲或傳輸 PHI，但可以用來保護與 PHI 一起操作的 Web 應用程序。因此，參與時不需要特殊配置 AWS Shield。

所有 AWS 客戶都可享受的自動保護功能 AWS Shield Standard，無需額外付費。 AWS Shield Standard 防禦針對其網站或應用程式的常見、經常發生的網路和傳輸層 DDoS 攻擊。如需針對在 Elastic Load Balancing (ELB)、Amazon 和 Amazon CloudFront Route 53 資源上執行之 Web 應用程式的攻擊提供更高層級的保護，客戶可以 AWS Shield Advanced訂閱。

AWS Snowball

使用 AWS Snowball (Snowball)，客戶可以在現場部署資料中心和 Amazon Simple Storage Service (Amazon S3) 之間傳輸數百 TB 或 PB 的資料。存儲在其中的 PHI AWS Snowball 必須按照指南進行靜態加密。建立匯入工作時，客戶必須指定 ARN 作為要用來保護 Snowball 中資料的 AWS KMS 金鑰。此外，在建立匯入任務期間，客戶應選擇符合指導所設定加密標準的目標 S3 儲存貯體。

雖然 Snowball 目前不支援使用 AWS KMS受管金鑰 (SSE-KMS) 進行伺服器端加密，或使用客戶提供的金鑰 (SSE-C) 進行伺服器端加密，但 Snowball 確實支援使用 Amazon S3 代管加密金鑰 (SSE-S3) 的伺服器端加密。如需詳細資訊，請參閱使用伺服器端加密與 Amazon S3 受管加密金鑰 (SSE-S3) 保護資料。

或者，客戶可以使用他們選擇的加密方法來加密 PHI，然後再將資料儲存在其中 AWS Snowball。

目前，客戶可以使用標準 AWS Snowball 設備作為我們 BAA 的一部分。

AWS Snowball 邊

AWS Snowball Edge 使用標準儲存介面連接至現有客戶應用程式和基礎架構，簡化資料傳輸程序，並將設定和整合降至最低。Snowball Edge 可以叢集在一起形成本機儲存層，並在現場處理客戶資料，協助客戶確保他們的應用程式即使無法存取雲端也能繼續執行。

為了確保 PHI 在使用 Snowball Edge 時保持加密狀態，客戶在使用提供支援的 AWS Lambda 程序將 PHI 從 Snowball Edge 外部資源傳輸到/傳輸 PHI 時，應確保使用加密的連線通訊協定，例如 HTTPS

或 SSL/TLS。 AWS IoT Greengrass 此外，PHI 應該在儲存在 Snowball Edge 的本機磁碟區時加密，不論是透過本機存取或透過 NFS。使用 Snowball 管理主控台和 API 將加密自動套用至放入 Snowball Edge 的資料，以便大量傳輸到 S3。如需將資料傳輸至 S3 的詳細資訊，請參閱the section called “AWS Snowball”.

AWS Step Functions

AWS Step Functions 可以使用視覺化工作流程輕鬆協調分散式應用程式和微服務的元件。 AWS Step Functions 無法儲存、傳輸或處理 PHI。PHI 不應放置在任何任務 AWS Step Functions 或狀態機器定義的元數據中，也不應放置在元數據中。 AWS Step Functions 用 AWS CloudTrail 於記錄所有 API 呼叫。

AWS Storage Gateway

AWS Storage Gateway 是一種混合式儲存服務，可讓客戶的現場部署應用程式順暢使用 AWS 雲端儲存。閘道使用開放標準儲存協定，將現有的儲存應用程式和工作流程連接到 AWS 雲端儲存服務，以減少程序中斷情況。

檔案閘道

檔案閘道是一種 AWS Storage Gateway 支援 Amazon S3 檔案界面的類型，可新增至目前的區塊式磁碟區和 VTL 儲存。檔案閘道使用 HTTPS 與 S3 通訊，並依預設使用 SSE-S3 將所有加密的物件存放在 S3 上，或使用用戶端加密與存放在中的金鑰 AWS KMS。檔案中繼資料 (例如檔案名稱) 會保持未加密，且不應包含任何 PHI。

磁碟區閘道

磁碟區閘道提供雲端支援的儲存磁碟區，客戶可從內部部署應用程式伺服器掛接為網際網路小型電腦系統介面 (iSCSI) 裝置 客戶應根據其內部合規性和法規需求，將本機磁碟作為上傳緩衝區和快取連接至磁碟區閘道虛擬機器。建議對於 PHI 來說，這些磁碟應該能夠提供靜態加密。磁碟區閘道虛擬機器與 AWS 之間的通訊會使用 TLS 1.2 加密，以確保傳輸中的 PHI 安全。

