PHILIPS

HealthSuite Imaging

Des solutions de Cloud sécurisées afin d'assurer la protection des données et d'améliorer l'efficacité opérationnelle

Sommaire

Résumé

Philips s'engage à fournir des solutions d'imagerie fiables, sécurisées et confidentielles, permettant aux cliniciens et radiologues de poser des diagnostics rapides et précis.

HealthSuite Imaging (HSI) illustre pleinement cet engagement par son approche sécurisée dès la conception, exploitant la puissance du Cloud pour simplifier la gestion des images, la collaboration et la production de comptes rendus. HealthSuite Imaging, notre service de radiologie cloud proposé en solution SaaS, libère les professionnels de santé de la gestion opérationnelle en s'appuyant sur des partenaires de confiance : Philips et Amazon Web Services (AWS), dont le rôle est d'assurer la mise à jour permanente, la supervision et la conformité de la plateforme.

Ce document décrit les principes de sécurité, les contrôles et les technologies intégrés à l'architecture cloud de HSI pour protéger les données médicales sensibles et garantir l'intégrité opérationnelle. Il a pour objectif de fournir aux établissements de santé, aux professionnels IT et aux décideurs une vision globale de la manière dont HSI protège les informations des patients et des systèmes dans un environnement cloud.

Le Cloud s'accompagne de nouveaux défis et de nouvelles mesures de protection

Les services de radiologie sont confrontés à un environnement exigeant et en constante évolution en matière de cybersécurité, en raison de leur dépendance à des systèmes interconnectés, de leur disponibilité permanente et de leur capacité élevée de traitement des données. Les nouveaux défis liés aux plateformes basées sur le cloud nécessitent des mesures de protection avancées (gestion solide des identités, stockage de données cryptées, contrôles des journaux d'audit et de la conformité) dans le but de prévenir toute création de nouveaux points d'accès exploitables par des pirates. Cependant, les solutions cloud s'accompagnent également d'améliorations significatives en matière de sécurité grâce à la simplification des mises à niveau et de l'application des correctifs, ainsi qu'à la centralisation et à la consolidation des points d'entrée.

Présentation de HealthSuite Imaging

Disponible en tant que solution Software as a Service (SaaS), HSI propose une gamme modulaire de services destinés au PACS Philips. Ces services couvrent aussi bien la planification des examens, l'enregistrement des patients et la documentation que le traitement des images, ou encore l'interprétation à des fins de diagnostic et la transmission des résultats.

HealthSuite Imaging offre une architecture mettant l'accent sur la sécurité : elle est conçue pour limiter les menaces auxquelles sont exposées les données hébergées sur le cloud. Elle transfère la charge opérationnelle des prestataires de soins de santé vers des partenaires de confiance (Philips et Amazon Web Services (AWS)) qui garantissent la mise à jour continue, le contrôle et la conformité de la plateforme. La sécurité est intégrée à chaque couche, du cryptage des données aux contrôles des accès, en passant par la gestion des vulnérabilités et la détection des menaces en temps réel. Les équipes informatiques du secteur de la santé se donnent ainsi les moyens de garder une avance décisive face à des menaces en perpétuelle évolution, sans compromettre les performances du système ni la disponibilité clinique.

Sécurité avancée des environnements cloud

HealthSuite Imaging repose sur une infrastructure cloud moderne et sécurisée dont la protection est nettement supérieure à celle des environnements locaux traditionnels.

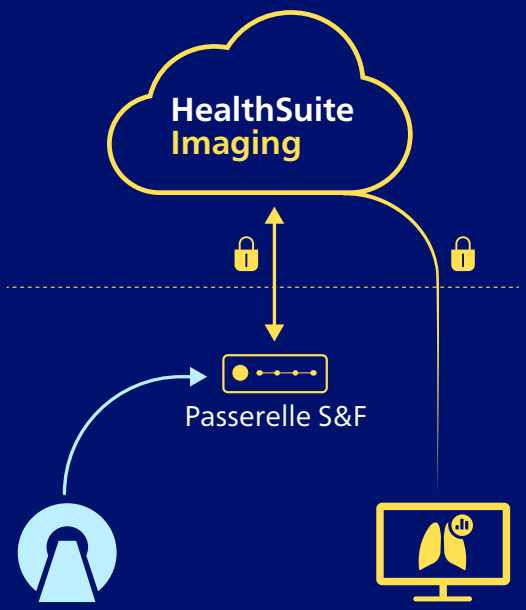
Chaque instance HSI est déployée dans une région AWS choisie par Philips en fonction de sa proximité avec le prestataire de soins de santé, assurant ainsi une faible latence et des performances optimales. Cette architecture permet un accès rapide aux analyses d'imagerie tout en respectant les exigences locales de résidence des données et de performance. HSI utilise l'ensemble des services AWS pour sécuriser son infrastructure, notamment Amazon EC2, S3, ELB, VPC, IAM, KMS, CloudWatch, AppStream, Route53, WAF et CloudTrail.

