AWS ホワイトペーパー

Architecting for HIPAA Security and Compliance on Amazon Web Services

Architecting for HIPAA Security and Compliance on Amazon Web Services: AWS ホワイトペーパー

Table of Contents

Architecting for HIPAA Security and Compliance on Amazon Web Services

発行日: 2022 年 9 月 28 日 (ドキュメントの改訂)

このホワイトペーパーでは、お客様が Amazon Web Services (AWS) を使用して、米国の医療保険の相互運用性と説明責任に関する法律 (HIPAA) で規制されている機密性の高いワークロードを実行する方法の概要を説明します。保護対象保健情報 (PHI) を保護するための HIPAA プライバシーおよびセキュリティルール、AWS を使用して転送中および保管中のデータを暗号化する方法、および PHI を含むワークロードを実行するために AWS の機能を使用する方法に焦点を当てます。

序章

1996 年の医療保険の相互運用性と説明責任に関する法律 (HIPAA) は、「対象エンティティ」と「事業提携」に適用されます。HIPAA は 2009 年に Health Information Technology for Medical and Medical Health (HITAK) Act によって拡張されました。

HIPAA と HITAK は、PHI のセキュリティとプライバシーを保護することを目的とした一連の連邦基準を確立します。HIPAA と HITAK は、保護対象の医療情報 (PHI) の使用と開示、PHI、個人権利、管理上の責任を保護するための適切な保護に関する要件を課します。HIPAA と HITAK の詳細については、「Health Information Privacy Home」を参照してください。

対象エンティティとそのビジネスアソシエイトは、Amazon Web Services (AWS) が提供する安全でスケーラブルな低コストの IT コンポーネントを使用して、HIPAA および HITAK コンプライアンス要件に従ってアプリケーションを設計できます。AWS は、 commercial-off-the-shelfISO 27001、FedRAMP、Service Organization Control Report (SOC1, SOC2、SOC3) など、業界で認められている認定と監査を備えたインフラストラクチャプラットフォームを提供します。AWS のサービスとデータセンターには、顧客データの整合性と安全性を確保するために役立つ運用上および物理的なセキュリティが複数レイヤーあります。最低料金なしで、用語ベースの契約や pay-as-you-use 料金も必要ない AWS は、医療業界のアプリケーションの増加に対する信頼性が高く効果的なソリューションです。

AWS は、HIPAA の対象となるエンティティとそのビジネスアソシエイトが PHI を安全に処理、保存、および送信できるようにします。さらに、2013 年 7 月現在、AWS はそのようなお客様向けに標準化された事業提携契約 (BAA) を提供しています。AWS BAA を実行するお客様は、HIPAA アカウントとして指定されたアカウントで任意の AWS サービスを使用できますが、AWS BAA で定義されている HIPAA 対象サービスを使用してのみ PHI を処理、保存、および送信できます。これらのサービスの完全なリストについては、「HIPAA 対応サービスリファレンス」ページを参照してください。

AWS は、HIPAA 対象サービスが HIPAA の管理、技術、および物理的な保護を特にサポートするように、標準ベースのリスク管理プログラムを維持しています。これらのサービスを使用して PHI を保存、処理、送信することで、AWS のお客様と AWS は AWS ユーティリティベースの運用モデルに適用される HIPAA 要件に対応することができます。

AWS の BAA では、「Secretary of Health and Human Services (HHS): Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (「Guidance」) 」のガイダンスに従って、HIPAA 対象サービスに保存または送信されている PHI を暗号化することをお客様に要求しています。更新される可能性があり、HHS によって指

定された後継サイト (または関連サイト) で利用可能になる可能性があるため、このサイトを参照してください。

AWS は、 AWS Key Management Service () など、PHI のキー管理と暗号化を容易にし、監査を簡素化するための包括的な機能とサービスを提供しますAWS KMS。HIPAA コンプライアンス要件を持つお客様は、PHI の暗号化要件を満たす方法に多くの柔軟性があります。

暗号化の実装方法を決定する際、お客様は HIPAA 対応サービスにネイティブな暗号化機能を評価して活用できます。または、お客様は HHS からのガイダンスに従って、他の方法で暗号化要件を満たすことができます。

AWS での PHI の暗号化と保護

HIPAA セキュリティルールには、転送時 (「転送中」) および保管時 (保管中」) の PHI の暗号化に関するアドレス指定可能な実装仕様が含まれています。これは HIPAA のアドレス指定可能な実装仕様ですが、AWS では、HIPAA 対象サービスを使用して保存または転送される PHI を、「Secretary of Health and Human Services (HHS): Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (「Guidance」)」のガイダンスに従って暗号化する必要があります。更新される可能性があり、HHS によって指定された後継 (または関連サイト) で利用できるようになる可能性があるため、このサイトを参照してください。

AWS は、 AWS Key Management Service () など、PHI のキー管理と暗号化を容易にし、監査を簡素化するための包括的な機能とサービスを提供しますAWS KMS。HIPAA コンプライアンス要件を持つお客様は、PHI の暗号化要件を満たす方法に多くの柔軟性があります。

暗号化の実装方法を決定する際、お客様は HIPAA 対象サービスにネイティブな暗号化機能を評価して活用したり、HSH からのガイダンスに従って暗号化要件を満たすことができます。以下のセクションでは、PHI の暗号化に HIPAA 対象の各サービスおよびその他のパターンで使用可能な暗号化機能を使用する方法、および AWS で PHI の暗号化に使用されるキーを AWS KMS で暗号化する方法の概要を説明します。

トピック

- Amazon DocumentDB (MongoDB 互換性)
- 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 for Redis
- Amazon OpenSearch サービス
- Amazon EMR
- Amazon EventBridge
- Amazon Forecast
- Amazon FSx
- Amazon GuardDuty
- Amazon HealthLake
- Amazon Inspector
- Amazon Managed Service for Apache Flink
- 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 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 アプリケーション移行サービス
- 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 Elastic ディザスタリカバリ
- AWS Fargate
- AWS Firewall Manager
- AWS Global Accelerator
- AWS Glue
- AWS Glue DataBrew
- AWS IoT Core と AWS IoT Device Management
- AWS IoT Greengrass
- AWS Lambda
- AWS Managed Services
- AWS OpsWorks Chef Automate 用の
- AWS OpsWorks Puppet Enterprise 用
- AWS OpsWorks スタック
- AWS Organizations
- AWS RoboMaker
- AWS SDK メトリクス
- AWS Secrets Manager

- AWS Security Hub
- AWS Server Migration Service
- AWS Serverless Application Repository
- Service Catalog
- AWS Shield
- AWS Snowball
- AWS Snowball エッジ
- AWS Step Functions
- AWS Storage Gateway
- AWS Systems Manager
- AWS Transfer for SFTP
- AWS WAF – ウェブアプリケーションファイアウォール
- AWS X-Ray
- Elastic Load Balancing
- FreeRTOS
- PHI の暗号化 AWS KMS に を使用する
- VM Import/Export

Amazon API Gateway

お客様は Amazon API Gateway を使用して、保護対象の医療情報 (PHI) を処理および送信できます。Amazon API Gateway は転送中の暗号化に HTTPS エンドポイントを自動的に使用しますが、クライアント側でペイロードを暗号化することもできます。API Gateway は、キャッシュされていないすべてのデータをメモリ経由で渡し、ディスクに書き込むことはありません。お客様は API Gateway での認証に AWS 署名バージョン 4 を使用できます。詳細については、次を参照してください。

- Amazon API Gateway FAQs: セキュリティと認可
- API Gateway での REST API へのアクセスの制御と管理

PHI が関係する場合、サービスが Guidance および BAA と一致するように設定されていれば、お客様は API Gateway に接続されている任意のサービスと統合できます。API Gateway をバックエンド

サービスと統合する方法については、「API Gateway で REST API メソッドを設定する」を参照してください。

お客様は、 AWS CloudTrail と Amazon を使用して CloudWatch 、ログ記録の要件と一致するログ記録を有効にできます。API Gateway を介して送信される PHI (ヘッダー、URLs、リクエスト/レスポンスなど) が、 ガイダンスと一致するように設定された HIPAA 対象サービスによってのみキャプチャされていることを確認します。API Gateway を使用したログ記録の詳細については、「API Gateway REST API または API のトラブルシューティングのために CloudWatch ログを有効にするにはどうすればよいですか？」を参照してください WebSocket 。

Amazon AppFlow

Amazon AppFlow は、Salesforce、Marketo、Slack、 などの S oftware-as-aサービス (SaaS) アプリケーション間、および Amazon S3 や Amazon Redshift などの AWS サービス間でデータを安全に転送できるようにするフルマネージド統合サービスです。 AppFlow は ServiceNow、スケジュールに従って、ビジネスイベントに応答して、またはオンデマンドで、お客様が選択した頻度でデータフローを実行できます。お客様は、フィルタリングや検証などのデータ変換機能を設定して、追加のステップなしで、フロー自体の一部として豊富な ready-to-use データを生成することもできます。

Amazon AppFlow は、PHI を含むデータの処理と転送に使用できます。 AppFlow と設定された送信元/送信先の間で転送中のデータの暗号化は、TLS 1.2 以降を使用してデフォルトで提供されます。S3 に保存されているデータは、お客様が指定した AWS KMS キー (以前の CMK) を使用して自動的に暗号化されます。S3 以外の宛先に転送される PHI データの場合、選択した宛先の保管時のストレージがセキュリティニーズを満たしていることを確認する必要があります。 と統合 AWS CloudTrail して API コールをログに記録し、Amazon EventBridge でフロー実行イベントを発行することで、アプリケーションモニタリング AppFlow を有効にします。

Amazon AppStream 2.0

Amazon AppStream 2.0 は、フルマネージド型のアプリケーションストリーミングサービスです。お客様はデータを所有し、規制要件を満たす方法で必要な Windows アプリケーションを設定する必要があります。お客様は、ホームフォルダを介して永続的ストレージを設定できます。転送中のファイルやフォルダは Amazon S3 の SSL エンドポイントを使用して暗号化されます。ファイルとフォルダは、Amazon S3-managed暗号化キーを使用して保管時に暗号化されます。詳細については、「Enable and Administer Persistent Storage for Your AppStream 2.0 Users」を参照してください。お客様がサードパーティーのストレージソリューションを使用することを選択した場合、そのソリューションの設定がガイダンスと一致することを確認する責任があります。Amazon

AppStream 2.0 とのすべてのパブリック API 通信は、TLS を使用して暗号化されます。詳細については、「Amazon AppStream 2.0 ドキュメント」を参照してください。

Amazon AppStream 2.0 は と統合されています。これは AWS CloudTrail、お客様の AWS アカウントで Amazon AppStream 2.0 によって行われた API コール、または Amazon AppStream 2.0 API から行われた指定された Amazon S3 bucket. CloudTrail captures AppStream API コールにログファイルを配信するサービスです。お客様は、Amazon を使用してリソース使用状況メトリクス CloudWatch を記録することもできます。詳細については、「Amazon AppStream 2.0 リソースのモニタリング」および「 を使用した AppStream 2.0 API コールのログ記録 AWS CloudTrail」を参照してください。

Amazon Athena

Amazon Athena は、標準的な SQL を使用して Amazon Simple Storage Service (Amazon S3) 内のデータを直接分析することを容易にする、インタラクティブなクエリサービスです。Athena は、Amazon S3 に保存されている非構造化データ、半構造化データ、および構造化データをお客様が分析するのに役立ちます。たとえば、CSV 形式、JSON 形式、列データ形式 (Apache Parquet や Apache ORC など) に対応しています。お客様は Athena を使用して、データを集約したり Athena にロードしたりすることなく、ANSI SQL を使用してアドホッククエリを実行できます。

Amazon Athena を使用して、PHI を含むデータを処理できるようになりました。Amazon Athena と S3 間の転送中のデータの暗号化は、デフォルトで SSL/TLS を使用して提供されます。S3 での保管中の PHI の暗号化は、S3 セクションに記載されているガイダンスに従って実行する必要があります。ステージングされた結果を含め、Amazon Athena 内からのクエリ結果の暗号化は、Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)、 AWS KMSマネージドキーによるサーバー側の暗号化 (SSE-KMS)、または マネージドキーによるクライアント側の暗号化 (CSE-KMS) AWS KMSを使用して有効にする必要があります。Amazon Athena は AWS CloudTrail を使用してすべての API コールをログに記録します。

Amazon Aurora

Amazon Aurora では、 で管理するキーを使用して、Aurora データベースクラスターと保管時のスナップショットを暗号化できます AWS KMS。Amazon Aurora 暗号化で実行されているデータベースインスタンスでは、自動バックアップ、リードレプリカ、スナップショットと同様に、基盤となるストレージに保存されているデータは暗号化されます。

ガイダンスは更新される可能性があるため、お客様は引き続き Amazon Aurora 暗号化がコンプライアンスおよび規制要件を満たしているかどうかを評価し、判断する必要があります。Amazon Aurora

を使用した保管時の暗号化の詳細については、「暗号化を使用したデータの保護」を参照してください。

Aurora MySQL を実行している DB クラスターへの接続には、Secure Socket Layer (SSL) または Transport Layer Security (TLS) を利用して、トランスポート暗号化を使用する必要があります。SSL/TLS の実装の詳細については、「Aurora MySQL DB クラスターでの SSL/TLS の使用」を参照してください。

Amazon Aurora PostgreSQL

Amazon Aurora では、 で管理するキーを使用して、Aurora データベースクラスターと保管時のスナップショットを暗号化できます AWS KMS。Amazon Aurora 暗号化で実行されているデータベースインスタンスでは、自動バックアップ、リードレプリカ、スナップショットと同様に、基盤となるストレージに保存されているデータは暗号化されます。

ガイダンスは更新される可能性があるため、お客様は引き続き Amazon Aurora 暗号化がコンプライアンスおよび規制要件を満たしているかどうかを評価し、判断する必要があります。Amazon Aurora を使用した保管時の暗号化の詳細については、「暗号化を使用したデータの保護」を参照してください。

Aurora PostgreSQL を実行している DB クラスターへの接続には、Secure Socket Layer (SSL) または Transport Layer Security (TLS) を利用したトランスポート暗号化を使用する必要があります。SSL/TLS の実装の詳細については、「SSL による Aurora PostgreSQL データの保護」を参照してください。

Amazon CloudFront

Amazon CloudFront は、カスタマーウェブサイト、APIs、またはその他のウェブアセットの配信を高速化するグローバルコンテンツ配信ネットワーク (CDN) サービスです。他のアマゾン ウェブ サービス製品と統合されているため、開発者や企業が最小限の使用コミットメントなしでエンドユーザーへのコンテンツを簡単に高速化できます。との転送中に PHI を確実に暗号化するには CloudFront、オリジン end-to-end からビューワー CloudFront に HTTPS を使用するように を設定する必要があります。

これには、 CloudFront とビューワー間のトラフィック、カスタムオリジンからの CloudFront 再分散、Amazon S3 オリジンからの CloudFront 配信が含まれます。また、データを にキャッシュしている間も保管中の暗号化が維持されるように、オリジンでデータが暗号化されていることを確認する必要があります CloudFront。Amazon S3 をオリジンとして使用する場合、お客様は S3 サーバー側

の暗号化機能を利用できます。お客様がカスタムオリジンから配信する場合は、データがオリジンで暗号化されていることを確認する必要があります。

Lambda@Edge

Lambda@Edge は、AWS エッジロケーションで Lambda 関数を実行できるようにするコンピューティングサービスです。Lambda@Edge を使用して、 を介して配信されるコンテンツをカスタマイズできます CloudFront。PHI で Lambda@Edge を使用する場合は、 の使用に関するガイダンスに従う必要があります CloudFront。Lambda@Edge との間のすべての接続は、HTTPS または SSL/TLS を使用して暗号化する必要があります。

Amazon CloudWatch

Amazon CloudWatch は、AWS クラウドリソースと、お客様が AWS で実行するアプリケーションのモニタリングサービスです。お客様は Amazon を使用して、メトリクス CloudWatch の収集と追跡、ログファイルの収集とモニタリング、アラームの設定を行うことができます。Amazon CloudWatch 自体は PHI を生成、保存、送信しません。お客様は、 を使用して CloudWatch API コールをモニタリングできます AWS CloudTrail。詳細については、「 を使用した Amazon CloudWatch API コールのログ記録 AWS CloudTrail」を参照してください。

設定要件の詳細については、「Amazon CloudWatch Logs」セクションを参照してください。

Amazon CloudWatch イベント

Amazon CloudWatch Events は、AWS リソースの変更を示すシステムイベントの near-real-time ストリームを提供します。お客様は、PHI が CloudWatch イベントに流入しないこと、および PHI を保存、処理、または送信する CloudWatch イベントを発行する AWS リソースが ガイダンスに従って設定されていることを確認する必要があります。

お客様は、 で AWS API コールとして登録するように Amazon CloudWatch Events を設定できます CloudTrail。詳細については、「 を使用した AWS API コールでトリガーする CloudWatch イベントルールの作成 AWS CloudTrail」を参照してください。

Amazon CloudWatch Logs

お客様は Amazon CloudWatch Logs を使用して、Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、Amazon Route 53、およびその他のソースからのログファイルをモニタリング AWS CloudTrail、保存、およびアクセスできます。その後、ログから関連する CloudWatch ログデータを

取得できます。ログデータは、転送中および保管中に暗号化されます。そのため、他の のサービスによって出力され、 CloudWatch ログに配信される PHI を再暗号化する必要はありません。

Amazon Comprehend

ドキュメントの内容に関するインサイトの抽出用に、Amazon Comprehend では自然言語処理を使用しています。Amazon Comprehend は、UTF-8 形式のテキストファイルを処理します。ドキュメント内のエンティティ、キーフレーズ、言語、感情、その他の共通要素を認識することでインサイトを作り上げます。Amazon Comprehend は、PHI を含むデータで使用できます。Amazon Comprehend はデータを保持または保存せず、API へのすべての呼び出しは SSL/TLS で暗号化されます。Amazon Comprehend は CloudTrail を使用してすべての API コールをログに記録します。

AWS Identity and Access Management

Amazon Comprehend へのアクセスには認証や承認などのセキュリティアクセス機能が必要で、AWS Identity and Access Management (IAM) で制御でき、認証情報を使用して IAM にアクセスできます。詳細については、「Amazon Comprehend ユーザーガイド」の「Amazon Comprehend の認証とアクセスコントロールAmazon Comprehend」を参照してください。

アカウント管理

デフォルトでは、IAM ユーザーには Amazon Comprehend リソースを作成または変更したり、Amazon Comprehend API を使用してタスクを実行したりするアクセス許可はありません。ユーザーがリソースを作成または変更し、タスクを実行できるようにするには、ユーザーが使用する必要がある特定のリソース (Amazon Comprehend や API アクションなど) に対するアクセス許可をユーザーに付与する IAM ポリシーを活用し、特定のアクセス許可を必要とするユーザーまたはグループにポリシーをアタッチする必要があります。

Amazon Comprehend では、 AWS Identity and Access Management (IAM) を使用して、Amazon Comprehend アクセス許可を有効にするためのポリシーがアタッチされたユーザーを作成できます。オプションで、ロールにアタッチするカスタムポリシーを作成することもできます。その後、組織で定義されたロールベースのアクセスと最小特権の原則に従って、Amazon Comprehend 管理のために API の を呼び出す機能を備えた管理者をロールに追加できます。

ID とアクセス

Amazon Comprehend では、組織の認証要件に従って、多要素認証 AWS を使用して への認証をユーザーに要求できます。

を使用すると AWS Management Console、IAM 管理者は、ユーザーが自分の認証情報と MFA デバイスを管理するために必要なアクセス許可を除く、すべてのアクセス許可を拒否するカスタマー管理ポリシーを作成できます。JSON ポリシーテンプレートは、IAM コンソールの「マイセキュリティ認証情報」ページにあります。

オプションで、IAM パートナーと互換性のあるサードパーティー MFA 機能を活用できます。詳細については、「IAM パートナー」を参照してください。

管理

Amazon Comprehend は、アカウント管理者が IAM アイデンティティ (ユーザー、グループ、ロール) にアクセス許可ポリシーをアタッチし、それによって Amazon Comprehend リソースでオペレーションを実行するアクセス許可を付与できるアイデンティティベースのポリシーを選択することをお勧めします。

Amazon Comprehend の API アクションのリストは、「 API リファレンスガイド」に記載されています。また、事前定義された IAM ポリシー、カスタマー IAM ポリシー、および API アクションへのアクセスを、最小特権およびロールベースの組織要件に従ってユーザーまたはロールに許可することも検討する必要があります。詳細については、「 デベロッパーガイド」の「Amazon Comprehend API の使用」を参照してください。

外部認証

Amazon Comprehend は、IAM ロールを使用した ID フェデレーションと互換性があります。これにより、管理者がプロビジョニングしたロールを引き受け AWS ることで、Amazon Comprehend ユーザーが を認証できるようになります。組織またはサードパーティーの認証情報 AWS を使用して にアクセスするユーザーは、間接的にロールを引き受けます。