磁帶閘道

磁帶閘道為執行內部部署的協力廠商備份應用程式提供 VTL (虛擬磁帶櫃) 介面。客戶在設定磁帶備份工作時，應在第三方備份應用程式中啟用 PHI 的加密功能。磁帶閘道虛擬機器與 AWS 之間的通訊會使用 TLS 1.2 加密，以確保傳輸中的 PHI 安全。搭配 PHI 使用任何 Storage Gateway 組態的客戶應啟用完整記錄功能。如需詳細資訊，請參閱什麼是 AWS Storage Gateway？

AWS Systems Manager

AWS Systems Manager 這是一個統一的界面，可讓客戶輕鬆地集中管理操作資料、跨 AWS 資源自動執行任務，以及縮短偵測和解決基礎設施中操作問題的時間。Systems Manager 提供客戶基礎架構效能與組態的完整檢視、簡化資源與應用程式管理，並讓您輕鬆大規模地操作及管理其基礎架構。

將可能包含 PHI 的資料輸出到其他服務 (例如 Amazon S3) 時，客戶必須遵循接收服務的存放 PHI 指引。客戶不應在中繼資料或識別碼中包含 PHI，例如文件名稱和參數名稱。

AWS Transfer for SFTP

AWS Transfer for SFTP 輸提供對客戶 S3 資源的安全檔案傳輸協定 (SFTP) 存取。客戶會看到虛擬伺服器，虛擬伺服器可在區域服務端點使用標準 SFTP 通訊協定進行存取。從 AWS 客戶和 SFTP 用戶端的角度來看，SFTP 閘道看起來像是標準、高可用性的 SFTP 伺服器。雖然服務本身不存放、處理或傳輸 PHI，但客戶在 Amazon S3 上存取的資源應該以符合指導方針的方式進行設定。客戶也可以使用記錄 AWS CloudTrail 對適用於 SFTP 的 AWS 傳輸所做的 API 呼叫。

AWS WAF — 網路應用程式防火牆

AWS WAF 是一種 Web 應用程式防火牆，可協助保護客戶 Web 應用程式免受可能影響應用程式可用性、危及安全性或耗用過多資源的常見 Web 入侵程式。客戶可以將 AWS WAF 放置在 AWS 上託管且與 PHI 交換或交換 PHI 的 Web 應用程式及其最終使用者之間。就像在 AWS 上傳輸任何 PHI 一樣，包含 PHI 的資料在傳輸過程中必須加密。請參閱 Amazon EC2 指南，以進一步了解可用的加密選項。

AWS X-Ray

AWS X-Ray 是一項服務，可收集客戶應用程式所提供之請求的相關資料，並提供工具，讓他們可以用來檢視、篩選和深入瞭解該資料，以識別問題和最佳化機會。對於對客戶應用程式的任何追蹤請求，他們不僅可以查看有關請求和回應的詳細資訊，還可以查看應用程式對下游 AWS 資源、微型服務、資料庫和 HTTP Web API 進行呼叫的詳細資訊。 AWS X-Ray 不應用於儲存或處理 PHI。根據預設，傳送至和傳出的資訊 AWS X-Ray 都是加密的。使用時 AWS X-Ray，請勿在區段註釋或區段中繼資料中放置任何 PHI。

Elastic Load Balancing

客戶可以使用 Elastic Load Balancing 來終止和處理包含 PHI 的工作階段。客戶可以選擇「Classic Load Balancer」或「Application Load Balancer」。由於包含 PHI 的所有網路流量在傳輸過程中都必須加密 end-to-end，因此客戶可以彈性地實作兩種不同的架構：

客戶可以透過建立使用加密通訊協定進行連線的負載平衡器，在 Elastic Load Balancing 上終止 HTTPS、透過 TLS 的 HTTP/2 或 SSL/TLS。此功能可啟用負載平衡器和起始 HTTPS、HTTP/2 (透過 TLS 或 SSL/TLS 工作階段) 的用戶端之間的流量加密，以及負載平衡器與客戶後端執行個體之間的連線。包含 PHI 的工作階段必須加密前端和後端接聽程式，才能進行傳輸 客戶應評估其憑證和工作階段協商原則，並維持與指導方針的一致性。如需詳細資訊，請參閱 C lassic Load Balancer 的 HTTPS 接聽程式。

