Whitepaper AWS

# Architecting for HIPAA Security and Compliance on Amazon Web Services

# Architecting for HIPAA Security and Compliance on Amazon Web Services: Whitepaper AWS

# Table of Contents

# Architecting for HIPAA Security and Compliance on Amazon Web Services

Data di pubblicazione: 28 settembre 2022 () Revisioni del documento

Questo paper descrive brevemente come i clienti possono utilizzare Amazon Web Services (AWS) per eseguire carichi di lavoro sensibili regolati dall'U.S. Health Insurance Portability and Accountability Act (HIPAA). Ci concentreremo sulle regole di privacy e sicurezza HIPAA per proteggere le informazioni sanitarie protette (PHI), su come utilizzare AWS per crittografare i dati in transito e a riposo e su come utilizzare le funzionalità di AWS per eseguire carichi di lavoro contenenti PHI.

# Introduzione

L'Health Insurance Portability and Accountability Act del 1996 (HIPAA) si applica alle «entità coperte» e ai «soci d'affari». L'HIPAA è stato ampliato nel 2009 dall'Health Information Technology for Economic and Clinical Health (HITECH) Act.

HIPAA e HITECH stabiliscono una serie di standard federali volti a proteggere la sicurezza e la privacy delle PHI. HIPAA e HITECH impongono requisiti relativi all'uso e alla divulgazione di informazioni sanitarie protette (PHI), garanzie adeguate per proteggere le PHI, diritti individuali e responsabilità amministrative. Per ulteriori informazioni su HIPAA e HITECH, vai alla Health Information Privacy Home.

Le entità coperte e i loro partner commerciali possono utilizzare i componenti IT sicuri, scalabili e a basso costo forniti da Amazon Web Services (AWS) per progettare applicazioni in linea con i requisiti di conformità HIPAA e HITECH. AWS offre una piattaforma di commercial-off-the-shelf infrastruttura con certificazioni e audit riconosciuti dal settore come ISO 27001, FedRAMP e Service Organization Control Reports (SOC1, SOC2 e SOC3). I servizi e i data center AWS dispongono di più livelli di sicurezza operativa e fisica per contribuire a garantire l'integrità e la sicurezza dei dati dei clienti. Senza costi minimi, contratti a termine e pay-as-you-use prezzi, AWS è una soluzione affidabile ed efficace per la crescita delle applicazioni del settore sanitario.

AWS consente alle entità coperte e ai loro partner commerciali soggetti all'HIPAA di elaborare, archiviare e trasmettere le informazioni PHI in modo sicuro. Inoltre, a partire da luglio 2013, AWS offre un Business Associate Addendum (BAA) standardizzato per tali clienti. I clienti che eseguono un AWS BAA possono utilizzare qualsiasi servizio AWS in un account designato come account HIPAA, ma possono elaborare, archiviare e trasmettere PHI solo utilizzando i servizi idonei HIPAA definiti nel BAA AWS. Per un elenco completo di questi servizi, consulta la pagina di riferimento dei servizi idonei alla normativa HIPAA.

AWS mantiene un programma di gestione del rischio basato su standard per garantire che i servizi idonei all'HIPAA supportino specificamente le protezioni amministrative, tecniche e fisiche dell'HIPAA. L'utilizzo di questi servizi per archiviare, elaborare e trasmettere PHI aiuta i nostri clienti e AWS a soddisfare i requisiti HIPAA applicabili al modello operativo basato sulle utilità AWS.

La BAA di AWS richiede ai clienti di crittografare i dati PHI archiviati o trasmessi utilizzando servizi idonei all'HIPAA in conformità alle linee guida del Secretary of Health and Human Services (HHS): Guida per rendere le informazioni sanitarie protette non sicure inutilizzabili, illeggibili o indecifrabili per

individui non autorizzati («Guida»). Si prega di fare riferimento a questo sito perché potrebbe essere aggiornato e potrebbe essere reso disponibile su un sito successivo (o correlato) designato da HHS.

AWS offre un set completo di funzionalità e servizi per rendere la gestione delle chiavi e la crittografia di PHI facili da gestire e più semplici da controllare, tra cui AWS Key Management Service ()AWS KMS. I clienti con requisiti di conformità HIPAA hanno una grande flessibilità nel modo in cui soddisfano i requisiti di crittografia per PHI.

Nel determinare come implementare la crittografia, i clienti possono valutare e sfruttare le funzionalità di crittografia native dei servizi idonei all'HIPAA. In alternativa, i clienti possono soddisfare i requisiti di crittografia con altri mezzi, in linea con le indicazioni di HHS.

# Crittografia e protezione di PHI in AWS

La regola di sicurezza HIPAA include specifiche di implementazione indirizzabili per la crittografia dei PHI in trasmissione («in transito») e in archiviazione («a riposo»). Sebbene si tratti di una specifica di implementazione indirizzabile in HIPAA, AWS richiede ai clienti di crittografare i PHI archiviati o trasmessi utilizzando servizi idonei all'HIPAA in conformità alle linee guida del Secretary of Health and Human Services (HHS): Guida per rendere le informazioni sanitarie protette non sicure inutilizzabili, illeggibili o indecifrabili per individui non autorizzati («Guida»). Si prega di fare riferimento a questo sito perché potrebbe essere aggiornato e reso disponibile su un sito successivo (o correlato) designato da HHS.

AWS offre un set completo di funzionalità e servizi per rendere la gestione delle chiavi e la crittografia di PHI facili da gestire e più semplici da controllare, tra cui AWS Key Management Service ()AWS KMS. I clienti con requisiti di conformità HIPAA hanno una grande flessibilità nel modo in cui soddisfano i requisiti di crittografia per PHI.

Nel determinare come implementare la crittografia, i clienti possono valutare e sfruttare le funzionalità di crittografia native dei servizi idonei all'HIPAA, oppure possono soddisfare i requisiti di crittografia con altri mezzi coerenti con le indicazioni di HHS. Le seguenti sezioni forniscono dettagli di alto livello sull'uso delle funzionalità di crittografia disponibili in ciascuno dei servizi idonei alla normativa HIPAA e altri modelli per la crittografia dei PHI e su come AWS KMS può essere utilizzato per crittografare le chiavi utilizzate per la crittografia dei PHI su AWS.

Argomenti

- Amazon API Gateway
- Amazon AppFlow
- Amazon AppStream 2.0
- Amazon Athena
- Amazon Aurora
- Amazon Aurora PostgreSQL
- Amazon CloudFront
- Amazon CloudWatch
- CloudWatch Eventi Amazon
- CloudWatch Registri Amazon

- Amazon Comprehend
- Amazon Comprehend Medical
- Amazon Connect
- Amazon DocumentDB (compatibile con MongoDB)
- 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 per Redis
- OpenSearch Servizio Amazon
- Amazon EMR
- Amazon EventBridge
- Amazon Forecast
- Amazon FSx
- Amazon GuardDuty
- Amazon HealthLake
- Amazon Inspector
- Servizio gestito da Amazon per Apache Flink
- Amazon Data Firehose
- Amazon Kinesis Streams
- Flusso di video Amazon Kinesis
- Amazon Lex
- Amazon Managed Streaming for Apache Kafka (Amazon MSK)
- Amazon MQ
- Amazon Neptune

- AWS Network Firewall
- Amazon Pinpoint
- Amazon Polly
- Database Amazon Quantum Ledger (Amazon QLDB)
- Amazon QuickSight
- Amazon RDS per MariaDB
- Amazon RDS per MySQL
- Amazon RDS per Oracle
- Amazon RDS per PostgreSQL
- Amazon RDS per SQL Server
- Amazon Redshift
- Amazon Rekognition
- Amazon Route 53
- Amazon S3 Glacier
- Amazon S3 Transfer Acceleration
- Amazon SageMaker
- Servizio di notifica semplice Amazon (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 Servizio di migrazione delle applicazioni
- 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 Disaster Recovery
- AWS Fargate
- AWS Firewall Manager
- AWS Global Accelerator
- AWS Glue
- AWS Glue DataBrew
- AWS IoT Core e AWS IoT Device Management
- AWS IoT Greengrass
- AWS Lambda
- AWS Managed Services

- AWS OpsWorks per Chef Automate
- AWS OpsWorks per Puppet Enterprise
- AWS OpsWorks Stack
- AWS Organizations
- AWS RoboMaker
- Metriche dell'SDK AWS
- AWS Secrets Manager
- AWS Security Hub
- AWS Server Migration Service
- AWS Serverless Application Repository
- Catalogo dei servizi
- AWS Shield
- AWS Snowball
- AWS Snowball Edge
- AWS Step Functions
- AWS Storage Gateway
- AWS Systems Manager
- AWS Transfer for SFTP
- AWS WAF: firewall per applicazioni Web
- AWS X-Ray
- Sistema di bilanciamento del carico elastico
- FreeRTOS
- AWS KMS Utilizzo per la crittografia di PHI
- VM Import/Export

## Amazon API Gateway

I clienti possono utilizzare Amazon API Gateway per elaborare e trasmettere informazioni sanitarie protette (PHI). Sebbene Amazon API Gateway utilizzi automaticamente gli endpoint HTTPS per la crittografia in corso, i clienti possono anche scegliere di crittografare i payload lato client. API

Gateway passa tutti i dati non memorizzati nella cache attraverso la memoria e non li scrive su disco. I clienti possono utilizzare AWS Signature versione 4 per l'autorizzazione con API Gateway. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Domande frequenti su Amazon API Gateway: sicurezza e autorizzazione
- Controllo e gestione dell'accesso a un'API REST in API Gateway

I clienti possono integrarsi con qualsiasi servizio connesso ad API Gateway, a condizione che, quando è coinvolto PHI, il servizio sia configurato in modo coerente con la Guida e la BAA. Per informazioni sull'integrazione di API Gateway con i servizi di backend, consulta Configurare i metodi API REST in API Gateway.

I clienti possono utilizzare AWS CloudTrail Amazon CloudWatch per abilitare una registrazione coerente con i loro requisiti di registrazione. Assicurati che qualsiasi PHI inviato tramite API Gateway (ad esempio nelle intestazioni, negli URL e nella richiesta/risposta) venga acquisito solo dai servizi idonei all'HIPAA che sono stati configurati per essere coerenti con la Guida. Per ulteriori informazioni sulla registrazione con API Gateway, vedi Come posso abilitare i CloudWatch log per la risoluzione dei problemi dell'API o WebSocket dell'API REST di API Gateway?

## Amazon AppFlow

Amazon AppFlow è un servizio di integrazione completamente gestito che consente ai clienti di trasferire in modo sicuro i dati tra applicazioni oftware-as-a S-Service (SaaS) come Salesforce, Marketo, Slack e servizi ServiceNow AWS come Amazon S3 e Amazon Redshift. AppFlow può eseguire flussi di dati alla frequenza scelta dal cliente, secondo una pianificazione, in risposta a un evento aziendale o su richiesta. I clienti possono anche configurare funzionalità di trasformazione dei dati come il filtraggio e la convalida per generare ready-to-use dati complessi come parte del flusso stesso, senza passaggi aggiuntivi.

Amazon AppFlow può essere utilizzato per elaborare e trasferire dati contenenti PHI. La crittografia dei dati in transito tra AppFlow e la sorgente/destinazione configurata viene fornita di default tramite TLS 1.2 o versione successiva. I dati archiviati in archivio in S3 vengono crittografati automaticamente utilizzando una AWS KMS chiave (precedentemente CMK) specificata dal cliente. Per i dati PHI trasferiti verso destinazioni diverse da S3, i clienti devono assicurarsi che lo storage a riposo per la destinazione scelta soddisfi le loro esigenze di sicurezza. AppFlow consente il monitoraggio delle applicazioni mediante l'integrazione con AWS CloudTrail to log delle chiamate API e Amazon EventBridge per emettere eventi di esecuzione del flusso.

# Amazon AppStream 2.0

Amazon AppStream 2.0 è un servizio di streaming di applicazioni completamente gestito. I clienti possiedono i propri dati e devono configurare le applicazioni Windows necessarie in modo da soddisfare i requisiti normativi. I clienti possono configurare l'archiviazione persistente tramite Home Folders. I file e le cartelle sono crittografati in transito utilizzando gli endpoint SSL di Amazon S3. I file e le cartelle vengono crittografati quando sono archiviati utilizzando chiavi di crittografia gestite da Amazon S3. Per ulteriori informazioni, consulta Abilitare e amministrare lo storage persistente per gli utenti AppStream 2.0. Se i clienti scelgono di utilizzare una soluzione di storage di terze parti, hanno la responsabilità di garantire che la configurazione di tale soluzione sia coerente con le linee guida. Tutte le comunicazioni API pubbliche con Amazon AppStream 2.0 sono crittografate tramite TLS. Per ulteriori informazioni, consulta la documentazione di Amazon AppStream 2.0.

Amazon AppStream 2.0 è integrato con AWS CloudTrail, un servizio che registra le chiamate API effettuate da o per conto di Amazon AppStream 2.0 nell'account AWS del cliente e consegna i file di registro al bucket Amazon S3 specificato. CloudTrail acquisisce le chiamate API effettuate dalla console Amazon AppStream 2.0 o dall'API Amazon AppStream 2.0. I clienti possono anche utilizzare Amazon CloudWatch per registrare i parametri di utilizzo delle risorse. Per ulteriori informazioni, consulta Monitoraggio delle risorse Amazon AppStream 2.0 e registrazione delle chiamate API AppStream 2.0 con AWS CloudTrail.

# Amazon Athena

Amazon Athena è un servizio interattivo di esecuzione di query che semplifica l'analisi di dati direttamente in Amazon Simple Storage Service (Amazon S3) con SQL standard. Athena aiuta i clienti ad analizzare dati non strutturati, semistrutturati e strutturati archiviati in Amazon S3. Tra gli esempi figurano CSV, JSON o formati di dati colonnari come Apache Parquet e Apache ORC. I clienti possono utilizzare Athena per eseguire query ad hoc utilizzando ANSI SQL, senza la necessità di aggregare o caricare i dati in Athena.

Amazon Athena può ora essere utilizzato per elaborare dati contenenti PHI. La crittografia dei dati in transito tra Amazon Athena e S3 viene fornita di default tramite SSL/TLS. La crittografia di PHI mentre è inattivo su S3 deve essere eseguita secondo le linee guida fornite nella sezione S3. La crittografia dei risultati delle query da e all'interno di Amazon Athena, inclusi i risultati staged, deve essere abilitata utilizzando la crittografia lato server con chiavi gestite di Amazon S3 (SSE-S3), chiavi gestite (SSE-KMS) o la crittografia lato client con chiavi AWS KMS gestite (CSE-KMS). AWS KMS Amazon Athena utilizza AWS CloudTrail per registrare tutte le chiamate API.

# Amazon Aurora

Amazon Aurora consente ai clienti di crittografare i cluster e le istantanee di database Aurora inattivi utilizzando le chiavi tramite le quali gestiscono. AWS KMS Su un'istanza di database in esecuzione con crittografia Amazon Aurora, i dati archiviati inattivi nello storage sottostante sono crittografati, così come i backup automatici, le repliche di lettura e le istantanee.

Poiché la Guida potrebbe essere aggiornata, i clienti devono continuare a valutare e determinare se la crittografia Amazon Aurora soddisfa i requisiti normativi e di conformità. Per ulteriori informazioni sulla crittografia a riposo con Amazon Aurora, consulta Protezione dei dati tramite crittografia.

Le connessioni ai cluster DB che eseguono Aurora MySQL devono utilizzare la crittografia di trasporto, utilizzando Secure Socket Layer (SSL) o Transport Layer Security (TLS). Per ulteriori informazioni sull'implementazione di SSL/TLS, consulta Uso di SSL/TLS con i cluster Aurora MySQL DB.

# Amazon Aurora PostgreSQL

Amazon Aurora consente ai clienti di crittografare i cluster e le istantanee di database Aurora inattivi utilizzando le chiavi tramite le quali gestiscono. AWS KMS Su un'istanza di database in esecuzione con crittografia Amazon Aurora, i dati archiviati inattivi nello storage sottostante sono crittografati, così come i backup automatici, le repliche di lettura e le istantanee.

Poiché la Guida potrebbe essere aggiornata, i clienti devono continuare a valutare e determinare se la crittografia Amazon Aurora soddisfa i requisiti normativi e di conformità. Per ulteriori informazioni sulla crittografia a riposo con Amazon Aurora, consulta Protezione dei dati tramite crittografia.

Le connessioni ai cluster DB che eseguono Aurora PostgreSQL devono utilizzare la crittografia di trasporto, utilizzando Secure Socket Layer (SSL) o Transport Layer Security (TLS). Per ulteriori informazioni sull'implementazione di SSL/TLS, consulta Proteggere i dati di Aurora PostgreSQL con SSL.

# Amazon CloudFront

Amazon CloudFront è un servizio di rete di distribuzione di contenuti (CDN) globale che accelera la distribuzione di siti Web, API, contenuti video o altre risorse Web dei clienti. Si integra con altri prodotti Amazon Web Services per offrire a sviluppatori e aziende un modo semplice per accelerare i contenuti per gli utenti finali senza impegni minimi di utilizzo. Per garantire la crittografia del PHI

durante il trasferimento CloudFront, i clienti devono configurare CloudFront l'utilizzo di HTTPS end-to-end dall'origine al visualizzatore.

Ciò include il traffico tra CloudFront e il visualizzatore, la CloudFront ridistribuzione da un'origine personalizzata e la CloudFront distribuzione da un'origine Amazon S3. I clienti devono inoltre assicurarsi che i dati siano crittografati all'origine per garantire che rimangano crittografati anche quando sono memorizzati nella cache. CloudFront Se utilizzano Amazon S3 come origine, i clienti possono utilizzare le funzionalità di crittografia lato server di S3. Se i clienti distribuiscono da un'origine personalizzata, devono assicurarsi che i dati siano crittografati all'origine.

### Lambda@Edge

Lambda @Edge è un servizio di elaborazione che consente l'esecuzione di funzioni Lambda nelle edge location AWS. Lambda @Edge può essere utilizzata per personalizzare i contenuti distribuiti tramite. CloudFront Quando utilizzano Lambda @Edge con PHI, i clienti devono seguire la Guida per l'uso di. CloudFront Tutte le connessioni in entrata e in uscita da Lambda @Edge devono essere crittografate tramite HTTPS o SSL/TLS.

## Amazon CloudWatch

Amazon CloudWatch è un servizio di monitoraggio per le risorse del cloud AWS e le applicazioni che i clienti eseguono su AWS. I clienti possono utilizzare Amazon CloudWatch per raccogliere e tenere traccia delle metriche, raccogliere e monitorare i file di registro e impostare allarmi. Amazon CloudWatch stessa non produce, archivia o trasmette PHI. I clienti possono monitorare le chiamate CloudWatch API con AWS CloudTrail. Per ulteriori informazioni, consulta Logging Amazon CloudWatch API Calls with AWS CloudTrail.

Per maggiori dettagli sui requisiti di configurazione, consulta la sezione Amazon CloudWatch Logs.

## CloudWatch Eventi Amazon

Amazon CloudWatch Events offre un near-real-time flusso di eventi di sistema che descrivono i cambiamenti nelle risorse AWS. I clienti devono assicurarsi che il PHI non confluisca in CloudWatch Events e che qualsiasi risorsa AWS che emette un CloudWatch evento che memorizza, elabora o trasmette PHI sia configurata in conformità con la Guida.

I clienti possono configurare Amazon CloudWatch Events per registrarsi come chiamata API AWS CloudTrail. Per ulteriori informazioni, consulta Creazione di una regola di CloudWatch eventi che si attiva su una chiamata API AWS utilizzando AWS CloudTrail.

# CloudWatch Registri Amazon

I clienti possono utilizzare Amazon CloudWatch Logs per monitorare, archiviare e accedere ai propri file di log da AWS CloudTrail istanze Amazon Elastic Compute Cloud (Amazon EC2), Amazon Route 53 e altre fonti. Possono quindi recuperare i dati di log associati da Logs. CloudWatch I dati di registro vengono crittografati durante il transito e mentre sono inattivi. Di conseguenza, non è necessario crittografare nuovamente il PHI emesso da qualsiasi altro servizio e fornito a Logs. CloudWatch

# Amazon Comprehend

Amazon Comprehend utilizza l'elaborazione del linguaggio naturale per estrarre informazioni dettagliate sul contenuto dei documenti. Amazon Comprehend elabora qualsiasi file di testo in formato UTF-8. Sviluppa informazioni basandosi su entità, frasi chiave, linguaggio, sentimenti e altri elementi comuni in un documento. Amazon Comprehend può essere utilizzato con dati contenenti PHI. Amazon Comprehend non conserva né archivia alcun dato e tutte le chiamate all'API sono crittografate con SSL/TLS. Amazon Comprehend utilizza CloudTrail per registrare tutte le chiamate API.

## AWS Identity and Access Management

Le funzioni di accesso di sicurezza come l'autenticazione e l'autorizzazione sono necessarie per accedere ad Amazon Comprehend e possono essere controllate con AWS Identity and Access Management(IAM) e le credenziali possono essere utilizzate per accedere a IAM. Per ulteriori informazioni, consulta Authentication and Access Control for Amazon Comprehend nella Amazon Comprehend User Guide.

### Gestione dell'account

Per impostazione predefinita, gli utenti IAM non dispongono dell'autorizzazione per creare o modificare risorse Amazon Comprehend o eseguire attività utilizzando l'API Amazon Comprehend. Per consentire agli utenti di creare o modificare risorse ed eseguire attività, i clienti hanno la responsabilità di sfruttare le policy IAM che concedono agli utenti le autorizzazioni per le risorse specifiche (come Amazon Comprehend e le azioni API) che gli utenti devono utilizzare e quindi allegare le policy agli utenti o ai gruppi che richiedono autorizzazioni specifiche.

Con Amazon Comprehend puoi utilizzare AWS Identity and Access Management (IAM) per creare un utente con una policy allegata per abilitare le autorizzazioni di Amazon Comprehend. Facoltativamente, puoi scegliere di creare politiche personalizzate da associare a un ruolo. Quindi,

puoi aggiungere amministratori al ruolo con la possibilità di richiamare le API per l'amministrazione di Amazon Comprehend in conformità ai principi di accesso basato sui ruoli e privilegi minimi definiti dall'organizzazione.

