Architecture de la sécurité et de la conformité HIPAA dans Amazon Web Services

Janvier 2017

Mentions légales

Ce document est fourni à titre informatif uniquement. Il présente l'offre de produits et les pratiques actuelles d'AWS à la date de publication de ce document, des informations qui sont susceptibles d'être modifiées sans préavis. Il incombe aux clients de procéder à leur propre évaluation indépendante des informations contenues dans ce document et chaque client est responsable de son utilisation des produits ou services AWS, chacun étant fourni « en l'état », sans garantie d'aucune sorte, qu'elle soit explicite ou implicite. Ce document n'offre pas de garantie, représentation, engagement contractuel, condition ou assurance de la part d'AWS, de ses sociétés apparentées, fournisseurs ou concédants de licence. Les responsabilités et obligations d'AWS vis-à-vis de ses clients sont régies par les contrats AWS. Le présent document ne fait partie d'aucun contrat et ne modifie aucun contrat entre AWS et ses clients.

Table des matières

Résumé

Ce document décrit succinctement comment des sociétés peuvent utiliser Amazon Web Services (AWS) pour créer des applications conformes à HIPAA (Health Insurance Portability and Accountability Act). Nous expliquons les règles de confidentialité et de sécurité HIPAA liées à la protection des informations de santé protégées (PHI), comment utiliser AWS pour chiffrer des données en transit et au repos et comment utiliser des fonctions AWS pour répondre aux exigences HIPAA en termes d'audit, sauvegardes et reprise après sinistre.

Introduction

Le Health Insurance Portability and Accountability Act (HIPAA) de 1996 s'applique aux « entités couvertes » et à leurs « partenaires ». Ces entités couvertes incluent des fournisseurs de soins de santé engagés dans certaines transactions électroniques, régimes de santé et prestataires de soins de santé. Les partenaires sont des entités qui fournissent à une entité couverte des services impliquant l'accès du partenaire à des informations de santé protégées (PHI) ainsi que des entités qui créent, reçoivent, gèrent ou transmettent des PHI pour le compte d'un autre partenaire. La loi HIPAA a été renforcée par la loi HITECH (Health Information Technology for Economic and Clinical Health Act) en 2009. Les lois HIPAA et HITECH établissent un ensemble de normes fédérales destinées à préserver la sécurité et la confidentialité des données de santé protégées. Les lois HIPAA et HITECH imposent des exigences concernant l'utilisation et la divulgation des données de santé protégées, les mesures de protection appropriées des données de santé, les droits individuels et les responsabilités administratives. Pour plus d'informations sur HIPAA et HITECH, consultez http://www.hhs.gov/ocr/privacy/.

Les entités couvertes et leurs partenaires peuvent utiliser les composants informatiques sûrs, évolutifs et économiques d'AWS (Amazon Web Services) pour concevoir des applications qui respectent les exigences de conformité HIPAA et HITECH. AWS offre une plate-forme d'infrastructure commerciale prête à l'emploi avec des certifications reconnues par le secteur et des audits comme ISO 27001, FedRAMP, ainsi que des rapports Service Organization Control (SOC1, SOC2 et SOC3). Les services et centres de données AWS possèdent plusieurs couches de sécurité physiques et opérationnelles pour vous aider à assurer l'intégrité et la sécurité des données utilisateur. AWS constitue une solution fiable et efficace pour développer des applications pour le secteur de la santé sans frais minimum et obligation contractuelle et en ne payant que ce que vous utilisez.

AWS permet aux entités couvertes et à leurs partenaires soumis à HIPAA de traiter, stocker et transmettre des PHI en toute sécurité. AWS, tel qu'en juillet 2013, offre en outre un addendum au contrat partenariat (BAA) normalisé pour ce type de clients.