AWS Kerberos と Active Directory のサポートにより、データベースユーザーのシングルサインオンと集中認証の利点が得られます。 AWS ユーザーは、Microsoft Active Directory AWS Directory Service の またはお客様のオンプレミス Active Directory でユーザー認証情報を管理および保存できます。

データフローの適用

AWS お客様および APN パートナーは、データコントローラーまたはデータ処理者として、 AWS クラウド および Amazon Comprehend に配置する個人データについて責任を負います。IAM ポリシーを使用して、Amazon Comprehend のデータ入力と出力へのフローを制御する責任があります。

データ保護とシークレット管理

AWS 責任共有モデルは、Amazon Comprehend のデータ保護に適用されます。このモデルで説明されているように、 AWS はすべての AWS クラウドを実行するグローバルインフラストラクチャを保護する責任を担います。このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任はユーザーにあります。このコンテンツには、使用する AWS サービスのセキュリティ設定および管理タスクが含まれます。データプライバシーの詳細については、「データプライバシーのよくある質問」を参照してください。

Amazon Comprehend デベロッパーガイドの「Amazon Comprehend でのデータ保護」セクションには、送信に TLS を使用したり、タグや自由形式のフィールドへの機密情報の配置を回避したりするなど、データ保護に関するヒントが記載されています。 Amazon Comprehend

の暗号化 data-at-rest

Amazon Comprehend と AWS Key Management Service (AWS KMS) と連携することで、データの暗号化を強化することができます。Amazon Simple Storage Service (Amazon S3) では、テキスト分析、トピックモデリング、またはカスタム Amazon Comprehend ジョブを作成するときに、入力ドキュメントを暗号化できます。との統合 AWS KMS により、ストレージボリューム内のデータを start* ジョブと create* ジョブ用に暗号化し、start* ジョブの出力結果を独自の AWS KMS キーを使用して暗号化できます。

Amazon Comprehend ユーザーは、組織のポリシーに従って、利用可能な Amazon S3 S3 バケットを暗号化するのがベストプラクティスです。

では AWS Management Console、Amazon Comprehend カスタムモデルを独自の AWS KMS キーで暗号化します。の場合 AWS CLI、Amazon Comprehend は独自の AWS KMS キーまたは提供されたカスタマーマネージドキー (CMK) を使用してカスタムモデルを暗号化できます。

の使用時に暗号化を選択する場合は AWS Management Console、次のオプションメソッドのいずれかまたは両方を選択できます。

- ボリュームの暗号化 - Comprehend が使用する EBS ボリュームのデータがトレーニング/推論中に暗号化されます (データはトレーニング/推論後にフラッシュされるため、このキーはジョブの進行中にのみ関連します) 。
- 出力結果の暗号化 - 顧客提供の AWS KMS キーを使用して、顧客のバケット内の comprehend によって保存された出力を暗号化します。

ボリューム暗号化などの暗号化タイプの詳細については、AWS KMS 「Amazon Comprehend での暗号化」を参照してください。

個人を特定できる情報

Amazon Comprehend コンソールまたは API を使用して、英語のテキスト文書に含まれる個人を特定できる情報 (PII)を検出できます。PII エンティティの検出とラベル付け、およびさまざまな PII 分析ジョブの運用の詳細については、「Amazon Comprehend デベロッパーガイド」の「個人を特定できる情報」セクションを参照してください。

データの削除

Amazon S3 を使用しており、独自の AWS KMS キーを管理する Amazon Comprehend のお客様の場合は、 AWS KMS キーを取り消し、組織の要件に従って行う手続きの根拠を定義することを検討する必要があります。Amazon S3 の AWS KMS キーを取り消すと、使用できないデータや読み取れないデータがレンダリングされます。

ネットワークのセグメンテーションと強化

マネージドサービスである Amazon Comprehend は、AWS 「セキュリティ、アイデンティティ、コンプライアンスのベストプラクティス」に準拠しています。

推奨されるネットワークセキュリティ保護措置については、「Amazon Comprehend デベロッパーガイド」の「Amazon Comprehend のインフラストラクチャセキュリティAmazon Comprehend」を参照してください。

Amazon Virtual Private Cloud (Amazon VPC) を使用してジョブを保護する

Amazon Comprehend では、さまざまなセキュリティ対策を使用して、データおよび、Amazon Comprehend の使用中にそのデータが保存されるジョブコンテナの安全性を確保することができます。ただし、ジョブコンテナは、データやモデルアーティファクトを保存する Amazon S3 バケットなどの AWS リソースにインターネット経由でアクセスします。

データへのアクセスを制御するには、仮想プライベートクラウド (VPC) を作成して、データおよびコンテナがインターネット経由でアクセスできないように設定すことをお勧めします。VPC の作成と設定の詳細については、「Amazon VPC ユーザーガイド」の「Amazon VPC の開始方法」を参照してください。VPC を利用すると、インターネットに接続されないように VPC を設定できるため、ジョブコンテナとデータを保護することができます。VPC 利用すると、VPC フローログを使ってジョブコンテナとの間のすべてのネットワークトラフィックを監視することもできます。詳細については、Amazon VPC ユーザーガイドのVPC フローログを参照してください。

VPC 設定は、サブネットとセキュリティグループを指定してモデルを作成するときに指定します。サブネットとセキュリティグループが指定されると、Amazon Comprehend はサブネットの 1 つのセキュリティグループに関連付けられている Elastic Network Interface (ENI) を作成します。ENI により、ジョブコンテナが VPC のリソースに接続できるようになります。ENI については、『Amazon VPC ユーザーガイド』の「Elastic Network Interfaces」を参照してください。

> **Note**
>
> ジョブの場合は、デフォルトのテナンシー VPC を使用してのみサブネットを設定できます。この VPC では、インスタンスは共有ハードウェアで実行されます。VPC のテナンシー属性の詳細については、『Amazon EC2 ユーザーガイド - Linux インスタンス』の「専有インスタンス」を参照してください。

インターフェイス VPC エンドポイントを作成すると、VPC と Amazon Comprehend との間のプライベート接続を確立できます。詳細については、「Amazon Comprehend とインターフェイス VPC エンドポイント (AWS PrivateLink) 」を参照してください。

ホストとイメージの強化

AWS 責任共有モデル に基づいて、Amazon Comprehend の AWS 環境のホストとイメージの強化は、 が提供するサービス AWS として によって管理されます。

マルチテナンシー

レコメンデーションの安全性を高めるために、次のマルチテナンシーセキュリティレコメンデーションを実装することをお勧めします。

- ドメインの一致に基づいたテナントへのユーザーアクセスを承認するために、検証済みの E メールアドレスのみを使用します。E メールアドレスと電話番号は、アプリが検証するか、外部 IdP が検証の証明を提供しない限り、信頼しないでください。これらの許可を設定する方法の詳細については、「属性の許可と範囲」を参照してください。
- テナントを識別するユーザープロファイル属性には、イミュータブル属性またはミュータブル属性を使用します。管理者はこれらの属性を変更できる必要があります。また、アプリクライアントに属性への読み取り専用アクセスを許可します。
- 外部 IdP とアプリケーションクライアントの間の 1:1 マッピングを使用して、承認されていないクロステナントアクセスを防止します。外部 IdP によって認証され、有効な Amazon Cognito セッ

ション Cookie を持つユーザーは、同じ IdP を信頼する他のテナントアプリケーションにアクセスできます。

- アプリケーションにテナントマッチングおよび認可ロジックを実装する場合は、テナントへのユーザーアクセスを認可する基準を変更できないようにユーザーを制限してください。また、フェデレーションのために外部 IdP が使用されている場合は、テナント ID プロバイダー管理者がユーザーアクセスを変更できないように制限してください。

サービス間の混乱した代理の防止

「混乱した代理」問題は、アクションを実行する許可を持たないエンティティが、より特権のあるエンティティにアクションを実行するよう強制できるマルチテナンシーのセキュリティ上の問題です。では AWS、サービス間でなりすましを行うと、混乱した代理問題が発生する可能性があります。サービス間でのなりすましは、1 つのサービス (呼び出し元サービス) が、別のサービス (呼び出し対象サービス) を呼び出すときに発生する可能性があります。呼び出し元サービスは、本来ならアクセスすることが許可されるべきではない方法でその許可を使用して、別のお客様のリソースに対する処理を実行するように操作される場合があります。これを防ぐために、 は、アカウント内のリソースへのアクセスが許可されているサービスプリンシパルを使用して、すべてのサービスのデータを保護するのに役立つツール AWS を提供します。このセキュリティ問題に対処するために考慮すべき保護策を含む詳細については、「Amazon Comprehend デベロッパーガイド」の「サービス間の混乱した代理の防止」を参照してください。

Amazon Comprehend Medical

ガイダンスについては、前のAmazon Comprehendセクションを参照してください。

Amazon Connect

Amazon Connect は、動的で個人向けの自然なカスタマーエンゲージメントをあらゆる規模で実現する、セルフサービスのクラウドベースのコンタクトセンターサービスです。お客様は、Amazon Connect 内のユーザー、セキュリティプロファイル、および問い合わせフローの管理に関連するフィールドに PHI を含めないでください。

Amazon Connect の一機能である Amazon Connect Customer Profiles は、コンタクトセンターエージェントに、顧客プロファイルをより統一されたビューと最新の情報を提供し、よりパーソナライズされたカスタマーサービスを提供します。Customer Profiles は、複数のアプリケーションからの顧客情報を統合顧客プロファイルに自動的にまとめ、サポートコールややり取りが開始されるとすぐに

プロファイルをエージェントに直接配信するように設計されています。お客様は、PHI データを使用してドメインまたはオブジェクトキーに名前を付けることはできません。ドメインとオブジェクトの内容は暗号化および保護されますが、キー識別子は暗号化されません。

Amazon DocumentDB (MongoDB 互換性)

Amazon DocumentDB (MongoDB 互換) (Amazon DocumentDB) は、 経由でクラスター作成時に保管時の暗号化を提供します。これにより AWS KMS、AWS またはカスタマーマネージドキーを使用してデータベースを暗号化できます。暗号化を有効にして実行されているデータベースインスタンスでは、保管時に保存されるデータは、自動バックアップ、リードレプリカ、スナップショットと同様に、このホワイトペーパーの公開時に有効なガイダンスに従って暗号化されます。ガイダンスは更新される可能性があるため、お客様は Amazon DocumentDB 暗号化がコンプライアンスと規制の要件を満たしているかどうかを引き続き評価して判断する必要があります。Amazon DocumentDB を使用した保管時の暗号化の詳細については、「保管中の Amazon DocumentDB データの暗号化」を参照してください。

PHI を含む Amazon DocumentDB への接続には、暗号化トランスポート (HTTPS) を受け入れるエンドポイントを使用する必要があります。デフォルトでは、新しく作成された Amazon DocumentDB クラスターは、Transport Layer Security (TLS) を使用した安全な接続のみを受け入れます。詳細については、「転送中のデータの暗号化」を参照してください。Amazon DocumentDB は AWS CloudTrail を使用してすべての API コールをログに記録します。詳細については、「Amazon DocumentDB でのログ記録とモニタリング」を参照してください。

特定の管理機能について、Amazon DocumentDB は Amazon RDS と共有されるオペレーショナルテクノロジーを使用します。Amazon DocumentDB コンソール、AWS CLI、および API コールは、Amazon RDS API への呼び出しとして記録されます。

Amazon DynamoDB

PHI を含む Amazon DynamoDB への接続には、暗号化トランスポート (HTTPS) を受け入れるエンドポイントを使用する必要があります。リージョンエンドポイントのリストについては、「AWS サービスエンドポイント」を参照してください。

Amazon DynamoDB は DynamoDB 暗号化を提供しています。これにより、お客様は を通じてお客様が管理するキーを使用してデータベースを暗号化できます AWS KMS。Amazon DynamoDB 暗号化で実行されているデータベースインスタンスでは、基盤となるストレージに保存されているデータは、自動バックアップ、リードレプリカ、スナップショットと同様に、このホワイトペーパーの公開時に有効なガイダンスに従って暗号化されます。

ガイダンスは更新される可能性があるため、お客様は Amazon DynamoDB 暗号化がコンプライアンスおよび規制要件を満たしているかどうかを引き続き評価して判断する必要があります。Amazon DynamoDB を使用した保管時の暗号化の詳細については、「保管時の DynamoDB 暗号化」を参照してください。

Amazon Elastic Block Store

Amazon EBS 保管時の暗号化は、このホワイトペーパーの公開時に有効なガイダンスと一致しています。ガイダンスは更新される可能性があるため、お客様は引き続き Amazon EBS 暗号化がコンプライアンスおよび規制要件を満たしているかどうかを評価し、判断する必要があります。Amazon EBS 暗号化では、EBS ボリュームごとに一意のボリューム暗号化キーが生成されます。お客様は、各ボリュームキーの暗号化 AWS Key Management Service に使用する KMS キーを柔軟に選択できます。詳細については、「Amazon EBS 暗号化」を参照してください。

Amazon Elastic Compute Cloud

Amazon EC2 は、スケーラブルでユーザー設定可能なコンピューティングサービスで、保管中のデータを暗号化するための複数の方法をサポートしています。例えば、お客様は、Amazon EC2 インスタンスでホストされているアプリケーションまたはデータベースプラットフォーム内で処理される PHI のアプリケーションレベルまたはフィールドレベルの暗号化を実行することを選択できます。アプローチには、Java や .NET などのアプリケーションフレームワークの標準ライブラリを使用したデータの暗号化、Microsoft SQL や Oracle の透過的なデータ暗号化機能の利用、他のサードパーティーや Software as a Service (SaaS) ベースのソリューションをアプリケーションに統合することが含まれます。

お客様は、Amazon EC2 で実行されているアプリケーションを AWS KMS SDKsと統合することを選択できるため、キーの管理とストレージのプロセスが簡素化されます。また、 AWS Marketplace パートナーのサードパーティーソフトウェアやネイティブファイルシステム暗号化ツール (dm-crypt、LUKS など) を使用して、ファイルレベルまたはフルディスク暗号化 (FDE) を使用して保管中のデータの暗号化を実装することもできます。

PHI を含むネットワークトラフィックは、転送中のデータを暗号化する必要があります。外部ソース (インターネットや従来の IT 環境など) と Amazon EC2 間のトラフィックについては、 ガイダンスに従って、Transport Layer Security (TLS) や IPsec 仮想プライベートネットワーク (VPNsなどのオープンスタンダードトランスポート暗号化メカニズムを使用する必要があります。Amazon EC2 インスタンス間のデータ移動のために Amazon Amazon Virtual Private Cloud (VPC) 内部で、PHI を含むネットワークトラフィックも暗号化する必要があります。ほとんどのアプリケーションは、 ガ

イダンスと一致するように設定できる TLS またはその他の転送中の暗号化プロトコルをサポートしています。暗号化をサポートしていないアプリケーションやプロトコルの場合、PHI を送信するセッションは、IPsec またはインスタンス間の同様の実装を使用して、暗号化されたトンネルを介して送信できます。

Amazon Elastic Container Registry

Amazon Elastic Container Registry (Amazon ECR) は Amazon Elastic Container Service (Amazon ECS) と統合されており、Amazon ECS で実行されているアプリケーションのコンテナイメージを簡単に保存、実行、管理できます。お客様がタスク定義で Amazon ECR リポジトリを指定すると、Amazon ECS はアプリケーションに適したイメージを取得します。

PHI を含むコンテナイメージで Amazon ECR を使用するための特別なステップは必要ありません。コンテナイメージは転送中に暗号化され、Amazon S3 サーバー側の暗号化 (SSE-S3) を使用して保管中に暗号化されて保存されます。

Amazon Elastic Container Service

Amazon Elastic Container Service (Amazon ECS) は、Docker コンテナをサポートする非常にスケーラブルで高性能なコンテナ管理サービスであり、お客様は Amazon EC2 インスタンスのマネージドクラスターでアプリケーションを簡単に実行できます。Amazon ECS により、お客様は独自のクラスター管理インフラストラクチャをインストール、運用、スケーリングする必要がなくなります。

シンプルな API コールを使用すると、Docker 対応アプリケーションを起動および停止し、クラスターの完全な状態をクエリし、セキュリティグループ、Elastic Load Balancing、EBS ボリューム、IAM ロールなど、多くの使い慣れた機能にアクセスできます。お客様は Amazon ECS を使用して、リソースのニーズと可用性の要件に基づいて、クラスター全体でコンテナの配置をスケジュールできます。

PHI を処理するワークロードで ECS を使用する場合、追加の設定は必要ありません。ECS は、EC2 上のコンテナ (S3 に保存されているイメージ) の起動を調整するオーケストレーションサービスとして機能し、オーケストレーション対象のワークロード内のデータに対して動作または動作しません。HIPAA 規制および AWS 事業提携契約に従い、ECS で起動されたコンテナから PHI にアクセスするときは、転送中および保管時に暗号化する必要があります。各 AWS ストレージオプション (S3、EBS、KMS など) では、保管時の暗号化のためのさまざまなメカニズムを使用できます。コンテナ間で送信される PHI の完全な暗号化を確保すると、お客様が冗長な暗号化レイヤーを提供するためにオーバーレイネットワーク (VNS3、Weave Net など) をデプロイする必要もあります。ただ

し、完全なログ記録も有効にし（など）、 CloudTrailすべてのコンテナインスタンスログを に送信する必要があります CloudWatch。

PHI を処理するワークロードで Firelens と AWS for Fluent Bit を使用する場合、ログに PHI が含まれない限り、追加の設定は必要ありません。ログに PHI が含まれている場合は、ディスク暗号化が有効になっていない限り、ログファイルに出力しないでください。代わりに、 によって自動的に収集される標準出力/エラーにログを送信するようにアプリケーションを設定します FireLens。同様に、ディスク暗号化も有効になっていない限り、Fluent Bit のファイルバッファリングを有効にしないでください。最後に、ログ送信先は をサポートする必要があります encryption-in-transit。AWS for Fluent Bit のすべての AWS サービス出力プラグインは、常に TLS 暗号化を使用してログをエクスポートします。

Amazon Elastic File System (Amazon EFS)

Amazon Elastic File System (Amazon EFS) は、 AWS クラウドサービスおよびオンプレミスリソースで使用できる、シンプルでスケーラブルな伸縮自在なファイルストレージを提供します。使いやすく、顧客がファイルシステムを迅速かつ簡単に作成および設定できるシンプルなインターフェイスを提供します。Amazon EFS は、アプリケーションを中断することなく、お客様がファイルを追加または削除すると自動的に拡張および縮小することなく、オンデマンドで伸縮自在にスケーリングするように構築されています。

PHI を保管中に暗号化するという要件を満たすために、EFS で 2 つのパスを使用できます。EFS は、新しいファイルシステムの作成時に保管時の暗号化をサポートします。作成時に、「保管中のデータの暗号化を有効にする」のオプションを選択する必要があります。このオプションを選択すると、EFS ファイルシステムに配置されたすべてのデータが AES-256 暗号化キーと AWS KMSマネージドキーを使用して暗号化されます。お客様は、EFS に配置される前にデータを暗号化することもできますが、暗号化プロセスとキー管理の管理はお客様の責任となります。

PHI は、ファイル名またはフォルダ名のすべてまたは一部として使用しないでください。Amazon EFS の転送中の PHI の暗号化は、EFS サービスとファイルシステムをマウントするインスタンス間の Transport Layer Security (TLS) EFS によって提供されます。EFS には、TLS を使用したファイルシステムへの接続を容易にするマウントヘルパーが用意されています。デフォルトでは、TLS は使用されず、EFS マウントヘルパーを使用してファイルシステムをマウントするときに有効にする必要があります。マウントコマンドに TLS 暗号化を有効にする「-o tls」オプションが含まれていることを確認します。または、EFS マウントヘルパーを使用しないことを選択したお客様は、EFS ドキュメントの指示に従って、TLS トンネルを介して接続するように NFS クライアントを設定できます。

Amazon Elastic Kubernetes Service (Amazon EKS)

Amazon Elastic Kubernetes Service (Amazon EKS) は、お客様が独自の Kubernetes コントロールプレーンを立ち上げたり維持したりすることなく、AWS で Kubernetes を簡単に実行できるようにするマネージド型サービスです。Kubernetes は、コンテナ化されたアプリケーションのデプロイ、スケーリング、および管理を自動化するためのオープンソースシステムです。セキュリティとコンプライアンスに関する追加情報については、ホワイトペーパー「Architecting for HIPAA Security and Compliance on Amazon EKS」を参照してください。

Amazon ElastiCache for Redis

Amazon ElastiCache for Redis は、データストアまたはキャッシュとして使用できる Redis 互換のインメモリデータ構造サービスです。PHI を保存するには、Redis エンジンバージョンと現行世代のノードタイプ ElastiCache に対して最新の HIPAA 対応 を実行していることを確認する必要があります。Amazon ElastiCache for Redis では、次のノードタイプと Redis エンジンバージョンの PHI の保存がサポートされています。

- ノードタイプ: 現行世代のみ (例えば、このホワイトペーパーの公開時点での M4, M5, R4, R5, T2, T3)
- ElastiCache for Redis エンジンバージョン: 3.2.6 および 4.0.10 以降