### Identità e accesso

Con Amazon Comprehend puoi richiedere all'utente di autenticarsi per AWS utilizzare l'autenticazione a più fattori in base ai requisiti organizzativi per l'autenticazione.

Utilizzando AWS Management Console, gli amministratori IAM possono creare una policy gestita dal cliente che neghi tutte le autorizzazioni tranne quelle necessarie agli utenti per gestire le proprie credenziali e i dispositivi MFA. Un modello di policy JSON è disponibile nella pagina Le mie credenziali di sicurezza nella console IAM.

Facoltativamente, puoi sfruttare funzionalità MFA di terze parti compatibili con i partner IAM. Per ulteriori informazioni, consulta IAM Partners.

### Amministrazione

Ti consigliamo di selezionare con Amazon Comprehend policy basate sull'identità in cui gli amministratori di account possano associare policy di autorizzazione alle identità IAM (utenti, gruppi e ruoli) e quindi concedere le autorizzazioni per eseguire operazioni sulle risorse Amazon Comprehend.

Un elenco di azioni API per Amazon Comprehend è disponibile nella guida di riferimento delle API. Dovresti inoltre prendere in considerazione la possibilità di autorizzare l'accesso a politiche IAM predefinite, politiche IAM dei clienti e azioni API per utenti o ruoli in base ai loro requisiti organizzativi basati sui privilegi minimi e sui ruoli. Per ulteriori informazioni, consulta Using the Amazon Comprehend API nella Developer Guide.

### Autenticazione esterna

Amazon Comprehend è compatibile con la federazione delle identità utilizzando i ruoli IAM. Ciò consente ai tuoi utenti di autenticarsi con Amazon Comprehend AWS assumendo un ruolo assegnato dagli amministratori. Gli utenti che accedono AWS utilizzando le credenziali della propria organizzazione o di terze parti assumono un ruolo indirettamente.

AWS il supporto per Kerberos e Active Directory offre i vantaggi del single sign-on e dell'autenticazione centralizzata degli utenti del database. AWS gli utenti possono scegliere di gestire e archiviare le credenziali utente in AWS Directory Service Microsoft Active Directory o nell'Active Directory locale del cliente.

### Applicazione del flusso di dati

AWS i clienti e i partner APN, che agiscono in qualità di titolari o incaricati del trattamento dei dati, sono responsabili di tutti i dati personali che inseriscono in Amazon Cloud AWS Comprehend. Sei responsabile del controllo del flusso verso gli input e gli output dei dati per Amazon Comprehend utilizzando le policy IAM.

## Protezione dei dati e gestione dei segreti

Il modello di responsabilità AWS condivisa si applica alla protezione dei dati in Amazon Comprehend. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutto il AWS cloud. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Questo contenuto include le attività di configurazione e gestione della sicurezza per i AWS servizi che utilizzi. Per ulteriori informazioni sulla privacy dei dati, consulta Domande frequenti sulla privacy dei dati.

La sezione Protezione dei dati in Amazon Comprehend della Amazon Comprehend Developer Guide fornisce suggerimenti da prendere in considerazione per proteggere i dati, ad esempio usare TLS per la trasmissione ed evitare l'inserimento di informazioni sensibili in tag o campi in formato libero.

### Crittografia di data-at-rest

Amazon Comprehend collabora con AWS Key Management Service(AWS KMS) per fornire una crittografia avanzata per i tuoi dati. Amazon Simple Storage Service (Amazon S3) ti consente già di crittografare i documenti di input durante la creazione di analisi del testo, modellazione di argomenti o job Amazon Comprehend personalizzati. L'integrazione con AWS KMS consente di crittografare i dati nel volume di storage per i processi start* e create* e crittografa i risultati di output dei processi start* utilizzando la tua chiave. AWS KMS

È buona prassi per gli utenti di Amazon Comprehend crittografare i bucket Amazon S3 utilizzati per i documenti di input utilizzando le soluzioni di crittografia S3 disponibili in conformità con le loro politiche organizzative.

Il AWS Management Console, crittografa i modelli personalizzati di Amazon Comprehend con una propria AWS KMS chiave. Inoltre AWS CLI, Amazon Comprehend può crittografare modelli personalizzati utilizzando la propria AWS KMS chiave o una chiave gestita dal cliente (CMK) fornita.

Se selezioni la crittografia quando usi il AWS Management Console, puoi scegliere uno o entrambi i seguenti metodi opzionali:

- Crittografia del volume: assicura che i dati su un volume EBS utilizzato da Comprehend siano crittografati durante l'addestramento o l'inferenza (i dati vengono scaricati dopo l'addestramento o l'inferenza, quindi questa chiave è rilevante solo mentre il lavoro è in corso).
- Crittografia dei risultati di output: per crittografare l'output archiviato da Comprehend nel bucket del cliente utilizzando una chiave fornita dal cliente. AWS KMS

Per ulteriori informazioni sui tipi di crittografia come la crittografia dei volumi, consulta AWS KMS Encryption in Amazon Comprehend.

### Informazioni di identificazione personale

Puoi utilizzare la console o le API di Amazon Comprehend per rilevare informazioni di identificazione personale (PII) nei documenti di testo in inglese. Per ulteriori informazioni sul rilevamento e l'etichettatura delle entità PII e sull'esecuzione di vari processi di analisi delle PII, consulta la sezione Informazioni di identificazione personale nella Amazon Comprehend Developer Guide.

### Eliminazione dei dati

Se sei un cliente Amazon Comprehend che utilizza Amazon S3 e scegli di gestire le AWS KMS tue chiavi, dovresti prendere in considerazione la possibilità di AWS KMS revocare le chiavi e definire la giustificazione procedurale per farlo in base ai requisiti organizzativi. La revoca della AWS KMS chiave per Amazon S3 rende tutti i dati inutilizzabili/illeggibili.

## Segmentazione e rafforzamento della rete

Come servizio gestito, Amazon Comprehend aderisce alle AWS migliori pratiche per la sicurezza, l'identità e la conformità.

Per le misure di sicurezza di rete consigliate, consulta Infrastructure Security in Amazon Comprehend nella Amazon Comprehend Developers Guide.

### Proteggi i lavori utilizzando un Amazon Virtual Private Cloud (Amazon VPC)

Amazon Comprehend utilizza una serie di misure di sicurezza per garantire la sicurezza dei tuoi dati con i nostri job container in cui vengono archiviati mentre vengono utilizzati da Amazon Comprehend. Tuttavia, i job container accedono a AWS risorse, come i bucket Amazon S3 in cui archiviare dati e modellare artefatti, tramite Internet.

Per controllare l'accesso ai tuoi dati, ti consigliamo di creare un cloud privato virtuale (VPC) e configurarlo in modo che i dati e i contenitori non siano accessibili su Internet. Per ulteriori

informazioni sulla creazione e sulla configurazione di un VPC, consulta Nozioni di base su Amazon VPC nella Guida per l'utente di Amazon VPC. L'utilizzo di un VPC aiuta a proteggere i dati perché è possibile configurare il VPC in modo che non sia connesso a Internet. L'utilizzo di un VPC consente inoltre di monitorare tutto il traffico di rete in entrata e in uscita dai nostri container di lavoro utilizzando i log di flusso VPC. Per ulteriori informazioni, consulta Log di flusso VPC nella Guida per l'utente di Amazon VPC.

La configurazione del VPC viene specificata quando si crea un lavoro, specificando le sottoreti e i gruppi di sicurezza. Quando specifichi le sottoreti e i gruppi di sicurezza, Amazon Comprehend crea interfacce di rete elastiche (ENI) associate ai tuoi gruppi di sicurezza in una delle sottoreti. Gli ENI consentono ai nostri container di lavoro di connettersi alle risorse del tuo VPC. Per informazioni sulle ENI, consulta Interfacce di rete elastiche nella Guida per l'utente di Amazon VPC.

> **Note**
>
> Per i lavori, puoi configurare solo le sottoreti con un VPC di tenancy predefinito in cui l'istanza viene eseguita su hardware condiviso. Per ulteriori informazioni sull'attributo tenancy per i VPC, consulta Dedicated Instances nella Amazon EC2 User Guide for Linux Instances.

Puoi stabilire una connessione privata tra il tuo VPC e Amazon Comprehend creando un endpoint VPC di interfaccia. Per ulteriori informazioni, consulta Amazon Comprehend and Interface VPC Endpoints ().AWS PrivateLink

## Rafforzamento dell'host e dell'immagine

In base al modello di responsabilità AWS condivisa, il rafforzamento dell'host e dell'immagine dell' AWS ambiente per Amazon Comprehend viene AWS gestito come servizio fornito.

## Multilocazione

Per rendere più sicura la tua raccomandazione, ti consigliamo di implementare i seguenti consigli di sicurezza multi-tenancy:

- Usa solo un indirizzo e-mail verificato per autorizzare l'accesso degli utenti a un tenant in base alla corrispondenza del dominio. Non fidarti degli indirizzi e-mail e dei numeri di telefono a meno che la tua app non li verifichi o che l'IdP esterno fornisca una prova di verifica. Per maggiori dettagli sull'impostazione di queste autorizzazioni, consulta la sezione Autorizzazioni e ambiti degli attributi.

- Utilizza attributi immutabili o mutabili per gli attributi del profilo utente che identificano i tenant. Gli amministratori devono essere in grado di modificare questi attributi. Fornisci inoltre ai client di app l'accesso in sola lettura agli attributi.
- Utilizza una mappatura 1:1 tra IdP esterno e client di applicazioni in modo da impedire l'accesso non autorizzato tra tenant. Un utente autenticato da un IdP esterno e dotato di un cookie di sessione Amazon Cognito valido, può accedere ad altre App tenant che considerano lo stesso IdP come affidabile.
- Quando implementi la logica di autorizzazione e corrispondenza tenant nell'applicazione, imposta delle limitazioni affinché le autorizzazioni di accesso degli utenti ai tenant non possano essere modificate dagli utenti stessi. Inoltre, se per la federazione viene utilizzato un IdP esterno, limita gli amministratori del provider di identità del tenant in modo che non possano modificare l'accesso degli utenti.

### Prevenzione del problema "confused deputy" tra servizi

Il confuso problema secondario è un problema di sicurezza multi-tenancy in cui un'entità che non dispone dell'autorizzazione per eseguire un'azione può costringere un'entità con più privilegi a eseguire l'azione. Nel frattempo AWS, l'impersonificazione tra servizi può portare alla confusione del vicesceriffo. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare che ciò accada, AWS fornisce strumenti che possono aiutarvi a proteggere i vostri dati per tutti i servizi, con responsabili del servizio a cui è stato concesso l'accesso alle risorse del vostro account. Per ulteriori informazioni sulle misure di protezione da prendere in considerazione per risolvere questo problema di sicurezza, consulta Cross-service Confused Deputy Prevention nella Amazon Comprehend Developer Guide.

## Amazon Comprehend Medical

Per informazioni, consulta la sezione precedente. Amazon Comprehend

## Amazon Connect

Amazon Connect è un servizio di contact center self-service basato sul cloud che consente un coinvolgimento dinamico, personale e naturale dei clienti su qualsiasi scala. I clienti non devono

includere alcun PHI nei campi associati alla gestione degli utenti, dei profili di sicurezza e dei flussi di contatti all'interno di Amazon Connect.

Amazon Connect Customer Profiles, una funzionalità di Amazon Connect, fornisce agli agenti dei contact center una visione più unificata del profilo del cliente con le informazioni più aggiornate, per fornire un servizio clienti più personalizzato. Customer Profiles è progettato per riunire automaticamente le informazioni sui clienti provenienti da più applicazioni in un profilo cliente unificato, fornendo il profilo direttamente all'agente non appena inizia la chiamata di supporto o l'interazione. I clienti devono astenersi dal denominare domini o chiavi di oggetti con dati PHI. I contenuti di Domini e Oggetti sono crittografati e protetti, ma gli identificatori chiave no.

## Amazon DocumentDB (compatibile con MongoDB)

Amazon DocumentDB (con compatibilità con MongoDB) (Amazon DocumentDB) offre la crittografia a riposo durante la creazione di cluster tramite, AWS KMS che consente ai clienti di crittografare i database utilizzando AWS o chiavi gestite dal cliente. Su un'istanza di database in esecuzione con crittografia abilitata, i dati archiviati a riposo sono crittografati in conformità con le Linee guida in vigore al momento della pubblicazione di questo white paper, così come i backup automatici, le repliche di lettura e le istantanee. Poiché la Guida potrebbe essere aggiornata, i clienti devono continuare a valutare e determinare se la crittografia di Amazon DocumentDB soddisfa i requisiti normativi e di conformità. Per ulteriori informazioni sulla crittografia a riposo con Amazon DocumentDB, consulta Encrypting Amazon DocumentDB Data at Rest.

Le connessioni ad Amazon DocumentDB contenenti PHI devono utilizzare endpoint che accettano il trasporto crittografato (HTTPS). Per impostazione predefinita, un cluster Amazon DocumentDB appena creato accetta solo connessioni sicure tramite Transport Layer Security (TLS). Per ulteriori informazioni, consulta Encrypting Data in Transit. Amazon DocumentDB utilizza AWS CloudTrail per registrare tutte le chiamate API. Per ulteriori informazioni, consulta Logging and Monitoring in Amazon DocumentDB.

Per alcune funzionalità di gestione, Amazon DocumentDB utilizza una tecnologia operativa condivisa con Amazon RDS. La console Amazon DocumentDB, l'interfaccia della riga di comando AWS e le chiamate API vengono registrate come chiamate effettuate all'API Amazon RDS.

# Amazon DynamoDB

Le connessioni ad Amazon DynamoDB contenenti PHI devono utilizzare endpoint che accettano il trasporto crittografato (HTTPS). Per un elenco degli endpoint regionali, consulta AWS service endpoints.

Amazon DynamoDB offre la crittografia DynamoDB, che consente ai clienti di crittografare i database utilizzando chiavi gestite dai clienti. AWS KMS Su un'istanza di database in esecuzione con crittografia Amazon DynamoDB, i dati archiviati a riposo nello storage sottostante sono crittografati in conformità con le Linee guida in vigore al momento della pubblicazione di questo white paper, così come i backup automatici, le repliche di lettura e le istantanee.

Poiché la Guida potrebbe essere aggiornata, i clienti dovrebbero continuare a valutare e determinare se la crittografia Amazon DynamoDB soddisfa i requisiti normativi e di conformità. Per ulteriori informazioni sulla crittografia a riposo con Amazon DynamoDB, consulta DynamoDB Encryption at Rest.

# Amazon Elastic Block Store

La crittografia a riposo di Amazon EBS è coerente con la Guida in vigore al momento della pubblicazione di questo white paper. Poiché la Guida potrebbe essere aggiornata, i clienti devono continuare a valutare e determinare se la crittografia Amazon EBS soddisfa i requisiti normativi e di conformità. Con la crittografia Amazon EBS, viene generata una chiave di crittografia del volume unica per ogni volume EBS. I clienti hanno la flessibilità di scegliere quale chiave KMS utilizzare per crittografare ogni chiave di volume. AWS Key Management Service Per ulteriori informazioni, consulta la pagina Amazon EBS encryption (Crittografia Amazon EBS).

# Amazon Elastic Compute Cloud

Amazon EC2 è un servizio di elaborazione scalabile e configurabile dall'utente che supporta diversi metodi per crittografare i dati inattivi. Ad esempio, i clienti potrebbero scegliere di eseguire la crittografia a livello di applicazione o di campo del PHI mentre viene elaborato all'interno di un'applicazione o di una piattaforma di database ospitata in un'istanza Amazon EC2. Gli approcci spaziano dalla crittografia dei dati utilizzando librerie standard in un framework applicativo come Java o.NET, all'utilizzo delle funzionalità di Transparent Data Encryption di Microsoft SQL o Oracle o all'integrazione di altre soluzioni di terze parti basate su SaaS (Software as a Service) nelle loro applicazioni.

I clienti possono scegliere di integrare le loro applicazioni in esecuzione in Amazon EC2 con AWS KMS gli SDK, semplificando il processo di gestione e archiviazione delle chiavi. I clienti possono inoltre implementare la crittografia dei dati inattivi utilizzando la crittografia a livello di file o dell'intero disco (FDE) utilizzando software di terze parti dei Marketplace AWS partner o strumenti di crittografia nativi dei file system (come dm-crypt, LUKS, ecc.).

Il traffico di rete contenente PHI deve crittografare i dati in transito. Per il traffico tra fonti esterne (come Internet o un ambiente IT tradizionale) e Amazon EC2, i clienti devono utilizzare meccanismi di crittografia di trasporto standard aperti come Transport Layer Security (TLS) o reti private virtuali (VPN) IPSec, coerenti con la Guida. Interno a un Amazon Virtual Private Cloud (VPC) per i dati che viaggiano tra istanze Amazon EC2, anche il traffico di rete contenente PHI deve essere crittografato; la maggior parte delle applicazioni supporta TLS o altri protocolli che forniscono la crittografia in transito che può essere configurata per essere coerente con la Guida. Per le applicazioni e i protocolli che non supportano la crittografia, le sessioni che trasmettono PHI possono essere inviate attraverso tunnel crittografati utilizzando IPSec o implementazioni simili tra le istanze.

## Amazon Elastic Container Registry

Amazon Elastic Container Registry (Amazon ECR) è integrato con Amazon Elastic Container Service (Amazon ECS) e consente ai clienti di archiviare, eseguire e gestire facilmente le immagini dei container per le applicazioni in esecuzione su Amazon ECS. Dopo che i clienti hanno specificato il repository Amazon ECR nella definizione delle attività, Amazon ECS recupererà le immagini appropriate per le loro applicazioni.

Non sono necessari passaggi speciali per utilizzare Amazon ECR con immagini di container che contengono PHI. Le immagini dei container vengono crittografate durante il transito e archiviate crittografate quando sono inattive utilizzando la crittografia lato server di Amazon S3 (SSE-S3).

## Amazon Elastic Container Service

Amazon Elastic Container Service (Amazon ECS) è un servizio di gestione dei container altamente scalabile e ad alte prestazioni che supporta i contenitori Docker e consente ai clienti di eseguire facilmente applicazioni su un cluster gestito di istanze Amazon EC2. Amazon ECS elimina la necessità per i clienti di installare, gestire e scalare la propria infrastruttura di gestione dei cluster.

Con semplici chiamate API, i clienti possono avviare e interrompere applicazioni compatibili con Docker, interrogare lo stato completo del cluster e accedere a molte funzionalità familiari come gruppi di sicurezza, Elastic Load Balancing, volumi EBS e ruoli IAM. I clienti possono utilizzare Amazon ECS

per pianificare il posizionamento dei container nel proprio cluster in base alle esigenze di risorse e ai requisiti di disponibilità.

L'utilizzo di ECS con carichi di lavoro che elaborano PHI non richiede alcuna configurazione aggiuntiva. ECS funge da servizio di orchestrazione che coordina il lancio dei container (le cui immagini sono archiviate in S3) su EC2 e non funziona con o sui dati all'interno del carico di lavoro da orchestrare. In linea con le normative HIPAA e il AWS Business Associate Addendum, i PHI devono essere crittografati in transito e a riposo quando vi si accede dai container lanciati con ECS. Per ogni opzione di AWS storage sono disponibili diversi meccanismi di crittografia a riposo (ad esempio, S3, EBS e KMS). Garantire la crittografia completa dei PHI inviati tra i container può anche indurre i clienti a implementare una rete overlay (come VNS3, Weave Net o simili), al fine di fornire un livello di crittografia ridondante. Tuttavia, è necessario abilitare anche la registrazione completa (ad esempio, tramite CloudTrail) e indirizzare tutti i registri delle istanze del contenitore a. CloudWatch

L'utilizzo di Firelens e AWS per Fluent Bit con carichi di lavoro che elaborano PHI non richiede alcuna configurazione aggiuntiva, a meno che i log non contengano PHI. Se i registri contengono PHI, non devono essere emessi nei file di registro, a meno che la crittografia del disco non sia abilitata. Configura invece l'applicazione in modo che emetta i log in formato standard out/error, che verranno raccolti automaticamente da. FireLens Analogamente, non attivate il buffering dei file per Fluent Bit, a meno che non sia abilitata anche la crittografia del disco. Infine, la destinazione dei log deve essere supportata encryption-in-transit; tutti i plugin di output del AWS servizio in AWS for Fluent Bit utilizzeranno sempre la crittografia TLS per esportare i log.

# Amazon Elastic File System (Amazon EFS)

Amazon Elastic File System (Amazon EFS) offre uno storage di file semplice, scalabile ed elastico da utilizzare con servizi AWS cloud e risorse locali. È facile da usare e offre un'interfaccia semplice che consente ai clienti di creare e configurare file system in modo rapido e semplice. Amazon EFS è progettato per scalare in modo elastico su richiesta senza interrompere le applicazioni, e cresce e si riduce automaticamente man mano che i clienti aggiungono e rimuovono file.

Per soddisfare il requisito che i PHI siano crittografati a riposo, su EFS sono disponibili due percorsi. EFS supporta la crittografia a riposo quando viene creato un nuovo file system. Durante la creazione, è necessario selezionare l'opzione «Abilita la crittografia dei dati inattivi». La selezione di questa opzione garantisce che tutti i dati inseriti nel file system EFS vengano crittografati utilizzando la crittografia AES-256 e AWS KMS le chiavi gestite. In alternativa, i clienti possono scegliere di crittografare i dati prima che vengano inseriti in EFS, ma sono quindi responsabili della gestione del processo di crittografia e della gestione delle chiavi.

PHI non deve essere utilizzato come tutto o parte di alcun nome di file o nome di cartella. La crittografia dei PHI in transito per Amazon EFS è fornita da Transport Layer Security (TLS) tra il servizio EFS e l'istanza che monta il file system. EFS offre un supporto di montaggio per facilitare la connessione a un file system tramite TLS. Per impostazione predefinita, TLS non viene utilizzato e deve essere abilitato durante il montaggio del file system utilizzando l'helper di montaggio EFS. Assicurati che il comando mount contenga l'opzione «-o tls» per abilitare la crittografia TLS. In alternativa, i clienti che scelgono di non utilizzare l'EFS mount helper possono seguire le istruzioni nella documentazione EFS per configurare i propri client NFS per la connessione tramite un tunnel TLS.