Les clients qui exécutent un BAA AWS peuvent utiliser n'importe quel service AWS sur un compte désigné comme compte HIPAA, mais ils ne peuvent que traiter, stocker et transmettre des PHI à l'aide de services éligibles HIPAA définis dans le BAA AWS. À la date de publication de ce livre blanc, les services éligibles HIPAA incluent les suivants :

- Amazon DynamoDB
- Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Elastic Load Balancing
- Amazon Elastic MapReduce (Amazon EMR)
- Amazon Glacier
- Amazon Redshift
- Amazon Relational Database Service (Amazon RDS) pour MySQL
- Amazon RDS pour Oracle
- Amazon RDS pour PostgreSQL
- Amazon Aurora (version compatible MySQL)
- Amazon Simple Storage Service (Amazon S3)
- AWS Import/Export Snowball

AWS gère un programme de gestion des risques reposant sur des normes pour s'assurer que les services conformes à la législation HIPAA prennent en charge les protections administratives, techniques et physiques requises par la loi HIPAA. L'utilisation de ces services pour stocker, traiter et transmettre des PHI permet à nos clients et à AWS de satisfaire aux exigences HIPAA applicables à notre modèle de fonctionnement opérationnel.

Chiffrement et protection des PHI dans AWS

La règle de sécurité HIPAA inclut des spécifications d'implémentation adressables pour le chiffrement des PHI dans la transmission (« en transit ») et dans le stockage (« au repos »). Même s'il s'agit d'une spécification d'implémentation adressable dans HIPAA, AWS exige que les clients chiffrent les PHI stockées ou transmises à l'aide de services éligibles HIPAA, conformément aux instructions du HHS (Health and Human Services) contenues dans le Guide « Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals ». Veuillez consulter ce site, car il a peut-être été mis à jour et rendu accessible sur un successeur (ou site associé) désigné par HHS.

AWS propose un ensemble complet de fonctions et services qui facilitent la gestion des clés et du chiffrement des PHI et simplifient l'audit, y compris AWS Key Management Service (AWS KMS). Les clients ayant des exigences de conformité HIPAA disposent d'une grande flexibilité pour répondre aux besoins de chiffrement des PHI.

À l'heure de déterminer comment appliquer le chiffrement, les clients peuvent évaluer et tirer profit des fonctions de chiffrement inhérentes aux services éligibles HIPAA ou satisfaire aux exigences de chiffrement à l'aide d'autres moyens qui respectent les instructions de HHS. Les sections suivantes décrivent en détail l'utilisation des fonctions de chiffrement disponibles dans chaque service éligible HIPAA et autres modèles de chiffrement des PHI, et explique comment utiliser AWS KMS pour chiffrer les clés employées pour le chiffrement des PHI dans AWS.

Amazon EC2

Amazon EC2 est un service de calcul évolutif et configurable par l'utilisateur qui prend en charge plusieurs méthodes de chiffrement des données au repos. Les clients peuvent, par exemple, choisir de chiffrer les PHI au niveau de l'application ou du champ au fur et à mesure de leur traitement au sein d'une plate-forme d'application ou de base de données hébergée dans une instance Amazon EC2. Les approches varient entre le chiffrement des données à l'aide de bibliothèques standard dans un cadre de travail d'application tel que Java ou .NET et l'exploitation des fonctions de Transparent Data Encryption dans Microsoft SQL ou Oracle, en passant par l'intégration de logiciels tiers sous forme de solutions basées sur un logiciel en tant que service (SaaS) dans leurs applications. Les clients peuvent choisir d'intégrer leurs applications fonctionnant dans Amazon EC2 avec des SDK AWS KMS, en simplifiant le processus de gestion des clés et du stockage. Il est également possible d'appliquer le chiffrement des données au repos à l'aide du chiffrement au niveau du fichier ou du disque complet en utilisant un logiciel tiers depuis AWS Marketplace Partners ou des outils de chiffrement de système de fichiers natif (tels que dm-crypt, LUKS, etc.).

Le trafic réseau contenant des PHI doit chiffrer les données en transit. Pour le trafic entre des sources externes (telles qu'Internet ou un environnement informatique traditionnel) et Amazon EC2, les clients doivent employer les mécanismes de chiffrement de transport standard du secteur comme TLS ou les réseaux privés virtuels (VPN) IPsec, en respectant le Guide. Le trafic réseau contenant des PHI doit aussi être chiffré, car il s'agit d'un trafic interne à un Amazon Virtual Private Cloud (VPC) pour des données voyageant entre des instances Amazon EC2 ; la plupart des applications prennent en charge TLS ou d'autres protocoles assurant un chiffrement en transit qui peut être configuré pour être conforme au Guide. Pour les applications et protocoles ne prenant pas le chiffrement en charge, des sessions de transmission de PHI peuvent être envoyées via des tunnels cryptés à l'aide d'IPsec ou d'implémentations similaires entre des instances.