La plateforme cloud est conçue avec une segmentation réseau renforcée, isolant les services exposés au public (par exemple les visionneuses de diagnostic et les portails d'entreprise) des services backend (bases de données et stockage). Les Réseaux privés virtuels (VPC), les groupes de sécurité et les listes de contrôle d'accès réseau (NACL) sont mis en œuvre pour gérer rigoureusement les flux réseau entrants et sortants, garantissant un accès sécurisé et maîtrisé à toutes les ressources.

HealthSuite Imaging (HSI) est disponible selon deux modes de déploiement :

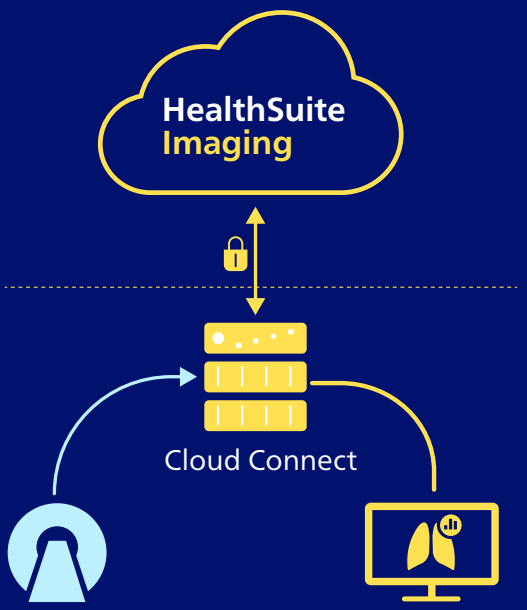
Un déploiement intégral sur le cloud de la solution HealthSuite Imaging correspond à une configuration dans laquelle tous les services d'imagerie médicale sont entièrement hébergés dans le cloud. Cela signifie que les données et les applications sont stockées et gérées sur des serveurs distants, plus précisément sur Amazon Web Services (AWS).

Services RIS et PACS 100 % Cloud



Un déploiement hybride sur le cloud de la solution HealthSuite Imaging combine à la fois des composants sur site et basés sur le cloud. Cette configuration est particulièrement adaptée aux prestataires de soins de santé ou aux environnements de petite taille, présentant des performances réseau limitées. Elle inclut un dispositif sur site, appelé Cloud Connect, qui gère le stockage local des données et l'accès rapide aux images, tout en synchronisant les données avec un environnement partagé et multi-locataires dans AWS.