## Amazon Elastic Kubernetes Service (Amazon EKS)

Amazon Elastic Kubernetes Service (Amazon EKS) è un servizio gestito che consente ai clienti di eseguire Kubernetes su AWS senza dover installare o mantenere il proprio piano di controllo Kubernetes. Kubernetes è un sistema open source per automatizzare l'implementazione, il dimensionamento e la gestione di applicazioni containerizzate. Per ulteriori informazioni su sicurezza e conformità, consulta il white paper Architecting for HIPAA Security and Compliance on Amazon EKS.

## Amazon ElastiCache per Redis

Amazon ElastiCache for Redis è un servizio di struttura dati in memoria compatibile con Redis che può essere utilizzato come archivio dati o cache. Per archiviare PHI, i clienti devono assicurarsi di utilizzare la versione più recente del motore Redis conforme alla normativa HIPAA e i tipi di nodi dell'attuale ElastiCache generazione. Amazon ElastiCache for Redis supporta l'archiviazione di PHI per i seguenti tipi di nodi e versioni del motore Redis:

- Tipi di nodi: solo la generazione attuale (ad esempio, al momento della pubblicazione di questo white paper, M4, M5, R4, R5, T2, T3)
- ElastiCache per la versione del motore Redis: 3.2.6 e 4.0.10 in poi

Per ulteriori informazioni sulla scelta dei nodi di generazione attuale, consulta i ElastiCache prezzi di Amazon. Per ulteriori informazioni sulla scelta di un motore ElastiCache per Redis, consulta What Is Amazon ElastiCache for Redis?

I clienti devono inoltre assicurarsi che il cluster e i nodi all'interno del cluster siano configurati per crittografare i dati inattivi, abilitare la crittografia di trasporto e abilitare l'autenticazione dei comandi

Redis. Inoltre, i clienti devono assicurarsi che i propri cluster Redis siano sempre aggiornati con gli ultimi aggiornamenti del servizio di tipo «Sicurezza» entro o prima della «Data di applicazione consigliata» (la data entro la quale si consiglia di applicare l'aggiornamento) in qualsiasi momento. Per ulteriori informazioni, consulta le sezioni seguenti.

Argomenti



## Crittografia dei dati inattivi

Amazon ElastiCache for Redis fornisce la crittografia dei dati per il suo cluster per proteggere i dati archiviati. Quando i clienti abilitano la crittografia a riposo per un cluster al momento della creazione, Amazon ElastiCache for Redis crittografa i dati su disco e i backup Redis automatici. I dati dei clienti su disco vengono crittografati utilizzando chiavi simmetriche Advanced Encryption Standard (AES) -512 con accelerazione hardware. I backup Redis sono crittografati tramite chiavi di crittografia gestite da Amazon S3 (SSE-S3). Un bucket S3 con crittografia lato server abilitata crittograferà i dati utilizzando chiavi simmetriche Advanced Encryption Standard (AES) -256 con accelerazione hardware prima di salvarli nel bucket.

Per ulteriori dettagli sulle chiavi di crittografia gestite da Amazon S3 (SSE-S3), consulta Protezione dei dati utilizzando la crittografia lato server con le chiavi di crittografia gestite da Amazon S3 (SSE-S3). Su un cluster ElastiCache Redis (singolo o multinodo) con crittografia, i dati archiviati in archivio sono crittografati in conformità con le Linee guida in vigore al momento della pubblicazione di questo white paper. Ciò include i dati su disco e i backup automatici nel bucket S3. Poiché la Guida potrebbe essere aggiornata, i clienti dovrebbero continuare a valutare e determinare se la crittografia Amazon ElastiCache for Redis soddisfa i propri requisiti di conformità e normativi. Per ulteriori informazioni sulla crittografia a riposo con Amazon ElastiCache for Redis, consulta What Is Amazon ElastiCache for Redis?

## Crittografia del trasporto

Amazon ElastiCache for Redis utilizza TLS per crittografare i dati in transito. Le connessioni a ElastiCache For Redis contenenti PHI devono utilizzare la crittografia di trasporto e

valutare la coerenza della configurazione con la Guida. Per ulteriori informazioni, consulta. CreateReplicationGroup Per ulteriori informazioni sull'attivazione della crittografia di trasporto, consulta ElastiCache Redis In-Transit Encryption (TLS).

## Autenticazione

I cluster Amazon ElastiCache for Redis (singolo/multinodo) che contengono PHI devono fornire un token Redis AUTH per abilitare l'autenticazione dei comandi Redis. Redis AUTH è disponibile quando sono abilitate sia la crittografia a riposo che la crittografia in transito. I clienti devono fornire un token sicuro per Redis AUTH con i seguenti vincoli:

- Devono essere stampabili solo caratteri ASCII
- Deve contenere almeno 16 caratteri e non più di 128 caratteri
- Non può contenere nessuno dei seguenti caratteri: '/', "" o «@»

Questo token deve essere impostato all'interno del parametro di richiesta al momento della creazione del gruppo di replica Redis (singolo/multinodo) e può essere aggiornato in seguito con un nuovo valore. AWS crittografa questo token utilizzando AWS Key Management Service (AWS KMS). Per ulteriori informazioni su Redis AUTH, consulta Redis In-Transit ElastiCache Encryption (TLS).

## Applicazione degli aggiornamenti del servizio ElastiCache

I cluster Amazon ElastiCache for Redis (singolo/multinodo) che contengono PHI devono essere aggiornati con gli ultimi aggiornamenti del servizio di tipo «Sicurezza» entro o prima della «Data di applicazione consigliata». ElastiCache offre questa funzionalità self-service che i clienti possono utilizzare per applicare gli aggiornamenti in qualsiasi momento, su richiesta e in tempo reale. Ogni aggiornamento del servizio viene fornito con «Severità» e «Applicazione consigliata per data» ed è disponibile solo per i gruppi di replica Redis applicabili.

Il campo «SLA Met» nella funzionalità di aggiornamento del servizio indicherà se l'aggiornamento è stato applicato entro o prima della «Applicazione consigliata per data». Se i clienti scelgono di non applicare gli aggiornamenti ai gruppi di replica Redis applicabili entro la «Data di applicazione consigliata», non ElastiCache intraprenderanno alcuna azione per applicarli. I clienti possono utilizzare la dashboard della cronologia degli aggiornamenti del servizio per verificare l'applicazione degli aggiornamenti ai propri gruppi di replica Redis nel tempo. Per ulteriori informazioni su come utilizzare questa funzionalità, consulta la sezione Aggiornamenti self-service in Amazon ElastiCache.

# OpenSearch Servizio Amazon

Amazon OpenSearch Service consente ai clienti di eseguire un cluster OSS Elasticsearch gestito OpenSearch o legacy in un Amazon Virtual Private Cloud (Amazon VPC) dedicato. Quando utilizzano OpenSearch Service with PHI, i clienti devono utilizzare Elasticsearch 6.0 OpenSearch o versione successiva. I clienti devono assicurarsi che il PHI sia crittografato a riposo e in transito all'interno di Amazon Service. OpenSearch I clienti possono utilizzare AWS KMS la crittografia a chiave per crittografare i dati archiviati nei loro domini di OpenSearch servizio, disponibile solo per OpenSearch Elasticsearch 5.1 o versioni successive. Per ulteriori informazioni su come crittografare i dati inattivi, consulta Encryption of data at rest for Amazon OpenSearch Service.

Ogni dominio OpenSearch di servizio viene eseguito nel proprio VPC. I clienti devono abilitare node-to-node la crittografia, disponibile in tutte le OpenSearch versioni e in Elasticsearch 6.0 o versioni successive. Se i clienti inviano dati al OpenSearch Servizio tramite HTTPS, la node-to-node crittografia aiuta a garantire che i dati rimangano crittografati durante la OpenSearch distribuzione (e la ridistribuzione) in tutto il cluster. Se i dati arrivano non crittografati tramite HTTP, OpenSearch Service li crittografa dopo che hanno raggiunto il cluster. Pertanto, qualsiasi PHI che entra in un cluster OpenSearch di Amazon Service deve essere inviato tramite HTTPS. Per ulteriori informazioni, consulta la sezione ode-to-node Crittografia N per Amazon OpenSearch Service.

I log dell'API di configurazione del OpenSearch servizio possono essere archiviati in AWS CloudTrail. Per ulteriori informazioni, consulta Monitoraggio delle chiamate API di Amazon OpenSearch Service con AWS CloudTrail.

# Amazon EMR

Amazon EMR distribuisce e gestisce un cluster di istanze Amazon EC2 nell'account di un cliente. Per informazioni sulla crittografia con Amazon EMR, consulta Opzioni di crittografia.

# Amazon EventBridge

Amazon EventBridge (precedentemente Amazon CloudWatch Events) è un bus di eventi serverless che consente di creare applicazioni scalabili basate sugli eventi. EventBridge fornisce un flusso di dati in tempo reale da fonti di eventi, come Zendesk, Datadog o Pagerduty, e indirizza tali dati verso obiettivi come. AWS Lambda

Per impostazione predefinita, EventBridge crittografa i dati utilizzando Advanced Encryption Standard (AES-256) a 256 bit con un CMK di proprietà di AWS, che aiuta a proteggere i dati dei clienti da

accessi non autorizzati. I clienti devono assicurarsi che qualsiasi risorsa AWS che emette un evento che memorizza, elabora o trasmette PHI sia configurata secondo le migliori pratiche.

Amazon EventBridge è integrato con AWS CloudTrail e i clienti possono visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Per ulteriori informazioni, consulta la sezione EventBridge Informazioni in CloudTrail.

## Amazon Forecast

Amazon Forecast è un servizio completamente gestito che utilizza l'apprendimento automatico per fornire previsioni estremamente accurate. Basato sulla stessa tecnologia di previsione basata sull'apprendimento automatico utilizzata da Amazon.com. Ogni interazione che i clienti hanno con Amazon Forecast è protetta da crittografia. Qualsiasi contenuto elaborato da Amazon Forecast viene crittografato con le chiavi del cliente tramite Amazon Key Management Service e crittografato a riposo nella regione AWS in cui i clienti utilizzano il servizio.

Amazon Forecast è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un servizio AWS in Amazon Forecast. CloudTrail acquisisce tutte le chiamate API per Amazon Forecast come eventi. Le chiamate acquisite includono chiamate dalla console Amazon Forecast e chiamate in codice alle operazioni dell'API Amazon Forecast. Se i clienti creano un percorso, possono abilitare la distribuzione continua di CloudTrail eventi in un bucket Amazon S3, inclusi gli eventi per Amazon Forecast. Per ulteriori informazioni, consulta Logging Forecast API Calls with AWS CloudTrail.

Per impostazione predefinita, i file di log forniti dal relativo bucket sono crittografati mediante CloudTrail crittografia lato server di Amazon con chiavi di crittografia gestite da Amazon S3 (SSE-S3). Per fornire un livello di sicurezza gestibile direttamente, i clienti possono invece utilizzare la crittografia lato server con chiavi gestite (SSE-KMS) per i propri file di registro. AWS KMS CloudTrail L'abilitazione della crittografia lato server consente di crittografare i file di log, ma non i file digest, con SSE-KMS. I file digest sono crittografati mediante le chiavi di crittografia gestite da Amazon S3 (SSE-S3).

AWS Forecast importa ed esporta dati da/verso i bucket S3. Quando importano ed esportano dati da Amazon S3, i clienti devono assicurarsi che i bucket S3 siano configurati in modo coerente con le linee guida. Per ulteriori informazioni, consulta Nozioni di base su .

# Amazon FSx

Amazon FSx è un servizio completamente gestito che fornisce file system ricchi di funzionalità e ad alte prestazioni. Amazon FSx for Windows File Server offre uno storage di file altamente affidabile e scalabile ed è accessibile tramite il protocollo Server Message Block (SMB). Amazon FSx for Lustre offre storage ad alte prestazioni per carichi di lavoro di elaborazione ed è alimentato da Lustre, il file system ad alte prestazioni più popolare al mondo.

Amazon FSx supporta due forme di crittografia per i file system, la crittografia dei dati in transito e la crittografia a riposo. Amazon FSx for Windows File Server supporta anche la registrazione di tutte le chiamate API che utilizzano. AWS CloudTrail

La crittografia dei dati in transito è supportata da Amazon FSx for Windows File Server su istanze di calcolo che supportano il protocollo SMB 3.0 o versione successiva e da Amazon FSx for Lustre su istanze Amazon EC2 che supportano la crittografia in transito. In alternativa, i clienti possono crittografare i dati prima di archiviarli su Amazon FSx, ma sono quindi responsabili del processo di crittografia e della gestione delle chiavi.

La crittografia dei dati inattivi viene abilitata automaticamente durante la creazione di un file system Amazon FSx, utilizzando l'algoritmo di crittografia AES-256 e le chiavi gestite. AWS KMS I dati e i metadati vengono crittografati automaticamente prima di essere scritti nel file system e decrittografati automaticamente prima di essere presentati all'applicazione. PHI non deve essere usato in nessun nome di file o cartella.

# Amazon GuardDuty

Amazon GuardDuty è un servizio gestito di rilevamento delle minacce che monitora continuamente i comportamenti dannosi o non autorizzati per aiutare i clienti a proteggere i propri account e carichi di lavoro AWS. Monitora attività come chiamate API insolite o implementazioni potenzialmente non autorizzate che indicano una possibile compromissione dell'account. Amazon rileva GuardDuty anche istanze o sistemi di ricognizione potenzialmente compromessi da parte degli aggressori.

Amazon monitora e analizza GuardDuty continuamente le seguenti fonti di dati: log di flusso VPC, registri AWS CloudTrail eventi e registri DNS. Utilizza feed di intelligence sulle minacce, come elenchi di IP e domini dannosi, e l'apprendimento automatico per identificare attività impreviste e potenzialmente non autorizzate e dannose all'interno di un ambiente AWS. Pertanto, Amazon non GuardDuty dovrebbe riscontrare alcun PHI poiché questi dati non devono essere archiviati in nessuna delle fonti di dati basate su AWS elencate sopra.

# Amazon HealthLake

Amazon HealthLake consente ai clienti del settore sanitario e delle scienze della vita di archiviare, trasformare, interrogare e analizzare i dati sanitari su scala petabyte. I clienti possono utilizzare Amazon HealthLake per trasmettere, elaborare e archiviare PHI. Per impostazione predefinita, Amazon HealthLake crittografa i dati inattivi negli archivi dati dei clienti. Tutti i dati e i metadati del servizio sono crittografati con una chiave KMS di proprietà del servizio. In base alle specifiche Fast Healthcare Interoperability Resources (FHIR), se un cliente elimina una risorsa FHIR, questa verrà nascosta solo al recupero e verrà conservata dal servizio per il controllo delle versioni. Quando i clienti utilizzano l'ImportJob API StartFHIR, Amazon HealthLake applicherà l'obbligo di esportare i dati in un bucket Amazon S3 crittografato.

Amazon HealthLake crittografa i dati sia in transito che a riposo. Per la crittografia dei dati in transito, puoi utilizzare le chiamate API pubblicate da AWS per accedere HealthLake tramite la rete. I client devono supportare Transport Layer Security (TLS) 1.0 o versioni successive. È richiesto TLS 1.2 ed è consigliato TLS 1.3. I client devono, inoltre, supportare le suite di crittografia con PFS (Perfect Forward Secrecy), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità. Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa, i clienti possono utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per firmare le richieste. Per la crittografia dei dati inattivi, Amazon HealthLake crittografa i dati negli archivi dati dei clienti con una chiave AWS KMS di proprietà del cliente o con una chiave AWS KMS di proprietà del servizio per impostazione predefinita. Tutti i dati e i metadati del servizio sono crittografati quando sono inattivi con una chiave AWS KMS di proprietà del servizio.

Amazon HealthLake è integrato con AWS CloudTrail. CloudTrail acquisisce tutte le chiamate API ad Amazon HealthLake come eventi, incluse le chiamate effettuate a seguito dell'interazione con AWS Management Console l'interfaccia a riga di comando (CLI) e utilizzando programmaticamente il kit di sviluppo software (SDK).

# Amazon Inspector

Amazon Inspector è un servizio di valutazione della sicurezza automatizzato per i clienti che desiderano migliorare la sicurezza e la conformità delle applicazioni distribuite su AWS. Amazon Inspector valuta automaticamente le applicazioni per rilevare vulnerabilità o deviazioni dalle best practice. Dopo aver eseguito una valutazione, Amazon Inspector produce un elenco dettagliato di risultati di sicurezza con priorità in base al livello di gravità. I clienti possono eseguire Amazon

Inspector su istanze EC2 che contengono PHI. Amazon Inspector crittografa tutti i dati trasmessi sulla rete e tutti i dati di telemetria archiviati in archivio.

## Servizio gestito da Amazon per Apache Flink

Amazon Managed Service per Apache Flink consente ai clienti di creare rapidamente codice SQL che legge, elabora e archivia continuamente i dati quasi in tempo reale. Utilizzando query SQL standard sui dati di streaming, i clienti possono creare applicazioni che trasformano e forniscono approfondimenti sui propri dati. Managed Service for Apache Flink supporta gli input dei flussi di distribuzione Kinesis Data Streams e Firehose come fonti per applicazioni di analisi. Se lo stream è crittografato, Managed Service for Apache Flink accede ai dati nello stream crittografato senza ulteriori configurazioni. Il servizio gestito per Apache Flink non archivia i dati non crittografati letti da Kinesis Data Streams. Per ulteriori informazioni, consulta Configurazione dell'input delle applicazioni.

Managed Service for Apache Flink si integra sia con Amazon Logs che con AWS CloudTrail Amazon CloudWatch Logs per il monitoraggio delle applicazioni. Per ulteriori informazioni, consulta Monitoring Tools e Working with Amazon CloudWatch Logs.

## Amazon Data Firehose

Quando i clienti inviano dati dai loro produttori di dati al loro flusso di dati Kinesis, Amazon Kinesis Data Streams crittografa i dati utilizzando AWS KMS una chiave prima di archiviarli su disco. Quando il flusso di distribuzione Firehose legge i dati dal flusso Kinesis, Kinesis Data Streams prima decrittografa i dati e poi li invia a Firehose. Firehose memorizza i dati in memoria in base ai suggerimenti di buffering specificati dal cliente.

Quindi consegna i dati alle destinazioni senza archiviare i dati non crittografati a riposo. Per ulteriori informazioni sulla crittografia con Firehose, consulta la sezione Protezione dei dati in Amazon Data Firehose.

AWS fornisce diversi strumenti che i clienti possono utilizzare per monitorare Amazon Data Firehose, tra cui i CloudWatch parametri Amazon, Amazon CloudWatch Logs, Kinesis Agent e la cronologia delle API. Per ulteriori informazioni, consulta Monitoring Amazon Data Firehose.

## Amazon Kinesis Streams

Amazon Kinesis Streams consente ai clienti di creare applicazioni personalizzate che elaborano o analizzano dati di streaming per esigenze specifiche. La funzionalità di crittografia lato server

consente ai clienti di crittografare i dati inattivi. Quando la crittografia lato server è abilitata, Kinesis Streams utilizzerà una AWS KMS chiave per crittografare i dati prima di archiviarli su dischi. Per ulteriori informazioni, consulta Protezione dei dati in Amazon Kinesis Data Streams. Le connessioni ad Amazon S3 contenenti PHI devono utilizzare endpoint che accettano il trasporto crittografato (ovvero HTTPS). Per un elenco degli endpoint regionali, consulta AWS service endpoints.

## Flusso di video Amazon Kinesis

Amazon Kinesis Video Streams è un servizio AWS completamente gestito che i clienti possono utilizzare per lo streaming di video in diretta dai dispositivi al cloud AWS o creare applicazioni per l'elaborazione video in tempo reale o l'analisi video orientata ai batch. La crittografia lato server è una funzionalità di Kinesis Video Streams che crittografa automaticamente i dati inattivi utilizzando AWS KMS una chiave (precedentemente CMK) specificata dal cliente. I dati vengono crittografati prima di essere scritti sul livello di archiviazione dello stream di Kinesis Video Streams e vengono decrittografati dopo essere stati recuperati dallo storage.

L'SDK Amazon Kinesis Video Streams può essere utilizzato per trasmettere dati video in streaming contenenti PHI. Per impostazione predefinita, l'SDK utilizza TLS per crittografare frame e frammenti generati dal dispositivo hardware su cui è installato. L'SDK non gestisce né influisce sui dati archiviati in archivio. Amazon Kinesis Video AWS CloudTrail Streams utilizza per registrare tutte le chiamate API.

## Amazon Lex

Amazon Lex è un servizio AWS per la creazione di interfacce conversazionali per applicazioni che utilizzano voce e testo. Con Amazon Lex, lo stesso motore conversazionale che alimenta Amazon Alexa è ora disponibile per tutti gli sviluppatori, permettendo ai clienti di creare chatbot sofisticati in linguaggio naturale nelle loro applicazioni nuove ed esistenti. Amazon Lex offre le funzionalità e la flessibilità avanzate della comprensione del linguaggio naturale (NLU) e del riconoscimento vocale automatico (ASR) in modo che i clienti possano creare esperienze utente altamente coinvolgenti con interazioni conversazionali realistiche e creare nuove categorie di prodotti.

Lex utilizza il protocollo HTTPS per comunicare sia con i client che con altri servizi AWS. L'accesso a Lex è basato su API e può essere applicato il privilegio minimo IAM appropriato. Per ulteriori informazioni, consulta la sezione Protezione dei dati in Amazon Lex.

Il monitoraggio è importante per mantenere l'affidabilità, la disponibilità e le prestazioni dei chatbot Amazon Lex dei clienti. Per monitorare lo stato dei bot di Amazon Lex, usa Amazon CloudWatch.

Con CloudWatch, i clienti possono ottenere parametri per le singole operazioni Amazon Lex o per le operazioni globali di Amazon Lex per il proprio account. I clienti possono anche impostare CloudWatch allarmi per ricevere notifiche quando una o più metriche superano una soglia definita dai clienti. Ad esempio, i clienti possono monitorare il numero di richieste fatte a un bot in un determinato periodo di tempo, visualizzare la latenza delle richieste riuscite o generare un allarme quando gli errori superano una soglia. Lex è inoltre integrato AWS CloudTrail per registrare le chiamate API Lex. Per ulteriori informazioni, consulta Monitoraggio in Amazon Lex.