Les instances Amazon EC2 employées par les clients pour traiter, stocker ou transmettre les PHI doivent fonctionner sur des instances dédiées (les hôtes dédiés sont aussi acceptables pour une éligibilité BAA), lesquelles instances s'exécutent dans un Amazon VPC sur un matériel dédié à un seul client. Les instances dédiées sont physiquement isolées au niveau matériel hôte des instances qui ne sont pas dédiées et des instances qui appartiennent à d'autres comptes AWS. Pour plus d'informations sur les instances dédiées, consultez http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/dedicated-instance.html.

Les clients peuvent lancer des instances dédiées Amazon EC2 de plusieurs manières :

- en réglant l'attribut de location d'un Amazon VPC sur « dédié » afin que toutes les instances lancées dans Amazon VPC fonctionnent comme des instances dédiées
- en définissant l'attribut de location de placement d'une configuration du lancement Auto-Scaling pour des instances lancées dans un Amazon VPC
- en définissant l'attribut de location d'une instance lancée dans un Amazon VPC

Amazon Virtual Private Cloud offre un ensemble de fonctions de sécurité réseau qui permettent de concevoir une architecture conforme à HIPAA. Des fonctions telles que les listes de contrôle d'accès réseau sans état et la réaffectation dynamique des instances dans des groupes de sécurité avec état assurent une protection souple des instances contre l'accès réseau non autorisé. Amazon VPC permet aussi aux clients d'étendre leur propre espace d'adresse réseau dans AWS et fournit plusieurs moyens pour connecter leurs centres de données à AWS. Les journaux de flux VPC fournissent une piste d'audit des connexions acceptées et rejetées à des instances qui traitent, transmettent ou stockent des PHI. Pour plus d'informations sur Amazon VPC, consultez http://aws.amazon.com/vpc/.

Amazon Elastic Block Store

Le chiffrement Amazon EBS au repos est conforme au Guide en vigueur au moment de la publication de ce livre blanc. Comme il se peut que le Guide ait été mis à jour, les clients doivent toujours évaluer et déterminer si le chiffrement Amazon EBS répond à leurs exigences réglementaires et de conformité. Le chiffrement Amazon EBS génère une clé de chiffrement de volume unique pour chaque volume EBS ; les clients peuvent choisir dans AWS Key Management Service la clé principale à utiliser pour chiffrer chaque clé de volume. Pour plus d'informations, consultez http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html.

Amazon Redshift

Amazon Redshift assure le chiffrement de base de données de ses clusters pour protéger les données au repos. Lorsque des clients activent le chiffrement pour un cluster, Amazon Redshift chiffre toutes les données, y compris les sauvegardes, en utilisant des clés symétriques AES-256 (Advanced Encryption Standard) à accélération matérielle. Amazon Redshift utilise une architecture à quatre niveaux de clés pour le chiffrement. Il s'agit de clés de chiffrement de données, d'une clé de base de données, d'une clé de cluster et d'une clé principale. La clé de cluster chiffre la clé de base de données du cluster Amazon Redshift. Les clients peuvent utiliser AWS KMS ou un AWS CloudHSM (module de sécurité matériel) pour gérer la clé de cluster. Le chiffrement Amazon Redshift au repos est conforme au Guide en vigueur au moment de la publication de ce livre blanc. Comme il se peut que le Guide ait été mis à jour, les clients doivent toujours évaluer et déterminer si le chiffrement Amazon Redshift répond à leurs exigences réglementaires et de conformité. Pour en savoir plus, consultez http://docs.aws.amazon.com/redshift/latest/mgmt/working-with-db-encryption.html.

Les connexions à Amazon Redshift contenant des PHI doivent utiliser le chiffrement de transport et les clients doivent vérifier si la configuration est conforme au Guide. Pour plus d'informations, consultez http://docs.aws.amazon.com/redshift/latest/mgmt/connecting-ssl-support.html.