Services PACS sur Cloud hybride



Déploiement hybride sur le cloud

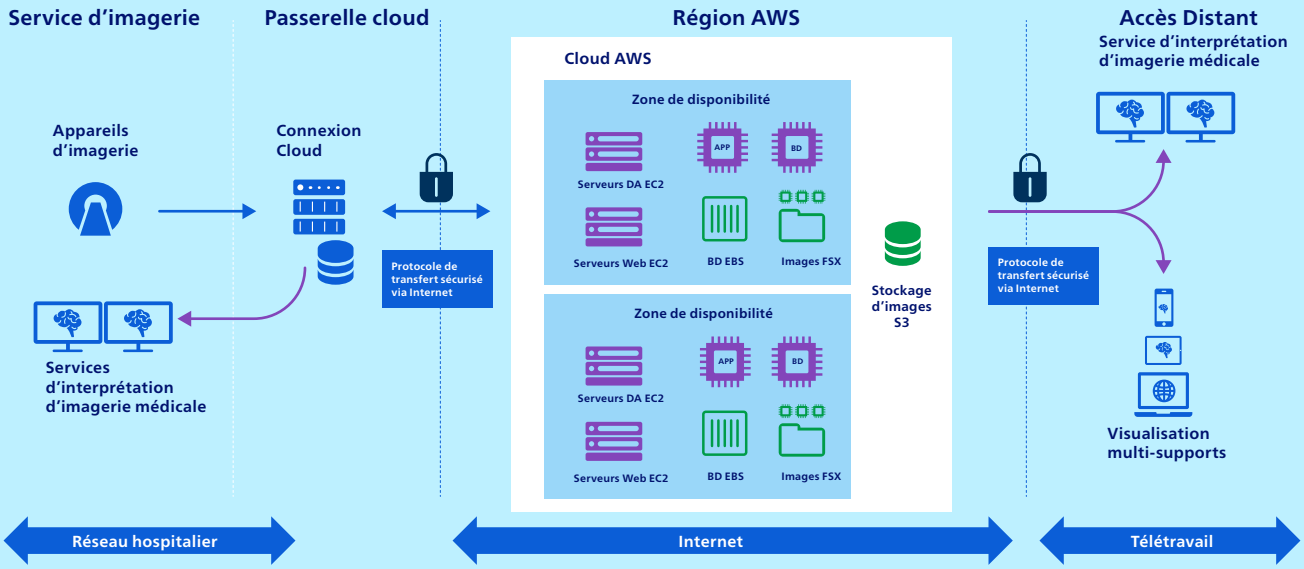


Figure 1 : Déploiement hybride

Déploiement intégral sur le cloud

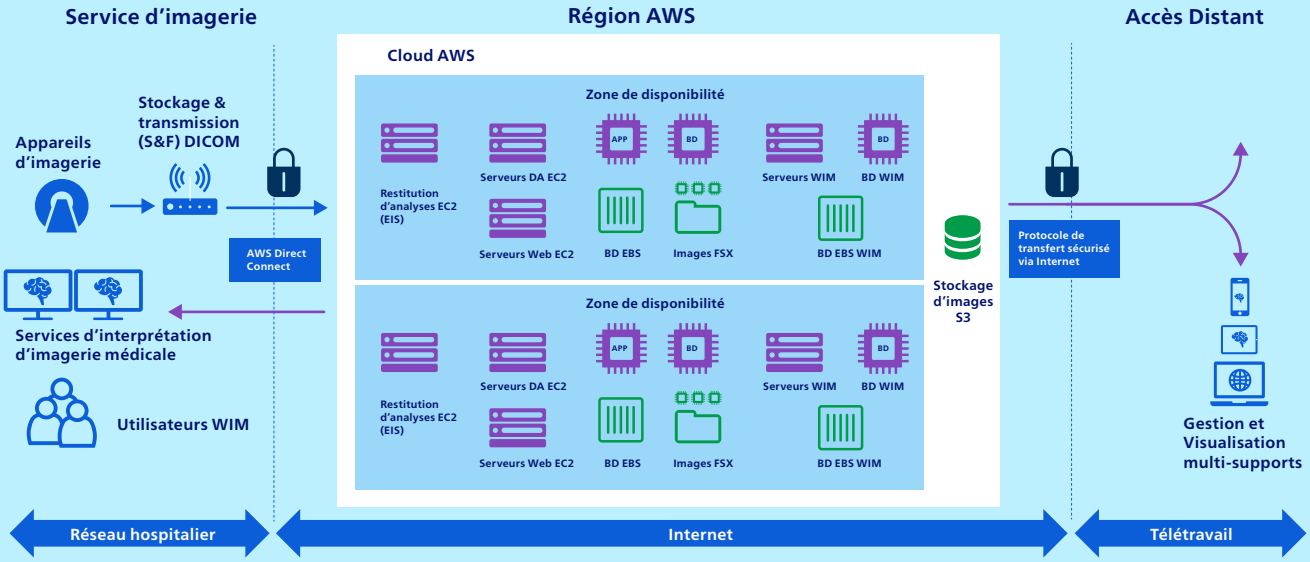


Figure 2 : Déploiement intégral sur le cloud

Avec le déploiement intégral sur le cloud de la solution HSI, chaque client dispose d'une instance dédiée sur AWS, offrant un environnement isolé et sécurisé pour ses données et ses applications. Ce modèle monolocataire maximise la sécurité et les performances, tout en offrant des configurations sur-mesure adaptées aux besoins spécifiques de chaque établissement de santé. Pour assurer un transfert efficace des données depuis les appareils d'imagerie vers le cloud, l'architecture inclut un système DICOM Store and Forward sur site. Ce système facilite le transfert des images médicales vers le cloud, garantissant une transmission fiable et performante des données.

Pare-feu d'applications Web

HSI déploie le pare-feu d'applications Web AWS (WAF) en amont direct des interfaces Web SIR et PACS, telles que l'Enterprise Viewer et la Diagnostic Client Gateway. Ce WAF agit comme une couche de défense en temps réel contre tout trafic malveillant, protégeant le système contre les exploitations de failles Web, les activités automatisées (bots), les tentatives d'attaque par déni de service, les adresses IP malveillantes, les scripts intersites (XSS) et les attaques par injections SQL. En inspectant le trafic HTTP/S avant qu'il n'atteigne la couche applicative, le WAF d'AWS préserve la disponibilité et l'intégrité du système, garantissant ainsi que seuls les utilisateurs légitimes accèdent aux interfaces cliniques critiques.