現行世代のノードの選択の詳細については、「Amazon の ElastiCache 料金」を参照してください。ElastiCache for Redis エンジンの選択の詳細については、「Amazon ElastiCache for Redis とは」を参照してください。

また、クラスターとクラスター内のノードが、保管中のデータを暗号化し、転送中の暗号化を有効にし、Redis コマンドの認証を有効にするように設定されていることも確認する必要があります。さらに、「日付による適用の推奨」 (更新の適用が推奨される日付) 以前の Redis クラスターが常に最新の「セキュリティ」タイプのサービス更新で更新されていることを確認する必要があります。詳細については、関連するセクションを参照してください。

トピック

- 保管時の暗号化
- 送信の暗号化
- 認証
- ElastiCache サービスの更新の適用

保管時の暗号化

Amazon ElastiCache for Redis は、クラスターのデータ暗号化を提供し、保管中のデータを保護します。お客様が作成時にクラスターの保管時の暗号化を有効にすると、Amazon ElastiCache for Redis はディスク上のデータと自動 Redis バックアップを暗号化します。ディスク上の顧客データは、ハードウェアアクセラレーション高度暗号化標準 (AES)-512 対称キーを使用して暗号化されます。Redis バックアップは、Amazon S3-managed暗号化キー (SSE-S3) によって暗号化されます。サーバー側の暗号化が有効になっている S3 バケットは、バケットに保存する前に、ハードウェアアクセラレーション高度暗号化標準 (AES)-256 対称キーを使用してデータを暗号化します。

Amazon S3-managed暗号化キー (SSE-S3) の詳細については、「Amazon S3-Managed暗号化キーによるサーバー側の暗号化 (SSE-S3) を使用したデータの保護」を参照してください。暗号化で実行されている ElastiCache Redis クラスター (単一ノードまたはマルチノード) では、保管時に保存されるデータは、このホワイトペーパーの公開時に有効なガイダンスに従って暗号化されます。これには、ディスク上のデータと S3 バケット内の自動バックアップが含まれます。ガイダンスは更新される可能性があるため、お客様は Amazon ElastiCache for Redis 暗号化がコンプライアンスおよび規制要件を満たしているかどうかを引き続き評価および判断する必要があります。Amazon ElastiCache for Redis を使用した保管時の暗号化の詳細については、「Amazon for Redis とは ElastiCache 」を参照してください。

送信の暗号化

Amazon ElastiCache for Redis は TLS を使用して転送中のデータを暗号化します。PHI を含む Redis の への接続 ElastiCacheでは、トランスポート暗号化を使用し、 ガイダンスと整合性について設定を評価する必要があります。詳細については、「」を参照してくださいCreateReplicationGroup。転送時の暗号化を有効にする方法の詳細については、ElastiCache 「 for Redis 転送時の暗号化 (TLS)」を参照してください。

認証

PHI を含む Amazon ElastiCache for Redis クラスター (単一/複数ノード) は、Redis コマンドの認証を有効にするために Redis AUTH トークンを提供する必要があります。Redis AUTH は、保管時の暗号化と転送中の暗号化の両方が有効になっている場合に使用できます。お客様は、以下の制約付きで Redis AUTH の強力なトークンを提供する必要があります。

- 印刷可能な ASCII 文字のみを使用する必要があります
- 16 文字以上、128 文字以下である必要があります
- 「/」、「」、「@」の文字を含めることはできません。

このトークンは、Redis レプリケーショングループ (単一/複数ノード) の作成時にリクエストパラメータ内から設定する必要があり、後で新しい値で更新できます。AWS は、 AWS Key Management Service () を使用してこのトークンを暗号化しますAWS KMS。Redis AUTH の詳細については、「 for ElastiCache Redis In-Transit Encryption (TLS)」を参照してください。

ElastiCache サービスの更新の適用

PHI を含む Amazon ElastiCache for Redis クラスター (単一/複数ノード) は、「日付による適用を推奨」以前の最新の「セキュリティ」タイプのサービス更新で更新する必要があります。 ElastiCache は、お客様がいつでもオンデマンドおよびリアルタイムで更新を適用するために使用できるセルフサービス機能としてこれを提供します。各サービスの更新には「重要度」と「日付による推奨適用」が付属しており、該当する Redis レプリケーショングループでのみ使用できます。

サービス更新機能の「SLA Met」フィールドには、「推奨される日付による適用」以前に更新が適用されたかどうかが表示されます。「日付による推奨適用」によって、お客様が該当する Redis レプリケーショングループに更新を適用しないことを選択した場合、 ElastiCache は更新を適用するアクションを実行しません。お客様は、サービス更新履歴ダッシュボードを使用して、時間の経過とともに Redis レプリケーショングループの更新の適用を確認できます。この機能の使用方法の詳細については、「Amazon でのセルフサービスの更新 ElastiCache」を参照してください。

Amazon OpenSearch サービス

Amazon OpenSearch Service を使用すると、お客様は専用の Amazon Virtual Private Cloud (Amazon VPC) でマネージド型 OpenSearch または従来の Elasticsearch OSS クラスターを実行できます。PHI で OpenSearch サービスを使用する場合は、 OpenSearch または Elasticsearch 6.0 以降を使用する必要があります。お客様は、PHI が Amazon OpenSearch Service 内で保管中および転送中に暗号化されていることを確認する必要があります。お客様は、 AWS KMS キー暗号化を使用して、 OpenSearch および Elasticsearch 5.1 以降でのみ使用できる OpenSearch サービスドメイン内の保管中のデータを暗号化できます。保管中のデータを暗号化する方法の詳細については、「Amazon OpenSearch Service の保管中のデータの暗号化」を参照してください。

各 OpenSearch サービスドメインは、独自の VPC で実行されます。お客様は、すべての OpenSearch バージョン、および Elasticsearch 6.0 以降で利用可能な node-to-node 暗号化を有効にする必要があります。お客様が HTTPS 経由で OpenSearch サービスにデータを送信した場合、 node-to-node 暗号化により、データがクラスター全体に OpenSearch 配信 (および再配布) される際に暗号化されたままになります。データが HTTP 経由で暗号化されずに到着した場合、OpenSearch サービスはクラスターに到達した後でデータを暗号化します。したがって、Amazon

OpenSearch Service クラスターに入る PHI は HTTPS 経由で送信する必要があります。詳細については、「Amazon OpenSearch Service の N ode-to-node 暗号化」を参照してください。

OpenSearch サービス設定 API からのログは、 でキャプチャできます AWS CloudTrail。詳細については、「 を使用した Amazon OpenSearch Service API コールのモニタリング AWS CloudTrail」を参照してください。

Amazon EMR

Amazon EMR は、Amazon EC2 インスタンスのクラスターをお客様のアカウントにデプロイおよび管理します。Amazon EMR での暗号化の詳細については、「暗号化オプション」を参照してください。

Amazon EventBridge

Amazon EventBridge（以前の Amazon CloudWatch Events) は、スケーラブルなイベント駆動型アプリケーションを作成できるサーバーレスイベントバスです。 は、Zendesk、Datadog、Pagerduty などのイベントソースからリアルタイムデータのストリームを EventBridge 配信し、そのデータをなどのターゲットにルーティングします AWS Lambda。

デフォルトでは、 は AWS 所有の CMK で 256 ビットの Advanced Encryption Standard (AES-256) を使用してデータを EventBridge 暗号化します。これにより、顧客データを不正アクセスから保護できます。お客様は、PHI を保存、処理、または送信するイベントを発行する AWS リソースが、 のベストプラクティスに従って設定されていることを確認する必要があります。

Amazon EventBridge は と統合 AWS CloudTrail されており、お客様は イベント履歴で CloudTrail コンソールで最新のイベントを表示できます。詳細については、「 EventBridge の情報 CloudTrail」を参照してください。

Amazon Forecast

Amazon Forecast は、機械学習を使用して高精度の予測を実現するフルマネージドサービスです。Amazon.com で使用されているのと同じ機械学習予測テクノロジーに基づく。顧客が Amazon Forecast とやり取りするたびに、暗号化によって保護されます。Amazon Forecast によって処理されるコンテンツは、Amazon Key Management Service を通じてカスタマーキーで暗号化され、お客様がサービスを使用している AWS リージョンで保管時に暗号化されます。

Amazon Forecast は AWS CloudTrail、Amazon Forecast のユーザー、ロール、または AWS のサービスによって実行されたアクションを記録するサービスである と統合されています。 は、Amazon

Forecast のすべての API コールをイベントとして CloudTrail キャプチャします。キャプチャされた呼び出しには、Amazon Forecast コンソールからの呼び出しと、Amazon Forecast API オペレーションへのコード呼び出しが含まれます。お客様が証跡を作成する場合、Amazon Forecast の CloudTrail イベントなど、Amazon S3 バケットへのイベントの継続的な配信を有効にすることができます。詳細については、「 を使用した Forecast API コールのログ記録 AWS CloudTrail」を参照してください。

デフォルトでは、 によってバケット CloudTrail に配信されるログファイルは、Amazon S3-managed暗号化キー (SSE-S3) を使用した Amazon サーバー側の暗号化によって暗号化されます。直接管理可能なセキュリティレイヤーを提供するために、代わりに が管理するキーによるサーバー側の暗号化 (SSE-KMS) AWS KMSを CloudTrail ログファイルに使用できます。サーバー側の暗号化を有効にすると SSE-KMS、を使用してログファイルが暗号化されますが、ダイジェストファイルは暗号化されません。ダイジェストファイルは、Amazon S3 で管理された暗号化キー (SSE-S3) を使用して暗号化されます。

AWS Forecast は、S3 バケットとの間でデータをインポートおよびエクスポートします。Amazon S3 からデータをインポートおよびエクスポートするときは、S3 バケットがガイダンスに従って設定されていることを確認する必要があります。詳細については、「 の使用開始」を参照してください。

Amazon FSx

Amazon FSx は、機能豊富な高性能なファイルシステムを提供するフルマネージドサービスです。Amazon FSx for Windows File Server は、信頼性が高くスケーラブルなファイルストレージを提供し、サーバーメッセージブロック (SMB) プロトコル経由でアクセスできます。Amazon FSx for Lustre は、コンピューティングワークロード用の高性能ストレージを提供し、世界で最も人気のある高性能ファイルシステムである Lustre を搭載しています。

Amazon FSx は、ファイルシステムの 2 つの暗号化形式、転送中のデータの暗号化と保管時の暗号化をサポートしています。Amazon FSx for Windows File Server は、 を使用したすべての API コールのログ記録もサポートしています AWS CloudTrail。

転送中のデータの暗号化は、SMB プロトコル 3.0 以降をサポートするコンピューティングインスタンスでは Amazon FSx for Windows File Server で、転送中の暗号化をサポートする Amazon EC2 インスタンスでは Amazon FSx for Lustre でサポートされています。または、Amazon FSx に保存する前にデータを暗号化することもできますが、暗号化プロセスとキー管理はお客様の責任となります。

保管中のデータの暗号化は、AES-256 暗号化アルゴリズムと AWS KMSマネージドキーを使用して Amazon FSx ファイルシステムを作成するときに自動的に有効になります。データおよびメタデータ

は、ファイルシステムに書き込まれる前に自動的に暗号化され、アプリケーションに提示される前に自動的に復号されます。PHI は、ファイル名やフォルダ名には使用しないでください。

Amazon GuardDuty

Amazon GuardDuty は、悪意のある動作や不正な動作を継続的にモニタリングし、AWS アカウントとワークロードを保護するマネージド脅威検出サービスです。異常な API コールや、アカウントの侵害の可能性を示す不正なデプロイなどのアクティビティをモニタリングします。Amazon は、侵害された可能性のあるインスタンスや攻撃者による偵察 GuardDuty も検出します。

Amazon は、VPC フローログ、 AWS CloudTrail イベントログ、DNS ログのデータソース GuardDuty を継続的にモニタリングおよび分析します。悪意のある IPs やドメインのリストなどの脅威インテリジェンスフィード、および機械学習を使用して、AWS 環境内の予期しないアクティビティや不正アクティビティ、悪意のあるアクティビティを特定します。そのため、Amazon GuardDuty は PHI に遭遇しないでください。このデータは、上記の AWS ベースのデータソースのいずれにも保存されないためです。

Amazon HealthLake

Amazon HealthLake では、医療およびライフサイエンス業界のお客様は、ヘルスデータをペタバイト規模で保存、変換、クエリ、分析できます。お客様は Amazon HealthLake を使用して PHI を送信、処理、保存できます。Amazon は、デフォルトで顧客のデータストアに保管中のデータを HealthLake 暗号化します。すべてのサービスデータとメタデータは、サービス所有の KMS キーで暗号化されます。FastTAK Interoperability Resources (FHIR) の仕様に従って、お客様が FHIR リソースを削除すると、そのリソースは取得からのみ非表示になり、バージョニングのためにサービスによって保持されます。お客様が StartFHIRImportJob API を使用する場合、Amazon HealthLake は暗号化された Amazon S3 バケットにデータをエクスポートする要件を適用します。

Amazon は、転送中と保管時の両方のデータを HealthLake 暗号化します。転送中のデータを暗号化するには、AWS が公開した API コールを使用して、ネットワーク HealthLake 経由で にアクセスできます。クライアントで Transport Layer Security (TLS) 1.0 以降がサポートされている必要があります。TLS 1.2、できれば TLS 1.3 が必要です。また、一時的ディフィー・ ヘルマン Ephemeral Diffie-Hellman (DHE) や Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートもクライアントでサポートされている必要があります。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。また、リクエストには、アクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token Service (AWS STS) を使用して、リク

エストに署名するための一時的なセキュリティ認証情報を生成することもできます。保管中のデータを暗号化するために、Amazon はデフォルトで、顧客所有の AWS KMS キーまたはサービス所有の AWS KMS キーを使用して、顧客のデータストア内のデータを HealthLake 暗号化します。すべてのサービスデータとメタデータは、サービス所有の AWS KMS キーで保管時に暗号化されます。

Amazon HealthLake は、 と統合されています AWS CloudTrail。 は、、コマンドラインインターフェイス (CLI) との対話の結果として行われた呼び出し、 Software Development Kit (SDK) を使用したプログラムによる呼び出しなど AWS Management Console、Amazon へのすべての API コールをイベント HealthLake として CloudTrail キャプチャします。

Amazon Inspector

Amazon Inspector は、AWS にデプロイされたアプリケーションのセキュリティとコンプライアンスの向上を検討しているお客様向けの自動セキュリティ評価サービスです。Amazon Inspector では、自動的にアプリケーションを評価し、脆弱性やベストプラクティスからの逸脱がないかどうかを確認できます。評価を実行すると、Amazon Inspector は重要度レベルによって優先順位付けされたセキュリティ検出結果の詳細なリストを生成します。お客様は、PHI を含む EC2 インスタンスで Amazon Inspector を実行できます。Amazon Inspector は、ネットワーク経由で送信されるすべてのデータと、保管時に保存されるすべてのテレメトリデータを暗号化します。

Amazon Managed Service for Apache Flink

Amazon Managed Service for Apache Flink を使用すると、ほぼリアルタイムでデータを継続的に読み取り、処理、保存する SQL コードをすばやく作成できます。ストリーミングデータに標準 SQL クエリを使用すると、データを変換してインサイトを提供するアプリケーションを構築できます。Managed Service for Apache Flink は、分析アプリケーションのソースとして Kinesis Data Streams および Firehose 配信ストリームからの入力をサポートします。ストリームが暗号化されている場合、Managed Service for Apache Flink は、暗号化されたストリーム内のデータにシームレスにアクセスし、それ以上の設定は必要ありません。Managed Service for Apache Flink は、Kinesis Data Streams から読み取られた暗号化されていないデータを保存しません。詳細については、「アプリケーション入力の設定」を参照してください。

Apache Flink 用 Managed Service は、アプリケーションモニタリングのために AWS CloudTrail と Amazon CloudWatch Logs の両方と統合されています。詳細については、「 ツールのモニタリング」および「Amazon CloudWatch Logs の使用」を参照してください。

Amazon Data Firehose

お客様がデータプロデューサーから Kinesis データストリームにデータを送信すると、Amazon Kinesis Data Streams は AWS KMS キーを使用してデータを暗号化してから保管時に保存します。Firehose 配信ストリームが Kinesis ストリームからデータを読み取ると、Kinesis Data Streams はまずデータを復号化してから Firehose に送信します。Firehose は、お客様が指定したバッファリングヒントに基づいてデータをメモリにバッファします。

その後、保管中の暗号化されていないデータを保存せずに、データを宛先に配信します。Firehose による暗号化の詳細については、「Amazon Data Firehose でのデータ保護」を参照してください。

AWS には、Amazon CloudWatch メトリクス、Amazon CloudWatch Logs、Kinesis Agent、API のログ記録と履歴など、Amazon Data Firehose のモニタリングに使用できるさまざまなツールが用意されています。詳細については、「Amazon Data Firehose のモニタリング」を参照してください。

Amazon Kinesis Streams

Amazon Kinesis Streams を使用すると、お客様は、特別なニーズに合わせてストリーミングデータを処理または分析するカスタムアプリケーションを構築できます。サーバー側の暗号化機能を使用すると、お客様は保管中のデータを暗号化できます。サーバー側の暗号化が有効になっている場合、Kinesis Streams は キーを使用して AWS KMS データを暗号化してからディスクに保存します。詳細については、「Amazon Kinesis Data Streams のデータ保護」を参照してください。PHI を含む Amazon S3 への接続には、暗号化されたトランスポート (HTTPS) を受け入れるエンドポイントを使用する必要があります。リージョンエンドポイントのリストについては、「AWS サービスエンドポイント」を参照してください。

Amazon Kinesis Video Streams

Amazon Kinesis Video Streams は、デバイスから AWS クラウドにライブ動画をストリーミングしたり、リアルタイムの動画処理やバッチ指向の動画分析用のアプリケーションを構築したりするために使用できるフルマネージドの AWS サービスです。サーバー側の暗号化は、お客様が指定した AWS KMS キー (以前の CMK) を使用して保管中のデータを自動的に暗号化する Kinesis Video Streams の機能です。データが Kinesis Video Streams ストリームストレージレイヤーに書き込まれる前に暗号化され、ストレージから取得された後で復号されます。

Amazon Kinesis Video Streams SDK を使用して、PHI を含むストリーミングビデオデータを送信できます。デフォルトでは、SDK は TLS を使用して、インストールされているハードウェアデバイ

スによって生成されたフレームとフラグメントを暗号化します。SDK は、保管時に保存されるデータを管理したり、それらに影響を与えたりすることはありません。Amazon Kinesis Video Streams は、 を使用してすべての API コール AWS CloudTrail をログに記録します。

Amazon Lex

Amazon Lex は、音声やテキストを使用した会話型インターフェイスをさまざまなアプリケーションに構築するための AWS のサービスです。Amazon Lex では、Amazon Alexa を強化するのと同じ会話型エンジンがすべてのデベロッパーで利用できるようになりました。これにより、お客様は高度な自然言語のチャットボットを新規および既存のアプリケーションに組み込むことができます。Amazon Lex は、自然言語理解 (NLU) と自動音声認識 (ASR) の深い機能と柔軟性を提供するため、顧客はリアルな会話型インタラクションで非常に魅力的なユーザーエクスペリエンスを構築し、新しいカテゴリの製品を作成できます。

Lex は HTTPS プロトコルを使用して、クライアントおよびその他の AWS のサービスと通信します。Lex へのアクセスは API 主導であり、適切な IAM 最小権限を適用できます。詳細については、「Amazon Lex でのデータ保護」を参照してください。

モニタリングは、お客様の Amazon Lex チャットボットの信頼性、可用性、パフォーマンスを維持する上で重要です。Amazon Lex ボットの状態を追跡するには、Amazon を使用します CloudWatch。を使用すると CloudWatch、お客様は、個々の Amazon Lex オペレーションまたはアカウントのグローバル Amazon Lex オペレーションのメトリクスを取得できます。お客様は、1 つ以上のメトリクスがお客様が定義したしきい値を超えたときに通知されるように CloudWatch アラームを設定することもできます。例えば、特定の期間にボットに対して行われたリクエストの数をモニタリングしたり、成功したリクエストのレイテンシーを表示したり、エラーがしきい値を超えたときにアラームを発生させたりできます。Lex は とも統合 AWS CloudTrail され、Lex API コールをログに記録します。詳細については、「Amazon Lex でのモニタリング」を参照してください。

Amazon Managed Streaming for Apache Kafka (Amazon MSK)

Amazon MSK には、保管中のデータと転送中のデータの暗号化機能があります。保管中のデータの暗号化では、Amazon MSK クラスターは Amazon EBS サーバー側の暗号化と AWS KMS キーを使用してストレージボリュームを暗号化します。転送中のデータの場合、Amazon MSK クラスターでは、ブローカー間通信のために TLS 経由で暗号化が有効になっています。

暗号化設定は、クラスターの作成時に有効になります。また、デフォルトでは、 CLI または AWS コンソールから作成されたクラスターの転送時の暗号化は TLS に設定されます。クライアントが TLS 暗号化を使用してクラスターと通信するには、追加の設定が必要です。お客様は、TLS/プレー