Amazon S3

Les clients disposent de plusieurs options pour chiffrer des données au repos en utilisant Amazon S3, y compris des méthodes côté serveur et côté client ainsi que plusieurs méthodes de gestion des clés. Pour plus d'informations, consultez http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html.

Les connexions à Amazon S3 contenant des PHI doivent utiliser des points de terminaison qui acceptent le transport chiffré (HTTPS). Pour obtenir la liste des points de terminaison régionaux, consultez http://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region.

Les clients ne doivent pas utiliser des PHI dans des noms de compartiment, des noms d'objet ou des metadonnées, car ces données ne sont pas chiffrées à l'aide du chiffrement côté serveur S3 et elles ne sont généralement pas chiffrées dans des architectures de chiffrement côté client.

Amazon Glacier

Amazon Glacier chiffre automatiquement les données au repos à l'aide de clés symétriques AES 256 bits et prend en charge le transfert sécurisé des données client via des protocoles sécurisés.

Les connexions à Amazon Glacier contenant des PHI doivent utiliser des points de terminaison qui acceptent le transport chiffré (HTTPS). Pour obtenir la liste des points de terminaison régionaux, consultez http://docs.aws.amazon.com/general/latest/gr/rande.html#glacier_region.

Les clients ne doivent pas utiliser des PHI dans des noms d'archive et de coffre ou dans des metadonnées, car ces données ne sont pas chiffrées à l'aide du chiffrement côté serveur Amazon Glacier et elles ne sont généralement pas chiffrées dans des architectures de chiffrement côté client.

Amazon RDS pour MySQL

Amazon RDS pour MySQL permet aux clients de chiffrer des bases de données MySQL à l'aide de clés qu'ils gèrent via AWS KMS. Dans une instance de base de données fonctionnant avec le chiffrement Amazon RDS, les données stockées au repos dans le stockage sous-jacent sont chiffrées conformément au Guide en vigueur au moment de la publication de ce livre blanc, de même que les sauvegardes automatisées, réplicas en lecture et instantanés. Comme il se peut que le Guide ait été mis à jour, les clients doivent toujours évaluer et déterminer si le chiffrement Amazon RDS pour MySQL répond à leurs exigences réglementaires et de conformité. Pour plus d'informations sur le chiffrement au repos à l'aide d'Amazon RDS, consultez http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html.

Les connexions à RDS pour MySQL contenant des PHI doivent utiliser le chiffrement de transport. Pour plus d'informations sur l'activation des connexions chiffrées, consultez http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html.

Amazon RDS pour Oracle

Les clients disposent de plusieurs options pour chiffrer des PHI au repos à l'aide d'Amazon RDS pour Oracle.

Les clients peuvent chiffrer des bases de données Oracle à l'aide de clés qu'ils gèrent via AWS KMS. Dans une instance de base de données fonctionnant avec le chiffrement Amazon RDS, les données stockées au repos dans le stockage sous-jacent sont chiffrées conformément au Guide en vigueur au moment de la publication de ce livre blanc, de même que les sauvegardes automatisées, réplicas en lecture et instantanés. Comme il se peut que le Guide ait été mis à jour, les clients doivent toujours évaluer et déterminer si le chiffrement Amazon RDS pour Oracle répond à leurs exigences réglementaires et de conformité. Pour plus d'informations sur le chiffrement au repos à l'aide d'Amazon RDS, consultez http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html.

Les clients peuvent aussi tirer parti d'Oracle Transparent Data Encryption (TDE) et ils doivent vérifier si la configuration est conforme au Guide. Oracle TDE est une fonction de l'option Oracle Advanced Security disponible dans Oracle Enterprise Edition. Cette fonction chiffre automatiquement les données avant qu'elles ne soient écrites dans le stockage et déchiffre automatiquement les données lorsqu'elles sont lues depuis le stockage. Les clients peuvent aussi utiliser AWS CloudHSM pour stocker des clés Oracle TDE Amazon RDS. Pour plus d'informations, consultez les ressources suivantes :

- Chiffrement de données transparent Amazon RDS pour Oracle : http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.Oracle.Options.AdvSecurity.html.
- Utilisation d'AWS CloudHSM pour stocker les clés TDE Amazon RDS Oracle : http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.OracleCloudHSM.html.