## Amazon Managed Streaming for Apache Kafka (Amazon MSK)

Amazon MSK offre funzionalità di crittografia per i dati inattivi e per i dati in transito. Per la crittografia dei dati a riposo, il cluster Amazon MSK utilizza la crittografia e le AWS KMS chiavi lato server di Amazon EBS per crittografare i volumi di storage. Per i dati in transito, i cluster Amazon MSK dispongono di crittografia abilitata tramite TLS per la comunicazione tra broker.

L'impostazione di configurazione della crittografia è abilitata quando viene creato un cluster. Inoltre, per impostazione predefinita, la crittografia in transito è impostata su TLS per i cluster creati da CLI o Console. AWS È necessaria una configurazione aggiuntiva per consentire ai client di comunicare con i cluster utilizzando la crittografia TLS. I clienti possono modificare l'impostazione di crittografia predefinita selezionando le impostazioni TLS/PlainText. Per ulteriori informazioni, consulta Amazon MSK Encryption.

I clienti possono monitorare le prestazioni dei cluster dei clienti utilizzando la console Amazon MSK, la CloudWatch console Amazon oppure possono accedere a JMX e alle metriche di hosting utilizzando Open Monitoring with Prometheus, una soluzione di monitoraggio open source.

Gli strumenti progettati per leggere dagli esportatori di Prometheus sono compatibili con Open Monitoring, come: Datadog, Lenses, New Relic, Sumologic o un server Prometheus. Per dettagli su Open Monitoring, consulta la documentazione di Amazon MSK Open Monitoring.

Tieni presente che la versione predefinita di Apache Zookeeper fornita in bundle con Apache Kafka non supporta la crittografia. Tuttavia, è importante notare che le comunicazioni tra i broker Apache Zookeeper e Apache Kafka si limitano alle informazioni sul broker, sull'argomento e sullo stato della partizione. L'unico modo in cui i dati possono essere prodotti e consumati da un cluster Amazon MSK è tramite una connessione privata tra i loro client nel loro VPC e il cluster Amazon MSK. Amazon MSK non supporta gli endpoint pubblici.

# Amazon MQ

Amazon MQ è un servizio di broker di messaggi gestito per Apache ActiveMQ che semplifica la configurazione e la gestione di broker di messaggi nel cloud. Amazon MQ funziona con applicazioni e servizi esistenti senza che il cliente debba gestire, utilizzare o mantenere il proprio sistema di messaggistica. Per fornire la crittografia dei dati PHI durante il transito, è necessario utilizzare i seguenti protocolli con TLS abilitato per accedere ai broker:

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

Amazon MQ crittografa i messaggi inattivi e in transito utilizzando chiavi di crittografia che gestisce e archivia in modo sicuro. Amazon MQ lo utilizza CloudTrail per registrare tutte le chiamate API.

# Amazon Neptune

Amazon Neptune è un servizio di database a grafo gestito rapido e affidabile che rende più semplice la creazione e l'esecuzione di applicazioni che funzionano con set di dati altamente connessi. Il cuore di Amazon Neptune è un motore di database grafico appositamente progettato e ad alte prestazioni, ottimizzato per archiviare miliardi di relazioni e interrogare il grafico con una latenza di millisecondi. Amazon Neptune supporta i più diffusi linguaggi di query grafiche TinkerPop Apache Gremlin e SPARQL del W3C.

I dati contenenti PHI possono ora essere conservati in un'istanza crittografata di Amazon Neptune. Un'istanza crittografata di Amazon Neptune può essere specificata solo al momento della creazione scegliendo «Abilita crittografia» dalla console Amazon Neptune. Tutti i log, i backup e le istantanee sono crittografati per un'istanza crittografata di Amazon Neptune. La gestione delle chiavi per le istanze crittografate di Amazon Neptune viene fornita tramite. AWS KMS La crittografia dei dati in transito viene fornita tramite SSL/TLS. Amazon Neptune CloudTrail utilizza per registrare tutte le chiamate API.

# AWS Network Firewall

AWS Network Firewall è un servizio firewall gestito che semplifica l'implementazione delle protezioni di rete essenziali per tutti i tuoi Amazon Virtual Private Cloud (Amazon VPC). Il servizio si adatta automaticamente al volume del traffico di rete per fornire protezioni ad alta disponibilità senza la necessità di configurare o mantenere l'infrastruttura sottostante. Sia le regole del cliente che i registri di accesso possono contenere indirizzi IP degli utenti finali, che sono crittografati sia a riposo che in transito all'interno dell'architettura. AWS Inoltre, AWS Network Firewall crittografa tutti i dati inattivi e in transito tra AWS i servizi componenti (Amazon S3, Amazon DynamoDB, Amazon Logs, Amazon CloudWatch EBS). Il servizio crittografa automaticamente i dati senza richiedere una configurazione speciale.

# Amazon Pinpoint

Amazon Pinpoint offre agli sviluppatori un singolo livello API, supporto CLI e supporto SDK lato client per estendere i canali di comunicazione delle applicazioni con gli utenti. I canali idonei includono: e-mail, messaggi di testo SMS, notifiche push per dispositivi mobili e canali personalizzati. Amazon Pinpoint fornisce anche un sistema di analisi che tiene traccia del comportamento e del coinvolgimento degli utenti delle app. Grazie a questo servizio, gli sviluppatori possono scoprire in che modo ogni utente preferisce interagire e personalizzare l'esperienza dell'utente per aumentarne la soddisfazione.

Amazon Pinpoint aiuta anche gli sviluppatori a risolvere diversi casi d'uso della messaggistica, come la messaggistica diretta o transazionale, la messaggistica mirata o basata su campagne e la messaggistica basata su eventi. Integrando e abilitando tutti i canali di coinvolgimento degli utenti finali tramite Amazon Pinpoint, gli sviluppatori possono creare una visione a 360 gradi del coinvolgimento degli utenti in tutti i punti di contatto con i clienti. Amazon Pinpoint archivia i dati di utenti, endpoint ed eventi in modo che i clienti possano creare segmenti, inviare messaggi ai destinatari e acquisire dati sul coinvolgimento.

Amazon Pinpoint crittografa i dati sia a riposo che in transito. Per ulteriori informazioni, consulta le domande frequenti su Amazon Pinpoint. Sebbene Amazon Pinpoint crittografi tutti i dati inattivi e in transito, il canale finale, come SMS o e-mail, potrebbe non essere crittografato e i clienti devono configurare qualsiasi canale in modo coerente con i propri requisiti.

Inoltre, i clienti che devono inviare PHI tramite il canale SMS devono utilizzare un codice breve dedicato (numeri di telefono di origine a 5, 6 cifre) allo scopo esplicito di inviare PHI. Per ulteriori

informazioni su come richiedere un codice breve, consulta Richiesta di codici brevi dedicati per la messaggistica SMS con Amazon Pinpoint. I clienti possono anche scegliere di non inviare PHI attraverso il canale finale e fornire invece un meccanismo per accedere in modo sicuro a PHI tramite HTTPS.

Le chiamate API verso Amazon Pinpoint possono essere acquisite utilizzando. AWS CloudTrail Le chiamate acquisite includono quelle provenienti dalla console Amazon Pinpoint e le chiamate in codice alle operazioni dell'API Amazon Pinpoint. Se i clienti creano un percorso, possono abilitare la distribuzione continua di AWS CloudTrail eventi in un bucket Amazon S3, inclusi gli eventi per Amazon Pinpoint. Se i clienti non configurano un percorso, possono comunque visualizzare gli eventi più recenti utilizzando la cronologia degli eventi sulla console. AWS CloudTrail Utilizzando le informazioni raccolte da AWS CloudTrail, i clienti possono determinare che la richiesta è stata effettuata ad Amazon Pinpoint, l'indirizzo IP della richiesta, chi ha effettuato la richiesta, quando è stata effettuata la richiesta e ulteriori dettagli. Per ulteriori informazioni, consulta Registrazione delle chiamate API Amazon Pinpoint con. AWS CloudTrail

## Amazon Polly

Amazon Polly è un servizio cloud che converte il testo in voce naturale. Amazon Polly offre operazioni API semplici che i clienti possono integrare facilmente con le applicazioni esistenti. Amazon Polly utilizza il protocollo HTTPS per comunicare con i client. L'accesso ad Amazon Polly è basato su API ed è possibile applicare il privilegio minimo IAM appropriato. Per ulteriori informazioni, consulta Protezione dei dati. Alcuni esempi di casi d'uso che includono PHI:

- Il caregiver converte un rapporto di testo contenente PHI in un discorso sintetizzato in modo che possa ascoltare il rapporto mentre cammina o svolge altre mansioni.
- Al paziente ipovedente viene fornita assistenza medica e la utilizza sotto forma di linguaggio sintetizzato.

Il canale di distribuzione finale di Amazon Polly potrebbe comportare la riproduzione di audio con PHI in uno spazio pubblico e occorre prendere precauzioni affinché la consegna tenga conto di questo aspetto. L'output vocale sintetizzato può anche essere inviato in modo asincrono a un bucket Amazon S3 con crittografia abilitata.

Quando si verifica un'attività di evento supportata in Amazon Polly, tale attività viene registrata in un AWS CloudTrail evento insieme ad altri eventi di AWS servizio nella Cronologia eventi. Per una registrazione continua degli eventi in un AWS account cliente, inclusi gli eventi per Amazon

Polly, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Utilizzando le informazioni raccolte da CloudTrail, i clienti possono determinare la richiesta effettuata ad Amazon Polly, l'indirizzo IP da cui è stata effettuata, chi ha effettuato la richiesta, quando è stata effettuata e ulteriori dettagli.

## Database Amazon Quantum Ledger (Amazon QLDB)

Amazon QLDB è un database di libro mastro completamente gestito che, in modo trasparente, immutabile, crittografato e verificabile, fornisce un log delle transazioni appartenenti a un'autorità centrale attendibile. Amazon QLDB tiene traccia di ogni singola modifica dei dati delle applicazioni e mantiene una cronologia completa e verificabile delle modifiche nel tempo. I dati contenenti PHI possono ora essere conservati in un'istanza QLDB. Per impostazione predefinita, tutti i dati Amazon QLDB in transito e a riposo sono crittografati. I dati in transito vengono crittografati tramite TLS e i dati inattivi vengono crittografati utilizzando AWS chiavi gestite. Ai fini della protezione dei dati, consigliamo ai clienti di proteggere le credenziali degli AWS account e di configurare account utente individuali con AWS Identity and Access Management (IAM), in modo che a ciascun utente vengano concesse solo le autorizzazioni necessarie per svolgere le proprie mansioni lavorative. Per ulteriori informazioni, consulta la sezione Protezione dei dati in Amazon QLDB.

Amazon QLDB è integrato AWS CloudTrail con un servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio in QLDB. CloudTrail acquisisce tutte le chiamate API del piano di controllo per QLDB come eventi. Le chiamate acquisite includono chiamate dalla console QLDB e chiamate di codice alle operazioni dell'API QLDB. Se i clienti creano un trail, possono abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon Simple Storage Service (Amazon S3), inclusi gli eventi per QLDB. Se i clienti non configurano un percorso, possono comunque visualizzare gli eventi più recenti sulla CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, i clienti possono determinare la richiesta effettuata a QLDB, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

## Amazon QuickSight

Amazon QuickSight è un servizio di analisi aziendale che i clienti possono utilizzare per creare visualizzazioni, eseguire analisi ad hoc e ottenere rapidamente informazioni aziendali dai propri dati. Amazon QuickSight individua le fonti di AWS dati, consente alle organizzazioni di scalare fino a centinaia di migliaia di utenti e offre prestazioni reattive utilizzando un robusto motore in-memory (SPICE).

I clienti possono utilizzare l'edizione Enterprise di Amazon solo QuickSight per lavorare con dati contenenti PHI in quanto fornisce supporto per la crittografia dei dati archiviati in archivio in SPICE. La crittografia dei dati viene eseguita utilizzando AWS chiavi gestite.

## Amazon RDS per MariaDB

Amazon RDS for MariaDB consente ai clienti di crittografare i database MariaDB utilizzando le chiavi tramite le quali gestiscono. AWS KMS Su un'istanza di database che utilizza la crittografia Amazon RDS, i dati archiviati a riposo nello storage sottostante sono crittografati in conformità con le Linee guida in vigore al momento della pubblicazione di questo white paper, così come i backup automatici, le repliche di lettura e le istantanee.

Poiché la Guida potrebbe essere aggiornata, i clienti devono continuare a valutare e determinare se la crittografia Amazon RDS for MariaDB soddisfa i requisiti normativi e di conformità. Per ulteriori informazioni sulla crittografia a riposo con Amazon RDS, consulta Encrypting Amazon RDS Resources.

Le connessioni a RDS per MariadB contenenti PHI devono utilizzare la crittografia di trasporto. Per ulteriori informazioni sull'abilitazione delle connessioni crittografate, consulta Uso di SSL/TLS per crittografare una connessione a un'istanza DB.

## Amazon RDS per MySQL

Amazon RDS for MySQL consente ai clienti di crittografare i database MySQL utilizzando chiavi gestite dai clienti. AWS KMS Su un'istanza di database che utilizza la crittografia Amazon RDS, i dati archiviati a riposo nello storage sottostante sono crittografati in conformità con le Linee guida in vigore al momento della pubblicazione di questo white paper, così come i backup automatici, le repliche di lettura e le istantanee.

Poiché la Guida potrebbe essere aggiornata, i clienti devono continuare a valutare e determinare se la crittografia Amazon RDS for MySQL soddisfa i requisiti normativi e di conformità. Per ulteriori informazioni sulla crittografia a riposo con Amazon RDS, consulta Encrypting Amazon RDS Resources.

Le connessioni a RDS for MySQL contenenti PHI devono utilizzare la crittografia di trasporto. Per ulteriori informazioni sull'abilitazione delle connessioni crittografate, consulta Uso di SSL/TLS per crittografare una connessione a un'istanza DB.

# Amazon RDS per Oracle

I clienti hanno a disposizione diverse opzioni per crittografare PHI a riposo utilizzando Amazon RDS for Oracle. I clienti possono crittografare i database Oracle utilizzando le chiavi tramite le quali gestiscono. AWS KMS Su un'istanza di database che utilizza la crittografia Amazon RDS, i dati archiviati a riposo nello storage sottostante sono crittografati in conformità con le Linee guida in vigore al momento della pubblicazione di questo white paper, così come i backup automatici, le repliche di lettura e le istantanee.

Poiché la Guida potrebbe essere aggiornata, i clienti devono continuare a valutare e determinare se la crittografia Amazon RDS for Oracle soddisfa i requisiti normativi e di conformità. Per ulteriori informazioni sulla crittografia a riposo con Amazon RDS, consulta Encrypting Amazon RDS Resources.

I clienti possono anche utilizzare Oracle Transparent Data Encryption (TDE) e devono valutare la configurazione per verificarne la coerenza con la Guida. Oracle TDE è una funzionalità dell'opzione Oracle Advanced Security disponibile in Oracle Enterprise Edition. Tale caratteristica consente la crittografia automatica dei dati prima che vengano trascritti nello storage e la loro decriptazione automatica durante la lettura dallo storage. I clienti possono anche utilizzare AWS CloudHSM per archiviare le chiavi Amazon RDS Oracle TDE. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Crittografia trasparente dei dati di Amazon RDS per Oracle: crittografia trasparente dei dati Oracle.
- Utilizzo AWS CloudHSM per archiviare le chiavi Oracle TDE di Amazon RDS: cos'è Amazon Relational Database Service (Amazon RDS)?

Le connessioni ad Amazon RDS for Oracle contenenti PHI devono utilizzare la crittografia di trasporto e valutare la coerenza della configurazione con la Guida. Questa operazione viene eseguita utilizzando Oracle Native Network Encryption e abilitata nei gruppi di opzioni Amazon RDS for Oracle. Per informazioni dettagliate, consulta Oracle Native Network Encryption.

# Amazon RDS per PostgreSQL

Amazon RDS for PostgreSQL consente ai clienti di crittografare i database PostgreSQL utilizzando chiavi gestite dai clienti. AWS KMS Su un'istanza di database che utilizza la crittografia Amazon RDS, i dati archiviati a riposo nello storage sottostante sono crittografati in conformità con le Linee

guida in vigore al momento della pubblicazione di questo white paper, così come i backup automatici, le repliche di lettura e le istantanee.

Poiché la Guida potrebbe essere aggiornata, i clienti devono continuare a valutare e determinare se la crittografia Amazon RDS for PostgreSQL soddisfa i requisiti normativi e di conformità. Per ulteriori informazioni sulla crittografia a riposo con Amazon RDS, consulta Encrypting Amazon RDS Resources.

Le connessioni a RDS for PostgreSQL contenenti PHI devono utilizzare la crittografia di trasporto. Per ulteriori informazioni sull'abilitazione delle connessioni crittografate, consulta Utilizzo di SSL/TLS per crittografare una connessione a un'istanza DB.

# Amazon RDS per SQL Server

RDS per SQL Server supporta l'archiviazione di PHI per le seguenti combinazioni di versioni ed edizioni:

- 2008 R2 - Solo Enterprise Edition
- 2012, 2014 e 2016 - Edizioni Web, Standard ed Enterprise

Importante: l'edizione SQL Server Express non è supportata e non deve mai essere utilizzata per l'archiviazione di PHI.

Per archiviare i dati PHI, i clienti devono assicurarsi che l'istanza sia configurata per crittografare i dati inattivi e abilitare la crittografia e il controllo del trasporto, come descritto di seguito.

## Crittografia dei dati inattivi

I clienti possono crittografare i database di SQL Server utilizzando le chiavi tramite le quali gestiscono. AWS KMS Su un'istanza di database in esecuzione con crittografia Amazon RDS, i dati archiviati inattivi nello storage sottostante sono crittografati in conformità con le Linee guida in vigore al momento della pubblicazione di questo white paper, così come i backup automatici e le istantanee. Poiché la Guida potrebbe essere aggiornata, i clienti devono continuare a valutare e determinare se la crittografia Amazon RDS for SQL Server soddisfa i requisiti normativi e di conformità. Per ulteriori informazioni sulla crittografia a riposo con Amazon RDS, consulta Encrypting Amazon RDS Resources.

Se i clienti utilizzano SQL Server Enterprise Edition, possono utilizzare Server Transparent Data Encryption (TDE) come alternativa. Tale caratteristica consente la crittografia automatica dei dati

prima che vengano trascritti nello storage e la loro decriptazione automatica durante la lettura dallo storage. Per ulteriori informazioni su RDS per SQL Server Transparent Data Encryption, vedere Support for Transparent Data Encryption in SQL Server.

### Crittografia del trasporto

Le connessioni ad Amazon RDS for SQL Server contenenti PHI devono utilizzare la crittografia di trasporto fornita da SQL Server Forced SSL. L'SSL forzato è abilitato all'interno del gruppo di parametri per Amazon RDS SQL Server. Per ulteriori informazioni su RDS per SQL Server Forced SSL, vedere Utilizzo di SSL con un'istanza DB di Microsoft SQL Server.

### Audit

Le istanze di RDS per SQL Server che contengono PHI devono avere il controllo abilitato. Il controllo è abilitato all'interno del gruppo di parametri per Amazon RDS SQL Server. Per ulteriori informazioni sul controllo di RDS per SQL Server, vedere Supporto del programma di conformità per le istanze database di Microsoft SQL Server.

## Amazon Redshift

Amazon Redshift fornisce la crittografia dei database per i suoi cluster per aiutare a proteggere i dati inattivi. Quando i clienti abilitano la crittografia per un cluster, Amazon Redshift crittografa tutti i dati, inclusi i backup, utilizzando chiavi simmetriche Advanced Encryption Standard (AES) -256 con accelerazione hardware. Per la crittografia Amazon Redshift usa un'architettura a quattro livelli basata su chiavi. Queste chiavi sono costituite da chiavi di crittografia dei dati, una chiave di database, una chiave cluster e una chiave KMS.

La chiave del cluster crittografa la chiave di database per il cluster Amazon Redshift. I clienti possono utilizzare una delle due AWS KMS o una AWS CloudHSM (Hardware Security Module) per gestire la chiave del cluster. La crittografia a riposo di Amazon Redshift è coerente con la Guida in vigore al momento della pubblicazione di questo white paper. Poiché la Guida potrebbe essere aggiornata, i clienti dovrebbero continuare a valutare e determinare se la crittografia Amazon Redshift soddisfa i requisiti normativi e di conformità. Per ulteriori informazioni, consulta Crittografia dei database di Amazon Redshift.

Le connessioni ad Amazon Redshift contenenti PHI devono utilizzare la crittografia di trasporto e i clienti devono valutare la coerenza della configurazione con la Guida. Per ulteriori informazioni, consulta Configurazione delle opzioni di sicurezza delle connessioni. Amazon Redshift Spectrum

consente ai clienti di eseguire query SQL di Amazon Redshift su exabyte di dati in Amazon S3. Redshift Spectrum è una funzionalità di Amazon Redshift e quindi rientra anche nell'ambito del BAA HIPAA.

## Amazon Rekognition

Amazon Rekognition semplifica l'aggiunta di analisi di immagini e video alle applicazioni dei clienti. Un cliente deve solo fornire un'immagine o un video all'API Amazon Rekognition e il servizio può identificare oggetti, persone, testo, scene e attività, nonché rilevare eventuali contenuti inappropriati. Amazon Rekognition fornisce anche analisi e riconoscimento facciali estremamente accurati.

Amazon Rekognition è idoneo a utilizzare immagini o video contenenti PHI. Amazon Rekognition funziona come servizio gestito e non presenta opzioni configurabili per la gestione dei dati. Amazon Rekognition utilizza, divulga e mantiene il PHI solo nella misura consentita dai termini della BAA. AWS Tutti i dati sono crittografati quando sono archiviati e in transito con Amazon Rekognition. Amazon AWS CloudTrail Rekognition utilizza per registrare tutte le chiamate API.