ンテキスト設定を選択して、デフォルトの暗号化設定を変更できます。詳細については、「Amazon MSK 暗号化」を参照してください。

お客様は、Amazon MSK コンソール、Amazon CloudWatch コンソール、またはオープンソースのモニタリングソリューションである Prometheus で Open Monitoring を使用して JMX にアクセスし、メトリクスをホストできます。

Prometheus エクスポーターから読み取るように設計されたツールは、Datadog、Lenses、New Relic、SumTAK、Prometheus サーバーなど、Open Monitoring と互換性があります。Open Monitoring の詳細については、「Amazon MSK Open Monitoring ドキュメント」を参照してください。

Apache Kafka にバンドルされた Apache Zookeeper のデフォルトバージョンは暗号化をサポートしていないことに注意してください。ただし、Apache Zookeeper と Apache Kafka ブローカー間の通信は、ブローカー、トピック、パーティションの状態情報に制限されていることに注意してください。Amazon MSK クラスターからデータを生成および消費する唯一の方法は、VPC 内のクライアントと Amazon MSK クラスター間のプライベート接続を使用することです。Amazon MSK はパブリックエンドポイントをサポートしていません。

Amazon MQ

Amazon MQ は Apache ActiveMQ 向けのマネージドメッセージブローカーサービスで、クラウドでのメッセージブローカーのセットアップと運用を容易にします。Amazon MQ は、お客様が独自のメッセージングシステムを管理、運用、維持することなく、既存のアプリケーションとサービスと連携します。転送中に PHI データを暗号化するには、TLS が有効になっている次のプロトコルを使用してブローカーにアクセスする必要があります。

- AMQP
- MQTT
- MQTT over WebSocket
- OpenWire
- STOMP
- 経由の STOMP WebSocket

Amazon MQ は、安全に管理および保存される暗号化キーを使用して、保管中および転送中のメッセージを暗号化します。Amazon MQ は CloudTrail を使用してすべての API コールをログに記録します。

Amazon Neptune

Amazon Neptune は、高速で信頼性に優れたフルマネージド型のグラフデータベースサービスで、高度に接続されたデータセットを使用するアプリケーションの構築と実行を容易にします。Amazon Neptune のコアは、数十億の関係を保存し、ミリ秒単位のレイテンシーでグラフをクエリするように最適化された、専用の高性能グラフデータベースエンジンです。Amazon Neptune は、一般的なグラフクエリ言語 Apache TinkerPop Gremlin と W3C の SPARQL をサポートしています。

PHI を含むデータは、Amazon Neptune の暗号化されたインスタンスに保持できるようになりました。Amazon Neptune の暗号化されたインスタンスは、Amazon Neptune コンソールから「暗号化を有効にする」を選択することで、作成時にのみ指定できます。すべてのログ、バックアップ、スナップショットは、Amazon Neptune 暗号化インスタンスに対して暗号化されます。Amazon Neptune の暗号化されたインスタンスのキー管理は、 を通じて提供されます AWS KMS。転送中のデータの暗号化は SSL/TLS を通じて提供されます。Amazon Neptune は を使用してすべての API コール CloudTrail をログに記録します。

AWS Network Firewall

AWS Network Firewall は、すべての Amazon Virtual Private Cloud (Amazon VPC) に不可欠なネットワーク保護を簡単にデプロイできるようにするマネージドファイアウォールサービスです。このサービスは、基盤となるインフラストラクチャをセットアップまたは維持することなく、高可用性保護を提供するために、ネットワークトラフィックボリュームに合わせて自動的にスケーリングされます。カスタマールールとアクセスログの両方にエンドユーザー IP アドレスが含まれている場合があり、エンドユーザー IP アドレスは、 AWS アーキテクチャ内で保管中と転送中の両方に暗号化されます。さらに、 AWS Network Firewall は、コンポーネント AWS サービス (Amazon S3、Amazon DynamoDB、Amazon CloudWatch Logs、Amazon EBS) 間で保管中および転送中のすべてのデータを暗号化します。このサービスは、特別な設定を必要とせずにデータを自動的に暗号化します。

Amazon Pinpoint

Amazon Pinpoint は、単一の API レイヤー、CLI サポート、およびクライアント側の SDK サポートを提供して、ユーザーとのアプリケーション通信チャネルを拡張します。対象となるチャネルには、E メール、SMS テキストメッセージ、モバイルプッシュ通知、カスタムチャネルが含まれます。Amazon Pinpoint は、アプリユーザーの行動とユーザーエンゲージメントを追跡する分析システムも提供します。このサービスを使用すると、デベロッパーは各ユーザーがどのように関与したいかを理解し、ユーザーのエクスペリエンスをパーソナライズしてユーザーの満足度を高めることができます。

また、Amazon Pinpoint は、デベロッパーがダイレクトメッセージングやトランザクションメッセージング、ターゲットメッセージングやキャンペーンメッセージング、イベントベースのメッセージングなど、複数のメッセージングユースケースに対応するのにも役立ちます。Amazon Pinpoint を介してすべてのエンドユーザーエンゲージメントチャネルを統合して有効にすることで、デベロッパーはすべてのカスタマータッチポイントにわたるユーザーエンゲージメントを 360 度表示することができます。Amazon Pinpoint は、ユーザー、エンドポイント、イベントデータを保存するため、お客様はセグメントの作成、受信者へのメッセージの送信、エンゲージメントデータの取得を行うことができます。

Amazon Pinpoint は、保管中と転送中の両方のデータを暗号化します。詳細については、「Amazon Pinpoint に関するFAQs」を参照してください。Amazon Pinpoint は保管中および転送中のすべてのデータを暗号化しますが、SMS や E メールなどの最終チャネルは暗号化されない可能性があるため、お客様は要件に合った方法でチャネルを設定する必要があります。

さらに、SMS チャネルを介して PHI を送信する必要があるお客様は、PHI の送信を明示的な目的に専用のショートコード (5 桁の 6 桁の発信元電話番号) を使用する必要があります。ショートコードをリクエストする方法の詳細については、「Amazon Pinpoint による SMS メッセージングの専用ショートコードのリクエスト」を参照してください。お客様は、最終チャネルを介して PHI を送信せず、代わりに HTTPS 経由で PHI に安全にアクセスするメカニズムを提供することもできます。

Amazon Pinpoint への API コールは、 を使用してキャプチャできます AWS CloudTrail。キャプチャされた呼び出しには、Amazon Pinpoint コンソールからの呼び出しと、Amazon Pinpoint API オペレーションへのコード呼び出しが含まれます。お客様が証跡を作成する場合、Amazon Pinpoint の AWS CloudTrail イベントなど、Amazon S3 バケットへのイベントの継続的な配信を有効にすることができます。 Amazon Pinpoint お客様が証跡を設定しない場合でも、 AWS CloudTrail コンソールのイベント履歴を使用して最新のイベントを表示できます。によって収集された情報を使用して AWS CloudTrail、お客様は Amazon Pinpoint に対してリクエストが行われたこと、リクエストの IP アドレス、リクエスト者、リクエストが行われた日時などの詳細を確認できます。詳細については、「を使用した Amazon Pinpoint API コールのログ記録 AWS CloudTrail」を参照してください。

Amazon Polly

Amazon Polly はテキストを肉声に近い音声に変換するクラウドサービスです。Amazon Polly には、既存のアプリケーションと簡単に統合できるシンプルな API オペレーションが用意されています。Amazon Polly は HTTPS プロトコルを使用してクライアントと通信します。Amazon Polly へのアクセスは API 主導であり、適切な IAM 最小権限を適用できます。詳細については、「データ保護」を参照してください。PHI を含むユースケースの例をいくつか示します。

- スギバーは、PHI を含むテキストレポートを合成音声に変換し、ウォーキングやその他の職務遂行中にレポートを聞くことができるようにします。
- 視覚的に障害のある患者には医療ガイダンスが与えられ、合成された音声形式でガイダンスが消費されます。

Amazon Polly の最終的な配信チャネルでは、パブリックスペースで PHI を使用して音声を再生する可能性があり、配信ではこれを考慮に入れる必要があります。合成された音声出力は、暗号化が有効になっている Amazon S3 バケットに非同期で送信することもできます。

Amazon Polly でサポートされているイベントアクティビティが発生すると AWS CloudTrail 、そのアクティビティはイベント履歴の他の AWS サービスイベントとともにイベントに記録されます。Amazon Polly のイベントなど、顧客 AWS アカウントのイベントの継続的な記録については、証跡を作成します。証跡により CloudTrail、 はログファイルを Amazon S3 バケットに配信できます。によって収集された情報を使用して CloudTrail、お客様は Amazon Polly に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

Amazon Quantum Ledger Database (Amazon QLDB)

Amazon QLDB はフルマネージド型の台帳データベースで、信頼された中央機関が所有する、透過的でイミュータブルであり、暗号的に検証可能なトランザクションログを提供します。Amazon QLDB は、各アプリケーションデータの変更を追跡し、完全で検証可能な変更履歴を長期にわたって保持します。PHI を含むデータを QLDB インスタンスに保持できるようになりました。デフォルトでは、転送中および保管中のすべての Amazon QLDB データは暗号化されます。転送中のデータは TLS を使用して暗号化され、保管中のデータは AWS マネージドキーを使用して暗号化されます。データ保護の目的で、お客様は AWS アカウントの認証情報を保護し、 AWS Identity and Access Management (IAM) を使用して個々のユーザーアカウントを設定して、各ユーザーに各自の職務を果たすために必要なアクセス許可のみが付与されるようにすることをお勧めします。詳細については、「Amazon QLDB でのデータ保護」を参照してください。

Amazon QLDB は AWS CloudTrail、QLDB のユーザー、ロール、または AWS のサービスによって実行されたアクションを記録するサービスである と統合されています。 は、QLDB のすべてのコントロールプレーン API コールをイベントとして CloudTrail キャプチャします。キャプチャされた呼び出しには、QLDB コンソールの呼び出しと、QLDB API オペレーションへのコード呼び出しが含まれます。お客様が証跡を作成する場合、QLDB の CloudTrail イベントなど、Amazon Simple Storage Service (Amazon S3) バケットへのイベントの継続的な配信を有効にすることができます。お客様が証跡を設定しない場合でも、 イベント履歴で CloudTrail コンソールで最新のイベントを表示できま

す。 によって収集された情報を使用して CloudTrail、お客様は QLDB に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

Amazon QuickSight

Amazon QuickSight は、お客様が視覚化の構築、アドホック分析の実行、データからのビジネス上の洞察の迅速な取得に使用できるビジネス分析サービスです。Amazon は AWS データソース QuickSight を検出し、組織は数十万のユーザーまでスケールでき、堅牢なインメモリエンジン (SPICE) を使用して応答性の高いパフォーマンスを提供します。

お客様は、SPICE に保存されているデータの暗号化をサポートしているため、PHI を含むデータを操作 QuickSight できるのは Amazon Enterprise Edition のみです。データ暗号化は、 AWS マネージドキーを使用して実行されます。

Amazon RDS for MariaDB

Amazon RDS for MariaDB では、 で管理するキーを使用して MariaDB データベースを暗号化できます AWS KMS。Amazon RDS 暗号化で実行されているデータベースインスタンスでは、基盤となるストレージに保存されているデータは、自動バックアップ、リードレプリカ、スナップショットと同様に、このホワイトペーパーの公開時に有効なガイダンスに従って暗号化されます。

ガイダンスは更新される可能性があるため、お客様は引き続き Amazon RDS for MariaDB 暗号化がコンプライアンスおよび規制要件を満たしているかどうかを評価し、決定する必要があります。Amazon RDS を使用した保管時の暗号化の詳細については、「Amazon RDS リソースの暗号化」を参照してください。

PHI を含む RDS for MariaDB への接続には、トランスポート暗号化を使用する必要があります。暗号化された接続を有効にする方法の詳細については、「SSL/TLS を使用した DB インスタンスへの接続の暗号化」を参照してください。

Amazon RDS for MySQL

Amazon RDS for MySQL では、お客様が を通じて管理するキーを使用して MySQL データベースを暗号化できます AWS KMS。Amazon RDS 暗号化で実行されているデータベースインスタンスでは、基盤となるストレージに保存されているデータは、自動バックアップ、リードレプリカ、スナップショットと同様に、このホワイトペーパーの公開時に有効なガイダンスに従って暗号化されます。

ガイダンスは更新される可能性があるため、お客様は Amazon RDS for MySQL 暗号化がコンプライアンスおよび規制要件を満たしているかどうかを引き続き評価および判断する必要があります

す。Amazon RDS を使用した保管時の暗号化の詳細については、「Amazon RDS リソースの暗号化」を参照してください。

PHI を含む RDS for MySQL への接続には、トランスポート暗号化を使用する必要があります。暗号化された接続を有効にする方法の詳細については、「SSL/TLS を使用した DB インスタンスへの接続の暗号化」を参照してください。

「Amazon RDS for Oracle」

お客様は、Amazon RDS for Oracle を使用して保管時の PHI を暗号化するためのいくつかのオプションがあります。お客様は、 を通じて管理するキーを使用して Oracle データベースを暗号化できます AWS KMS。Amazon RDS 暗号化で実行されているデータベースインスタンスでは、基盤となるストレージに保存されているデータは、自動バックアップ、リードレプリカ、スナップショットと同様に、このホワイトペーパーの公開時に有効なガイダンスに従って暗号化されます。

ガイダンスは更新される可能性があるため、お客様は引き続き Amazon RDS for Oracle 暗号化がコンプライアンスおよび規制要件を満たしているかどうかを評価し、決定する必要があります。Amazon RDS を使用した保管時の暗号化の詳細については、「Amazon RDS リソースの暗号化」を参照してください。

お客様は Oracle Transparent Data Encryption (TDE) を使用することもできます。お客様は、 ガイダンスに従って設定を評価する必要があります。Oracle TDE は、Oracle Enterprise Edition で使用できる Oracle Advanced Security オプションの機能です。この機能は、ストレージへの書き込み前に自動的にデータを暗号化し、ストレージからのデータの読み取り時に自動的にデータを復号します。お客様は、 AWS CloudHSM を使用して Amazon RDS Oracle TDE キーを保存することもできます。詳細については、次を参照してください。

- Amazon RDS for Oracle Transparent Data Encryption: Oracle Transparent Data Encryption。
- AWS CloudHSM を使用して Amazon RDS Oracle TDE キーを保存する: Amazon Relational Database Service (Amazon RDS) とは

PHI を含む Amazon RDS for Oracle への接続では、トランスポート暗号化を使用し、 ガイダンスと整合性について設定を評価する必要があります。これは、Oracle Native Network Encryption を使用して実現され、Amazon RDS for Oracle オプショングループで有効になります。詳細については、「Oracle Native Network Encryption」を参照してください。

Amazon RDS for PostgreSQL

Amazon RDS for PostgreSQL では、お客様が を通じて管理するキーを使用して PostgreSQL データベースを暗号化できます AWS KMS。Amazon RDS 暗号化で実行されているデータベースインスタンスでは、基盤となるストレージに保存されているデータは、自動バックアップ、リードレプリカ、スナップショットと同様に、このホワイトペーパーの公開時に有効なガイダンスに従って暗号化されます。

ガイダンスは更新される可能性があるため、お客様は Amazon RDS for PostgreSQL 暗号化がコンプライアンスおよび規制要件を満たしているかどうかを引き続き評価および判断する必要があります。Amazon RDS を使用した保管時の暗号化の詳細については、「Amazon RDS リソースの暗号化」を参照してください。

PHI を含む RDS for PostgreSQL への接続には、トランスポート暗号化を使用する必要があります。暗号化された接続を有効にする方法の詳細については、「SSL/TLS を使用した DB インスタンスへの接続の暗号化」を参照してください。

Amazon RDS for SQL Server

RDS for SQL Server では、次のバージョンとエディションの組み合わせの PHI の保存がサポートされています。

- 2008 R2 - Enterprise Edition のみ
- 2012、2014、2016 - Web、Standard、Enterprise エディション

重要： SQL Server Express エディションはサポートされていないため、PHI の保存には使用しないでください。

PHI を保存するには、以下で説明するように、インスタンスが保管中のデータを暗号化するように設定されていることを確認し、トランスポートの暗号化と監査を有効にする必要があります。

保管時の暗号化

お客様は、 で管理するキーを使用して SQL Server データベースを暗号化できます AWS KMS。Amazon RDS 暗号化で実行されているデータベースインスタンスでは、基盤となるストレージに保存されているデータは、自動バックアップやスナップショットと同様に、このホワイトペーパーの公開時に有効なガイダンスに従って暗号化されます。ガイダンスは更新される可能性があるた

め、お客様は引き続き Amazon RDS for SQL Server の暗号化がコンプライアンスおよび規制要件を満たしているかどうかを評価し、判断する必要があります。Amazon RDS を使用した保管時の暗号化の詳細については、「Amazon RDS リソースの暗号化」を参照してください。

SQL Server Enterprise Edition を使用している場合は、代わりに Server Transparent Data Encryption (TDE) を使用できます。この機能は、ストレージへの書き込み前に自動的にデータを暗号化し、ストレージからのデータの読み取り時に自動的にデータを復号します。RDS for SQL Server 透過的データ暗号化の詳細については、「SQL Server での透過的データ暗号化のサポート」を参照してください。

送信の暗号化

PHI を含む Amazon RDS for SQL Server への接続には、SQL Server 強制 SSL によって提供されるトランスポート暗号化を使用する必要があります。強制 SSL は、Amazon RDS SQL Server のパラメータグループ内から有効になります。RDS for SQL Server 強制 SSL の詳細については、「Microsoft SQL Server DB インスタンスでの SSL の使用」を参照してください。

監査

PHI を含む RDS for SQL Server インスタンスでは、監査が有効になっている必要があります。監査は、Amazon RDS SQL Server のパラメータグループ内から有効になります。RDS for SQL Server 監査の詳細については、「Microsoft SQL Server DB インスタンスのコンプライアンスプログラムサポート」を参照してください。

Amazon Redshift

Amazon Redshift は、保管中のデータを保護するために、クラスターのデータベース暗号化を提供します。お客様がクラスターの暗号化を有効にすると、Amazon Redshift はハードウェアアクセラレーション高度暗号化標準 (AES)-256 対称キーを使用して、バックアップを含むすべてのデータを暗号化します。Amazon Redshift は、暗号化に 4 階層のキーベースのアーキテクチャを使用します。これらのキーは、データ暗号化キー、データベースキー、クラスターキー、および KMS キーで構成されます。

クラスターキーは、Amazon Redshift クラスターのデータベースキーを暗号化します。お客様は、AWS KMS または AWS CloudHSM（ハードウェアセキュリティモジュール) を使用して、クラスターキーを管理できます。Amazon Redshift の保管時の暗号化は、このホワイトペーパーの公開時に有効なガイダンスと一致しています。ガイダンスは更新される可能性があるため、お客様は Amazon Redshift 暗号化がコンプライアンスおよび規制要件を満たしているかどうかを引き続き評価および判

断する必要があります。詳細については、「Amazon Redshift データベースの暗号化」を参照してください。

PHI を含む Amazon Redshift への接続はトランスポート暗号化を使用する必要があり、お客様は ガイダンスとの整合性について設定を評価する必要があります。詳細については、「接続のセキュリティオプションの設定」を参照してください。Amazon Redshift Spectrum を使用すると、Amazon S3 内のエクサバイトのデータに対して Amazon Redshift SQL クエリを実行できます。Redshift Spectrum は Amazon Redshift の機能であるため、HIPAA BAA の対象にもなります。

Amazon Rekognition

Amazon Rekognition を使用すると、イメージ分析とビデオ分析をお客様のアプリケーションに簡単に追加できます。お客様は Amazon Rekognition API にイメージまたはビデオを提供するだけで、サービスはオブジェクト、人物、テキスト、シーン、アクティビティを識別し、不適切なコンテンツを検出できます。Amazon Rekognition は、高精度の顔分析と顔認識も提供します。

Amazon Rekognition は、PHI を含むイメージまたはビデオを操作する資格があります。Amazon Rekognition はマネージドサービスとして動作し、データ処理の設定可能なオプションは表示されません。Amazon Rekognition は、 AWS BAA の条項で許可されている PHI のみを使用、公開、維持します。すべてのデータは、保管中および転送中に Amazon Rekognition で暗号化されます。Amazon Rekognition は AWS CloudTrail を使用してすべての API コールをログに記録します。

Amazon Route 53

Amazon Route 53 は、ドメイン名の登録、インターネットトラフィックの顧客ドメインリソースのルーティング、およびそれらのリソースの正常性の確認をお客様に提供するマネージド DNS サービスです。Amazon Route 53 は HIPAA 対応サービスですが、このようなデータの暗号化はサポートされていないため、Amazon Route 53 内のリソース名またはタグに PHI を保存しないでください。代わりに、Amazon Route 53 を使用して、Amazon EC2 で実行されているウェブサーバーや Amazon S3 などのストレージなどの PHI を送受信するカスタマードメインリソースへのアクセスを提供できます。

Amazon S3 Glacier

Amazon S3 Glacier は、AES 256 ビット対称キーを使用して保管中のデータを自動的に暗号化し、安全なプロトコルを介した顧客データの安全な転送をサポートします。PHI を含む Amazon S3 Glacier への接続には、暗号化トランスポート (HTTPS) を受け入れるエンドポイントを使用する必要