Les connexions à Amazon RDS pour Oracle contenant des PHI doivent utiliser le chiffrement de transport et il faut vérifier si la configuration est conforme au Guide. Cela se fait à l'aide du chiffrement réseau natif Oracle, activé dans Amazon RDS pour des groupes d'options Oracle. Pour plus d'informations, consultez http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.Oracle.Options.NetworkEncryption.html.

Amazon RDS pour PostgreSQL

Amazon RDS pour PostgreSQL permet aux clients de chiffrer les bases de données PostgreSQL à l'aide de clés qu'ils gèrent via AWS KMS. Dans une instance de base de données fonctionnant avec le chiffrement Amazon RDS, les données stockées au repos dans le stockage sous-jacent sont chiffrées conformément au Guide en vigueur au moment de la publication de ce livre blanc, de même que les sauvegardes automatisées, réplicas en lecture et instantanés. Le guide ayant peut-être été mis à jour, les clients doivent toujours évaluer et déterminer si le chiffrement Amazon RDS pour PostgreSQL répond à leurs exigences réglementaires et de conformité. Pour plus d'informations sur le chiffrement au repos à l'aide d'Amazon RDS, consultez http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html.

Les connexions à RDS pour PostgreSQL contenant les PHI doivent utiliser le chiffrement de transport. Pour plus d'informations sur l'activation des connexions chiffrées, consultez http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html.

Amazon Aurora

Amazon Aurora permet aux clients de chiffrer les bases de données Aurora à l'aide de clés qu'ils gèrent via AWS KMS. Dans une instance de base de données fonctionnant avec le chiffrement Amazon Aurora, les données stockées au repos dans le stockage sous-jacent sont chiffrées conformément au Guide en vigueur au moment de la publication de ce livre blanc, de même que les sauvegardes automatisées, les réplicas en lecture et les instantanés. Le guide ayant peut-être été mis à jour, les clients doivent toujours évaluer et déterminer si le chiffrement Amazon Aurora répond à leurs exigences réglementaires et de conformité. Pour plus d'informations sur le chiffrement au repos à l'aide d'Amazon RDS, consultez http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html.

Actuellement, les clients peuvent uniquement utiliser l'édition compatible MySQL d'Amazon Aurora dans le cadre de notre BAA.

Les connexions à Aurora contenant les PHI doivent utiliser le chiffrement de transport. Pour plus d'informations sur l'activation des connexions chiffrées, consultez http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html.

Elastic Load Balancing

Les clients peuvent utiliser Elastic Load Balancing pour terminer et traiter des sessions contenant des PHI. Les clients peuvent choisir entre Classic Load Balancer et Application Load Balancer. Comme la totalité du trafic contenant des PHI doit être chiffrée d'une extrémité à l'autre du transit, les clients ont la possibilité d'appliquer deux architectures distinctes :

Les clients peuvent terminer HTTPS, HTTP/2 sur TLS (pour les applications) ou SSL/TLS sur Elastic Load Balancing en créant un équilibreur de charge qui utilise un protocole chiffré pour les connexions. Cette fonction permet de chiffrer le trafic entre l'équilibreur de charge de l'utilisateur et les clients qui ouvrent des sessions HTTPS, HTTP/2 sur TLS ou SSL/TLS, ainsi que pour les connexions entre l'équilibreur de charge et les instances principales de l'utilisateur. Les sessions contenant des PHI doivent chiffrer les écouteurs frontaux et principaux à l'aide du chiffrement de transport. Les clients doivent évaluer leurs certificats et leurs stratégies de négociation de session à des fins de conformité avec le Guide. Pour plus d'informations, consultez http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-https-load-balancers.html.

Il est également possible de configurer Amazon ELB en mode TCP de base (pour Classique) ou sur les WebSockets (pour Application), et de transférer les sessions chiffrées vers les instances principales où la session chiffrée prend fin. Dans cette architecture, les clients gèrent leurs propres certificats ainsi que les stratégies de négociation TLS dans des applications tournant dans leurs propres instances. Pour plus d'informations, consultez http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-listener-config.html.

Dans les deux architectures, les clients doivent implémenter un niveau de journalisation qu'ils déterminent comme cohérent avec les exigences HIPAA et HITECH.