## Amazon Route 53

Amazon Route 53 è un servizio DNS gestito che offre ai clienti la possibilità di registrare nomi di dominio, indirizzare il traffico Internet alle risorse del dominio dei clienti e verificare lo stato di tali risorse. Sebbene Amazon Route 53 sia un servizio idoneo alla normativa HIPAA, nessun PHI deve essere memorizzato nei nomi o nei tag di risorse all'interno di Amazon Route 53, poiché non è disponibile alcun supporto per la crittografia di tali dati. Invece, Amazon Route 53 può essere utilizzato per fornire l'accesso a risorse del dominio del cliente che trasmettono o archiviano PHI, come server Web in esecuzione su Amazon EC2 o storage come Amazon S3.

## Amazon S3 Glacier

Amazon S3 Glacier crittografa automaticamente i dati inattivi utilizzando chiavi simmetriche AES a 256 bit e supporta il trasferimento sicuro dei dati dei clienti tramite protocolli sicuri. Le connessioni ad Amazon S3 Glacier contenenti PHI devono utilizzare endpoint che accettano il trasporto crittografato (HTTPS). Per un elenco degli endpoint regionali, consulta Service Endpoint.AWS

Non utilizzare PHI nei nomi o nei metadati di archivi e vault perché questi dati non sono crittografati utilizzando la crittografia lato server di Amazon S3 Glacier e generalmente non sono crittografati nelle architetture di crittografia lato client.

# Amazon S3 Transfer Acceleration

Amazon S3 Transfer Acceleration (S3TA) consente trasferimenti rapidi, facili e sicuri di file su lunghe distanze tra il client di un cliente e un bucket S3. Transfer Acceleration sfrutta le edge location distribuite a livello globale CloudFront di Amazon. Quando arrivano in una edge location, i dati vengono instradati ad Amazon S3 su un percorso di rete ottimizzato. I clienti devono assicurarsi che tutti i dati contenenti PHI trasferiti tramite AWS S3TA siano crittografati in transito e archiviati. Consulta la Guida per Amazon S3 per comprendere le opzioni di crittografia disponibili.

# Amazon SageMaker

Amazon SageMaker è un servizio di machine learning completamente gestito. Con Amazon SageMaker, data scientist e sviluppatori possono creare e addestrare modelli di machine learning in modo rapido e semplice e poi distribuirli direttamente in un ambiente ospitato pronto per la produzione. Fornisce un'istanza Jupyter authoring notebook integrata per un facile accesso alle fonti di dati per l'esplorazione e l'analisi. Amazon fornisce SageMaker anche algoritmi di machine learning comuni ottimizzati per funzionare in modo efficiente su dati estremamente grandi in un ambiente distribuito.

Con supporto bring-your-own-algorithms e framework nativi, Amazon SageMaker offre opzioni di formazione distribuite flessibili che si adattano ai flussi di lavoro specifici del cliente. Amazon SageMaker è idoneo a operare con dati contenenti PHI. La crittografia dei dati in transito è fornita da SSL/TLS e viene utilizzata sia per comunicare con l'interfaccia front-end di Amazon (verso il Notebook) sia ogni volta che Amazon SageMaker interagisce con qualsiasi altro AWS servizio SageMaker (ad esempio, estraendo dati da Amazon S3).

Per soddisfare il requisito che i PHI siano crittografati a riposo, la crittografia dei dati archiviati con l'istanza che esegue modelli con Amazon SageMaker è abilitata utilizzando AWS Key Management Service (KMS) durante la configurazione dell'endpoint (DescribeEndpointConfig: ID). KmsKey La crittografia dei risultati di addestramento del modello (artefatti) è abilitata utilizzando AWS KMS e le chiavi devono essere specificate utilizzando l'ID nella descrizione. KmsKey OutputDataConfig Se non viene fornito un ID chiave KMS, verrà utilizzata la chiave KMS Amazon S3 predefinita per l'account del ruolo. Amazon SageMaker lo utilizza AWS CloudTrail per registrare tutte le chiamate API.

# Servizio di notifica semplice Amazon (Amazon Simple Notification Service (Amazon SNS))

I clienti devono comprendere i seguenti requisiti di crittografia chiave per utilizzare Amazon Simple Notification Service (SNS) con Protected Health Information (PHI). I clienti devono utilizzare l'endpoint dell'API HTTPS fornito da SNS in ogni regione. AWS L'endpoint HTTPS sfrutta connessioni crittografate e protegge la privacy e l'integrità dei dati inviati a. AWSPer un elenco di tutti gli endpoint dell'API HTTPS, consulta AWS Service Endpoint.

Inoltre, Amazon SNS utilizza CloudTrail un servizio che acquisisce le chiamate API effettuate da o per conto di Amazon SNS nell' AWS account del cliente e invia i file di registro a un bucket Amazon S3 da lui specificato. CloudTrail acquisisce le chiamate API effettuate dalla console Amazon SNS o dall'API Amazon SNS. Utilizzando le informazioni raccolte da CloudTrail, i clienti possono determinare quale richiesta è stata effettuata ad Amazon SNS, l'indirizzo IP di origine da cui è stata effettuata la richiesta, chi ha effettuato la richiesta e quando è stata effettuata. Per ulteriori informazioni sulla registrazione delle operazioni SNS, consulta Registrazione delle chiamate API Amazon SNS tramite. CloudTrail

# Amazon Simple Email Service (Amazon SES)

Amazon Simple Email Service (Amazon SES) Simple Email Service (Amazon SES) è un servizio di invio e ricezione e-mail flessibile e altamente scalabile. Supporta i protocolli S/MIME e PGP per crittografare i messaggi per una end-to-end crittografia completa e tutte le comunicazioni con Amazon SES sono protette tramite SSL (TLS 1.2). I clienti hanno la possibilità di archiviare i messaggi crittografati in archivio configurando Amazon SES per ricevere e crittografare i messaggi prima di archiviarli in un bucket Amazon S3. Per ulteriori informazioni, consulta Come AWS KMS utilizza Amazon Simple Email Service (Amazon SES) per ulteriori informazioni sulla crittografia dei messaggi per lo storage. I messaggi sono protetti durante il transito verso Amazon SES tramite un endpoint HTTPS o una connessione SMTP crittografata.

Per i messaggi inviati da Amazon SES a un destinatario, Amazon SES tenterà innanzitutto di stabilire una connessione sicura al server di posta ricevente, ma se non è possibile stabilire una connessione sicura, invierà il messaggio in formato non crittografato. Per richiedere la crittografia per la consegna a un destinatario, i clienti devono creare un set di configurazione in Amazon SES e utilizzare il AWS CLI per impostare la TlsPolicy proprietà su Require. Per ulteriori informazioni, consulta Amazon SES e i protocolli di sicurezza. Amazon SES si integra con AWS CloudTrail per monitorare tutte le chiamate API. Utilizzando le informazioni raccolte da AWS CloudTrail, i clienti possono determinare

se la richiesta è stata effettuata ad Amazon SES, l'indirizzo IP della richiesta, chi ha effettuato la richiesta, quando è stata effettuata la richiesta e ulteriori dettagli. Per ulteriori informazioni, consulta Registrazione delle chiamate API Amazon SES con AWS CloudTrail. Amazon SES fornisce anche metodi per monitorare le attività di invio come invii, rifiuti, frequenze di rimbalzo, consegne, aperture e clic. Per ulteriori informazioni, consulta Monitoring Your Amazon SES Sending Activity.

## Amazon Simple Queue Service (Amazon SQS)

I clienti devono comprendere i seguenti requisiti di crittografia chiave per utilizzare Amazon SQS con PHI.

- La comunicazione con Amazon SQS Queue tramite la richiesta di query deve essere crittografata con HTTPS. Per ulteriori informazioni su come effettuare richieste SQS, consulta Making Query API request.
- Amazon SQS supporta la crittografia lato server integrata con la protezione dei dati AWS KMS inattivi. L'aggiunta della crittografia lato server consente ai clienti di trasmettere e ricevere dati sensibili con la maggiore sicurezza derivante dall'utilizzo di code crittografate. La crittografia lato server di Amazon SQS utilizza l'Advanced Encryption Standard a 256 bit (algoritmo AES-256 GCM) per crittografare il corpo di ogni messaggio. L'integrazione con AWS KMS consente ai clienti di gestire centralmente le chiavi che proteggono i messaggi Amazon SQS insieme alle chiavi che proteggono le altre AWS risorse. AWS KMS registra ogni utilizzo delle chiavi di crittografia per contribuire AWS CloudTrail a soddisfare le esigenze normative e di conformità. Per ulteriori informazioni e per verificare la disponibilità di SSE per Amazon SQS nella regione, consulta Encryption at Rest.
- Se non viene utilizzata la crittografia lato server, il payload del messaggio stesso deve essere crittografato prima di essere inviato a SQS. Un modo per crittografare il payload dei messaggi consiste nell'utilizzare Amazon SQS Extended Client insieme al client di crittografia Amazon S3. Per ulteriori informazioni sull'uso della crittografia lato client, consulta Crittografia dei payload dei messaggi utilizzando Amazon SQS Extended Client e Amazon S3 Encryption Client.

Amazon SQS utilizza CloudTrail un servizio che registra le chiamate API effettuate da o per conto di Amazon SQS nell' AWS account di un cliente e consegna i file di registro al bucket Amazon S3 specificato. CloudTrail acquisisce le chiamate API effettuate dalla console Amazon SQS o dall'API Amazon SQS. I clienti possono utilizzare le informazioni raccolte da CloudTrail per determinare quali richieste vengono fatte ad Amazon SQS, l'indirizzo IP di origine da cui viene effettuata la richiesta, chi ha effettuato la richiesta, quando viene effettuata e così via. Per ulteriori informazioni

sulla registrazione delle operazioni SQS, consulta Registrazione delle chiamate API di Amazon SQS utilizzando. AWS CloudTrail

## Amazon Simple Storage Service (Amazon S3)

I clienti hanno a disposizione diverse opzioni per la crittografia dei dati inattivi quando utilizzano Amazon S3, tra cui la crittografia lato server e lato client e diversi metodi di gestione delle chiavi. Per ulteriori informazioni, consulta Protezione dei dati mediante la crittografia.

Le connessioni ad Amazon S3 contenenti PHI devono utilizzare endpoint che accettano il trasporto crittografato (HTTPS). Per un elenco degli endpoint regionali, consulta Endpoint di servizio.AWS

Non utilizzare PHI nei nomi dei bucket, nei nomi degli oggetti o nei metadati perché questi dati non sono crittografati utilizzando la crittografia lato server S3 e generalmente non sono crittografati nelle architetture di crittografia lato client.

## Amazon Simple Workflow Service

Amazon Simple Workflow Service (Amazon SWF) consente agli sviluppatori di creare, eseguire e scalare lavori in background con passaggi paralleli o sequenziali. Amazon SWF può essere considerato un tracker di stato e un coordinatore di attività completamente gestito nel cloud.

Amazon Simple Workflow Service viene utilizzato per orchestrare i flussi di lavoro e non è in grado di archiviare o trasmettere dati. I PHI non devono essere inseriti nei metadati di Amazon SWF o all'interno di alcuna descrizione delle attività. Amazon SWF lo utilizza AWS CloudTrail per registrare tutte le chiamate API.

## Amazon Textract

Amazon Textract utilizza tecnologie di apprendimento automatico per estrarre automaticamente testo e dati dai documenti scansionati, andando oltre il semplice riconoscimento ottico dei caratteri (OCR) per identificare, comprendere ed estrarre dati da moduli e tabelle. Ad esempio, i clienti possono utilizzare Amazon Textract per estrarre automaticamente dati ed elaborare moduli con informazioni sanitarie protette (PHI) senza l'intervento umano per soddisfare le richieste mediche.

Amazon Textract può essere utilizzato anche per mantenere la conformità negli archivi di documenti. Ad esempio, i clienti possono utilizzare Amazon Textract per estrarre dati da richieste di risarcimento assicurative o prescrizioni mediche e riconoscere automaticamente le coppie chiave-valore in tali documenti in modo da poter oscurare quelli sensibili.

Amazon Textract supporta la crittografia lato server (SSE-S3 e SSE-KMS) per i documenti di input e la crittografia TLS per i dati in transito tra il servizio e l'agente. I clienti possono utilizzare Amazon CloudWatch per tenere traccia dei parametri di utilizzo delle risorse e AWS CloudTrail per acquisire chiamate API verso Amazon Textract.

## Amazon Transcribe

Amazon Transcribe utilizza tecnologie avanzate di apprendimento automatico per riconoscere il parlato nei file audio e trascriverlo in testo. Ad esempio, i clienti possono utilizzare Amazon Transcribe per convertire l'audio in inglese americano e spagnolo messicano in testo e per creare applicazioni che incorporano il contenuto di file audio. Amazon Transcribe può essere utilizzato con dati contenenti PHI. Amazon Transcribe non conserva né archivia alcun dato e tutte le chiamate all'API sono crittografate con SSL/TLS. Amazon Transcribe CloudTrail utilizza per registrare tutte le chiamate API.

## Amazon Translate

Amazon Translate utilizza tecnologie avanzate di apprendimento automatico per fornire traduzioni di alta qualità su richiesta. I clienti possono utilizzare Amazon Translate per tradurre documenti di testo non strutturati o per creare applicazioni che funzionano in più lingue. I documenti contenenti PHI possono essere elaborati con Amazon Translate. Non è richiesta alcuna configurazione aggiuntiva per la traduzione di documenti che contengono PHI. La crittografia dei dati in transito è fornita da SSL/TLS e nessun dato rimane inattivo con Amazon Translate. Amazon Translate lo utilizza CloudTrail per registrare tutte le chiamate API.

## Amazon Virtual Private Cloud

Amazon Virtual Private Cloud (Amazon VPC) offre una serie di funzionalità di sicurezza di rete ben allineate all'architettura per carichi di lavoro regolati dalla normativa HIPAA. Funzionalità come gli elenchi di controllo degli accessi alla rete stateless e la riassegnazione dinamica delle istanze in gruppi di sicurezza con stato offrono flessibilità nella protezione delle istanze da accessi non autorizzati alla rete.

Amazon VPC consente inoltre ai clienti di estendere il proprio spazio di indirizzi di rete AWS, oltre a fornire diversi modi per connettere i propri data center. AWS I log di flusso VPC forniscono un audit trail delle connessioni accettate e rifiutate alle istanze che elaborano, trasmettono o archiviano i PHI.

AWS Transit Gateway funge da hub di rete e semplifica la connettività tra Amazon VPC e reti locali. AWS Transit Gateway fornisce inoltre funzionalità di peering interregionale ad altri Transit Gateway per stabilire una rete globale utilizzando la dorsale. AWS Per ulteriori informazioni su Amazon VPC, consulta Amazon Virtual Private Cloud.

## Amazon WorkDocs

Amazon WorkDocs è un servizio di archiviazione e condivisione di file aziendali completamente gestito e sicuro con solidi controlli amministrativi e funzionalità di feedback che migliorano la produttività degli utenti. Amazon WorkDocs i file vengono crittografati quando sono archiviati utilizzando chiavi gestite dai clienti tramite AWS Key Management Service (AWS KMS). Tutti i dati in transito sono crittografati tramite SSL/TLS. AWS le applicazioni web e mobili e i client di sincronizzazione desktop trasmettono i file direttamente tramite SSL/TLS. Amazon WorkDocs

Utilizzando la console di Amazon WorkDocs gestione, WorkDocs gli amministratori possono visualizzare i registri di controllo per tenere traccia delle attività dei file e degli utenti in base all'ora e scegliere se consentire agli utenti di condividere file con altre persone esterne all'organizzazione. Amazon WorkDocs è inoltre integrato con CloudTrail (un servizio che acquisisce le chiamate API effettuate da o per conto dell' Amazon WorkDocs AWS account del cliente) e invia i file di CloudTrail registro a un bucket Amazon S3 specificato dai clienti.

L'autenticazione a più fattori (MFA) tramite un server RADIUS è disponibile e può fornire ai clienti un ulteriore livello di sicurezza durante il processo di autenticazione. Gli utenti accedono inserendo il nome utente e la password seguiti da un OTP (One-Time Passcode) fornito da un token hardware o software.

Per ulteriori informazioni, consultare:

- Amazon WorkDocs caratteristica
- Registrazione delle chiamate Amazon WorkDocs API utilizzando AWS CloudTrail

I clienti non devono memorizzare PHI nei nomi di file o nei nomi di directory.

## Amazon WorkSpaces

Amazon WorkSpaces è una soluzione esktop-as-a D-Service (DaaS) completamente gestita e sicura che funziona su. AWS Con Amazon WorkSpaces, i clienti possono fornire facilmente desktop

Microsoft Windows virtuali basati sul cloud per i propri utenti, fornendo loro l'accesso ai documenti, alle applicazioni e alle risorse di cui hanno bisogno, ovunque, in qualsiasi momento e da qualsiasi dispositivo supportato.

Amazon WorkSpaces archivia i dati in volumi Amazon Elastic Block Store. I clienti possono crittografare i volumi di WorkSpaces storage dei clienti utilizzando chiavi gestite AWS Key Management Service dai clienti. Quando la crittografia è abilitata su a WorkSpace, sia i dati archiviati in archivio nello storage sottostante che i backup automatici (EBS Snapshots) dello storage su disco vengono crittografati in conformità con la Guida. La comunicazione dai WorkSpace client a è protetta tramite WorkSpace SSL/TLS. Per ulteriori informazioni sulla crittografia a riposo con Amazon WorkSpaces, consulta Encrypted WorkSpaces.

## AWS App Mesh

AWS App Mesh è una service mesh che fornisce reti a livello di applicazione per facilitare la comunicazione tra i tuoi servizi attraverso diversi tipi di infrastruttura di elaborazione, come Amazon ECS, Amazon EKS o Amazon EC2. App Mesh configura i proxy Envoy per raccogliere e trasmettere dati di osservabilità ai vizi del set di monitoraggio che configuri, per darti visibilità. end-to-end Può indirizzare il traffico in base al routing e alle politiche di traffico configurate per garantire l'elevata disponibilità delle applicazioni. Il traffico tra le applicazioni può essere configurato per utilizzare TLS. App Mesh può essere utilizzato utilizzando AWS SDK o il controller App Mesh per Kubernetes. Sebbene AWS App Mesh sia un servizio idoneo allo standard HIPAA, nessun PHI deve essere memorizzato nei nomi/attributi delle risorse all'interno, AWS App Mesh poiché non è disponibile alcun supporto per la protezione di tali dati. AWS App Mesh Può invece essere utilizzato per monitorare, controllare e proteggere le risorse del dominio del cliente che trasmettono o archiviano i PHI.

## AWS Servizio di migrazione delle applicazioni

AWS Application Migration Service (AWS MGN) consente di migrare rapidamente server e applicazioni verso AWS, senza modifiche e con tempi di inattività minimi. AWS MGN è il servizio di migrazione principale consigliato per le migrazioni lift and shift verso. AWS

AWS MGN utilizza la replica dei dati a livello di blocco per copiare i dischi di origine direttamente sui volumi EBS dell'account cliente: i dati non vengono mai trasmessi attraverso un ambiente cloud controllato da MGN. AWS Per impostazione predefinita, i dati replicati vengono crittografati in transito. I dati nei volumi EBS del cliente sono crittografati per impostazione predefinita utilizzando le chiavi del cliente.

# AWS Auto Scaling

AWS Auto Scaling consente ai clienti di configurare la scalabilità automatica per le AWS risorse che fanno parte dell'applicazione del cliente in pochi minuti. I clienti possono utilizzare AWS Auto Scaling per una serie di servizi che coinvolgono PHI, come Amazon DynamoDB, Amazon ECS, repliche Amazon RDS Aurora e istanze Amazon EC2 in un gruppo Auto Scaling.

AWS Auto Scaling è un servizio di orchestrazione che non elabora, archivia o trasmette direttamente i contenuti dei clienti; per questo motivo, i clienti possono utilizzare questo servizio con contenuti crittografati. Il modello di responsabilità AWS condivisa si applica alla protezione dei dati in AWS Auto Scaling: AWS è responsabile delle procedure di sicurezza della AWS rete, mentre il cliente è responsabile del mantenimento del controllo sui contenuti del cliente ospitati su questa infrastruttura. Questo contenuto include le attività di configurazione e gestione della sicurezza per i AWS servizi utilizzati dai clienti. Ai fini della protezione dei dati, consigliamo ai clienti di proteggere le credenziali degli AWS account e di configurare account utente individuali con AWS Identity and Access Management (IAM). In questo modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere il proprio lavoro.

Consigliamo vivamente ai clienti di non inserire mai informazioni identificative sensibili, come i numeri di conto dei clienti, in campi in formato libero come il campo Nome. Ciò include quando i clienti utilizzano AWS Auto Scaling o altri AWS servizi utilizzando l'API o AWS Management Console AWS gli AWS CLI SDK.

Tutti i dati che i clienti inseriscono in AWS Auto Scaling o in altri servizi potrebbero essere raccolti per essere inclusi nei registri di diagnostica. Quando i clienti forniscono un URL a un server esterno, non devono includere le informazioni sulle credenziali nell'URL per convalidare la richiesta a quel server. AWS consiglia inoltre ai clienti di proteggere i propri dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS Consigliamo TLS 1.2 o versioni successive
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno AWS dei servizi.
- Utilizza i servizi di sicurezza gestiti avanzati, ad esempio Amazon Macie, che aiutano a individuare e proteggere i dati personali archiviati in Amazon S3.

# AWS Backup

AWS Backup offre un servizio centralizzato, completamente gestito e basato su policy per proteggere i dati dei clienti e garantire la conformità tra i AWS servizi ai fini della continuità aziendale. Con AWS Backup, i clienti possono configurare centralmente le politiche di protezione dei dati (backup) e monitorare l'attività di backup su tutte AWS le risorse del cliente, inclusi i volumi Amazon EBS, i database Amazon Relational Database Service (Amazon RDS) (inclusi i cluster Aurora), le tabelle Amazon DynamoDB, Amazon Elastic File System (Amazon EFS), i file system Amazon FSx, Amazon EC2 inst. danze e volumi. AWS Storage Gateway

AWS Backup crittografa i dati dei clienti in transito e a riposo. I backup provenienti da servizi con funzionalità di snapshot esistenti vengono crittografati utilizzando la metodologia di crittografia delle istantanee del servizio di origine. Ad esempio, le istantanee EBS vengono crittografate utilizzando la chiave di crittografia del volume da cui è stata creata l'istantanea.