があります。リージョンエンドポイントのリストについては、「 AWS サービスエンドポイント」を参照してください。

アーカイブ名、ボールト名、メタデータに PHI を使用しないでください。このデータは Amazon S3 Glacier サーバー側の暗号化を使用して暗号化されず、クライアント側の暗号化アーキテクチャでは通常暗号化されないためです。

Amazon S3 Transfer Acceleration

Amazon S3 Transfer Acceleration (S3TA) を使用すると、お客様のクライアントと S3 バケットの間で、長距離にわたるファイルの転送を高速、簡単、安全に行えるようになります。Transfer Acceleration は、Amazon のグローバル CloudFrontに分散されたエッジロケーションを利用します。エッジロケーションに到着したデータは、最適化されたネットワークパスで Amazon S3 にルーティングされます。お客様は、 AWS S3TA を使用して転送された PHI を含むすべてのデータが転送中および保管時に暗号化されていることを確認する必要があります。使用可能な暗号化オプションについては、「Amazon S3 のガイダンス」を参照してください。

Amazon SageMaker

Amazon SageMaker はフルマネージド型の機械学習サービスです。Amazon を使用すると SageMaker、データサイエンティストとデベロッパーは、機械学習モデルをすばやく簡単に構築してトレーニングし、本番環境に対応したホスト環境に直接デプロイできます。統合された Jupyter オーサリングノートブックインスタンスを提供し、データソースに簡単にアクセスして探索と分析を行うことができます。Amazon は、分散環境の非常に大きなデータに対して効率的に実行するように最適化された一般的な機械学習アルゴリズム SageMaker も提供します。

bring-your-own-algorithms および フレームワークのネイティブサポートにより、Amazon SageMaker はお客様の特定のワークフローに合わせて調整できる柔軟な分散トレーニングオプションを提供します。Amazon SageMaker は、PHI を含むデータを操作できます。転送中のデータの暗号化は SSL/TLS によって提供され、Amazon SageMaker のフロントエンドインターフェイス (ノートブック) と通信するときと、Amazon が他の AWS サービスと SageMaker やり取りするとき (Amazon S3 からのデータの取得など) に使用されます。

PHI を保管時に暗号化するという要件を満たすために、Amazon でモデルを実行しているインスタンスに保存されているデータの暗号化 SageMaker は、エンドポイント AWS Key Management Service （ DescribeEndpointConfig：KmsKeyID) を設定するときに (KMS) を使用して有効になります。モデルトレーニング結果 (アーティファクト) の暗号化は を使用して有効 AWS KMS になり、

説明の KmsKey OutputDataConfig ID を使用してキーを指定する必要があります。KMS キー ID が指定されていない場合は、ロールのアカウントのデフォルトの Amazon S3 KMS キーが使用されます。Amazon SageMaker は AWS CloudTrail を使用してすべての API コールをログに記録します。

Amazon Simple Notification Service (Amazon SNS)

保護対象保健情報 (PHI) で Amazon Simple Notification Service (SNS) を使用するには、次のキー暗号化要件を理解する必要があります。お客様は、各 AWS リージョンで SNS が提供する HTTPS API エンドポイントを使用する必要があります。HTTPS エンドポイントは暗号化された接続を活用し、に送信されるデータのプライバシーと整合性を保護します AWS。すべての HTTPS API エンドポイントのリストについては、「 AWS サービスエンドポイント」を参照してください。

さらに、Amazon SNS は、お客様のアカウントで Amazon SNS によって、または Amazon SNSに代わって行われた API コールをキャプチャ AWS し CloudTrail、指定した Amazon S3 バケットにログファイルを配信するサービスである を使用します。 は、Amazon SNS コンソールまたは Amazon SNS API から実行された API コールを CloudTrail キャプチャします。によって収集された情報を使用して CloudTrail、お客様は Amazon SNS に対して行われたリクエスト、リクエスト元のソース IP アドレス、リクエスト者、リクエスト日時を判断できます。SNS オペレーションのログ記録の詳細については、「 を使用した Amazon SNS API コールのログ記録 CloudTrail」を参照してください。

Amazon Simple Email Service (Amazon SES)

Amazon Simple Email Service (Amazon SES) は、柔軟で拡張性の高い E メール送受信サービスです。S/MIME プロトコルと PGP プロトコルの両方をサポートしてメッセージを完全に end-to-end 暗号化し、Amazon SES とのすべての通信は SSL (TLS 1.2) を使用して保護されます。お客様は、Amazon S3 バケットに保存する前にメッセージを受信および暗号化するように Amazon SES Amazon S3を設定することで、保管時に暗号化されたメッセージを保存できます。詳細については、「Amazon Simple Email Service (Amazon SES) が AWS KMSを使用してストレージのメッセージの暗号化に関する詳細情報を確認する方法」を参照してください。メッセージは、HTTPS エンドポイントまたは暗号化された SMTP 接続を介して Amazon SES に転送される際に保護されます。

Amazon SES から受信者に送信されるメッセージの場合、Amazon SES はまず受信メールサーバーへの安全な接続を試みますが、安全な接続を確立できない場合は、暗号化されずにメッセージを送信します。受信者への配信に暗号化を要求するには、Amazon SES で設定セットを作成し、を使用して TlsPolicy プロパティを Require AWS CLI に設定する必要があります。詳細については、「Amazon SES とセキュリティプロトコル」を参照してください。Amazon SES は と統合 AWS CloudTrail して、すべての API コールをモニタリングします。によって収集された情報を使

用して AWS CloudTrail、お客様は、リクエストが Amazon SES に対して送信されたこと、リクエストの IP アドレス、リクエスト者、リクエストが行われた日時などの詳細を確認できます。詳細については、「 を使用した Amazon SES API コールのログ記録 AWS CloudTrail」を参照してください。Amazon SES には、送信、拒否、バウンス率、配信、開封、クリックなどの送信アクティビティをモニタリングする方法も用意されています。詳細については、「Amazon SES 送信アクティビティのモニタリング」を参照してください。

Amazon Simple Queue Service (Amazon SQS)

PHI で Amazon SQS を使用するには、お客様は以下のキー暗号化要件を理解する必要があります。

- クエリリクエストを介した Amazon SQS キューとの通信は、HTTPS で暗号化する必要があります。SQS リクエストの作成の詳細については、「クエリ API リクエストの作成」を参照してください。
- Amazon SQSは、保管中のデータを保護するために AWS KMS 、 と統合されたサーバー側の暗号化をサポートしています。サーバー側の暗号化を追加することで、暗号化されたキューを使用するセキュリティを強化して、お客様は機密データを送受信できます。Amazon SQS サーバー側の暗号化では、256 ビットの Advanced Encryption Standard (AES-256 GCM アルゴリズム) を使用して各メッセージの本文を暗号化します。との統合 AWS KMS により、お客様は Amazon SQSメッセージを保護するキーと、他の AWS リソースを保護するキーを一元管理できます。 は、規制やコンプライアンスのニーズを満たす AWS CloudTrail ために、暗号化キーを使用するたびに AWS KMS ログに記録します。詳細については、Amazon SQS の SSE の可用性についてリージョンをチェックするには、「保管時の暗号化」を参照してください。
- サーバー側の暗号化を使用しない場合、メッセージペイロード自体を暗号化してから SQS に送信する必要があります。メッセージペイロードを暗号化する方法の 1 つは、Amazon SQS 拡張クライアントと Amazon S3 暗号化クライアントを使用することです。クライアント側の暗号化の使用の詳細については、「Amazon SQS 拡張クライアントと Amazon S3 暗号化クライアントを使用したメッセージペイロードの暗号化」を参照してください。

Amazon SQS は CloudTrail、お客様のアカウントで Amazon SQS によって、または Amazon SQS に代わって行われた API コールをログに記録し、Amazon SQS コンソールまたは Amazon SQS API から行われた指定された Amazon S3 bucket. CloudTrail captures API コールにログファイルを AWS 配信するサービスAmazon SQSを使用します。お客様は、 によって収集された情報を使用して CloudTrail 、Amazon SQS に対して行われたリクエスト、リクエスト元のソース IP アドレス、リクエスト者、リクエスト日時などを判断できます。SQS オペレーションのログ記録の詳細については、「 を使用した Amazon SQS API コールのログ記録 AWS CloudTrail」を参照してください。

Amazon Simple Storage Service (Amazon S3)

Amazon S3 を使用する際の保管中のデータの暗号化には、サーバー側の暗号化とクライアント側の暗号化の両方、およびキーの管理方法など、複数のオプションがあります。詳細については、「暗号化 を使用したデータの保護」を参照してください。

PHI を含む Amazon S3 への接続には、暗号化トランスポート (HTTPS) を受け入れるエンドポイントを使用する必要があります。リージョンエンドポイントのリストについては、「 AWS サービスエンドポイント」を参照してください。

バケット名、オブジェクト名、メタデータに PHI を使用しないでください。このデータは S3 サーバー側の暗号化を使用して暗号化されず、クライアント側の暗号化アーキテクチャでは通常暗号化されません。

Amazon Simple Workflow Service

Amazon Simple Workflow Service (Amazon SWF) は、デベロッパーが並列またはシーケンシャルステップを持つバックグラウンドジョブを構築、実行、スケーリングするのに役立ちます。Amazon SWF は、 クラウドのフルマネージド状態トラッカーおよびタスクコーディネーターと考えることができます。

Amazon Simple Workflow Service はワークフローをオーケストレーションするために使用され、データを保存または送信することはできません。PHI は、Amazon SWF のメタデータやタスクの説明には配置しないでください。Amazon SWF は を使用してすべての API コール AWS CloudTrail をログに記録します。

Amazon Textract

Amazon Textract は機械学習テクノロジーを使用して、単純な光文字認識 (OCR) を超えるスキャンされたドキュメントからテキストとデータを自動的に抽出し、フォームとテーブルからデータを識別、理解、抽出します。例えば、Amazon Textract を使用すると、人間の介入なしで自動的にデータを抽出し、保護医療情報 (PHI) を使用してフォームを処理して医療請求を処理できます。

Amazon Textract は、ドキュメントアーカイブのコンプライアンスを維持するためにも使用できます。例えば、お客様は Amazon Textract を使用して保険請求または医療医療保険からデータを抽出し、機密のドキュメントを秘匿化できるように、それらのドキュメント内のキーと値のペアを自動的に認識できます。

Amazon Textract は、入力ドキュメントのサーバー側の暗号化 (SSE-S3 および SSE-KMS) と、サービスとエージェント間で転送されるデータの TLS 暗号化をサポートしています。お客様は、Amazon CloudWatch を使用してリソース使用状況メトリクスを追跡し AWS CloudTrail 、Amazon Textract への API コールをキャプチャできます。

Amazon Transcribe

Amazon Transcribe は、高度な機械学習テクノロジーを使用して音声ファイルの音声を認識し、テキストに文字起こしします。例えば、Amazon Transcribe を使用して、米国英語とメキシコスペイン語の音声をテキストに変換し、音声ファイルの内容を組み込んだアプリケーションを作成できます。Amazon Transcribe は、PHI を含むデータで使用できます。Amazon Transcribe はデータを保持または保存せず、API へのすべての呼び出しは SSL/TLS で暗号化されます。Amazon Transcribe は CloudTrail を使用してすべての API コールをログに記録します。

Amazon Translate

Amazon Translate では、高度な機械学習テクノロジーを使用して、高品質の翻訳をオンデマンドで提供します。お客様は Amazon Translate を使用して、非構造化テキストドキュメントを翻訳したり、複数の言語で機能するアプリケーションを構築したりできます。PHI を含むドキュメントは、Amazon Translate で処理できます。PHI を含むドキュメントを変換する場合、追加の設定は必要ありません。転送中のデータの暗号化は SSL/TLS によって提供され、Amazon Translate では保管中のデータは残りません。Amazon Translate では CloudTrail 、 を使用してすべての API コールをログに記録します。

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud (Amazon VPC) は、HIPAA 規制のワークロード向けに設計するために適切に調整された一連のネットワークセキュリティ機能を提供します。ステートレスネットワークアクセスコントロールリストやステートフルセキュリティグループへのインスタンスの動的な再割り当てなどの機能により、不正なネットワークアクセスからインスタンスを柔軟に保護できます。

Amazon VPC では、お客様は独自のネットワークアドレス空間を に拡張できるだけでなく AWS、データセンターを に接続するさまざまな方法も用意されています AWS。VPC Flow Logs は、PHI を処理、送信、または保存するインスタンスへの承諾および拒否された接続の監査証跡を提供します。

AWS Transit Gateway はネットワークハブとして機能し、Amazon VPCs とオンプレミスネットワーク間の接続を簡素化します。 は、他の Transit Gateway へのリージョン間ピアリング機能 AWS

Transit Gateway も提供し、 AWS バックボーンを使用してグローバルネットワークを確立します。Amazon VPC の詳細については、「Amazon Virtual Private Cloud」を参照してください。

Amazon WorkDocs

Amazon WorkDocs は、ユーザーの生産性を向上させる強力な管理制御とフィードバック機能を備えた、フルマネージドで安全なエンタープライズファイルストレージおよび共有サービスです。Amazon WorkDocs ファイルは、お客様が () で AWS Key Management Service 管理するキーを使用して保管時に暗号化されますAWS KMS。転送中のすべてのデータは、SSL/TLS. AWS web およびモバイルアプリケーション、デスクトップ同期クライアントを使用して暗号化され、SSL/TLS Amazon WorkDocs を使用してファイルを に直接送信します。

Amazon WorkDocs マネジメントコンソールを使用すると、 WorkDocs 管理者は監査ログを表示してファイルとユーザーのアクティビティを時間単位で追跡し、ユーザーが組織外の他のユーザーとファイルを共有できるようにするかどうかを選択できます。 Amazon WorkDocs は CloudTrail (Amazon WorkDocs お客様のアカウントに代わって によって行われた API コールをキャプチャするサービス AWS) とも統合され、お客様が指定した Amazon S3 バケットに CloudTrail ログファイルを配信します。

RADIUS サーバーを使用した多要素認証 (MFA) が利用でき、認証プロセス中にお客様にセキュリティレイヤーを追加できます。ユーザーは、ユーザー名とパスワードを入力し、その後にハードウェアまたはソフトウェアトークンによって提供される OTP (ワンタイムパスコード) を入力してログインします。

詳細については、以下を参照してください。

- Amazon WorkDocs 機能
- を使用した Amazon WorkDocs API コールのログ記録 AWS CloudTrail

お客様は PHI をファイル名またはディレクトリ名に保存しないでください。

Amazon WorkSpaces

Amazon WorkSpaces は、 で実行されるフルマネージド型のセキュアな D esktop-as-a- サービス (DaaS) ソリューションです AWS。Amazon を使用すると WorkSpaces、仮想クラウドベースの Microsoft Windows デスクトップをユーザー用に簡単にプロビジョニングし、サポートされているデバイスから必要なドキュメント、アプリケーション、リソースにいつでもアクセスできます。

Amazon は Amazon Elastic Block Store ボリュームにデータ WorkSpaces を保存します。お客様は、お客様が WorkSpaces を通じて管理するキーを使用して、お客様のストレージボリュームを暗号化できます AWS Key Management Service。で暗号化を有効にすると WorkSpace、基盤となるストレージに保管されているデータとディスクストレージの自動バックアップ (EBS スナップショット) の両方が ガイダンスに従って暗号化されます。 WorkSpace クライアントから への通信 WorkSpace は、SSL/TLS を使用して保護されます。Amazon を使用した保管時の暗号化の詳細については WorkSpaces、「暗号化された WorkSpaces」を参照してください。

AWS App Mesh

AWS App Mesh は、Amazon ECS、Amazon EKS、Amazon EC2 サービスなど、複数のタイプのコンピューティングインフラストラクチャ間でサービスが簡単に相互通信できるように、アプリケーションレベルのネットワークを提供するサービスメッシュです。App Mesh は Envoy プロキシを設定し、設定したモニタリングセットにオブザーバビリティデータを収集して送信します。これにより、 end-to-end 可視性が得られます。ルーティングとトラフィックポリシーに基づいてトラフィックをルーティングし、アプリケーションの高可用性を確保できます。アプリケーション間のトラフィックは、TLS を使用するように設定できます。App Mesh は、 AWS SDK または Kubernetes 用の App Mesh コントローラーを使用して使用できます。 AWS App Mesh は HIPAA 対応サービスですが、PHI は 内のどのリソース名/属性にも保存しないでください。 AWS App Mesh このようなデータの保護はサポートされていません。代わりに、 を使用して、PHI を送信または保存するカスタマードメインリソースをモニタリング、制御、保護 AWS App Mesh できます。

AWS アプリケーション移行サービス

AWS Application Migration Service (AWS MGN) を使用すると、サーバーとアプリケーションを に変更することなく AWS、最小限のダウンタイムですばやく移行できます。 AWS MGN は、 へのリフトアンドシフト移行に推奨される主要な移行サービスです AWS。

AWS MGN はブロックレベルのデータレプリケーションを使用して、ソースディスクをお客様のアカウントの EBS ボリュームに直接コピーします。データは AWS MGN が管理するクラウド環境を介して送信されることはありません。レプリケートされたデータは、デフォルトで転送中に暗号化されます。お客様の EBS ボリューム内のデータは、デフォルトでお客様の独自のキーを使用して暗号化されます。

AWS Auto Scaling

AWS Auto Scaling を使用すると、数分でお客様のアプリケーションの一部である AWS リソースのオートスケーリングを設定できます。お客様は、 AWS Auto Scaling グループ内の Amazon DynamoDB、Amazon ECS、Amazon RDS Aurora レプリカ、Amazon EC2 インスタンスなど、PHI に関連する多くのサービスに Auto Scaling を使用できます。

AWS Auto Scaling は、お客様のコンテンツを直接処理、保存、または送信しないオーケストレーションサービスです。そのため、お客様はこのサービスを暗号化されたコンテンツで使用できます。AWS Auto Scaling でのデータ保護には AWS 責任共有モデルが適用されます。 AWS ネットワークセキュリティ手順 AWS についてはお客様の責任となりますが、このインフラストラクチャでホストされているお客様のコンテンツに対する制御はお客様の責任となります。このコンテンツには、お客様が使用する AWS サービスのセキュリティ設定および管理タスクが含まれます。データ保護の目的で、お客様は AWS アカウントの認証情報を保護し、個々のユーザーアカウントを AWS Identity and Access Management (IAM) で設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な許可のみを各ユーザーに付与できます。

顧客は、顧客のアカウント番号などの機密性の高い識別情報を、名前フィールドなどの自由形式のフィールドに入れないことを強くお勧めします。これは、お客様が 、API AWS Management Console、 AWS CLIまたは AWS SDK を使用して AWS Auto Scaling または他の AWS サービスを使用する場合も同様です。 SDKs

顧客が AWS Auto Scaling や他のサービスに入力したデータはすべて、診断ログに取り込まれる可能性があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証するための認証情報を URL に含めないでください。 AWS では、次の方法でデータを保護することもお勧めします。

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 以降を推奨
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。
- AWS 暗号化ソリューションを、 サービス内のすべての AWS デフォルトのセキュリティコントロールとともに使用します。
- Amazon Macie などのアドバンストマネージドセキュリティサービスを使用します。これは、Amazon S3 に保存されている個人データの検出と保護を支援します。

AWS Backup

AWS Backup は、一元化されたフルマネージド型のポリシーベースのサービスを提供し、顧客データを保護し、ビジネス継続性の目的で AWS サービス全体のコンプライアンスを確保します。を使用すると AWS Backup、お客様はデータ保護 (バックアップ) ポリシーを一元的に設定し、Amazon EBS ボリューム、Amazon Relational Database Service (Amazon RDS) データベース (Aurora クラスターを含む) 、Amazon DynamoDB テーブル、Amazon Elastic File System (Amazon EFS)、Amazon FSx ファイルシステム、Amazon EC2 インスタンス、 AWS Storage Gateway ボリュームなど、お客様の AWS リソース全体のバックアップアクティビティをモニタリングできます。

AWS Backup は、転送中および保管中の顧客データを暗号化します。既存のスナップショット機能を持つサービスからのバックアップは、ソースサービスのスナップショット暗号化方法を使用して暗号化されます。例えば、EBS スナップショットは、スナップショットの作成元のボリュームの暗号化キーを使用して暗号化されます。

Amazon EFS など AWS Backup、 上に構築されたバックアップ機能を導入する新しい AWS サービスからのバックアップは、転送中および保管時にソースサービスと独立して暗号化されるため、お客様のバックアップは追加の保護レイヤーになります。暗号化はバックアップボールトレベルで設定されます。デフォルトのボールトは暗号化されます。お客様が新しいボールトを作成するときは、暗号化キーを選択する必要があります。

AWS Batch

AWS Batch を使用すると、開発者、サイエンティスト、エンジニアは数十万のバッチコンピューティングジョブを で簡単かつ効率的に実行できます AWS。 は、送信されたバッチジョブのボリュームと特定のリソース要件に基づいて、最適な量とタイプの AWS コンピューティングリソース (CPU やメモリ最適化インスタンスなど) を AWS Batch 動的にプロビジョニングします。 AWS Batch は、コンピューティングサービスおよび機能の全範囲にわたってバッチコンピューティングワークロードを計画、スケジュール、実行します。