Réseau privé virtuel (VPC)

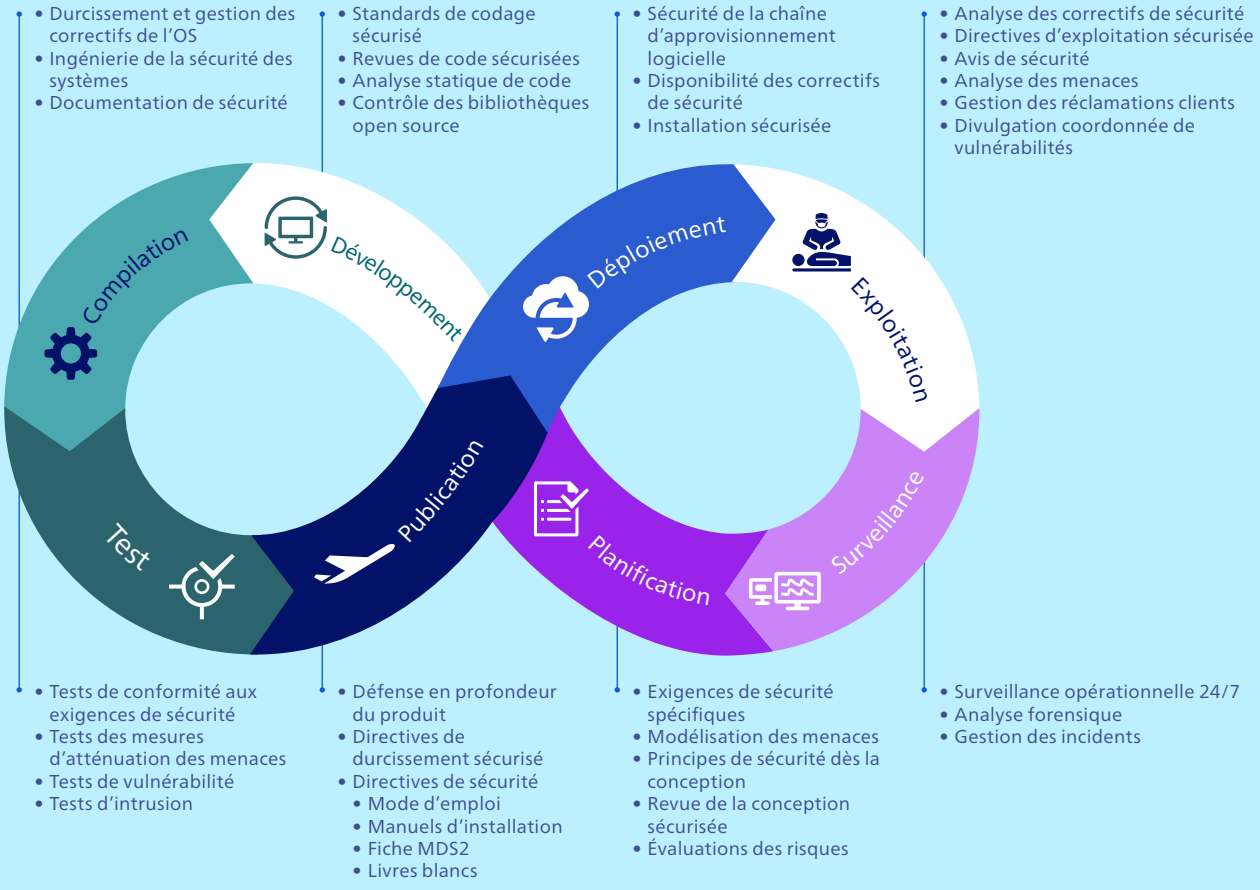
L'architecture du réseau privé virtuel AWS (VPC) adoptée pour chaque client HSI assure une segmentation stricte entre les services exposés à Internet et les composants internes. L'accès aux systèmes orientés utilisateurs, tels que la visionneuse de diagnostic, est isolé, tandis que les systèmes back-end, incluant les bases de données et les archives, sont confinés dans des sous-réseaux privés inaccessibles depuis Internet. Cette approche multicouche garantit la protection des données sensibles, réduit la surface d'exposition et permet un contrôle granulaire des flux réseau internes.