I backup provenienti da AWS servizi più recenti che introducono funzionalità di backup integrate AWS Backup, come Amazon EFS, sono crittografati in transito e a riposo indipendentemente dai servizi di origine, offrendo ai backup dei clienti un ulteriore livello di protezione. La crittografia è configurata a livello di Backup Vault. Il Vault predefinito è crittografato. Quando i clienti creano un nuovo vault, è necessario selezionare una chiave di crittografia.

# AWS Batch

AWS Batch consente a sviluppatori, scienziati e ingegneri di eseguire in modo semplice ed efficiente centinaia di migliaia di lavori di elaborazione in batch. AWS AWS Batch fornisce dinamicamente la quantità e il tipo ottimali di risorse di elaborazione (come CPU o istanze ottimizzate per la memoria) in base al volume e ai requisiti di risorse specifici dei processi batch inviati. AWS Batch pianifica, pianifica ed esegue carichi di lavoro di elaborazione in batch attraverso l'intera gamma di servizi e funzionalità di elaborazione. AWS

Analogamente alle linee guida per Amazon ECS, PHI non deve essere inserito direttamente nella definizione del lavoro, nella coda dei lavori o nei tag per. AWS Batch Invece, i lavori pianificati ed eseguiti con AWS Batch possono funzionare su PHI crittografati. Inoltre, tutte le informazioni restituite dalle fasi di un processo non AWS Batch devono contenere alcun PHI. Ogni volta che i lavori eseguiti da AWS Batch devono trasmettere o ricevere PHI, tale connessione deve essere crittografata utilizzando HTTPS o SSL/TLS.

# AWS Certificate Manager

AWS Certificate Manager è un servizio che consente ai clienti di fornire, gestire e distribuire facilmente certificati SSL/TLS pubblici e privati da utilizzare con i servizi e le relative risorse interne connesse. AWS AWS Certificate Manager utilizza per registrare tutte le chiamate CloudTrail API.

Gli utenti necessitano di un accesso programmatico se desiderano interagire con l' AWS AWS Management Console esterno di. Il modo per concedere l'accesso programmatico dipende dal tipo di utente che accede. AWS

Per fornire agli utenti l'accesso programmatico, scegli una delle seguenti opzioni.

| Quale utente necessita dell'accesso programmatico? | Per | Come |
|---|---|---|
| Identità della forza lavoro<br><br>(Utenti gestiti nel centro identità IAM) | Utilizza credenziali temporane e per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS | Segui le istruzioni per l'interfa ccia che desideri utilizzare.<br><br>• Per la AWS CLI, consulta Configurazione dell'uso AWS IAM Identity Center nella Guida AWS CLI per l'utente.AWS Command Line Interface<br>• Per AWS SDK, strumenti e AWS API, consulta l'autenticazione IAM Identity Center nella Guida di riferimento agli AWS SDK e agli strumenti. |
| IAM | Utilizza credenziali temporane e per firmare le richieste programmatiche agli SDK o alle API AWS CLI. AWS AWS | Segui le istruzioni in Uso delle credenziali temporanee con AWS risorse nella Guida per l'utente IAM. |
| IAM | (Non consigliato) | Segui le istruzioni per l'interfa ccia che desideri utilizzare. |

| Quale utente necessita dell'accesso programmatico? | Per | Come |
| --- | --- | --- |
| | Utilizza credenziali a lungo termine per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS | • Per la AWS CLI, consulta Autenticazione tramite credenziali utente IAM nella Guida per l'utente.AWS Command Line Interface<br>• Per gli AWS SDK e gli strumenti, consulta Autenticazione tramite credenziali a lungo termine nella Guida di riferimen to agli SDK e agli AWS strumenti.<br>• Per le AWS API, consulta Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente IAM. |

## AWS Cloud Map

AWS Cloud Map è un servizio di scoperta di risorse cloud. Con AWS Cloud Map, i clienti possono definire nomi personalizzati per le risorse delle applicazioni, come attività Amazon ECS, istanze Amazon EC2, bucket Amazon S3, tabelle Amazon DynamoDB, code Amazon SQS o qualsiasi altra risorsa cloud. I clienti possono quindi utilizzare questi nomi personalizzati per scoprire la posizione e i metadati delle risorse cloud dalle loro applicazioni utilizzando l'SDK AWS e le query API autenticate. Sebbene AWS Cloud Map sia un servizio idoneo alla normativa HIPAA, nessun PHI deve essere archiviato nei nomi/attributi delle risorse all'interno di AWS Cloud Map poiché non è disponibile alcun supporto per la protezione di tali dati. Al contrario, AWS Cloud Map può essere utilizzato per scoprire le risorse del dominio del cliente che trasmettono o archiviano PHI.

## AWS CloudFormation

AWS CloudFormation consente ai clienti di creare e fornire implementazioni di infrastrutture AWS in modo prevedibile e ripetuto. Aiuta i clienti a sfruttare prodotti AWS come Amazon EC2, Amazon

Elastic Block Store, Amazon SNS, Elastic Load Balancing e Auto Scaling per creare applicazioni altamente affidabili, altamente scalabili ed economiche nel cloud senza preoccuparsi di creare e configurare l'infrastruttura AWS sottostante. AWS CloudFormation consente ai clienti di utilizzare un file modello per creare ed eliminare una raccolta di risorse insieme come una singola unità (uno stack).

AWS CloudFormation di per sé non archivia, trasmette o elabora PHI. Viene invece utilizzato per creare e distribuire architetture che utilizzano altri servizi AWS che potrebbero archiviare, trasmettere e/o elaborare PHI. Con PHI devono essere utilizzati solo i servizi idonei alla normativa HIPAA. Si prega di fare riferimento alle voci relative a tali servizi in questo white paper per indicazioni sull'uso di PHI con tali servizi. AWS CloudFormation utilizza per registrare AWS CloudTrail tutte le chiamate API.

# AWS CloudHSM

AWS CloudHSM è un modulo di sicurezza hardware (HSM) basato sul cloud che consente ai clienti di generare e utilizzare facilmente le proprie chiavi di crittografia sul cloud AWS. Con CloudHSM, i clienti possono gestire le proprie chiavi di crittografia utilizzando HSM convalidati FIPS 140-2 di livello 3. CloudHSM offre ai clienti la flessibilità necessaria per l'integrazione con le loro applicazioni utilizzando API standard aperte, come PKCS #11, Java Cryptography Extensions (JCE) e le librerie Microsoft CryptoNG (CNG).

CloudHSM è inoltre conforme agli standard e consente ai clienti di esportare tutte le proprie chiavi nella maggior parte degli altri HSM disponibili in commercio. Come un servizio di gestione delle chiavi di un dispositivo hardware, non AWS CloudHSM è in grado di archiviare o trasmettere PHI. I clienti non devono memorizzare PHI nei tag (metadati). Non sono richieste altre indicazioni speciali.

# AWS CloudTrail

AWS CloudTrail è un servizio che consente la governance, la conformità, il controllo operativo e il controllo del rischio degli account AWS. Con CloudTrail, i clienti possono registrare, monitorare continuamente e conservare le attività dell'account relative alle azioni sulla propria infrastruttura AWS. CloudTrail fornisce la cronologia degli eventi dell'attività dell'account AWS, incluse le azioni intraprese tramite gli SDK AWS AWS Management Console, gli strumenti a riga di comando e altri servizi AWS. Questa cronologia degli eventi semplifica l'analisi della sicurezza, il monitoraggio delle modifiche alle risorse e la risoluzione dei problemi.

AWS CloudTrail è abilitato per l'uso con tutti gli account AWS e può essere utilizzato per la registrazione di audit, come richiesto dalla AWS BAA. È necessario creare percorsi specifici utilizzando la CloudTrail console o l'interfaccia a riga di comando AWS. CloudTrail crittografa tutto il traffico in transito e in stato di riposo quando viene creato un Trail crittografato. È necessario creare un percorso crittografato quando esiste la possibilità di registrare PHI.

Per impostazione predefinita, un Trail crittografato archivia le voci in Amazon S3 utilizzando la crittografia lato server con chiavi gestite Amazon S3 (SSE-S3). Se si desidera una gestione aggiuntiva delle chiavi, è possibile configurarla anche con -managed keys (SSE-KMS). AWS KMS Poiché CloudTrail è la destinazione finale per le voci di log di AWS e quindi un componente fondamentale di qualsiasi architettura che gestisce PHI, è necessario abilitare la convalida dell'integrità dei file di CloudTrail registro e i file CloudTrail digest associati devono essere rivisti periodicamente. Una volta abilitata, è possibile stabilire un'affermazione positiva che i file di log non sono stati modificati o alterati.

# AWS CodeBuild

AWS CodeBuild è un servizio di compilazione completamente gestito nel cloud. AWS CodeBuild compila il codice sorgente, esegue test unitari e produce artefatti pronti per l'implementazione. AWS CodeBuild utilizza una AWS KMS chiave per crittografare gli artefatti di output della build. È necessario creare e configurare una chiave KMS prima di creare elementi che contengano PHI, segreti/password, certificati, ecc. utilizzati per registrare tutte le chiamate API. AWS CodeBuild AWS CloudTrail

# AWS CodeDeploy

AWS CodeDeploy è un servizio di distribuzione completamente gestito che automatizza le distribuzioni di software su una varietà di servizi di elaborazione tra cui Amazon EC2 e server locali. AWS Fargate AWS Lambda I clienti lo utilizzano AWS CodeDeploy per rilasciare rapidamente nuove funzionalità di carico di lavoro containerizzato e gestire la complessità dell'aggiornamento delle applicazioni.

AWS CodeDeploy supporta la crittografia lato server (SSE-S3) per gli artefatti di distribuzione e la crittografia TLS per i dati in transito tra il servizio e l'agente. I clienti possono utilizzare Amazon CloudWatch Events per tenere traccia delle distribuzioni e AWS CloudTrail acquisire chiamate API verso. AWS CodeDeploy

# AWS CodeCommit

AWS CodeCommit è un servizio di controllo del codice sorgente sicuro, altamente scalabile e gestito che ospita repository Git privati. AWS CodeCommit elimina la necessità per i clienti di gestire il proprio sistema di controllo del codice sorgente o di preoccuparsi di scalare la propria infrastruttura.

AWS CodeCommit crittografa tutto il traffico e le informazioni archiviate mentre sono in transito e a riposo. Per impostazione predefinita, quando viene creato un repository all'interno AWS CodeCommit, viene creata una chiave gestita AWS con AWS KMS e viene utilizzata solo da tale repository per crittografare tutti i dati archiviati in archivio. AWS CodeCommit utilizza per registrare AWS CloudTrail tutte le chiamate API.

# AWS CodePipeline

AWS CodePipeline è un servizio di distribuzione continua completamente gestito che aiuta i clienti ad automatizzare le pipeline di rilascio per aggiornamenti rapidi e affidabili delle applicazioni e dell'infrastruttura. I clienti utilizzano AWS CodePipeline per consentire ai ricercatori di elaborare automaticamente i dati degli studi clinici, i risultati di laboratorio e i dati genomici: questi sono alcuni esempi di pipeline di flussi di lavoro utilizzati dai clienti.

AWS CodePipeline supporta la crittografia lato server (SSE-S3 e SSE-KMS) per gli artefatti del codice e la crittografia TLS per i dati in transito tra il servizio e l'agente. I clienti possono utilizzare Amazon CloudWatch Events per tenere traccia delle modifiche AWS CloudTrail alla pipeline e acquisire chiamate API verso AWS CodePipeline.

# AWS Config

AWS Config fornisce una visione dettagliata delle risorse associate all'account AWS di un cliente, incluso il modo in cui sono configurate, come sono correlate tra loro e come le configurazioni e le loro relazioni sono cambiate nel tempo.

AWS Config non può essere utilizzato di per sé per archiviare o trasmettere PHI.

Può invece essere sfruttato per monitorare e valutare architetture create con altri servizi AWS, comprese le architetture che gestiscono PHI, per determinare se rimangono conformi all'obiettivo di progettazione previsto. Le architetture che gestiscono PHI devono essere create solo con i servizi idonei alla normativa HIPAA. AWS Config utilizza per registrare tutti i AWS CloudTrail risultati.

# AWS Data Exchange

AWS Data Exchange semplifica la ricerca, la sottoscrizione e l'utilizzo di dati di terze parti nel cloud. Una volta abbonati a un prodotto di dati, i clienti possono utilizzare l'API AWS Data Exchange per caricare i dati direttamente in Amazon S3 e poi analizzarli con un'ampia varietà di servizi di analisi e apprendimento automatico AWS. Per i fornitori di dati, AWS Data Exchange semplifica il contatto con i milioni di clienti AWS che migrano al cloud eliminando la necessità di creare e mantenere un'infrastruttura per l'archiviazione, la distribuzione, la fatturazione e l'autorizzazione dei dati.

AWS Data Exchange crittografa sempre tutti i prodotti di dati archiviati nel servizio a riposo senza richiedere alcuna configurazione aggiuntiva. Questa crittografia viene eseguita automaticamente tramite una chiave KMS gestita dal servizio. AWS Data Exchange utilizza Transport Layer Security (TLS) e la crittografia lato client per la crittografia in transito. La comunicazione con AWS Data Exchange avviene sempre tramite HTTPS, quindi i dati dei clienti sono sempre crittografati in transito. Questa crittografia è configurata per impostazione predefinita quando i clienti utilizzano AWS Data Exchange. Per ulteriori informazioni, consulta la sezione Protezione dei dati in AWS Data Exchange.

AWS Data Exchange è integrato con AWS CloudTrail. AWS CloudTrail acquisisce tutte le chiamate alle API di AWS Data Exchange come eventi, incluse le chiamate dalla console AWS Data Exchange e le chiamate di codice alle operazioni dell'API AWS Data Exchange. Alcune azioni che i clienti possono intraprendere sono solo azioni da console. Non esiste un'API corrispondente nell'SDK AWS o nell'AWS CLI. Si tratta di azioni che si basano su Marketplace AWS funzionalità, come la pubblicazione o l'abbonamento a un prodotto. AWS Data Exchange fornisce CloudTrail i log per un sottoinsieme di queste azioni solo per console. Per ulteriori informazioni, consulta Logging with AWS CloudTrail AWS Data Exchange API Calls.

Tieni presente che tutte le offerte che utilizzano AWS Data Exchange devono rispettare le linee guida per la pubblicazione di AWS Data Exchange e le domande frequenti su AWS Data Exchange per i Marketplace AWS fornitori, che limitano determinate categorie di dati. Per ulteriori informazioni, consulta le domande frequenti su AWS Data Exchange.

# AWS Database Migration Service

AWS Database Migration Service (AWS DMS) aiuta i clienti a migrare i database in AWS in modo semplice e sicuro. I clienti possono migrare i propri dati da e verso i database commerciali e open source più utilizzati, come Oracle, MySQL e PostgreSQL. Il servizio supporta le migrazioni omogenee, come la migrazione da Oracle a Oracle, così come le migrazioni eterogenee tra piattaforme di database diverse, come la migrazione da Oracle a PostgreSQL o da MySQL a Oracle.

I database in esecuzione in locale e in fase di migrazione al cloud con AWS DMS possono contenere dati PHI. AWS DMS crittografa i dati durante il transito e durante lo staging dei dati per la migrazione finale nel database di destinazione su AWS. AWS DMS crittografa lo storage utilizzato da un'istanza di replica e le informazioni di connessione agli endpoint. Per crittografare lo storage utilizzato da un'istanza di replica, AWS DMS utilizza una AWS KMS chiave unica per l'account AWS. Fai riferimento alla Guida per il database di destinazione appropriato per garantire che i dati rimangano crittografati una volta completata la migrazione. AWS DMS utilizza CloudTrail per registrare tutte le chiamate API.

# AWS DataSync

AWS DataSync è un servizio di trasferimento online che semplifica, automatizza e accelera lo spostamento dei dati tra lo storage locale e AWS. I clienti possono utilizzare AWS DataSync per connettere le proprie fonti di dati ad Amazon S3 o Amazon EFS. I clienti devono assicurarsi che Amazon S3 e Amazon EFS siano configurati in modo coerente con la Guida. Per impostazione predefinita, i dati dei clienti vengono crittografati in transito utilizzando TLS 1.2. Per ulteriori informazioni sulla crittografia e AWS DataSync, consulta le DataSynccaratteristiche di AWS. I clienti possono monitorare le DataSync attività utilizzando AWS CloudTrail. Per ulteriori informazioni sulla registrazione con CloudTrail, consulta Logging with AWS DataSync API Calls with. AWS CloudTrail

# AWS Directory Service

## AWS Directory Service for Microsoft AD

AWS Directory Service for Microsoft Active Directory (Enterprise Edition), noto anche come AWS Microsoft AD, consente ai carichi di lavoro basati sulle directory e alle risorse AWS di utilizzare Active Directory gestito nel cloud AWS. AWS Microsoft AD archivia i contenuti delle directory (inclusi i contenuti contenenti PHI) in volumi Amazon Elastic Block Store crittografati utilizzando chiavi di crittografia gestite da AWS. Per ulteriori informazioni, consulta Crittografia Amazon EBS.

I dati in transito da e verso i client Active Directory vengono crittografati quando viaggiano attraverso il Lightweight Directory Access Protocol (LDAP) sulla rete Amazon Virtual Private Cloud (VPC) del cliente. Se un client Active Directory risiede in una rete locale, il traffico arriva al VPC del cliente tramite un collegamento di rete privata virtuale o un collegamento. AWS Direct Connect

## Directory del cloud Amazon

Amazon Cloud Directory consente ai clienti di creare directory flessibili native del cloud per organizzare gerarchie di dati su più dimensioni. I clienti possono anche creare directory per una varietà di casi d'uso, come organigrammi, cataloghi di corsi e registri di dispositivi. Ad esempio, i clienti possono creare un organigramma che può essere consultato attraverso gerarchie separate per la struttura, l'ubicazione e il centro di costo dei report. Amazon Cloud Directory crittografa automaticamente i dati inattivi e in transito utilizzando chiavi di crittografia a 256 bit gestite da (). AWS Key Management Service AWS KMS

# AWS Elastic Beanstalk

Con AWS Elastic Beanstalk, i clienti possono distribuire e gestire rapidamente le applicazioni nel cloud AWS senza dover conoscere l'infrastruttura che esegue tali applicazioni. I clienti possono semplicemente caricare il codice e gestire AWS Elastic Beanstalk automaticamente la distribuzione, dal provisioning della capacità, al bilanciamento del carico, al ridimensionamento automatico al monitoraggio dello stato delle applicazioni. Allo stesso tempo, i clienti mantengono il pieno controllo sulle risorse AWS che alimentano la loro applicazione e possono accedere alle risorse sottostanti in qualsiasi momento.

AWS Elastic Beanstalk di per sé non archivia, trasmette o elabora PHI. I clienti possono invece utilizzarlo per creare e distribuire architetture con altri servizi AWS che potrebbero archiviare, trasmettere e/o elaborare PHI. I clienti devono assicurarsi che, al momento di scegliere i servizi da distribuire, utilizzino solo i servizi idonei alla normativa AWS Elastic Beanstalk HIPAA con PHI. Per indicazioni sull'uso di PHI con tali servizi, consulta le voci relative a tali servizi in questo white paper.

I clienti non devono includere PHI in alcun campo in formato libero all'interno, ad esempio nel campo Nome. AWS Elastic Beanstalk  AWS Elastic Beanstalk utilizza AWS CloudTrail per registrare tutte le chiamate API.

# AWS Elastic Disaster Recovery

AWS Elastic Disaster Recovery (AWS DRS) riduce al minimo i tempi di inattività e la perdita di dati con un ripristino rapido e affidabile di applicazioni locali e basate sul cloud utilizzando storage conveniente, elaborazione e ripristino minimi. point-in-time

I clienti possono configurare AWS Elastic Disaster Recovery sui propri server di origine per avviare una replica sicura dei dati. I loro dati vengono replicati in una sottorete dell'area di staging del tuo

account AWS, nella regione AWS selezionata. La progettazione dell'area di staging riduce i costi utilizzando uno storage conveniente e risorse di elaborazione minime per mantenere una replica continua. I dati dei clienti replicati da AWS Elastic Disaster Recovery sono crittografati in transito utilizzando TLS 1.2 e trasferiti direttamente dai loro server di origine al loro VPC. I clienti possono sfruttare la connettività privata come AWS Direct Connect o VPN per configurare il percorso di replica. I dati dei clienti possono anche essere crittografati quando sono inattivi su AWS utilizzando la crittografia Amazon EBS.

I clienti possono eseguire test senza interruzione delle attività per confermare che l'implementazione è completa. Durante il normale funzionamento, garantite la disponibilità monitorando la replica ed eseguendo periodicamente procedure di ripristino e failback senza interruzioni. Se i clienti devono ripristinare le applicazioni, possono avviare istanze di ripristino su AWS in pochi minuti, utilizzando la maggior parte dello stato del up-to-date server o un point-in-time precedente. Dopo che le applicazioni dei clienti sono state eseguite su AWS, possono scegliere di mantenerle lì oppure possono avviare la replica dei dati sul loro sito primario una volta risolto il problema. I clienti possono tornare al loro sito principale ogni volta che sono pronti.

## AWS Fargate

AWS Fargate è una tecnologia che consente ai clienti di utilizzare container senza dover gestire server o cluster. In questo modo AWS Fargate, i clienti non devono più effettuare il provisioning, configurare e scalare i cluster di macchine virtuali per eseguire i container. Ciò elimina la necessità di scegliere i tipi di server, decidere quando scalare i cluster o ottimizzare l'imballaggio dei cluster. AWS Fargate elimina la necessità per i clienti di interagire o pensare a server o cluster. Con Fargate, i clienti si concentrano sulla progettazione e sulla creazione delle proprie applicazioni anziché sulla gestione dell'infrastruttura che le esegue.

Fargate non richiede alcuna configurazione aggiuntiva per funzionare con carichi di lavoro che elaborano PHI. I clienti possono eseguire carichi di lavoro di container su Fargate utilizzando servizi di orchestrazione dei container come Amazon ECS. Fargate gestisce solo l'infrastruttura sottostante e non opera con o su dati all'interno del carico di lavoro orchestrato. In linea con i requisiti dell'HIPAA, i dati PHI devono comunque essere crittografati ogni volta che sono in transito o inattivi quando vi si accede dai container lanciati con Fargate. Per ogni opzione di storage AWS descritta in questo paper sono disponibili diversi meccanismi per la crittografia a riposo. Per ulteriori informazioni sulla sicurezza e la configurazione HIPAA, consulta il white paper Architecting for HIPAA Security and Compliance on Amazon EKS.