Amazon EMR

Amazon EMR déploie et gère un cluster d'instances Amazon EC2 dans un compte du client. Toutes les instances Amazon EC2 qui traitent, stockent ou transmettent des PHI doivent être des instances dédiées. Pour satisfaire cette exigence, des clusters EMR doivent être créés dans un VPC dont l'attribut de location est réglé sur « dédié ». Cela garantit que tous les nœuds du cluster (instances) lancés dans le VPC fonctionneront comme des instances dédiées.

Pour plus d'informations sur le chiffrement avec Amazon EMR, consultez https://docs.aws.amazon.com/ElasticMapReduce/latest/ReleaseGuide/emr-data-encryption-options.html.

Amazon DynamoDB

Les connexions à Amazon DynamoDB contenant des PHI doivent utiliser des points de terminaison qui acceptent le transport chiffré (HTTPS). Pour obtenir la liste des points de terminaison régionaux, consultez http://docs.aws.amazon.com/general/latest/gr/rande.html#ddb_region.

Des PHI stockés dans Amazon DynamoDB doivent être chiffrés au repos conformément au Guide. Les clients Amazon DynamoDB peuvent utiliser le cadre de travail de développement d'application de leur choix pour chiffrer des PHI dans des applications avant de stocker les données dans Amazon DynamoDB. Une bibliothèque côté client pour le chiffrement de contenu est également disponible à partir du référentiel AWS Labs GitHub. Les clients peuvent évaluer la conformité au Guide de cette implémentation. Pour plus d'informations, consultez https://github.com/awslabs/aws-dynamodb-encryption-java. Il faut être extrêmement vigilant lors de la sélection des clés principales et de la création d'index afin que des PHI ne soient pas requises pour des requêtes et des analyses dans Amazon DynamoDB.

Utilisation d'AWS KMS pour le chiffrement des PHI

Des clés principales dans AWS KMS peuvent être utilisées pour chiffrer/déchiffrer des clés de chiffrement de données utilisées pour crypter des PHI dans des applications du client ou dans des services AWS qui sont intégrés à AWS KMS. AWS KMS peut être employé conjointement avec un compte HIPAA, mais des PHI ne peuvent être traitées, stockées ou transmises que dans des services éligibles HIPAA. KMS ne doit pas être un service éligible HIPAA pour autant qu'il sert à générer et à gérer des clés pour des applications fonctionnant dans d'autres services éligibles HIPAA. Par exemple, une application qui traite des PHI dans Amazon EC2 pourrait utiliser l'appel d'API GenerateDataKey pour générer des clés de chiffrement de données pour chiffrer et déchiffrer des PHI dans l'application. Les clés de chiffrement des données doivent être protégées par des clés principales du client stockées dans AWS KMS, en créant une hiérarchie de clés à haut niveau d'audit, car les appels d'API vers AWS KMS sont consignés dans AWS CloudTrail.

AWS Snowball

Avec AWS Snowball (Snowball), vous pouvez transférer des centaines de téraoctets ou pétaoctets de données entre vos centres de données sur site et Amazon Simple Storage Service (Amazon S3).

Les PHI stockés dans AWS Snowball doivent être chiffrés au repos conformément au Guide. Lors de la création d'une tâche d'importation, les clients doivent spécifier l'ARN de la clé principale AWS Key Management Service (AWS KMS) à utiliser pour protéger les données au sein de la Snowball. De plus, pendant la création de la tâche d'importation, les clients doivent choisir un compartiment S3 de destination qui répond aux nomes de chiffrement définies par le Guide. Tandis que Snowball ne prend pas en charge actuellement le chiffrement côté serveur avec les clés AWS KMS (SSE-KMS) ou le chiffrement côté serveur avec les clés fournies par le client (SSE-C), Snowball prend bien en charge le chiffrement côté serveur avec les clés de chiffrement Amazon S3 (SSE-S3). Pour plus d'informations, consultez Protection des données à l'aide du chiffrement côté serveur avec les clés de chiffrement Amazon S3 (SSE-S3).

Sinon, les clients peuvent utiliser la méthodologie de chiffrement de leur choix pour chiffrer les PHI avant de stocker les données dans AWS Snowball.