或者，客戶可以在基本 TCP 模式 (針對傳統) 或以上 WebSockets (針對應用程式) 設定 Amazon ELB，並將加密工作階段傳遞至終止加密工作階段的後端執行個體。在此架構中，客戶可以在自己的執行個體中執行的應用程式中管理自己的憑證和 TLS 交涉原則。如需詳細資訊，請參閱 C lassic Load Balancer 的接聽程式。在這兩種架構中，客戶都應實作一定程度的記錄，他們確定與 HIPAA 和 HITECH 要求一致。

FreeRTOS

FreeRTOS 是適用於微控制器的作業系統，可讓小型、低功率的邊緣裝置輕鬆進行程式設計、部署、保護、連線和管理。FreeRTOS 以 FreeRTOS 核心為基礎，這是一種常用於微控制器的開放原始碼作業系統，並透過軟體程式庫進行擴充，可輕鬆將小型、低功耗裝置安全地連接到 AWS 雲端服務 (例如 AWS IoT Core) 或執行中更強大的邊緣裝置。 AWS IoT Greengrass

現在，在使用執行 FreeRTOS 的合格裝置時，可以在傳輸過程中和靜態時加密包含 PHI 的資料。FreeRTOS 提供兩個程式庫來提供平台安全性：TLS 和 PKCS #11。TLS API 應該用於加密和驗證包含 PHI 的所有網路流量。PKCS #11 提供軟體加密作業的標準介面，應該用來加密儲存在執行 FreeRTOS 之合格裝置上的任何 PHI。

用 AWS KMS 於 PHI 的加密

KMS 金鑰可用來加密/解密資料加密金鑰，用來在客戶的應用程式或使用的 AWS 服務中加密 PHI。AWS KMS AWS KMS 可與 HIPAA 帳戶一起使用，但 PHI 只能在 HIPAA 合格服務中處理、儲存或傳輸。 AWS KMS 通常用於為在其他 HIPAA 合格服務中運行的應用程序生成和管理密鑰。

例如，在 Amazon EC2 中處理 PHI 的應用程式可以使用 GenerateDataKey API 呼叫產生資料加密金鑰，以便在應用程式中加密和解密 PHI。資料加密金鑰會受到 AWS KMS 儲存在其中的客戶 KMS 金鑰的保護 AWS KMS，並在登入 API 呼叫時建立高度可稽核的金鑰階層。 AWS CloudTrail PHI 不應該存儲在中存儲的任何密鑰的標籤（元數據）中 AWS KMS。

VM Import/Export

VM 匯入/匯出可讓客戶輕鬆地將虛擬機器映像從現有環境匯入 Amazon EC2 執行個體，並將其匯出回現場部署環境。此產品可讓客戶利用您為滿足 TheIRIT 安全性、組態管理及其合規要求而建置的虛擬機器中的現有投資，方法是將這些虛擬機器做為 ready-to-use 執行個體帶入 Amazon EC2。客戶也可以將匯入的執行個體匯出回其內部部署虛擬化基礎架構，讓他們能夠跨 IT 基礎架構部署工作負載。

除了 Amazon EC2 和 Amazon S3 的標準用量費用外，虛擬機器匯入/匯出功能無需額外付費。

若要匯入客戶映像，客戶可以使用 AWS CLI 或其他開發人員工具從其 VMware 環境匯入虛擬機器 (VM) 映像。如果客戶使用 VMware vSphere 虛擬化平台，他們也可以使用 vCenter 專用的 AWS 管理入口網站匯入其虛擬機器。在匯入程序中，VM Import 會將客戶虛擬機器轉換為 Amazon EC2 AMI，以便用來執行 Amazon EC2 執行個體。匯入虛擬機器之後，他們就可以利用 Amazon 的彈性、可擴展性和監控功能，透過 Auto Scaling 展、Elastic Load Balancing 等產品，並 CloudWatch 支援匯入的映像檔。

客戶可以使用 Amazon EC2 API 工具匯出先前匯入的 Amazon EC2 執行個體。只要指定目標執行個體、虛擬機器檔案格式和目的地 Amazon S3 儲存貯體，VM Export 就會自動將執行個體匯出到 Amazon S3 儲存貯體，以及加密選項，以確保其 VM 映像的傳輸和儲存安全。然後，客戶可以在其內部部署虛擬化基礎架構中下載並啟動匯出的 VM。

客戶可以匯入使用 VMware ESX 或工作站、Microsoft 超 V 和思傑 Xen 虛擬化格式的視窗和 Linux 虛擬機器。客戶可以將先前匯入的 Amazon EC2 執行個體匯出至 VMware ESX、Microsoft 超 V 或思傑 Xen 格式。如需支援的作業系統、版本和格式的完整清單，請參閱虛擬機器匯入/匯出需求。AWS 計劃在 future 增加對其他作業系統、版本和格式的支援。