# AWS Firewall Manager

AWS Firewall Manager è un servizio di gestione della sicurezza che consente ai clienti di configurare e gestire centralmente le regole del firewall tra gli account e le applicazioni dei clienti in. AWS Organizations Man mano che vengono create nuove applicazioni, Firewall Manager semplifica la conformità di nuove applicazioni e risorse applicando un set comune di regole di sicurezza. Ora i clienti dispongono di un unico servizio per creare regole firewall, creare politiche di sicurezza e applicarle in modo coerente e gerarchico sull'intera infrastruttura, da un account di amministratore centrale.

AWS Firewall Manager è un servizio di orchestrazione che non elabora, archivia o trasmette direttamente i dati degli utenti. Il servizio non crittografa i contenuti dei clienti, ma i servizi sottostanti che AWS Firewall Manager utilizza, come DynamoDB, crittografano i dati degli utenti.

# AWS Global Accelerator

AWS Global Accelerator è un servizio globale di bilanciamento del carico che migliora la disponibilità e la latenza delle applicazioni multiregionali. Per garantire che PHI rimanga crittografato in transito e a riposo durante l'utilizzo AWS Global Accelerator, le architetture bilanciate dal carico di Global Accelerator devono utilizzare un protocollo crittografato, come HTTPS o SSL/TLS. Consulta le linee guida per Amazon EC2, Elastic Load Balancing e altri servizi AWS per comprendere meglio le opzioni di crittografia disponibili per le risorse di backend. AWS Global Accelerator utilizza AWS CloudTrail per registrare tutte le chiamate API.

# AWS Glue

AWS Glue è un servizio ETL (estrazione, trasformazione e caricamento) completamente gestito che consente ai clienti di classificare i propri dati, pulirli, arricchirli e spostarli in modo semplice ed economico tra vari archivi di dati. Per garantire la crittografia dei dati contenenti PHI durante il transito, AWS Glue deve essere configurato per utilizzare connessioni JDBC agli archivi dati con SSL/TLS. Inoltre, per mantenere la crittografia durante il transito, l'impostazione per la crittografia lato server (SSE-S3) deve essere passata come parametro ai job ETL con cui vengono eseguiti. AWS Glue Tutti i dati archiviati in archivio all'interno del Data Catalog di vengono crittografati utilizzando chiavi gestite da AWS KMS quando la crittografia AWS Glue è abilitata al momento della creazione di un oggetto Data Catalog. AWS Glue utilizza CloudTrail per registrare tutte le chiamate API.

# AWS Glue DataBrew

AWS Glue DataBrew è un servizio di preparazione dei dati visivi completamente gestito che consente agli analisti e ai data scientist di dati di pulire e normalizzare i dati per prepararli all'analisi e all'apprendimento automatico. Per garantire la crittografia dei dati contenenti PHI durante il transito, DataBrew deve essere configurato per utilizzare connessioni JDBC agli archivi dati con SSL/TLS. Quando ti connetti a sorgenti dati JDBC, DataBrew utilizza le impostazioni sulla tua connessione AWS Glue, inclusa l'opzione «Richiedi connessione SSL». Inoltre, per mantenere la crittografia quando è inattiva nei bucket S3, l'impostazione per la crittografia lato server (SSE-S3 o SSE-KMS) deve essere passata come parametro ai job. DataBrew

# AWS IoT Core e AWS IoT Device Management

AWS IoT AWS IoT Device Management Gestisci e fornisci comunicazioni sicure e bidirezionali tra dispositivi connessi a Internet, come sensori, attuatori, microcontrollori integrati o elettrodomestici intelligenti, e il cloud AWS. AWS IoT Core e ora AWS IoT Device Management può ospitare dispositivi che trasmettono dati contenenti PHI. Tutte le comunicazioni con AWS IoT Core AWS IoT Device Management sono crittografate tramite TLS. AWS IoT Core e AWS IoT Device Management utilizza AWS CloudTrail per registrare tutte le chiamate API.

# AWS IoT Greengrass

AWS IoT Greengrass consente ai clienti di eseguire funzionalità locali di elaborazione, messaggistica, memorizzazione nella cache dei dati, sincronizzazione e inferenza ML per i dispositivi connessi in modo sicuro. AWS IoT Greengrass utilizza certificati X.509, sottoscrizioni gestite, AWS IoT policy e ruoli IAM per garantire la sicurezza delle applicazioni Greengrass del cliente. AWS IoT Greengrass utilizza il modello di sicurezza del AWS IoT trasporto per crittografare la comunicazione con il cloud tramite TLS. Inoltre, AWS IoT Greengrass i dati vengono crittografati quando sono inattivi (nel cloud). Per ulteriori informazioni sulla sicurezza di Greengrass, vedere Panoramica della AWS IoT Greengrass sicurezza.

I clienti possono registrare le azioni delle AWS IoT Greengrass API utilizzando AWS CloudTrail. Per ulteriori informazioni, consulta Registrazione delle chiamate AWS IoT Greengrass API con AWS CloudTrail.

# AWS Lambda

AWS Lambda consente ai clienti di eseguire il codice senza effettuare il provisioning o gestire i server autonomamente. AWS Lambda utilizza una flotta di elaborazione di istanze Amazon Elastic Compute Cloud (Amazon EC2) su più zone di disponibilità in una regione, che fornisce l'elevata disponibilità, sicurezza, prestazioni e scalabilità dell'infrastruttura AWS.

Per garantire che PHI rimanga crittografato durante l'utilizzo AWS Lambda, le connessioni a risorse esterne devono utilizzare un protocollo crittografato come HTTPS o SSL/TLS. Ad esempio, quando si accede a S3 da una procedura Lambda, è necessario risolvere il problema con https://bucket.s3-aws-region.amazonaws.com.

Se un PHI viene collocato a riposo o inattivo all'interno di una procedura in esecuzione, deve essere crittografato lato client o lato server con chiavi ottenute da o. AWS KMS AWS CloudHSM Segui le relative linee guida per Amazon API Gateway quando attivi AWS Lambda funzioni tramite il servizio. Quando si utilizzano eventi di altri servizi AWS per attivare AWS Lambda funzioni, i dati degli eventi non devono contenere (di per sé) PHI. Ad esempio, quando una procedura Lambda viene attivata da un evento S3, come l'arrivo di un oggetto in S3, il nome dell'oggetto che viene inoltrato a Lambda non deve avere alcun PHI, sebbene l'oggetto stesso possa contenere tali dati.

# AWS Managed Services

AWS Managed Services fornisce una gestione continua delle infrastrutture AWS. Implementando le migliori pratiche per la manutenzione dell'infrastruttura del cliente, AWS Managed Services aiuta a ridurre i costi operativi e i rischi. AWS Managed Services automatizza attività comuni come richieste di modifica, monitoraggio, gestione delle patch, sicurezza e servizi di backup e fornisce servizi per l'intero ciclo di vita per la fornitura, la gestione e il supporto delle infrastrutture.

I clienti possono utilizzare AWS Managed Services per gestire carichi di lavoro AWS che operano con dati contenenti PHI. L'utilizzo di AWS Managed Services non modifica i servizi AWS idonei all'uso con PHI. Gli strumenti e l'automazione forniti da AWS Managed Services non possono essere utilizzati per l'archiviazione o la trasmissione di PHI.

# AWS OpsWorks per Chef Automate

AWS OpsWorks for Chef Automate è un servizio di gestione della configurazione completamente gestito che ospita Chef Automate, un set di strumenti di automazione di Chef per la gestione dell'infrastruttura e delle applicazioni. Il servizio stesso non contiene, trasmette o gestisce

informazioni PHI o informazioni sensibili, ma i clienti devono assicurarsi che tutte le risorse configurate da OpsWorks for Chef Automate siano configurate in modo coerente con la Guida. Le chiamate API vengono acquisite con. AWS CloudTrail Per ulteriori informazioni, consulta Logging AWS OpsWorks Stacks API Calls with. AWS CloudTrail

## AWS OpsWorks per Puppet Enterprise

AWS OpsWorks for Puppet Enterprise è un servizio di gestione della configurazione completamente gestito che ospita Puppet Enterprise, un set di strumenti di automazione di Puppet per la gestione dell'infrastruttura e delle applicazioni. Il servizio in sé non contiene, trasmette o gestisce informazioni PHI o informazioni sensibili, ma i clienti devono assicurarsi che qualsiasi risorsa configurata da OpsWorks for Puppet Enterprise sia configurata in modo coerente con la Guida. Le chiamate API vengono acquisite con. AWS CloudTrail Per ulteriori informazioni, consulta Logging AWS OpsWorks Stacks API Calls with. AWS CloudTrail

## AWS OpsWorks Stack

AWS OpsWorks Stacks offre un modo semplice e flessibile per creare e gestire stack e applicazioni. I clienti possono utilizzare AWS OpsWorks Stacks per distribuire e monitorare le applicazioni nei propri stack.

AWS OpsWorks Stacks crittografa tutto il traffico in transito. Tuttavia, i data bag crittografati (un meccanismo di archiviazione dei dati di Chef) non sono disponibili e tutte le risorse che devono essere archiviate in modo sicuro, come PHI, segreti/password, certificati e così via, devono essere archiviate in un bucket crittografato in Amazon S3. AWS OpsWorks Stack lo utilizza AWS CloudTrail per registrare tutte le chiamate API.

## AWS Organizations

AWS Organizations aiuta i clienti a gestire e governare centralmente il proprio ambiente man mano che crescono e scalano le proprie risorse AWS. Utilizzando AWS Organizations, possono creare in modo programmatico nuovi account AWS e allocare risorse, raggruppare account per organizzare i flussi di lavoro, applicare policy ad account o gruppi per la governance e semplificare la fatturazione utilizzando un unico metodo di pagamento per tutti i loro account.

Inoltre, AWS Organizations è integrato con altri servizi AWS in modo che i clienti possano definire configurazioni centrali, meccanismi di sicurezza, requisiti di audit e condivisione delle risorse tra gli

account della propria organizzazione. AWS Organizations è disponibile per tutti i clienti AWS senza costi aggiuntivi.

AWS Organizations è un servizio di orchestrazione che non elabora, archivia o trasmette direttamente i dati degli utenti. Il servizio non crittografa i contenuti dei clienti, ma i servizi sottostanti che vengono lanciati all'interno crittografano AWS Organizations i dati degli utenti. AWS Organizations è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un servizio AWS in AWS Organizations.

# AWS RoboMaker

AWS RoboMaker consente ai clienti di eseguire codice nel cloud per lo sviluppo di applicazioni e fornisce un servizio di simulazione robotica per accelerare i test delle applicazioni. AWS fornisce RoboMaker anche un servizio di gestione della flotta di robotica per la distribuzione, l'aggiornamento e la gestione di applicazioni remote.

Il traffico di rete contenente PHI deve crittografare i dati in transito. Tutte le comunicazioni di gestione con il server di simulazione avvengono tramite TLS e i clienti devono utilizzare meccanismi di crittografia di trasporto a standard aperti per le connessioni ad altri servizi AWS. AWS si integra RoboMaker anche con CloudTrail per registrare tutte le chiamate API verso uno specifico bucket Amazon S3.

RoboMaker I log AWS non contengono PHI e i volumi EBS utilizzati dal server di simulazione sono crittografati. Quando trasferiscono dati che possono contenere PHI ad altri servizi, come Amazon S3, i clienti devono seguire le linee guida del servizio ricevente per l'archiviazione dei PHI. Per quanto riguarda le implementazioni su robot, i clienti devono garantire che la crittografia dei dati in transito e in archivio sia coerente con la loro interpretazione della Guida.

# Metriche dell'SDK AWS

I clienti aziendali possono utilizzare l' CloudWatch agente AWS con AWS SDK Metrics for Enterprise Support (SDK Metrics) per raccogliere metriche dagli SDK AWS sui loro host e client. Queste metriche sono condivise con AWS Enterprise Support. SDK Metrics può aiutare i clienti a raccogliere metriche e dati diagnostici pertinenti sulle connessioni delle loro applicazioni ai servizi AWS senza aggiungere strumentazione personalizzata al codice e riduce il lavoro manuale necessario per condividere log e dati. AWS Support

Tieni presente che SDK Metrics è disponibile solo per i clienti AWS con un abbonamento Enterprise Support. I clienti possono utilizzare SDK Metrics con qualsiasi applicazione che richiama direttamente

i servizi AWS e che è stata creata utilizzando un SDK AWS che è una delle versioni elencate nella documentazione di AWS Metrics.

SDK Metrics monitora le chiamate effettuate dall'SDK AWS e utilizza l' CloudWatch agente in esecuzione nello stesso ambiente di un'applicazione client.

L' CloudWatch agente crittografa i dati in transito dal computer locale fino alla consegna nel gruppo di log di destinazione. Il gruppo di log può essere configurato per essere crittografato seguendo le istruzioni riportate in Encrypt Log Data in CloudWatch Logs Using. AWS KMS

## AWS Secrets Manager

AWS Secrets Manager è un servizio AWS che semplifica la gestione dei «segreti» da parte dei clienti. I segreti possono essere credenziali di database, password, chiavi API di terze parti e persino testo arbitrario. AWS Secrets Manager potrebbe essere usato per memorizzare PHI se tali informazioni sono contenute all'interno di «segreti». Tutti i segreti archiviati da AWS Secrets Manager sono crittografati in archivio utilizzando AWS Key Management System (KMS). Gli utenti possono selezionare la AWS KMS chiave utilizzata per creare un nuovo segreto. Se non è selezionata alcuna chiave, verrà utilizzata la chiave predefinita per l'account. AWS Secrets Manager utilizza AWS CloudTrail per registrare tutte le chiamate API.

## AWS Security Hub

AWS Security Hub raccoglie e consolida i risultati dei servizi di sicurezza AWS abilitati nell'ambiente del cliente, come i risultati del rilevamento delle intrusioni di Amazon, le scansioni di vulnerabilità di Amazon Inspector GuardDuty, i risultati delle bucket policy di Amazon S3 di Amazon Macie, le risorse accessibili al pubblico e interaccount di IAM Access Analyzer e le risorse prive di copertura WAF di. AWS Firewall Manager AWS Security Hub consolida inoltre i risultati delle soluzioni di sicurezza AWS Partner Network (APN) integrate.

AWS Security Hub si integra con Amazon CloudWatch Events, consentendo ai clienti di creare flussi di lavoro di risposta e correzione personalizzati. I clienti possono inviare facilmente i risultati a SIEM, strumenti di chat, sistemi di ticketing, strumenti di Security Orchestration Automation and Response (SOAR) e piattaforme di gestione delle chiamate. Le azioni di risposta e riparazione possono essere completamente automatizzate oppure possono essere attivate manualmente nella console. I clienti possono anche utilizzare documenti e AWS Lambda funzioni di AWS Systems Manager automazione per creare flussi di lavoro di riparazione automatizzati da cui è possibile avviare. AWS Step Functions AWS Security Hub

Per garantire la protezione dei dati, AWS Security Hub crittografa i dati inattivi e i dati in transito tra i servizi componenti. I revisori di terze parti valutano la sicurezza e la conformità nell' AWS Security Hub ambito di più programmi di conformità AWS. AWS Security Hub fa parte dei programmi di conformità SOC, ISO, PCI e HIPAA di AWS.

# AWS Server Migration Service

AWS Server Migration Service (AWS SMS) automatizza la migrazione di macchine virtuali VMware vSphere o Microsoft Hyper-v/SCVMM locali sul cloud AWS. AWS SMS replica in modo incrementale le macchine virtuali server come Amazon Machine Images (AMI) ospitate nel cloud pronte per la distribuzione su Amazon EC2.

I server in esecuzione in locale e in fase di migrazione al cloud con (AWS SMS) possono contenere dati PHI. AWS SMS crittografa i dati durante il transito e quando le immagini delle macchine virtuali del server vengono organizzate per il posizionamento finale su EC2. Consulta le linee guida per EC2 e la configurazione di volumi di storage crittografati durante la migrazione di una macchina virtuale server contenente PHI con AWS SMS. AWS SMS utilizza CloudTrail per registrare tutte le chiamate API.

# AWS Serverless Application Repository

Il AWS Serverless Application Repository (SAR) è un repository gestito per applicazioni serverless. Consente a team, organizzazioni e singoli sviluppatori di archiviare e condividere applicazioni riutilizzabili e di assemblare e implementare facilmente architetture serverless in modi nuovi e potenti. Le applicazioni sono AWS CloudFormation modelli che contengono le definizioni dell'infrastruttura dell'applicazione e i file binari compilati del codice funzionale dell'applicazione. AWS Lambda

Sebbene sia possibile che le applicazioni in uso elaborino il AWS Serverless Application Repository PHI, lo faranno solo dopo essere state installate sull'account del cliente e non come parte del SAR stesso. AWS Serverless Application Repository Crittografa i file caricati dai clienti, inclusi i pacchetti di distribuzione e gli archivi di livello. Per i dati in transito, AWS Serverless Application Repository utilizza TLS per crittografare i dati tra il servizio e l'agente. AWS Serverless Application Repository è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un servizio AWS in AWS Serverless Application Repository.

# Catalogo dei servizi

Service Catalog consente agli amministratori IT di creare, gestire e distribuire portafogli di prodotti approvati agli utenti finali, che possono quindi accedere ai prodotti di cui hanno bisogno in un portale personalizzato. Service Catalog viene utilizzato per catalogare, condividere e distribuire soluzioni self-service su AWS e non può essere utilizzato per archiviare, trasmettere o elaborare PHI. Il codice PHI non deve essere inserito in alcun metadato per gli articoli del Service Catalog o all'interno di alcuna descrizione dell'articolo. Service Catalog utilizza AWS CloudTrail per registrare tutte le chiamate API.

# AWS Shield

AWS Shield è un servizio di protezione DDoS (Distributed Denial of Service) gestito che protegge le applicazioni Web in esecuzione su AWS. AWS Shield fornisce un rilevamento sempre attivo e mitigazioni automatiche in linea che riducono al minimo i tempi di inattività e la latenza delle applicazioni, quindi non è necessario impegnarsi per trarre vantaggio dalla protezione DDoS. AWS Support

AWS Shield non può essere utilizzato per archiviare o trasmettere PHI, ma può invece essere utilizzato per proteggere le applicazioni Web che funzionano con PHI. Pertanto, non è necessaria alcuna configurazione speciale durante l'interazione. AWS Shield

Tutti i clienti AWS beneficiano delle protezioni automatiche di AWS Shield Standard, senza costi aggiuntivi. AWS Shield Standard difende dagli attacchi DDoS più comuni e frequenti a livello di rete e trasporto che prendono di mira i loro siti Web o le loro applicazioni. Per livelli di protezione più elevati contro gli attacchi diretti alle loro applicazioni Web in esecuzione su risorse Elastic Load Balancing (ELB) CloudFront, Amazon e Amazon Route 53, i clienti possono abbonarsi. AWS Shield Advanced

# AWS Snowball

Con AWS Snowball (Snowball), i clienti possono trasferire centinaia di terabyte o petabyte di dati tra i data center locali e Amazon Simple Storage Service (Amazon S3). I dati PHI archiviati AWS Snowball devono essere crittografati quando sono archiviati, in conformità con la Guida. Quando creano un processo di importazione, i clienti devono specificare l'ARN della AWS KMS chiave da utilizzare per proteggere i dati all'interno di Snowball. Inoltre, durante la creazione del processo di importazione, i clienti devono scegliere un bucket S3 di destinazione che soddisfi gli standard di crittografia stabiliti dalla Guida.

Sebbene attualmente Snowball non supporti la crittografia lato server con chiavi AWS KMS gestite (SSE-KMS) o la crittografia lato server con chiavi fornite dal cliente (SSE-C), Snowball supporta la crittografia lato server con chiavi di crittografia gestite da Amazon S3 (SSE-S3). Per ulteriori informazioni, consulta Protezione dei dati mediante la crittografia Server side con chiavi gestite da Amazon S3 (SSE-S3).

In alternativa, i clienti possono utilizzare la metodologia di crittografia di loro scelta per crittografare PHI prima di archiviare i dati. AWS Snowball

Attualmente, i clienti possono utilizzare l' AWS Snowball appliance standard come parte del nostro BAA.

## AWS Snowball Edge

AWS Snowball Edge si connette alle applicazioni e all'infrastruttura dei clienti esistenti utilizzando interfacce di storage standard, semplificando il processo di trasferimento dei dati e riducendo al minimo la configurazione e l'integrazione. Snowball Edge può raggrupparsi per formare un livello di storage locale ed elaborare i dati dei clienti in loco, aiutandoli a garantire che le loro applicazioni continuino a funzionare anche quando non sono in grado di accedere al cloud.

Per garantire che PHI rimanga crittografato durante l'utilizzo di Snowball Edge, i clienti devono assicurarsi di utilizzare un protocollo di connessione crittografato come HTTPS o SSL/TLS quando AWS Lambda utilizzano procedure basate AWS IoT Greengrass su tecnologia per trasmettere PHI da/a risorse esterne a Snowball Edge. Inoltre, i PHI devono essere crittografati durante l'archiviazione nei volumi locali di Snowball Edge, tramite accesso locale o tramite NFS. La crittografia viene applicata automaticamente ai dati inseriti in Snowball Edge utilizzando la Snowball Management Console e l'API per il trasporto di massa in S3. Per ulteriori informazioni sul trasporto dei dati in S3, consulta la relativa guida per. the section called “AWS Snowball”

## AWS Step Functions

AWS Step Functions semplifica il coordinamento dei componenti delle applicazioni distribuite e dei microservizi utilizzando flussi di lavoro visivi. AWS Step Functions non è in grado di archiviare, trasmettere o elaborare PHI. PHI non deve essere inserito nei metadati o all'interno di alcuna definizione di attività AWS Step Functions o macchina a stati. AWS Step Functions utilizza AWS CloudTrail per registrare tutte le chiamate API.