Amazon ECS のガイダンスと同様に、PHI をジョブ定義、ジョブキュー、または のタグに直接配置しないでください AWS Batch。代わりに、 でスケジュールおよび実行されるジョブは、暗号化された PHI で動作する AWS Batch 可能性があります。ジョブのステージによって に返される情報にも AWS Batch PHI を含めないでください。によって実行されるジョブが PHI を送受信 AWS Batch する必要がある場合は必ず、その接続を HTTPS または SSL/TLS を使用して暗号化する必要があります。

AWS Certificate Manager

AWS Certificate Manager は、 のサービスおよび内部に接続されたリソースで使用するパブリックおよびプライベートの SSL/TLS 証明書を簡単にプロビジョニング、管理、デプロイできる AWS サービスです。 AWS Certificate Manager は、すべての API コールをログ CloudTrail に記録するために使用されます。

ユーザーが の AWS 外部で とやり取りする場合は、プログラムによるアクセスが必要です AWS Management Console。プログラムによるアクセスを許可する方法は、 にアクセスしているユーザーのタイプによって異なります AWS。

ユーザーにプログラマチックアクセス権を付与するには、以下のいずれかのオプションを選択します。

プログラマチックアクセス権を必要とするユーザー	目的	方法
ワークフォースアイデンティティ (IAM Identity Center で管理されているユーザー)	一時的な認証情報を使用して、 AWS CLI、 AWS SDKs、または AWS APIs。	使用するインターフェイス用の手引きに従ってください。 • については AWS CLI、「 ユーザーガイド」の「 を使用する AWS CLI ための の設定 AWS IAM Identity CenterAWS Command Line Interface 」を参照してください。 • AWS SDKs「 SDK とツールのリファレンスガイド」の「IAM Identity Center 認証」を参照してください。AWS APIs AWS SDKs
IAM	一時的な認証情報を使用して、 AWS CLI、 AWS SDKs、または AWS APIs。	「IAM ユーザーガイド」の「 AWS リソースでの一時的な認証情報の使用」の手順に従います。

プログラマチックアクセス権を必要とするユーザー	目的	方法
IAM	(非推奨) 長期認証情報を使用して、AWS CLI、 AWS SDKsまたはAWS APIs。	使用するインターフェイス用の手引きに従ってください。 • については AWS CLI、「 AWS Command Line Interface ユーザーガイド」の「IAM ユーザー認証情報を使用した認証」を参照してください。 • AWS SDKs「 SDK とツールのリファレンスガイド」の「長期認証情報を使用した認証」を参照してください。 AWS SDKs • AWS APIs「IAM ユーザーガイド」の「IAM ユーザーのアクセスキーの管理」を参照してください。

AWS Cloud Map

AWS Cloud Map はクラウドリソース検出サービスです。AWS Cloud Map を使用すると、Amazon ECS タスク、Amazon EC2 インスタンス、Amazon S3 バケット、Amazon DynamoDB テーブル、Amazon SQS キュー、その他のクラウドリソースなどのアプリケーションリソースのカスタム名を定義できます。その後、お客様はこれらのカスタム名を使用して、AWS SDK と認証された API クエリを使用して、アプリケーションからクラウドリソースの場所とメタデータを検出できます。AWS Cloud Map は HIPAA 対応サービスですが、このようなデータの保護はサポートされていないため、PHI は AWS Cloud Map 内のリソース名/属性に保存しないでください。代わりに、AWS Cloud Map を使用して、PHI を送信または保存するカスタマードメインリソースを検出できます。

AWS CloudFormation

AWS CloudFormation では、お客様は AWS インフラストラクチャのデプロイを予測どおりに繰り返し作成およびプロビジョニングできます。これにより、お客様は Amazon EC2、Amazon Elastic Block Store、Amazon SNS、Elastic Load Balancing、Auto Scaling などの AWS 製品を活用して、基盤となる AWS インフラストラクチャの作成と設定を行うことなく、信頼性が高く、スケーラブルで、費用対効果の高いアプリケーションをクラウドで構築できます。 では、テンプレートファイルを使用して、リソースのコレクションを 1 つのユニット (スタック) として作成および削除 AWS CloudFormation できます。

AWS CloudFormation はそれ自体で PHI を保存、送信、または処理しません。代わりに、PHI を保存、送信、または処理する他の AWS のサービスを使用するアーキテクチャを構築およびデプロイするために使用されます。PHI で使用するのは HIPAA 対応サービスのみです。これらのサービスでの PHI の使用に関するガイダンスについては、このホワイトペーパーのこれらのサービスのエントリを参照してください。 AWS CloudFormation は を使用してすべての API コール AWS CloudTrail を ログに記録します。

AWS CloudHSM

AWS CloudHSM はクラウドベースのハードウェアセキュリティモジュール (HSM) で、お客様は AWS クラウドで独自の暗号化キーを簡単に生成して使用できます。CloudHSM では、FIPS 140-2 レベル 3 検証済み HSMsを使用して独自の暗号化キーを管理できます。CloudHSM は、PKCS#11、Java Cryptography Extensions (JCE)、Microsoft CryptoNG (CNG) ライブラリなどのオープンスタンダード APIs を使用して、アプリケーションを柔軟に統合できます。

CloudHSM も標準に準拠しており、顧客はすべてのキーを他のほとんどの商用利用可能な HSMsにエクスポートできます。ハードウェアアプライアンスのキー管理サービス AWS CloudHSM と同様に、PHI を保存または送信することはできません。お客様は PHI をタグ (メタデータ) に保存しないでください。特別なガイダンスは必要ありません。

AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。 CloudTrailを使用すると、お客様は AWS インフラストラクチャ全体のアクションに関連するアカウントアクティビティをログに記録し、継続的にモニタリングし AWS Management Console、保持できます。 は、、AWS SDKs、コマンドラインツール、その他の AWS のサービスを通じて実行されたアクションなど、AWS アカウントアクティビティのイベント履歴

CloudTrail を提供します。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングが簡素化されます。

AWS CloudTrail は、すべての AWS アカウントでの使用が有効になっており、AWS BAA の要求に応じて監査ログ記録に使用できます。特定の証跡は、 CloudTrail コンソールまたは AWS コマンドラインインターフェイスを使用して作成する必要があります。 は、転送中および保管時のすべてのトラフィックを、暗号化された証跡の作成時に CloudTrail 暗号化します。PHI を記録する可能性のある が存在する場合は、暗号化された証跡を作成する必要があります。

デフォルトでは、暗号化された証跡は、Amazon S3 によるサーバー側の暗号化 (SSE-S3) マネージドキーを使用して Amazon S3 にエントリを保存します。キーに対する追加の管理が必要な場合は、 AWS KMSマネージドキー (SSE-KMS) を使用して設定することもできます。AWS ログエントリ CloudTrail の最終送信先と同様に、PHI を処理するアーキテクチャの重要なコンポーネントであるログファイルの CloudTrail 整合性検証を有効にし、関連する CloudTrail ダイジェストファイルを定期的に確認する必要があります。有効にすると、ログファイルが変更されていないという肯定的なアサーションを確立できます。

AWS CodeBuild

AWS CodeBuild は、cloud. AWS CodeBuild compiles ソースコードの完全マネージド型のビルドサービスであり、ユニットテストを実行して、すぐにデプロイできるアーティファクトを生成します。 キー AWS CodeBuild を使用して AWS KMS ビルド出力アーティファクトを暗号化します。すべての API コールをログ AWS CodeBuild AWS CloudTrail に記録するには、PHI、シークレット/パスワード、証明書などを含むアーティファクトを構築する前に、KMS キーを作成して設定する必要があります。

AWS CodeDeploy

AWS CodeDeploy は、Amazon EC2、 AWS Fargate AWS Lambda、オンプレミスサーバーなどのさまざまなコンピューティングサービスへのソフトウェアデプロイを自動化するフルマネージドデプロイサービスです。お客様は AWS CodeDeploy を使用して、コンテナ化されたワークロードの新機能を迅速にリリースし、アプリケーションの更新の複雑さを処理します。

AWS CodeDeploy は、デプロイアーティファクトのサーバー側の暗号化 (SSE-S3) と、サービスとエージェント間の転送中のデータの TLS 暗号化をサポートします。お客様は Amazon CloudWatch Events を使用してデプロイを追跡し、 への API コール AWS CloudTrail をキャプチャできます AWS CodeDeploy。

AWS CodeCommit

AWS CodeCommit は、プライベート Git リポジトリをホストする、安全で拡張性の高いマネージド型のソース管理サービスです。 AWS CodeCommit は、お客様が独自のソース管理システムを管理したり、インフラストラクチャのスケーリングを心配したりする必要性を排除します。

AWS CodeCommit は、転送中および保管中のすべてのトラフィックと保存された情報を暗号化します。デフォルトでは、リポジトリが 内に作成されると AWS CodeCommit、AWS マネージドキーはで作成 AWS KMS され、そのリポジトリによってのみ使用され、保管時に保存されるすべてのデータを暗号化 AWS CodeCommit AWS CloudTrail してすべての API コールを記録します。

AWS CodePipeline

AWS CodePipeline は、フルマネージド型の継続的デリバリーサービスであり、お客様のリリースパイプラインを自動化して、アプリケーションとインフラストラクチャを迅速かつ確実に更新できます。お客様は AWS CodePipeline 、 を使用して、臨床医が臨床トライアルデータ、ラボ結果、分子データを自動的に処理できるようにします。これは、お客様が使用するワークフローパイプラインの例にすぎません。

AWS CodePipeline は、コードアーティファクトのサーバー側の暗号化 (SSE-S3 および SSE-KMS) と、サービスとエージェント間で転送されるデータの TLS 暗号化をサポートします。お客様は Amazon CloudWatch Events を使用して、パイプラインの変更を追跡し AWS CloudTrail 、 への API コールをキャプチャできます AWS CodePipeline。

AWS Config

AWS Config では、設定内容、相互の関連、時間の経過とともに設定と関係がどのように変化したかなど、お客様の AWS アカウントに関連付けられたリソースの詳細が提供されます。

AWS Config は、それ自体を PHI の保存または送信に使用することはできません。

代わりに、PHI を処理するアーキテクチャなど、他の AWS のサービスで構築されたアーキテクチャをモニタリングおよび評価して、意図した設計目標に準拠しているかどうかを判断できます。PHI を処理するアーキテクチャは、すべての結果をログに記録する AWS CloudTrail ために HIPAA 対応 Services. AWS Config uses でのみ構築する必要があります。

AWS Data Exchange

AWS Data Exchange を使用すると、クラウド内のサードパーティデータを簡単に検索、サブスクライブ、使用できます。データ製品をサブスクライブすると、お客様は AWS Data Exchange API を使用してデータを Amazon S3 に直接ロードし、さまざまな AWS 分析および機械学習サービスを使用して分析できます。データプロバイダーの場合、AWS Data Exchange を使用すると、データストレージ、配信、請求、および利用のためのインフラストラクチャを構築して維持する必要がなくなるため、クラウドに移行している何百万もの AWS のお客様に簡単にアクセスできます。

AWS Data Exchange は、保管中のサービスに保存されているすべてのデータ製品を常に暗号化します。追加の設定は必要ありません。この暗号化は、サービスマネージド KMS キーを介して自動的に行われます。AWS Data Exchange は、転送中の暗号化に Transport Layer Security (TLS) とクライアント側の暗号化を使用します。AWS Data Exchange との通信は常に HTTPS 経由で行われるため、お客様のデータは転送中に常に暗号化されます。この暗号化は、お客様が AWS Data Exchange を使用する場合にデフォルトで設定されます。詳細については、「AWS Data Exchange でのデータ保護」を参照してください。

AWS Data Exchange は と統合されています AWS CloudTrail。 は、AWS Data Exchange コンソールからの呼び出しや AWS Data Exchange APIs オペレーションへのコード呼び出しを含む、AWS Data Exchange API へのすべての呼び出しをイベントとして AWS CloudTrail キャプチャします。お客様が実行できるアクションの中には、コンソール専用のアクションもあります。AWS SDK または AWS CLI に対応する API はありません。これらは、製品の公開やサブスクライブなど、 AWS Marketplace 機能に依存するアクションです。AWS Data Exchange は、これらのコンソール専用アクションのサブセットの CloudTrail ログを提供します。詳細については、「 を使用した AWS Data Exchange API コールのログ記録 AWS CloudTrail」を参照してください。

AWS Data Exchange を使用するすべてのリストは、特定のカテゴリのデータを制限する AWS Data Exchange の AWS Marketplace プロバイダー向け公開ガイドラインと AWS Data Exchange FAQsに従う必要があります。詳細については、「AWS Data Exchange に関するFAQs」を参照してください。

AWS Database Migration Service

AWS Database Migration Service (AWS DMS) は、顧客がデータベースを簡単かつ安全に AWS に移行するのに役立ちます。お客様は、Oracle、MySQL、PostgreSQL など、広く使用されている商用データベースやオープンソースデータベースとの間でデータを移行できます。このサービスでは、Oracle から Oracle など、同機種間の移行をサポートしているほか、Oracle から

PostgreSQL、MySQL から Oracle など、異なるデータベースプラットフォーム間の異機種の移行もサポートしています。

オンプレミスで実行され、AWS DMS を使用してクラウドに移行されるデータベースには、PHI データを含めることができます。AWS DMS は、転送中、および AWS 上のターゲットデータベースへの最終移行のためにデータをステージング中にデータを暗号化します。AWS DMS は、レプリケーションインスタンスで使用されるストレージとエンドポイント接続情報を暗号化します。レプリケーション インスタンスで使用されるストレージを暗号化するために、AWS DMS は AWS アカウントに固有の AWS KMS キーを使用します。移行完了後もデータが暗号化されたままであることを確認するには、適切なターゲットデータベースのガイダンスを参照してください。AWS DMS は を使用してすべての API コール CloudTrail をログに記録します。

AWS DataSync

AWS DataSync は、オンプレミスストレージと AWS 間のデータの移動を簡素化、自動化、高速化するオンライン転送サービスです。お客様は AWS を使用してデータソースを Amazon S3 または Amazon EFS DataSync に接続できます。お客様は、Amazon S3 と Amazon EFS が ガイダンスと一致する方法で設定されていることを確認する必要があります。デフォルトでは、顧客データは TLS 1.2 を使用して転送中に暗号化されます。暗号化と AWS の詳細については DataSync、「AWS DataSync の機能」を参照してください。お客様は を使用して DataSync アクティビティをモニタリングできます AWS CloudTrail。を使用したログ記録の詳細については CloudTrail、「 を使用した AWS DataSync API コールのログ記録 AWS CloudTrail」を参照してください。

AWS Directory Service

Microsoft AD 用の AWS Directory Service

AWS Directory Service for Microsoft Active Directory (Enterprise Edition) は、AWS Microsoft AD とも呼ばれ、ディレクトリ対応のワークロードと AWS リソースで AWS クラウドのマネージド Active Directory を使用できます。AWS Microsoft AD は、AWS が管理する暗号化キーを使用して、暗号化された Amazon Elastic Block Store ボリュームにディレクトリコンテンツ (PHI を含むコンテンツを含む) を保存します。詳細については、「Amazon EBS Encryption」を参照してください。

Active Directory クライアントとの間で送受信されるデータは、お客様の Amazon Virtual Private Cloud (VPC) ネットワーク経由で Lightweight Directory Access Protocol (LDAP) を通過するときに暗号化されます。Active Directory クライアントがオンプレミスネットワークに存在する場合、トラフィックは仮想プライベートネットワークリンクまたは AWS Direct Connect リンクを介してお客様の VPC に移動します。

Amazon Cloud Directory

Amazon Cloud Directory を使用すると、柔軟なクラウドネイティブディレクトリを構築して、データの階層を複数のディメンションに沿って整理できます。お客様は、組織図、コースカタログ、デバイスレジストリなど、さまざまなユースケースのディレクトリを作成することもできます。例えば、お客様は、レポート構造、場所、コストセンターの個別の階層間を移動できる組織図を作成できます。Amazon Cloud Directory は、 AWS Key Management Service () によって管理される 256 ビット暗号化キーを使用して、保管中および転送中のデータを自動的に暗号化しますAWS KMS。

AWS Elastic Beanstalk

を使用すると AWS Elastic Beanstalk、お客様はアプリケーションを実行するインフラストラクチャについて知ることなく、AWS クラウドでアプリケーションを迅速にデプロイおよび管理できます。お客様はコードをアップロードするだけで、容量のプロビジョニング、負荷分散、自動スケーリングからアプリケーションの状態モニタリングまで、デプロイ AWS Elastic Beanstalk を自動的に処理できます。同時に、お客様はアプリケーションを強化する AWS リソースを完全に制御でき、基盤となるリソースにいつでもアクセスできます。

AWS Elastic Beanstalk はそれ自体で PHI を保存、送信、または処理しません。代わりに、お客様は PHI を保存、送信、または処理する他の AWS のサービスを使用してアーキテクチャを構築およびデプロイできます。お客様は、PHI で HIPAA 対応サービスのみを使用する AWS Elastic Beanstalk ように、 によってデプロイされたサービスを選択するときに を確保する必要があります。これらのサービスでの PHI の使用に関するガイダンスについては、このホワイトペーパーのこれらのサービスのエントリを参照してください。

お客様は、すべての API コールをログに記録する AWS CloudTrail ために、Name field. AWS Elastic Beanstalk uses AWS Elastic Beanstalk など、 内の自由形式のフィールドに PHI を含めないでください。

AWS Elastic ディザスタリカバリ

AWS Elastic Disaster Recovery (AWS DRS) は、低コストのストレージ、最小限のコンピューティング、およびリカバリを使用して、オンプレミスおよびクラウドベースのアプリケーションの迅速かつ信頼性の高い point-in-time リカバリにより、ダウンタイムとデータ損失を最小限に抑えます。

お客様はソースサーバーで AWS Elastic Disaster Recovery を設定して、安全なデータレプリケーションを開始できます。それらのデータは、選択した AWS リージョンの AWS アカウントのステー

ジングエリアサブネットにレプリケートされます。ステージングエリア設計により、コストが削減されます。そのためには、低価格のストレージと最小限のコンピューティングリソースを使用して、継続的なレプリケーションを維持します。AWS Elastic Disaster Recovery によってレプリケートされた顧客データは、TLS 1.2 を使用して転送中に暗号化され、ソースサーバーから VPC に直接転送されます。お客様は、AWS Direct Connect や VPN などのプライベート接続を利用してレプリケーションルートを設定できます。お客様のデータは、Amazon EBS 暗号化を使用して AWS で保管中に暗号化することもできます。

お客様は中断のないテストを実行して、実装が完了したことを確認できます。通常のオペレーションでは、レプリケーションをモニタリングし、中断のない復旧とフェイルバックの演習を定期的に実行することで、準備状況を維持します。アプリケーションを復旧する必要がある場合は、 up-to-date サーバーの状態が最も多いか、前の時点を使用して、数分以内に AWS で復旧インスタンスを起動できます。お客様のアプリケーションが AWS で実行された後、アプリケーションはそこで保持するか、問題が解決したときにプライマリサイトへのデータレプリケーションを再開するかを選択できます。お客様は、準備ができたらいつでもプライマリサイトにフェイルバックできます。

AWS Fargate

AWS Fargate は、お客様がサーバーやクラスターを管理することなくコンテナを実行できるようにするテクノロジーです。を使用すると AWS Fargate、コンテナを実行するために仮想マシンのクラスターをプロビジョニング、設定、スケーリングする必要がなくなります。これにより、サーバータイプの選択、クラスターのスケーリング時期の決定、クラスターのパッキングの最適化が不要になります。 AWS Fargate は、お客様がサーバーやクラスターを操作したり、検討したりする必要がなくなります。Fargate を使用すると、お客様はアプリケーションを実行するインフラストラクチャを管理するのではなく、アプリケーションの設計と構築に集中できます。

Fargate は、PHI を処理するワークロードを操作するために追加の設定を必要としません。お客様は、Amazon ECS などのコンテナオーケストレーションサービスを使用して Fargate でコンテナワークロードを実行できます。Fargate は基盤となるインフラストラクチャのみを管理し、オーケストレーション対象のワークロード内のデータに対して動作または動作しません。HIPAA の要件に従って、Fargate で起動されたコンテナから PHI にアクセスするときは、転送中または保管中に暗号化する必要があります。このホワイトペーパーで説明されている各 AWS ストレージオプションでは、保管時の暗号化のためのさまざまなメカニズムを使用できます。HIPAA のセキュリティと設定に関する追加情報については、ホワイトペーパー「Architecting for HIPAA Security and Compliance on Amazon EKS」を参照してください。