Actuellement, les clients ne peuvent qu'utiliser l'appliance AWS Snowball standard dans le cadre de notre BAA.

Audit, sauvegardes et reprise après sinistre

La règle de sécurité HIPAA exige également des capacités d'audit en profondeur, des procédures de sauvegarde de données et des mécanismes de reprise après sinistre. Les services d'AWS incluent de nombreuses fonctions qui aident les clients à respecter ces exigences.

Lors de la conception d'un système d'information conforme aux exigences HIPAA et HITECH, les clients doivent mettre en place des capacités d'audit afin que les analystes de la sécurité puissent consulter les journaux d'activité ou les rapports détaillés pour identifier les personnes ayant accès au système, l'entrée d'adresse IP, les données sollicitées, etc. Ces données doivent être suivies, consignées et stockées à long terme en un lieu centralisé en vue d'un audit. Amazon EC2 permet aux client d'exécuter des fichiers de journal d'activité et des audits jusqu'à la couche des paquets sur leurs serveurs virtuels, exactement comme sur du matériel traditionnel. Ils peuvent également suivre tout trafic IP qui atteint leur instance de serveur virtuel. Les administrateurs du client peuvent sauvegarder des fichiers journaux dans Amazon S3 à des fins de stockage à long terme.

Conformément à HIPAA, les entités couvertes doivent avoir un plan de contingence pour protéger les données en cas d'urgence ; elles doivent aussi créer et gérer des copies récupérables exactes des PHI électroniques. Pour implémenter un plan de sauvegarde de données dans AWS, Amazon EBS propose le stockage permanent pour des instances de serveur virtuel Amazon EC2. Ces volumes peuvent être exposés en tant que périphériques de stockage en mode bloc standard et offrent un stockage hors instance qui perdure indépendamment de la vie d'une instance. Pour respecter les instructions HIPAA, les clients peuvent créer des instantanés des volumes Amazon EBS à un instant dans le passé ; ils sont stockés automatiquement dans Amazon S3 et répliqués dans plusieurs zones de disponibilité. Ces zones sont des emplacements distincts conçus pour être isolés des défaillances survenant dans d'autres zones de disponibilité. Ces instantanés sont accessibles à tout moment et peuvent protéger des données à long terme. Amazon S3 fournit aussi une solution à haut niveau de disponibilité pour le stockage de données et les sauvegardes automatisées. En chargeant simplement un fichier ou une image dans Amazon S3, plusieurs copies redondantes sont créées automatiquement et stockées dans des centres de données séparés. Ces fichiers sont accessibles à tout moment, à partir de n'importe où (sur base d'autorisations) et sont protégés contre toute suppression involontaire.

La reprise après sinistre, qui consiste à protéger des données de l'organisation et l'infrastructure informatique en cas de sinistre, est généralement une des exigences HIPAA les plus difficiles à respecter. Elle implique la gestion de systèmes à haut niveau de disponibilité pour répliquer les données et le système hors site tout en permettant l'accès permanent aux deux. AWS offre de manière inhérente une grande variété de mécanismes de reprise après sinistre.

Amazon EC2 permet aux administrateurs de démarrer des instances serveur très rapidement et d'utiliser une adresse IP Elastic (une adresse IP statique pour l'environnement de cloud computing) à des fins de basculement approprié d'une machine vers une autre. Amazon EC2 fournit également des zones de disponibilité. Les administrateurs peuvent lancer des instances Amazon EC2 dans plusieurs zones de disponibilité pour créer à divers endroits géographiques des systèmes tolérants aux pannes et à haut niveau de résilience en cas de défaillance réseau, catastrophe naturelle et autres éventuelles sources d'immobilisation. Via Amazon S3, les données du client sont répliquées et stockées automatiquement dans des centres de données séparés pour assurer le stockage fiable des données avec une disponibilité de 99,99 %.

Pour plus d'informations sur la reprise après sinistre, consultez le livre blanc sur la reprise après sinistre AWS disponible à l'adresse http://aws.amazon.com/disaster-recovery/.

Révisions du document

Date	Description
Janvier 2017	Brève description des révisions
Octobre 2016	Première publication