稽核、備份和災難復原

HIPAA 的安全性規則具有與深入稽核功能、資料備份程序和災難復原機制相關的詳細要求。AWS 中的服務包含許多可協助客戶滿足其需求的功能。例如，客戶應考慮建立稽核功能，讓安全分析師檢查詳細的活動記錄檔或報告，以瞭解誰擁有存取權限、IP 位址項目、存取的資料等。

在進行稽核的情況下，應該長時間在中央位置追蹤、記錄和儲存此資料。使用 Amazon EC2，客戶可以在虛擬伺服器上執行活動日誌檔並稽核至封包層，就像在傳統硬體上一樣。他們還可以跟踪到達其虛擬服務器實例的任何 IP 流量。客戶的管理員可以將日誌檔備份到 Amazon S3，以獲得長期可靠的儲存。

HIPAA 還有與維護應變計劃以在緊急情況下保護數據相關的詳細要求，並且必須創建和維護可檢索的電子 PHI 的精確副本。為了在 AWS 上實作資料備份計劃，Amazon EBS 為 Amazon EC2 虛擬伺服器執行個體提供持久性儲存。這些磁碟區可以公開為標準區塊裝置，並提供獨立於執行個體生命週期的非執行個體儲存。為了符合 HIPAA 準則，客戶可以建立 Amazon EBS 磁碟區的 point-in-time快照，這些快照會自動存放在 Amazon S3 中，並跨多個可用區域複寫，這些可用區域是專為隔離其他可用區域中的故障而設計的獨立位置。

您可以隨時存取這些快照，並可保護資料的長期持久性。Amazon S3 也為資料儲存和自動備份提供高可用性解決方案。只要將檔案或影像載入 Amazon S3，就會自動建立多個備援副本，並將其存放在不同的資料中心。這些文件可以隨時訪問，從任何地方（基於權限），並存儲，直到有意刪除。

此外，AWS 本質上提供了各種災難復原機制。災難復原是在災難發生時保護組織資料和 IT 基礎架構的程序，包括維護高可用性系統、保持資料和系統異地複製，以及持續存取兩者。

使用 Amazon EC2，管理員可以非常快速地啟動伺服器執行個體，並且可以使用彈性 IP 地址 (雲端運算環境的靜態 IP 地址) 在一台機器之間進行正常容錯移轉至另一台機器。Amazon EC2 還提供可用區域。管理員可以在多個可用區域啟動 Amazon EC2 執行個體，以建立不同地理位置的容錯系統，這些系統在網路故障、自然災害和大多數其他可能的停機來源時具有高度彈性。

使用 Amazon S3，客戶的資料會複寫並自動存放在不同的資料中心，以提供可靠的資料儲存，專為提供 99.99% 的可用性而設計。

使用 AWS 彈性災難復原 (AWS DRS)，客戶可以快速復原 AWS 上的應用程式，無論是在應用程式的最大 up-to-date 狀態，或從較早的時間點復原應用程式。

文件修訂

若要收到有關此白皮書更新的通知，請訂閱 RSS 摘要。

變更	描述	日期
次要更新	次要更新	2023 年 5 月 12 日
次要更新	更新白皮書以擴展服務的可用內容。	2022 年 9 月 28 日
次要更新	修復非包容性語言。	2022 年 4 月 6 日
白皮書已更新	已新增有關 AWS 應用程式遷移服務的資訊，以及 Amazon ECS 的更新資訊	2021 年 12 月 6 日
白皮書已更新	Amazon 健康湖和 Amazon VPC 部分中的更新信息	2021 年 11 月 9 日
白皮書已更新	新增 AWS Network Firewall 的相關資訊	2021 年 9 月 9 日
白皮書已更新	Amazon Connect 客戶檔案的更新信息	2021 年 8 月 26 日
白皮書已更新	增加了部分 Amazon AppFlow 和 AWS AWS Glue DataBrew	2021 年 7 月 22 日
白皮書已更新	更新了導航和組織。	2021 年 4 月 26 日
白皮書已更新	添加了以下部分： AWS CodeDeploy AWS CodePipeline, Amazon Aurora, Aurora PostgreSQL, Amazon Textract, Amazon Polly, Amazon FSX, AWS Auto Scaling,,,,,,, AWS Backup AWS Elastic Beanstalk, 虛	2021 年 3 月 31 日