AWS Firewall Manager

AWS Firewall Manager は、 のお客様のアカウントとアプリケーション全体でファイアウォールルールを一元的に設定および管理できるセキュリティ管理サービスです AWS Organizations。新しいアプリケーションが作成されると、Firewall Manager は共通のセキュリティルールを適用することで、新しいアプリケーションとリソースを簡単にコンプライアンス状態にすることができます。これで、お客様はファイアウォールルールを構築し、セキュリティポリシーを作成し、中央管理者アカウントからインフラストラクチャ全体に一貫した階層的な方法で適用する単一のサービスができました。

AWS Firewall Manager は、ユーザーデータを直接処理、保存、または送信しないオーケストレーションサービスです。このサービスはお客様のコンテンツを暗号化しませんが、DynamoDB などのが AWS Firewall Manager 使用する基盤となる サービスはユーザーデータを暗号化します。

AWS Global Accelerator

AWS Global Accelerator は、マルチリージョンアプリケーションの可用性とレイテンシーを改善するグローバル負荷分散サービスです。の使用中に PHI が転送中も保管中も暗号化されたままになるようにするには AWS Global Accelerator、Global Accelerator によって負荷分散されるアーキテクチャは、HTTPS や SSL/TLS などの暗号化プロトコルを使用する必要があります。バックエンドリソースで使用可能な暗号化オプションの詳細については、Amazon EC2、Elastic Load Balancing、およびその他の AWS サービスのガイダンスを参照してください。 AWS Global Accelerator は を使用してすべての API コール AWS CloudTrail をログに記録します。

AWS Glue

AWS Glue はフルマネージド型の ETL (抽出、変換、ロード) サービスで、簡単でコスト効率の高い方法でデータを分類し、クリーニングし、強化し、さまざまなデータストア間で確実に移動できます。転送中に PHI を含むデータを暗号化するには、SSL/TLS を使用してデータストアへの JDBC 接続を使用するように を設定 AWS Glue する必要があります。さらに、転送中に暗号化を維持するには、 で実行される ETL ジョブに、サーバー側の暗号化 (SSE-S3) の設定をパラメータとして渡す必要があります AWS Glue。の Data Catalog 内に保管されるすべてのデータは AWS Glue 、Data Catalog オブジェクトの作成時に暗号化が有効になってい AWS KMS る場合、 によって管理されるキーを使用して暗号化されます。 AWS Glue は CloudTrail を使用してすべての API コールをログに記録します。

AWS Glue DataBrew

AWS Glue DataBrew はフルマネージド型のビジュアルデータ準備サービスで、データアナリストやデータサイエンティストがデータをクリーニングおよび正規化して、分析や機械学習の準備を簡単に行うことができます。転送中に PHI を含むデータを暗号化するには、SSL/TLS を使用してデータストアへの JDBC 接続を使用するように を設定 DataBrew する必要があります。JDBC データソースに接続する場合、 は「SSL 接続が必要」オプションを含む AWS Glue 接続の設定 DataBrew を使用します。さらに、S3 バケットに保管中の暗号化を維持するには、サーバー側の暗号化 (SSE-S3 または SSE-KMS) の設定をパラメータとして DataBrew ジョブに渡す必要があります。

AWS IoT Core と AWS IoT Device Management

AWS IoT Core と AWS IoT Device Management は、センサー、アクチュエータ、組み込みマイクロコントローラー、スマートアプライアンスなどのインターネットに接続されたデバイスと、PHI を含むデータを送信するデバイスに対応 AWS IoT AWS IoT Device Management できるようになりました。 AWS IoT Core および とのすべての通信 AWS IoT Device Management は、TLS. AWS IoT Core を使用して暗号化され、 AWS IoT Device Management を使用してすべての API コール AWS CloudTrail を ログに記録します。

AWS IoT Greengrass

AWS IoT Greengrass では、接続されたデバイスのローカルコンピューティング、メッセージング、データキャッシュ、同期、ML 推論機能を安全な方法で実行できます。 は X.509 証明書、マネージドサブスクリプション、 AWS IoT ポリシー、IAM ポリシーとロール AWS IoT Greengrass を使用して、顧客の Greengrass アプリケーションが安全であることを確認します。 はトランスポートセキュリティモデル AWS IoT Greengrass を使用して AWS IoT 、TLS を使用してクラウドとの通信を暗号化します。さらに、 AWS IoT Greengrass データは保管時 (クラウド内) に暗号化されます。Greengrass セキュリティの詳細については、AWS IoT Greengrass 「セキュリティの概要」を参照してください。

お客様は を使用して AWS IoT Greengrass API アクションをログに記録できます AWS CloudTrail。詳細については、「 を使用した AWS IoT Greengrass API コールのログ記録 AWS CloudTrail」を参照してください。

AWS Lambda

AWS Lambda を使用すると、お客様はサーバーをプロビジョニングしたり管理したりすることなく、コードを自分で実行できます。 は、リージョン内の複数のアベイラビリティーゾーンにまたがる Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのコンピューティングフリート AWS Lambda を使用します。これにより、AWS インフラストラクチャの高可用性、セキュリティ、パフォーマンス、スケーラビリティが実現されます。

の使用中に PHI が暗号化されたままになるように、外部リソースへの接続には AWS Lambda HTTPS や SSL/TLS などの暗号化プロトコルを使用する必要があります。例えば、Lambda プロシージャから S3 にアクセスする場合は、https://bucket.s3-aws-region.amazonaws.com. で対処する必要があります。

実行中の手順で PHI が保管中またはアイドル状態になっている場合は、 または から取得したキーを使用して、クライアント側 AWS KMS またはサーバー側で暗号化する必要があります AWS CloudHSM。サービスを通じて AWS Lambda 関数をトリガーする場合は、Amazon API Gateway の関連ガイダンスに従ってください。他の AWS のサービスからのイベントを使用して AWS Lambda 関数をトリガーする場合、イベントデータに (それ自体で) PHI を含めることはできません。例えば、S3 内のオブジェクトの到着などの S3 イベントから Lambda プロシージャがトリガーされた場合、Lambda に中継されるオブジェクト名には PHI を含めないでください。ただし、オブジェクト自体にはそのようなデータを含めることができます。

AWS Managed Services

AWS Managed Services は、AWS インフラストラクチャの継続的な管理を提供します。顧客のインフラストラクチャを維持するためのベストプラクティスを導入することで、運用上のオーバーヘッドとリスクを軽減 AWS Managed Services できます。 は、変更リクエスト、モニタリング、パッチ管理、セキュリティ、バックアップサービスなどの一般的なアクティビティ AWS Managed Services を自動化し、インフラストラクチャをプロビジョニング、実行、サポートするためのフルライフサイクルサービスを提供します。

お客様は を使用して AWS Managed Services 、PHI を含むデータで動作する AWS ワークロードを管理できます。を使用して AWS Managed Services も、PHI での使用の対象となる AWS のサービスは変更されません。が提供するツールと自動化 AWS Managed Services は、PHI の保存または送信には使用できません。

AWS OpsWorks Chef Automate 用の

AWS OpsWorks for Chef Automate は、インフラストラクチャとアプリケーション管理のための Chef の自動化ツールセットである Chef Automate をホストするフルマネージド型の設定管理サービスです。サービス自体には PHI や機密情報が含まれていない、送信されていない、または処理されていませんが、 for OpsWorks Chef Automate で設定されたリソースが ガイダンスに従って設定されていることを確認する必要があります。API コールは でキャプチャされます AWS CloudTrail。詳細については、「 を使用した AWS OpsWorks スタック API コールのログ記録 AWS CloudTrail」を参照してください。

AWS OpsWorks Puppet Enterprise 用

AWS OpsWorks for Puppet Enterprise は、インフラストラクチャとアプリケーション管理のための Puppet Enterprise の自動化ツールのセットをホストするフルマネージド型の設定管理サービスです。サービス自体には PHI や機密情報が含まれていない、送信されていない、または処理されていませんが、 for Puppet Enterprise によって OpsWorks設定されたリソースが ガイダンスに従って設定されていることを確認する必要があります。API コールは でキャプチャされます AWS CloudTrail。詳細については、「 を使用した AWS OpsWorks スタック API コールのログ記録 AWS CloudTrail」を参照してください。

AWS OpsWorks スタック

AWS OpsWorks スタックは、スタックとアプリケーションを作成および管理するためのシンプルで柔軟な方法を提供します。お客様は、 AWS OpsWorks スタックを使用して、スタック内のアプリケーションをデプロイおよびモニタリングできます。

AWS OpsWorks スタックは、転送中にすべてのトラフィックを暗号化します。ただし、暗号化されたデータバッグ (Chef データストレージメカニズム) は使用できないため、PHI、シークレット/パスワード、証明書など、安全に保存する必要があるアセットは、Amazon S3 の暗号化されたバケットに保存する必要があります。AWS OpsWorks スタックは を使用してすべての API コール AWS CloudTrail を ログに記録します。

AWS Organizations

AWS Organizations は、お客様が成長するにつれて環境を一元的に管理し、AWS リソースを拡張するのに役立ちます。を使用すると AWS Organizations、プログラムで新しい AWS アカウントを作成

し、リソースを割り当てたり、アカウントをグループ化してワークフローを整理したり、ガバナンスのためにポリシーをアカウントまたはグループに適用したり、すべてのアカウントに単一の支払い方法を使用して請求を簡素化したりできます。

さらに、 AWS Organizations は他の AWS のサービスと統合されているため、お客様は組織内のアカウント間で一元的な設定、セキュリティメカニズム、監査要件、リソース共有を定義できます。 AWS Organizations は、すべての AWS のお客様が追加料金なしで利用できます。

AWS Organizations は、ユーザーデータを直接処理、保存、または送信しないオーケストレーションサービスです。このサービスはお客様のコンテンツを暗号化しませんが、 内で起動される基盤となるサービスは AWS Organizations、ユーザーデータを暗号化します。 AWS Organizations は AWS CloudTrail、 のユーザー、ロール、または AWS のサービスによって実行されたアクションを記録するサービスである と統合されています AWS Organizations。

AWS RoboMaker

AWS RoboMaker では、お客様はアプリケーション開発のためにクラウドでコードを実行でき、アプリケーションのテストを加速するためのロボットシミュレーションサービスを提供します。AWS RoboMaker は、リモートアプリケーションのデプロイ、更新、管理のためのロボットフリート管理サービスも提供します。

PHI を含むネットワークトラフィックは、転送中のデータを暗号化する必要があります。シミュレーションサーバーとの管理通信はすべて TLS 経由です。お客様は、他の AWS のサービスへの接続にオープンスタンダードトランスポート暗号化メカニズムを使用する必要があります。 RoboMaker また、AWS は と統合 CloudTrail して、すべての API コールを特定の Amazon S3 バケットに記録します。

AWS RoboMaker ログには PHI が含まれず、シミュレーションサーバーで使用される EBS ボリュームは暗号化されます。PHI を含む可能性のあるデータを Amazon S3 などの他のサービスに転送する場合、お客様は PHI の保存に関する受信サービスのガイダンスに従う必要があります。ロボットへのデプロイでは、転送中および保管中のデータの暗号化がガイダンスの解釈と一致していることを確認する必要があります。

AWS SDK メトリクス

エンタープライズのお客様は、AWS CloudWatch エージェントと AWS SDK Metrics for Enterprise Support (SDK メトリクス) を使用して、ホストおよびクライアント上の AWS SDKsからメトリクスを収集できます。これらのメトリックスは AWS エンタープライズサポートと共有されます。SDK

メトリクスは、コードにカスタムインストルメンテーションを追加せずに、AWS のサービスへの接続に関する関連メトリクスを収集して診断するのに役立ちます。また、 とログやデータを共有するために必要な手動作業を減らすことができます AWS Support。

SDK メトリクスは、エンタープライズサポートサブスクリプションの AWS のお客様のみが使用できることに注意してください。お客様は、AWS のサービスを直接呼び出し、AWS メトリクスドキュメント に記載されているバージョンの 1 つである AWS SDK を使用して構築された任意のアプリケーションで SDK メトリクスを使用できます。

SDK メトリクスは、AWS SDK によって行われた呼び出しをモニタリングし、同じ環境で実行されている CloudWatch エージェントをクライアントアプリケーションとして使用します。

CloudWatch エージェントは、ローカルマシンから送信先ロググループの配信に転送中のデータを暗号化します。ロググループは、「 を使用した ログの CloudWatch ログデータの暗号化 AWS KMS」の指示に従って暗号化するように設定できます。

AWS Secrets Manager

AWS Secrets Manager は、お客様が「シークレット」を簡単に管理できるようにする AWS のサービスです。シークレットには、データベース認証情報、パスワード、サードパーティー API キー、さらには任意のテキストを使用できます。PHI が「シークレット」に含まれる場合、 AWS Secrets Manager を使用して PHI を保存することがあります。 AWS Secrets Manager に保存されているすべてのシークレットは、AWS Key Management System (KMS) を使用して保管時に暗号化されます。ユーザーは、新しいシークレットを作成するときに使用する AWS KMS キーを選択できます。キーが選択されていない場合は、アカウントのデフォルトキーが使用されます。 AWS Secrets Manager は AWS CloudTrail を使用してすべての API コールを記録します。

AWS Security Hub

AWS Security Hub は、Amazon からの侵入検知結果、Amazon Inspector からの脆弱性スキャン GuardDuty、Amazon Macie からの Amazon S3 バケットポリシー検出結果、IAM Access Analyzer からのパブリックアクセス可能なクロスアカウントリソース、 からの WAF カバレッジがないリソースなど、お客様の環境で有効になっている AWS セキュリティサービスから検出結果を収集して統合します AWS Firewall Manager。 は、統合された AWS パートナーネットワーク (APN) セキュリティソリューションからの検出結果 AWS Security Hub も統合します。

AWS Security Hub は Amazon CloudWatch Events と統合されているため、お客様はカスタムの応答および修復ワークフローを作成できます。お客様は、SIEMsチャットツール、チケット発行シス

テム、Security Orchestration Automation and Response (SOAR) ツール、オンコール管理プラットフォームに結果を簡単に送信できます。応答および修復アクションは、完全に自動化することも、コンソールで手動でトリガーすることもできます。お客様は、 AWS Systems Manager オートメーションドキュメント、および AWS Lambda 関数を使用して AWS Step Functions、 から開始できる自動修復ワークフローを構築することもできます AWS Security Hub。

データ保護を確保するために、 は保管中のデータとコンポーネントサービス間の転送中のデータを AWS Security Hub 暗号化します。サードパーティーの監査者は、複数の AWS コンプライアンスプログラム AWS Security Hub の一環として のセキュリティとコンプライアンスを評価します。 AWS Security Hub は、AWS の SOC、ISO、PCI、HIPAA コンプライアンスプログラムの一部です。

AWS Server Migration Service

AWS Server Migration Service (AWS SMS) は、オンプレミスの VMware vSphere または Microsoft Hyper-V/SCVMM 仮想マシンの AWS クラウドへの移行を自動化します。AWS SMS は、サーバー VMs Amazon EC2 にデプロイできるクラウドホスト型 Amazon マシンイメージ (AMIsとして段階的にレプリケートします。

オンプレミスで実行され、 (AWS SMS) を使用してクラウドに移行されるサーバーには、PHI データを含めることができます。AWS SMS は、転送中およびサーバー VM イメージが EC2 への最終配置のためにステージングされているときにデータを暗号化します。AWS SMS で PHI を含むサーバー VM を移行する場合は、EC2 のガイダンスと暗号化ストレージボリュームの設定を参照してください。AWS SMS は を使用してすべての API コール CloudTrail をログに記録します。

AWS Serverless Application Repository

AWS Serverless Application Repository (SAR) は、サーバーレスアプリケーション用のマネージドリポジトリです。これにより、チーム、組織、個々のデベロッパーは再利用可能なアプリケーションを保存および共有し、強力な新しい方法でサーバーレスアーキテクチャを簡単にアセンブルしてデプロイできます。アプリケーションは AWS CloudFormation テンプレートで、アプリケーションインフラストラクチャの定義とアプリケーション AWS Lambda 関数コードのコンパイル済みバイナリが含まれています。

にあるアプリケーションが PHI AWS Serverless Application Repository を処理することは可能ですが、これは SAR 自体の一部としてではなく、お客様のアカウントにデプロイされた後にのみ行います。は、デプロイパッケージやレイヤーアーカイブなど、お客様がアップロードするファイルを AWS Serverless Application Repository 暗号化します。転送中のデータの場合、 は TLS AWS

Serverless Application Repository を使用してサービスと エージェント間のデータを暗号化します。AWS Serverless Application Repository は AWS CloudTrail、 のユーザー、ロール、または AWS のサービスによって実行されたアクションを記録するサービスである と統合されています AWS Serverless Application Repository。

Service Catalog

Service Catalog を使用すると、IT 管理者は承認された製品のポートフォリオを作成、管理、エンドユーザーに配布し、エンドユーザーはパーソナライズされたポータルから必要な製品にアクセスできます。Service Catalog は、AWS でのセルフサービスソリューションのカタログ化、共有、デプロイに使用され、PHI の保存、送信、または処理には使用できません。PHI は、Service Catalog 項目のメタデータや項目の説明には配置しないでください。Service Catalog は AWS CloudTrail を使用してすべての API コールをログに記録します。

AWS Shield

AWS Shield は、AWS で実行されているウェブアプリケーションを保護するマネージド型 Distributed Denial of Service (DDoS) 保護サービスです。 は、アプリケーションのダウンタイムとレイテンシーを最小限に抑える常時オンの検出と自動インライン緩和 AWS Shield を提供するため、DDoS 保護のメリット AWS Support を享受する必要はありません。

AWS Shield を使用して PHI を保存または送信することはできませんが、PHI で動作するウェブアプリケーションを保護するために使用できます。そのため、 をエンゲージするときに特別な設定は必要ありません AWS Shield。

すべての AWS のお客様は AWS Shield Standard、追加料金なしで の自動保護を利用できます。 は、ウェブサイトまたはアプリケーションを対象とする最も一般的な、頻繁に発生するネットワークおよびトランスポートレイヤー DDoS 攻撃に対して AWS Shield Standard 防御されます。Elastic Load Balancing (ELB)、Amazon CloudFront、および Amazon Route 53 リソースで実行されているウェブアプリケーションをターゲットとする攻撃に対する保護レベルを高めるために、 をサブスクライブできます AWS Shield Advanced。

AWS Snowball

AWS Snowball (Snowball) を使用すると、オンプレミスのデータセンターと Amazon Simple Storage Service (Amazon S3) の間で数百テラバイトまたはペタバイトのデータを転送できます。に保存 AWS Snowball されている PHI は、 ガイダンスに従って保管時に暗号化する必要があります。イン

ポートジョブを作成するときは、Snowball 内のデータを保護するために使用する AWS KMS キーの ARN を指定する必要があります。さらに、インポートジョブの作成時に、 ガイダンスで設定された暗号化基準を満たす送信先 S3 バケットを選択する必要があります。

Snowball は現在、 AWS KMSマネージドキーによるサーバー側の暗号化 (SSE-KMS) またはお客様が用意したキーによるサーバー側の暗号化 (SSE-C) をサポートしていませんが、Snowball は Amazon S3-managed暗号化キーによるサーバー側の暗号化 (SSE-S3) をサポートしています。詳細については、「Amazon S3 で管理された暗号化キーによるサーバー側の暗号化 (SSE-S3) を使用したデータの保護」を参照してください。

または、選択した暗号化方法を使用して、データを に保存する前に PHI を暗号化することもできます AWS Snowball。

現在、お客様は BAA の一部として標準 AWS Snowball アプライアンスを使用できます。

AWS Snowball エッジ

AWS Snowball Edge は、標準のストレージインターフェイスを使用して既存のお客様のアプリケーションとインフラストラクチャに接続し、データ転送プロセスを合理化し、セットアップと統合を最小限に抑えます。Snowball Edge は、 をまとめてローカルストレージ階層を形成し、顧客データをオンサイトで処理できるため、クラウドにアクセスできない場合でもアプリケーションの実行を継続できます。

Snowball Edge の使用中に PHI が暗号化されたままになるように、 が提供する手順を使用して AWS Lambda Snowball Edge の外部リソースとの間で PHI AWS IoT Greengrass を送信する場合は、必ず HTTPS や SSL/TLS などの暗号化された接続プロトコルを使用する必要があります。さらに、PHI は、ローカルアクセスまたは NFS を介して Snowball Edge のローカルボリュームに保存されている間に暗号化する必要があります。暗号化は、Snowball マネジメントコンソールと API を使用して Snowball Edge に配置されたデータに自動的に適用され、S3 への一括転送に使用されます。S3 へのデータ転送の詳細については、 の関連ガイダンスを参照してくださいthe section called “AWS Snowball”。

AWS Step Functions

AWS Step Functions では、ビジュアルワークフローを使用して分散アプリケーションとマイクロサービスのコンポーネントを簡単に調整できます。 AWS Step Functions は PHI を保存、送信、または処理することはできません。PHI は、すべての API コールをログ AWS Step Functions AWS

CloudTrail に記録するために、 のメタデータ内 AWS Step Functions 、またはタスクやステートマシン定義内に配置しないでください。

AWS Storage Gateway

AWS Storage Gateway はハイブリッドストレージサービスで、オンプレミスアプリケーションが AWS クラウドストレージをシームレスに使用できます。ゲートウェイは、オープンスタンダードストレージプロトコルを使用して、既存のストレージアプリケーションとワークフローを AWS クラウドストレージサービスに接続し、プロセスの中断を最小限に抑えます。