# AWS Storage Gateway

AWS Storage Gateway è un servizio di storage ibrido che consente alle applicazioni locali dei clienti di utilizzare senza problemi lo storage nel cloud AWS. Il gateway utilizza protocolli di storage standard aperti per connettere le applicazioni di storage e i flussi di lavoro esistenti ai servizi di storage nel cloud AWS per ridurre al minimo le interruzioni dei processi.

## Gateway di file

Il gateway di file è un tipo AWS Storage Gateway che supporta un'interfaccia di file in Amazon S3 e che si aggiunge all'attuale volume basato su blocchi e allo storage VTL. Il gateway di file utilizza HTTPS per comunicare con S3 e archivia tutti gli oggetti crittografati in S3 utilizzando SSE-S3, per impostazione predefinita, o utilizzando la crittografia lato client con chiavi archiviate in. AWS KMS I metadati dei file, come i nomi dei file, rimangono non crittografati e non devono contenere alcun PHI.

## Gateway di volumi

Volume gateway fornisce volumi di storage basati sul cloud che i clienti possono montare come dispositivi Internet Small Computer System Interface (iSCSI) da server di applicazioni locali. I clienti devono collegare i dischi locali come buffer di caricamento e cache alla macchina virtuale Volume Gateway in conformità ai requisiti normativi e di conformità interni. Si raccomanda che, per PHI, questi dischi siano in grado di fornire la crittografia a riposo. La comunicazione tra la macchina virtuale Volume Gateway e AWS è crittografata utilizzando TLS 1.2 per proteggere PHI durante il trasporto.

## Gateway di nastri virtuali

Tape Gateway fornisce un'interfaccia VTL (Virtual Tape Library) per applicazioni di backup di terze parti in esecuzione in locale. I clienti devono abilitare la crittografia per PHI all'interno dell'applicazione di backup di terze parti quando configurano un processo di backup su nastro. La comunicazione tra la VM Tape Gateway e AWS è crittografata utilizzando TLS 1.2 per proteggere PHI durante il trasporto. I clienti che utilizzano una qualsiasi delle configurazioni di Storage Gateway con PHI devono abilitare la registrazione completa. Per ulteriori informazioni, consulta Che cos'è AWS Storage Gateway?

# AWS Systems Manager

AWS Systems Manager è un'interfaccia unificata che consente ai clienti di centralizzare facilmente i dati operativi, automatizzare le attività tra le risorse AWS e abbreviare i tempi necessari per rilevare e risolvere i problemi operativi nella propria infrastruttura. Systems Manager offre una visione completa delle prestazioni e della configurazione dell'infrastruttura del cliente, semplifica la gestione delle risorse e delle applicazioni e semplifica il funzionamento e la gestione dell'infrastruttura su larga scala.

Quando inviano dati che possono contenere PHI ad altri servizi, come Amazon S3, i clienti devono seguire le linee guida del servizio ricevente per l'archiviazione dei PHI. I clienti non devono includere PHI nei metadati o negli identificatori, come i nomi dei documenti e i nomi dei parametri.

# AWS Transfer for SFTP

AWS Transfer for SFTP fornisce l'accesso Secure File Transfer Protocol (SFTP) alle risorse S3 di un cliente. Ai clienti viene presentato un server virtuale, a cui si accede utilizzando il protocollo SFTP standard presso un endpoint di servizio regionale. Dal punto di vista del cliente AWS e del client SFTP, il gateway SFTP si presenta come un server SFTP standard ad alta disponibilità. Sebbene il servizio stesso non memorizzi, elabori o trasmetta PHI, le risorse a cui il cliente accede su Amazon S3 devono essere configurate in modo coerente con la Guida. I clienti possono anche utilizzare AWS CloudTrail per registrare le chiamate API effettuate su AWS Transfer for SFTP.

# AWS WAF: firewall per applicazioni Web

AWS WAF è un firewall per applicazioni Web che aiuta a proteggere le applicazioni Web dei clienti da exploit Web comuni che potrebbero influire sulla disponibilità delle applicazioni, compromettere la sicurezza o consumare risorse eccessive. I clienti possono collocare AWS WAF tra le loro applicazioni Web ospitate su AWS che operano con o scambiano PHI e i loro utenti finali. Come per la trasmissione di qualsiasi PHI su AWS, i dati contenenti PHI devono essere crittografati durante il transito. Consulta le linee guida per Amazon EC2 per comprendere meglio le opzioni di crittografia disponibili.

# AWS X-Ray

AWS X-Ray è un servizio che raccoglie dati sulle richieste soddisfatte dall'applicazione di un cliente e fornisce strumenti che il cliente può utilizzare per visualizzare, filtrare e acquisire informazioni

su tali dati per identificare problemi e opportunità di ottimizzazione. Per ogni richiesta tracciata all'applicazione di un cliente, possono visualizzare informazioni dettagliate non solo sulla richiesta e sulla risposta, ma anche sulle chiamate effettuate dall'applicazione verso risorse AWS, microservizi, database e API Web HTTP a valle. AWS X-Ray non devono essere utilizzate per archiviare o elaborare PHI. Le informazioni trasmesse da e verso AWS X-Ray sono crittografate per impostazione predefinita. Durante l'utilizzo AWS X-Ray, non inserite alcun PHI nelle annotazioni dei segmenti o nei metadati dei segmenti.

## Sistema di bilanciamento del carico elastico

I clienti possono utilizzare Elastic Load Balancing per terminare ed elaborare sessioni contenenti PHI. I clienti possono scegliere tra Classic Load Balancer o Application Load Balancer. Poiché tutto il traffico di rete contenente PHI deve essere crittografato in transito end-to-end, i clienti hanno la flessibilità necessaria per implementare due diverse architetture:

I clienti possono terminare HTTPS, HTTP/2 over TLS (per Application) o SSL/TLS su Elastic Load Balancing creando un load balancer che utilizza un protocollo crittografato per le connessioni. Questa funzionalità consente la crittografia del traffico tra il load balancer e i client che avviano sessioni HTTPS, HTTP/2 over TLS o SSL/TLS e per le connessioni tra il load balancer e le istanze di backend del cliente. Le sessioni contenenti PHI devono crittografare sia i listener front-end che quelli di backend per la crittografia del trasporto. I clienti devono valutare i propri certificati e le politiche di negoziazione delle sessioni e mantenerli coerenti con le Linee guida. Per ulteriori informazioni, consulta HTTPS Listeners for Your Classic Load Balancer.

In alternativa, i clienti possono configurare Amazon ELB in modalità TCP di base (per Classic) o over WebSockets (per Application) e passare sessioni crittografate a istanze di backend in cui la sessione crittografata viene interrotta. In questa architettura, i clienti gestiscono i propri certificati e le proprie politiche di negoziazione TLS nelle applicazioni eseguite nelle proprie istanze. Per ulteriori informazioni, consulta Listeners for Your Classic Load Balancer. In entrambe le architetture, i clienti devono implementare un livello di registrazione che ritengono coerente con i requisiti HIPAA e HITECH.

## FreeRTOS

FreerTOS è un sistema operativo per microcontrollori che semplifica la programmazione, l'implementazione, la protezione, la connessione e la gestione di dispositivi edge di piccole dimensioni e a basso consumo. FreerTOS si basa sul kernel FreerTOS, un popolare sistema operativo open source per microcontrollori, e lo estende con librerie software che semplificano il

collegamento sicuro di dispositivi di piccole dimensioni e a basso consumo ai servizi Cloud AWS come Core o a dispositivi edge più potenti in esecuzione. AWS IoT AWS IoT Greengrass

I dati contenenti PHI possono ora essere crittografati in transito e mentre sono inattivi quando si utilizza un dispositivo qualificato che esegue FreerTOS. FreerTOS fornisce due librerie per garantire la sicurezza della piattaforma: TLS e PKCS #11. L'API TLS deve essere utilizzata per crittografare e autenticare tutto il traffico di rete che contiene PHI. PKCS #11 fornisce un'interfaccia standard per le operazioni crittografiche del software e deve essere utilizzato per crittografare qualsiasi PHI archiviato su un dispositivo qualificato che esegue FreerTOS.

# AWS KMS Utilizzo per la crittografia di PHI

Le chiavi KMS possono essere utilizzate per crittografare/decrittografare le chiavi di crittografia dei dati utilizzate per crittografare PHI nelle applicazioni di un cliente o nei servizi AWS che utilizzano. AWS KMS AWS KMS possono essere utilizzate insieme a un account HIPAA, ma le informazioni PHI possono essere elaborate, archiviate o trasmesse solo nei servizi idonei all'HIPAA. AWS KMS viene normalmente utilizzato per generare e gestire chiavi per applicazioni in esecuzione in altri servizi idonei all'HIPAA.

Ad esempio, un'applicazione che elabora PHI in Amazon EC2 potrebbe utilizzare GenerateDataKey la chiamata API per generare chiavi di crittografia dei dati per crittografare e decrittografare PHI nell'applicazione. Le chiavi di crittografia dei dati sarebbero protette dalle chiavi KMS del cliente archiviate in AWS KMS, creando una gerarchia di chiavi altamente verificabile quando le chiamate API vengono registrate. AWS KMS AWS CloudTrail I PHI non devono essere memorizzati nei tag (metadati) delle chiavi archiviate in. AWS KMS

# VM Import/Export

VM Import/Export consente ai clienti di importare facilmente le immagini delle macchine virtuali dall'ambiente esistente alle istanze Amazon EC2 ed esportarle nuovamente nell'ambiente locale. Questa offerta consente ai clienti di sfruttare gli investimenti esistenti nelle macchine virtuali che hai creato per soddisfare la sicurezza IRIT, la gestione della configurazione e i requisiti di conformità, trasferendo tali macchine virtuali in Amazon EC2 come istanze. ready-to-use I clienti possono anche esportare le istanze importate nella propria infrastruttura di virtualizzazione locale, consentendo loro di distribuire carichi di lavoro nell'infrastruttura IT dell'azienda.

VM Import/Export è disponibile senza costi aggiuntivi oltre ai costi di utilizzo standard per Amazon EC2 e Amazon S3.

Per importare le immagini dei clienti, i clienti possono utilizzare questo AWS CLI o altri strumenti di sviluppo per importare l'immagine di una macchina virtuale (VM) dal proprio ambiente VMware. Se i clienti utilizzano la piattaforma di virtualizzazione VMware vSphere, possono anche utilizzare AWS Management Portal for vCenter per importare la propria macchina virtuale. Come parte del processo di importazione, VM Import convertirà la macchina virtuale del cliente in un'AMI Amazon EC2, che potrà utilizzare per eseguire istanze Amazon EC2. Una volta importata la macchina virtuale, possono sfruttare l'elasticità, la scalabilità e il monitoraggio di Amazon tramite offerte come Auto Scaling, Elastic Load Balancing e supportare le immagini importate. CloudWatch

I clienti possono esportare istanze Amazon EC2 importate in precedenza utilizzando gli strumenti API di Amazon EC2. Basta specificare l'istanza di destinazione, il formato di file della macchina virtuale e un bucket Amazon S3 di destinazione e VM Import/Export esporterà automaticamente l'istanza nel bucket Amazon S3 insieme alle opzioni di crittografia per proteggere la trasmissione e l'archiviazione delle immagini delle macchine virtuali. I clienti possono quindi scaricare e avviare la macchina virtuale esportata all'interno della propria infrastruttura di virtualizzazione locale.

I clienti possono importare macchine virtuali Windows e Linux che utilizzano i formati di virtualizzazione VMware ESX o Workstation, Microsoft Hyper-V e Citrix Xen. Inoltre, i clienti possono esportare istanze Amazon EC2 precedentemente importate nei formati VMware ESX, Microsoft Hyper-V o Citrix Xen. Per un elenco completo dei sistemi operativi, delle versioni e dei formati supportati, consulta VM Import/Export Requirements. AWS prevede di aggiungere il supporto per sistemi operativi, versioni e formati aggiuntivi in futuro.

# Controllo, backup e disaster recovery

La regola di sicurezza dell'HIPAA prevede requisiti dettagliati relativi a funzionalità di controllo approfondite, procedure di backup dei dati e meccanismi di disaster recovery. I servizi di AWS contengono molte funzionalità che aiutano i clienti a soddisfare le loro esigenze. Ad esempio, i clienti dovrebbero prendere in considerazione la possibilità di istituire funzionalità di controllo per consentire agli analisti della sicurezza di esaminare registri o report dettagliati delle attività per vedere chi aveva accesso, l'immissione dell'indirizzo IP, a quali dati è stato effettuato l'accesso, ecc.

Questi dati devono essere tracciati, registrati e archiviati in una posizione centrale per lunghi periodi di tempo, in caso di audit. Utilizzando Amazon EC2, i clienti possono eseguire i file di registro delle attività e gli audit fino al livello di pacchetto sui propri server virtuali, proprio come fanno sull'hardware tradizionale. Inoltre, possono tracciare qualsiasi traffico IP che raggiunge l'istanza del server virtuale. Gli amministratori di un cliente possono eseguire il backup dei file di registro in Amazon S3 per uno storage affidabile a lungo termine.

L'HIPAA prevede inoltre requisiti dettagliati relativi al mantenimento di un piano di emergenza per proteggere i dati in caso di emergenza e deve creare e conservare copie esatte recuperabili del PHI elettronico. Per implementare un piano di backup dei dati su AWS, Amazon EBS offre uno storage persistente per le istanze di server virtuali Amazon EC2. Questi volumi possono essere esposti come dispositivi a blocchi standard e offrono uno storage fuori istanza che persiste indipendentemente dalla durata di un'istanza. In linea con le linee guida HIPAA, i clienti possono creare point-in-time snapshot di volumi Amazon EBS che vengono archiviati automaticamente in Amazon S3 e replicati su più zone di disponibilità, che sono posizioni distinte progettate per essere isolate dai guasti in altre zone di disponibilità.

È possibile accedere a queste istantanee in qualsiasi momento e possono proteggere i dati per una durabilità a lungo termine. Amazon S3 offre anche una soluzione ad alta disponibilità per l'archiviazione dei dati e i backup automatici. Basta caricare un file o un'immagine in Amazon S3, più copie ridondanti vengono create automaticamente e archiviate in data center separati. È possibile accedere a questi file in qualsiasi momento, da qualsiasi luogo (in base alle autorizzazioni) e vengono archiviati fino all'eliminazione intenzionale.

Inoltre, AWS offre intrinsecamente una varietà di meccanismi di disaster recovery. Il disaster recovery, il processo di protezione dei dati e dell'infrastruttura IT di un'organizzazione in caso di emergenza, implica il mantenimento di sistemi ad alta disponibilità, la replica dei dati e del sistema fuori sede e l'accesso continuo a entrambi.

Con Amazon EC2, gli amministratori possono avviare le istanze del server molto rapidamente e utilizzare un indirizzo IP elastico (un indirizzo IP statico per l'ambiente di cloud computing) per un failover agevole da una macchina all'altra. Amazon EC2 offre anche zone di disponibilità. Gli amministratori possono avviare istanze Amazon EC2 in più zone di disponibilità per creare sistemi geograficamente diversi, tolleranti ai guasti e altamente resilienti in caso di guasti di rete, disastri naturali e la maggior parte delle altre probabili fonti di downtime.

Utilizzando Amazon S3, i dati di un cliente vengono replicati e archiviati automaticamente in data center separati per fornire uno storage dei dati affidabile progettato per fornire una disponibilità del 99,99%.

Utilizzando AWS Elastic Disaster Recovery (AWS DRS), i clienti possono ripristinare rapidamente le applicazioni su AWS, up-to-date nello stato più avanzato delle applicazioni o da un momento precedente.

# Revisioni del documento

Per ricevere notifiche sugli aggiornamenti di questo white paper, iscriviti al feed RSS.

| Modifica | Descrizione | Data |
| --- | --- | --- |
| Aggiornamento secondario | Aggiornamento secondario | 12 maggio 2023 |
| Aggiornamento secondario | Whitepaper aggiornato per ampliare i contenuti disponibili sui servizi. | 28 settembre 2022 |
| Aggiornamento secondario | Correggi il linguaggio non inclusivo. | 6 aprile 2022 |
| Whitepaper aggiornato | Sono state aggiunte informazioni su AWS Application Migration Service e informazioni aggiornate per Amazon ECS | 6 dicembre 2021 |
| Whitepaper aggiornato | Informazioni aggiornate nelle sezioni Amazon Healthlake e Amazon VPC | 9 novembre 2021 |
| Whitepaper aggiornato | Sono state aggiunte informazioni su AWS Network Firewall | 9 settembre 2021 |
| Whitepaper aggiornato | Informazioni aggiornate sui profili dei clienti Amazon Connect | 26 agosto 2021 |
| Whitepaper aggiornato | Sezioni aggiunte Amazon AppFlow e AWS Glue DataBrew | 22 luglio 2021 |
| Whitepaper aggiornato | Navigazione e organizzazione aggiornate. | 26 Aprile 2021 |

| | | |
|---|---|---|
| Whitepaper aggiornato | Sono state aggiunte le seguenti sezioni: AWS CodeDeploy, AWS CodePipeline, Amazon Aurora, Aurora PostgreSQL, Amazon Textract, Amazon Polly, Amazon FSx, AWS Auto AWS Backup Scaling,,,,,,,,, VM Import/Export, Amazon, Amazon. AWS Elastic Beanstalk AWS Firewall Manager AWS Organizations AWS Security Hub AWS Serverless Application Repository HealthLake EventBridge Sezione Amazon Aurora aggiornata. | 31 marzo 2021 |
| Whitepaper aggiornato | Aggiunta una sezione su AWS App Mesh e contenuti AWS System Manager aggiornati | 25 agosto 2020 |
| Whitepaper aggiornato | Sono state aggiunte sezioni Amazon Appstream 2.0, AWS SDK Metrics, AWS Data Exchange, Amazon MSK, Amazon Pinpoint, Amazon Lex, Amazon SES e Amazon Forecast, Amazon Quantum Ledger Database (QLDB),. AWS Cloud Map | 7 maggio 2020 |

| | | |
|---|---|---|
| Whitepaper aggiornato | Sono state aggiunte sezioni su Amazon CloudWatch, Amazon CloudWatch Events, Amazon Data Firehose, Amazon Managed Service per Apache Flink, Amazon Service, OpenSearch Amazon DocumentDB (con compatibilità MongoDB), AWS Mobile Hub, per AWS OpsWorks Chef Automate, per Puppet Enterprise, AWS AWS IoT Greengrass Transfer for SFTP, AWS, Amazon Comprehend Medical e AWS. AWS OpsWorks DataSync AWS Global Accelerator RoboMaker | 1 gennaio 2020 |
| Whitepaper aggiornato | Sono state aggiunte sezioni su Amazon Comprehend, Amazon Transcribe, Amazon Translate e AWS Certificate Manager. | 1 gennaio 2019 |
| Whitepaper aggiornato | Sono state aggiunte sezioni su Amazon Athena, Amazon EKS, AWS IoT Core e Amazon FreerTOS AWS IoT Device Management, Amazon, Amazon GuardDuty Neptune, AWS Server Migration Service, Amazon MQ e. AWS Database Migration Service AWS Glue | 1 novembre 2018 |

| | | |
|---|---|---|
| Whitepaper aggiornato | Sono state aggiunte sezioni su Amazon Elastic File System (EFS), Amazon Kinesis Video Streams, Amazon Rekogniti on, Amazon, SageMaker Amazon Simple Workflow, AWS Secrets Manage, Service Catalog e. AWS Step Functions | 1 giugno 2018 |
| Whitepaper aggiornato | Sono state aggiunte sezioni su AWS CloudFormation, AWS X-Ray, AWS CloudTrail, AWS CodeBuild AWS CodeCommi t AWS Config, e Stack. AWS OpsWorks | 1 aprile 2018 |
| Whitepaper aggiornato | È stata aggiunta una sezione su. AWS Fargate | 1 gennaio 2018 |

Aggiornamenti effettuati prima del 2018:

| Data | Descrizione |
|---|---|
| Novembre 2017 | Sono state aggiunte sezioni su Amazon EC2 Container Registry, Amazon Macie, QuickSight Amazon e. AWS Managed Services |
| Novembre 2017 | Sono state aggiunte sezioni su Amazon ElastiCache per Redis e Amazon CloudWatch. |
| Ottobre 2017 | Sono state aggiunte sezioni su Amazon SNS AWS Storage Gateway, Amazon Route 53 e. AWS CloudHSM Sezione aggiornata su. AWS Key Management Service |

| Data | Descrizione |
| --- | --- |
| Settembre 2017 | Sono state aggiunte sezioni su Amazon Connect, Amazon Kinesis Streams, Amazon RDS (Maria) DB, Amazon RDS SQL AWS Batch Server, AWS Lambda AWS Snowball , Edge e la funzionalità Lambda @Edge di Amazon. CloudFront |
| Agosto 2017 | Sono state aggiunte sezioni su Amazon EC2 Systems Manager e Amazon Inspector. |
| 2017 luglio | Sono state aggiunte sezioni su Amazon WorkSpaces, Amazon WorkDocs, AWS Directory Service e Amazon ECS. |
| Giugno 2017 | Sono state aggiunte sezioni su Amazon CloudFront, AWS WAF e Amazon S3 AWS Shield Transfer Acceleration. |
| Maggio 2017 | Rimosso il requisito per le istanze dedicate o gli host dedicati per l'elaborazione di PHI in EC2 ed EMR. |
| Marzo 2017 | Elenco aggiornato di servizi in modo che rimandino alla pagina AWS Services in Scope by Compliance Program. È stata aggiunta una descrizione per Amazon API Gateway. |
| Gennaio 2017 | Aggiornato al modello più recente. |
| Ottobre 2016 | Prima pubblicazione |

# Note

I clienti sono responsabili della propria valutazione indipendente delle informazioni contenute in questo documento. Questo documento: (a) è solo a scopo informativo, (b) rappresenta le attuali offerte e pratiche di prodotti AWS, che sono soggette a modifiche senza preavviso, e (c) non crea alcun impegno o garanzia da parte di AWS e delle sue affiliate, fornitori o licenzianti. I prodotti o i servizi AWS sono forniti «così come sono» senza garanzie, dichiarazioni o condizioni di alcun tipo, esplicite o implicite. Le responsabilità di AWS nei confronti dei propri clienti sono definite dai contratti AWS e il presente documento non costituisce parte né modifica qualsivoglia contratto tra AWS e i suoi clienti.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.