	擬機導入/導出 AWS Firewall Manager AWS Organizations AWS Security Hub AWS Serverless Application Repository, Amazon, Amazon。 HealthLake EventBridge更新 Amazon Aurora 部分。	
白皮書已更新	已新增 AWS App Mesh 區段，以及更新的 AWS 系統管理員內容	2020 年 8 月 25 日
白皮書已更新	添加了 Amazon 應用程序流 2.0，AWS 開發套件指標，AWS Data Exchange，Amazon MSK，Amazon Pinpoint，Amazon Lex 克斯，Amazon SES 和 Amazon Forecast，Amazon Quantum Ledger Database (QLDB) 的部分。 AWS Cloud Map	2020 年 5 月 7 日

白皮書已更新	添加了 Amazon，Amazon CloudWatch 活動 CloudWatch，Amazon 數據 Firehose，阿帕奇 Flink 的 Amazon 託管服務，Amazon 服 OpenSearch 務，亞馬遜 DocumentDB（與 MongoDB 兼容性），AWS Mobile Hub，用 AWS OpsWorks 於廚師自動化， AWS IoT Greengrass木偶企業， AWS OpsWorks AWS Transfer for SFTP，AWS DataSync AWS Global Accelerator，亞馬遜領域醫療和 AWS 的部分。RoboMaker	二零二零年一月一日
白皮書已更新	添加了有關 Amazon Comprehend，Amazon Transcribe，Amazon Translate 和 AWS Certificate Manager 的部分。	二○一九年一月一日
白皮書已更新	在 Amazon Athena，Amazon EKS， AWS IoT 核心和 Amazon FreeRTOS AWS IoT Device Management，Amazon，Amazon Neptune GuardDuty，AWS 服務器遷移服務 AWS Database Migration Service，Amazon MQ 和. AWS Glue	2018 年 11 月 1 日

白皮書已更新	新增 Amazon Elastic File System (EFS)、Amazon Kinesis Video Streams、Amazon Rekognition、Amazon 、Amazon 簡單工作流程 SageMaker、AWS 秘密管理、Service Catalog 等部分。AWS Step Functions	2018 年 6 月 1 日
白皮書已更新	已新增 AWS CloudFormation、、、 AWS X-Ray AWS CloudTrail AWS CodeBuild AWS CodeCommit、 AWS Config和「 AWS OpsWorks 堆疊」的區段。	二○一八年四月一日
白皮書已更新	增加了部分 AWS Fargate。	二○一八年一月一日

在 2018 年之前所做的更新：

日期	描述
2017 年 11 月	在 Amazon EC2 容器註冊表，Amazon Macie QuickSight，Amazon 和 AWS Managed Services.
2017 年 11 月	增加了在 Amazon ElastiCache 的 Redis 和 Amazon CloudWatch 部分。
2017 年 10 月	在 Amazon SNS，Amazon 路線 53 和 AWS CloudHSM. AWS Storage Gateway已更新章節 AWS Key Management Service。
2017 年 9 月	已新增有關 Amazon Connect、亞 Amazon Kinesis Streams、Amazon RDS (瑪麗亞) 資料庫、Amazon RDS SQL 伺服器 AWS

日期	描述
	Batch AWS Lambda、 AWS Snowball 邊緣和 Lambda @Edge 功能的區段。 CloudFront
2017 年 8 月	添加了 Amazon EC2 Systems Manager 和 Amazon Inspector 的部分。
2017 年 7 月	在 Amazon WorkSpaces，Amazon WorkDocs，AWS Directory Service 和 Amazon ECS 上添加了部分。
2017 年 6 月	添加了有關 Amazon CloudFront，AWS WAF 和 Amazon S3 Transfer Acceleration 的部分。 AWS Shield
2017 年 5 月	移除了在 EC2 和 EMR 中處理 PHI 的專用執行個體或專用主機的要求。
2017 年 3 月	已更新服務清單，以指向合規計劃的 AWS 服務範圍頁面。添加了 Amazon API Gateway 的說明。
2017 年 1 月	更新到最新的模板。
2016 年 10 月	首次出版

注意

客戶有責任對本文件中的資訊進行自己的獨立評定。本文件：(a) 僅供參考，(b) 代表目前的 AWS 產品供應項目和實務，如有變更恕不另行通知，且 (c) 不會向 AWS 及其關係企業、供應商或授權人建立任何承諾或保證。AWS 產品或服務係依其「原狀」提供，不含任何明示或暗示的保證、陳述或條件。AWS 對其客戶的責任與義務應由 AWS 協議管轄，本文並非 AWS 與其客戶之間的任何協議的一部分，也並非上述協議的修改。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。