ファイルゲートウェイ

ファイルゲートウェイは、Amazon S3 へのファイルインターフェイス AWS Storage Gateway をサポートし、現在のブロックベースのボリュームと VTL ストレージに追加する の一種です。ファイルゲートウェイは HTTPS を使用して S3 と通信し、SSE-S3 を使用するか、デフォルトで に保存されているキーによるクライアント側の暗号化を使用して、S3 で暗号化されたすべてのオブジェクトを保存します AWS KMS。 SSE-S3 ファイル名などのファイルメタデータは暗号化されず、PHI を含めることはできません。

ボリュームゲートウェイ

ボリュームゲートウェイは、オンプレミスアプリケーションサーバーからインターネットスモールコンピュータシステムインターフェイス (iSCSI) デバイスとしてマウントできるクラウドベースのストレージボリュームを提供します。お客様は、社内のコンプライアンスおよび規制要件に従って、ローカルディスクをアップロードバッファとして、ボリュームゲートウェイ VM にキャッシュとしてアタッチする必要があります。PHI の場合、これらのディスクは保管時の暗号化を提供できることをお勧めします。ボリュームゲートウェイ VM と AWS 間の通信は、TLS 1.2 を使用して暗号化され、転送中の PHI を保護します。

テープゲートウェイ

テープゲートウェイは、オンプレミスで実行されているサードパーティーのバックアップアプリケーションへの VTL (仮想テープライブラリ) インターフェイスを提供します。お客様は、テープバックアップジョブを設定するときに、サードパーティーのバックアップアプリケーション内で PHI の暗号化を有効にする必要があります。テープゲートウェイ VM と AWS 間の通信は、TLS 1.2 を使用して暗号化され、転送中の PHI を保護します。PHI で Storage Gateway 設定のいずれかを使用するお客様は、フルログ記録を有効にする必要があります。詳細については、「AWS Storage Gatewayとは」を参照してください。

AWS Systems Manager

AWS Systems Manager は、お客様が運用データを簡単に一元化し、AWS リソース全体でタスクを自動化し、インフラストラクチャ内の運用上の問題を検出して解決する時間を短縮できる統合インターフェイスです。Systems Manager は、お客様のインフラストラクチャのパフォーマンスと設定を完全に把握し、リソースとアプリケーションの管理を簡素化し、大規模なインフラストラクチャの運用と管理を容易にします。

PHI を含む可能性のあるデータを Amazon S3 などの他のサービスに出力する場合、お客様は PHI の保存に関する受信サービスのガイダンスに従う必要があります。お客様は、ドキュメント名やパラメータ名などのメタデータや識別子に PHI を含めないでください。

AWS Transfer for SFTP

AWS Transfer for SFTP は、お客様の S3 リソースへの Secure File Transfer Protocol (SFTP) アクセスを提供します。カスタマーには、リージョンサービスエンドポイントの標準 SFTP プロトコルを使用してアクセスされる仮想サーバーが表示されます。AWS のお客様と SFTP クライアントの観点から見ると、SFTP ゲートウェイは標準の高可用性 SFTP サーバーのように見えます。サービス自体は PHI を保存、処理、送信しませんが、顧客が Amazon S3 でアクセスしているリソースは、 ガイダンスと一致する方法で設定する必要があります。お客様は AWS CloudTrail を使用して、AWS Transfer for SFTP に対して行われた API コールをログに記録することもできます。

AWS WAF – ウェブアプリケーションファイアウォール

AWS WAF は、アプリケーションの可用性に影響を与えたり、セキュリティを侵害したり、過剰なリソースを消費したりする可能性のある一般的なウェブエクスプロイトからお客様のウェブアプリケーションを保護するのに役立つウェブアプリケーションファイアウォールです。お客様は、PHI を運用または交換する AWS でホストされているウェブアプリケーションとエンドユーザーの間に AWS WAF を配置できます。AWS での PHI の送信と同様に、PHI を含むデータは転送中に暗号化する必要があります。使用可能な暗号化オプションの詳細については、Amazon EC2 のガイダンスを参照してください。

AWS X-Ray

AWS X-Ray は、お客様のアプリケーションが処理するリクエストに関するデータを収集するサービスであり、データを表示、フィルタリング、インサイトを取得して問題や最適化の機会を特定する

ために使用できるツールを提供します。顧客のアプリケーションに対するトレース対象のリクエストの場合、リクエストとレスポンスに関する情報だけでなく、アプリケーションがダウンストリーム AWS リソース、マイクロサービス、データベース、および HTTP ウェブ APIsに対して行う呼び出しに関する詳細情報も確認できます。PHI の保存または処理に AWS X-Ray は使用しないでください。との間で送受信される情報は AWS X-Ray 、デフォルトで暗号化されます。を使用する場合は AWS X-Ray、セグメント注釈またはセグメントメタデータ内に PHI を配置しないでください。

Elastic Load Balancing

お客様は Elastic Load Balancing を使用して、PHI を含むセッションを終了して処理できます。お客様は、Classic Load Balancer または Application Load Balancer のいずれかを選択できます。PHI を含むすべてのネットワークトラフィックは転送時に暗号化する必要があるため end-to-end、お客様は 2 つの異なるアーキテクチャを実装できます。

お客様は、接続に暗号化プロトコルを使用するロードバランサーを作成することで、Elastic Load Balancing で HTTPS、HTTP/2 over TLS (アプリケーション用) 、または SSL/TLS を終了できます。この機能により、ロードバランサーと HTTPS、HTTP/2 over TLS、SSL/TLS セッションを開始するクライアント間のトラフィックの暗号化、およびロードバランサーとカスタマーバックエンドインスタンス間の接続が可能になります。PHI を含むセッションでは、転送時の暗号化のためにフロントエンドリスナーとバックエンドリスナーの両方を暗号化する必要があります。お客様は証明書とセッションネゴシエーションポリシーを評価し、ガイダンスとの整合性を維持する必要があります。詳細については、「Classic Load Balancer の HTTPS リスナー」を参照してください。

または、ベーシックな TCP モード (Classic の場合) または オーバー WebSockets (アプリケーションの場合) で Amazon ELB を設定し、暗号化されたセッションが終了したバックエンドインスタンスに暗号化されたセッションをパススルーすることもできます。このアーキテクチャでは、お客様は独自のインスタンスで実行されているアプリケーションで独自の証明書と TLS ネゴシエーションポリシーを管理します。詳細については、「Classic Load Balancer のリスナー」を参照してください。どちらのアーキテクチャでも、お客様は HIPAA および HITAK の要件に準拠していると判断したレベルのログ記録を実装する必要があります。

FreeRTOS

FreeRTOS は、小規模な省電力エッジデバイスのプログラミング、デプロイ、セキュア化、接続、管理を容易にするマイクロコントローラー用のオペレーティングシステムです。FreeRTOS は、マイクロコントローラー用の一般的なオープンソースオペレーティングシステムである FreeRTOS カーネルに基づいており、 AWS IoT Core などの AWS クラウドサービスや を実行するより強力な

エッジデバイスに、小型で低電力のデバイスを安全に接続できるソフトウェアライブラリで拡張します AWS IoT Greengrass。

PHI を含むデータは、FreeRTOS を実行する認定済みデバイスを使用するときに、転送中および保管中に暗号化できるようになりました。FreeRTOS には、プラットフォームセキュリティを提供するための TLS と PKCS#11 の 2 つのライブラリが用意されています。TLS API を使用して、PHI を含むすべてのネットワークトラフィックを暗号化および認証する必要があります。PKCS#11 は、ソフトウェア暗号化オペレーション用の標準インターフェイスを提供し、FreeRTOS を実行している認定デバイスに保存されている PHI を暗号化するために使用する必要があります。

PHI の暗号化 AWS KMS に を使用する

KMS キーは、お客様のアプリケーションまたは を使用する AWS のサービスで PHI を暗号化するために使用されるデータ暗号化キーを暗号化/復号するために AWS KMS 使用できます AWS KMS。PHI は HIPAA アカウントと組み合わせて使用できますが、PHI は HIPAA 対応サービスで処理、保存、または送信できます。通常は AWS KMS 、他の HIPAA 対応サービスで実行されているアプリケーションのキーを生成および管理するために使用されます。

例えば、Amazon EC2 で PHI を処理するアプリケーションは、 GenerateDataKey API コールを使用して、アプリケーションで PHI を暗号化および復号するためのデータ暗号化キーを生成できます。データ暗号化キーは、 に保存されているお客様の KMS キーによって保護され AWS KMS、への API コール AWS KMS が に記録されるにつれて、監査可能なキー階層が作成されます AWS CloudTrail。PHI は、 に保存されているキーのタグ (メタデータ) に保存しないでください AWS KMS。

VM Import/Export

VM Import/Export を使用すると、仮想マシンイメージを既存の環境から Amazon EC2 インスタンスにインポートし、オンプレミス環境にエクスポートし直すことができます。このサービスでは、お客様は、これらの仮想マシンを ready-to-use インスタンスとして Amazon EC2 に取り込むことで、theirIT セキュリティ、設定管理、コンプライアンス要件を満たすために構築した仮想マシンへの既存の投資を活用できます。また、インポートしたインスタンスをオンプレミスの仮想化インフラストラクチャにエクスポートし直し、IT インフラストラクチャ全体にワークロードをデプロイすることもできます。

VM Import/Export は、Amazon EC2 および Amazon S3 の標準使用料金以外の追加料金なしで利用できます。

カスタマーイメージをインポートするには、 AWS CLI またはその他のデベロッパーツールを使用して、VMware 環境から仮想マシン (VM) イメージをインポートします。VMware vSphere 仮想化プラットフォームを使用している場合は、vCenter 用 AWS Management Portal を使用して VM をインポートすることもできます。インポートプロセスの一環として、VM Import はお客様の VM を Amazon EC2 AMI に変換し、Amazon EC2 インスタンスの実行に使用できます。VM がインポートされると、Auto Scaling 、Elastic Load Balancing、 などのサービスを通じて Amazon の伸縮性、スケーラビリティ、モニタリングを活用して、インポートされたイメージ CloudWatch をサポートできます。

お客様は、Amazon EC2 API ツールを使用して、以前にインポートした Amazon EC2 インスタンスをエクスポートできます。ターゲットインスタンス、仮想マシンのファイル形式、送信先の Amazon S3 バケットを指定するだけで、VM Import/Export は、VM イメージの送信と保存を保護するための暗号化オプションとともに、インスタンスを Amazon S3 バケットに自動的にエクスポートします。その後、エクスポートした VM をオンプレミスの仮想化インフラストラクチャ内でダウンロードして起動できます。

お客様は、VMware ESX または Workstation、Microsoft Hyper-V、Citrix Xen 仮想化形式を使用する Windows および Linux VMs をインポートできます。また、以前にインポートした Amazon EC2 インスタンスを VMware ESX、Microsoft Hyper-V、Citrix Xen 形式にエクスポートできます。サポートされているオペレーティングシステム、バージョン、および形式の詳細なリストについては、「VM Import/Export の要件」を参照してください。AWS は、将来、追加のオペレーティングシステム、バージョン、形式のサポートを追加する予定です。

監査、バックアップ、ディザスタリカバリ

HIPAA のセキュリティルールには、詳細な監査機能、データのバックアップ手順、災害対策メカニズムに関連する詳細な要件があります。AWS の サービスには、お客様が要件を満たすのに役立つ多くの機能が含まれています。例えば、セキュリティアナリストが詳細なアクティビティログやレポートを調べて、誰がアクセスできるか、IP アドレスエントリ、アクセスされたデータなどを確認できるように、監査機能を確立することを検討する必要があります。

このデータは、監査の場合に備えて、長期間にわたって一元的な場所に追跡、記録、保存する必要があります。Amazon EC2 を使用すると、従来のハードウェアと同様に、アクティビティログファイルを実行し、仮想サーバー上のパケットレイヤーまで監査できます。また、仮想サーバーインスタンスに到達した IP トラフィックを追跡することもできます。お客様の管理者は、長期にわたる信頼性の高いストレージのためにログファイルを Amazon S3 にバックアップできます。

HIPAA には、緊急時にデータを保護するための緊急時対応計画の維持に関する詳細な要件も設定されており、電子 PHI の取得可能な正確なコピーを作成して維持する必要があります。AWS にデータバックアッププランを実装するために、Amazon EBS は Amazon EC2 仮想サーバーインスタンスの永続的ストレージを提供します。これらのボリュームは標準のブロックデバイスとして公開でき、インスタンスの存続期間とは無関係に持続するオフインスタンスストレージを提供します。HIPAA ガイドラインに準拠するために、お客様は Amazon S3 に自動的に保存され、複数のアベイラビリティーゾーンにレプリケートされる Amazon EBS ボリュームのスナップショットを作成できます point-in-time。このスナップショットは、他のアベイラビリティーゾーンの障害から隔離されるように設計された個別の場所です。

これらのスナップショットにはいつでもアクセスでき、データを保護して長期的な耐久性を確保できます。Amazon S3 は、データストレージと自動バックアップのための可用性の高いソリューションも提供します。Amazon S3 にファイルまたはイメージをロードするだけで、複数の冗長コピーが自動的に作成され、別々のデータセンターに保存されます。これらのファイルにはいつでもどこからでもアクセスでき (アクセス許可に基づく) 、意図的に削除されるまで保存されます。

さらに、AWS は本質的にさまざまなディザスタリカバリメカニズムを提供します。ディザスタリカバリとは、組織のデータと IT インフラストラクチャを災害時に保護するプロセスであり、可用性の高いシステムを維持し、データとシステムのレプリケーションをオフサイトに保持し、両方への継続的なアクセスを可能にします。

Amazon EC2 を使用すると、管理者はサーバーインスタンスをすばやく起動し、Elastic IP アドレス (クラウドコンピューティング環境の静的 IP アドレス) を使用して、あるマシンから別のマシンへの正常なフェイルオーバーを行うことができます。Amazon EC2 には、アベイラビリティーゾーンも

用意されています。管理者は、複数のアベイラビリティーゾーンで Amazon EC2 インスタンスを起動して、ネットワーク障害、自然災害、その他のダウンタイムの原因の可能性の高い場合に高い回復力を持つ、地理的に多様で耐障害性のあるシステムを作成できます。

Amazon S3 を使用すると、顧客のデータがレプリケートされ、個別のデータセンターに自動的に保存され、99.99% の可用性を実現するように設計された信頼性の高いデータストレージが提供されます。

AWS Elastic Disaster Recovery (AWS DRS) を使用すると、お客様はアプリケーションの最も up-to-date 大きな状態または以前の時点から、AWS 上のアプリケーションをすばやく復旧できます。

ドキュメントの改訂

このホワイトペーパーの更新に関する通知を受け取るには、RSS フィードにサブスクライブしてください。

変更	説明	日付
マイナーな更新	マイナーな更新	2023 年 5 月 12 日
マイナーな更新	ホワイトペーパーを更新して、 サービスで利用可能なコンテンツを展開しました。	2022 年 9 月 28 日
マイナーな更新	包括的でない言語を修正します。	2022 年 4 月 6 日
ホワイトペーパーの更新	AWS アプリケーション移行サービスに関する情報と Amazon ECS の更新情報を追加	2021 年 12 月 6 日
ホワイトペーパーの更新	Amazon Healthlake と Amazon VPC セクションの情報を更新	2021 年 11 月 9 日
ホワイトペーパーの更新	AWS Network Firewall に関する情報を追加	2021 年 9 月 9 日
ホワイトペーパーの更新	Amazon Connect Customer Profiles に関する情報を更新	2021 年 8 月 26 日
ホワイトペーパーの更新	Amazon AppFlow および AWS Glue DataBrew のセクションを追加	2021 年 7 月 22 日
ホワイトペーパーの更新	ナビゲーションと整理を更新しました。	2021 年 4 月 26 日

ホワイトペーパーの更新	次のセクションを追加しました： AWS CodeDeploy、AWS CodePipeline、Amazon Aurora、Aurora PostgreSQL、Amazon Textract、Amazon Polly、Amazon FSx、AWS Auto Scaling、AWS Backup、 AWS Elastic Beanstalk AWS Firewall Manager、 AWS Organizations AWS Security Hub、、VM Import/Export AWS Serverless Application Repository、Amazon HealthLake、Amazon EventBridge。Amazon Aurora セクションを更新しました。	2021 年 3 月 31 日
ホワイトペーパーの更新	AWS App Mesh に関するセクションを追加し、AWS System Manager のコンテンツを更新しました	2020 年 8 月 25 日
ホワイトペーパーの更新	Amazon Appstream 2.0、AWS SDK メトリクス、AWS Data Exchange、Amazon MSK、Amazon Pinpoint、Amazon Lex、Amazon SES、Amazon Forecast、Amazon Quantum Ledger Database (QLDB) の各セクションを追加しました AWS Cloud Map。	2020 年 5 月 7 日

ホワイトペーパーの更新	Amazon CloudWatch、Amazon CloudWatch Events、Amazon Data Firehose、Amazon Managed Service for Apache Flink、Amazon OpenSearch Service、Amazon DocumentDB (MongoDB 互換) 、AWS Mobile Hub AWS IoT Greengrass、 AWS OpsWorks for Chef Automate、 AWS OpsWorks for Puppet Enterprise、AWS Transfer for SFTP、AWS DataSync AWS Global Accelerator、Amazon Comprehend Medical、および AWS に関するセクションを追加しました RoboMaker。	2020 年 1 月 1 日
ホワイトペーパーの更新	Amazon Comprehend、Amazon Transcribe、Amazon Translate、AWS Certificate Manager に関するセクションを追加しました。	2019 年 1 月 1 日

ホワイトペーパーの更新	Amazon Athena 、Amazon EKS、 AWS IoT Core、および AWS IoT Device Management、Amazon FreeRTOS 、Amazon 、Amazon Neptune GuardDuty、AWS Server Migration Service、Amazon MQ AWS Database Migration Service、および に関するセクションを追加しました AWS Glue。 Amazon MQ	2018 年 11 月 1 日
ホワイトペーパーの更新	Amazon Elastic File System (EFS)、Amazon Kinesis Video Streams、Amazon Rekognition SageMaker、Amazon、Amazon Simple Workflow、AWS Secrets Manage、Service Catalog、および に関するセクションを追加しました AWS Step Functions。	2018 年 6 月 1 日
ホワイトペーパーの更新	AWS CloudFormation、 AWS X-Ray、 AWS CloudTrail、 AWS CodeBuild AWS CodeCommit AWS Config、および AWS OpsWorks スタックに関するセクションを追加しました。	2018 年 4 月 1 日
ホワイトペーパーの更新	に関するセクションを追加しました AWS Fargate。	2018 年 1 月 1 日

2018 年以前に行われた更新：

日付	説明
2017 年 11 月	Amazon EC2 Container Registry、Amazon Macie 、Amazon 、 QuickSightおよび に関するセクションを追加しました AWS Managed Services。
2017 年 11 月	Amazon ElastiCache for Redis と Amazon のセクションを追加しました CloudWatch。
2017 年 10 月 日	Amazon SNS 、Amazon Route 53 AWS Storage Gateway、および に関するセクションを追加しました AWS CloudHSM。に関するセクションを更新しました AWS Key Management Service。
2017 年 9 月 日	Amazon Connect、Amazon Kinesis Streams、Amazon RDS (Maria) DB、Amazon RDS SQL Server、 AWS Batch AWS Lambda、 AWS Snowball Edge、および Amazon の Lambda@Edge 機能に関するセクションを追加しました CloudFront。
2017 年 8 月	Amazon EC2 Systems Manager と Amazon Inspector に関するセクションを追加しました。
2017 年 7 月	Amazon WorkSpaces、Amazon 、AWS Directory Service WorkDocs、および Amazon ECS に関するセクションを追加しました。AWS Directory Service
2017 年 6 月	Amazon CloudFront、AWS WAF AWS Shield、および Amazon S3 Transfer Acceleration に関するセクションを追加しました。

日付	説明
2017 年 5 月 日	EC2 および EMR で PHI を処理するためのハードウェア専有インスタンスまたはハードウェア専有ホストの要件を削除しました。
2017 年 3 月 日	コンプライアンスプログラムによる AWS 対象範囲内のサービスページを指すようにサービスのリストを更新しました。Amazon API Gateway の説明を追加しました。
2017 年 1 月	最新のテンプレートに更新されました。
2016 年 10 月 日	初版発行

注意

お客様は、本書に記載されている情報を独自に評価する責任を負うものとします。本書は、(a) 情報提供のみを目的とし、(b) AWS の現行製品と慣行について説明しており、これらは予告なしに変更されることがあり、(c) AWS およびその関連会社、サプライヤー、またはライセンサーからの契約上の義務や保証をもたらすものではありません。AWS の製品やサービスは、明示または黙示を問わず、一切の保証、表明、条件なしに「現状のまま」提供されます。お客様に対する AWS の責任は AWS 契約によって規定されています。また、本文書は、AWS とお客様との間の契約に属するものではなく、また、当該契約が本文書によって修正されることもありません。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。