Principes de sécurité dès la conception : développement de produits et services

Philips intègre la cybersécurité à chaque phase de développement de ses produits et services, en s'appuyant sur un cadre global de sécurité des produits (Product Security Framework) aligné sur les normes internationales. Appliqué à l'ensemble de l'offre logicielle de Philips, ce cadre englobe des activités structurées telles que des évaluations de risques de sécurité des produits (PSRA), une architecture et une conception sécurisées, des tests de vulnérabilité et d'intrusion, ainsi que des formations à la sécurité organisées dans l'établissement de soins.

Au-delà des menaces technologiques

Philips déploie un Système de Gestion de la Sécurité de l'Information (SGSI) mature afin de protéger les activités de ses clients et d'atteindre les objectifs de confidentialité, d'intégrité et de disponibilité (la « triade CIA ») des données et des services. Ce SGSI repose sur une approche holistique de la sécurité de l'information, où les mesures d'atténuation des risques intègrent des contrôles organisationnels, humains, physiques et technologiques. L'adéquation continue du SGSI avec ses objectifs de sécurité est évaluée annuellement par des audits internes, réalisés par une entité indépendante au sein de Philips, ainsi que par des organismes de certification accrédités pour le maintien des certifications de sécurité de l'information (voir ci-dessous).



Cryptage des données en transit

Toutes les communications sur la plateforme HSI sont chiffrées à l'aide des protocoles les plus récents, conformes aux normes du secteur de la santé. Dans l'environnement cloud, les services internes communiquent via des protocoles propriétaires sécurisés par le protocole TLS (Transport Layer Security), empêchant toute interception ou altération non autorisée des données.

Déploiement HSI intégral sur le cloud :
Pour la communication avec les dispositifs d'imagerie médicale, HSI prend en charge le protocole DICOM TLS, garantissant des échanges de données chiffrés et authentifiés entre systèmes d'imagerie de confiance. Toutes les interfaces et applications Web utilisent le protocole HTTPS sécurisé via TLS 1.2 ou supérieur, offrant une protection robuste pour l'accès par navigateur aux outils d'imagerie et de compte rendu.

Lors de la connexion des environnements sur site au cloud, le système s'appuie sur AWS Direct Connect (DX), renforcé par le cryptage MACsec. Ce protocole assure la confidentialité et l'intégrité au niveau réseau (Couche 2), garantissant que toutes les données transmises entre l'établissement de santé et le cloud sont sécurisées par défaut, avant même l'application du cryptage au niveau applicatif. Cette approche multicouche garantit que les données de santé à caractère personnel restent protégées tout au long de leur parcours.

Déploiement HSI hybride sur le cloud :
La connexion entre l'environnement sur site et le cloud est sécurisée par un tunnel VPN, établi via un dispositif SSL, utilisant l'algorithme AES-256-CBC pour le cryptage et la fonction de hachage SHA256 pour l'authentification HMAC. Ce canal de communication chiffré repose sur le protocole TLS (Transport Layer Security) pour garantir la confidentialité et l'intégrité des données pendant leur transfert.

Cryptage des données au repos

HSI applique un cryptage au repos robuste à l'ensemble des données stockées, incluant les métadonnées et les images médicales, afin de les protéger contre tout accès non autorisé. Les identifiants de base de données, les certificats et les clés de chiffrement sont gérés de manière sécurisée via Oracle Wallets, dont l'accès est strictement réservé aux équipes Philips.

Les services de stockage natifs d'AWS, tels que S3, EBS et FSx, intègrent des capacités de cryptage pour les données d'imagerie et les fichiers associés. Ces services s'appuient sur AWS Key Management Service (KMS), utilisant des clés gérées par le client (CMK) exclusivement contrôlées par Philips. Les données de chaque client sont chiffrées avec une clé dédiée, garantissant une séparation stricte et la confidentialité des informations.

Le stockage local attaché aux instances EC2, les systèmes de fichiers FSx for Windows et les compartiments (buckets) Amazon S3 sont tous chiffrés à l'aide de clés AES-256 gérées via AWS KMS. L'accès à ces clés est strictement encadré par des politiques granulaires définissant quels composants du service Philips sont autorisés à déchiffrer les données. Cette architecture interdit à AWS d'accéder au contenu des volumes ou des objets chiffrés. En outre, les identifiants et les clés privées, gérés exclusivement par Philips, sont inaccessibles pour AWS, ce qui réduit considérablement la surface d'exposition.

Parmi les mesures de sécurité complémentaires figurent la rotation automatisée des clés, la journalisation complète des audits via AWS CloudTrail et des politiques de contrôle d'accès strictes via AWS IAM. Ces dispositifs garantissent que l'accès aux données cryptées est en permanence auditable et limité au seul personnel autorisé.

Protection des données en cours d'utilisation

En complément du cryptage des données au repos et en transit, HSI protège également les données pendant leur traitement. Cette protection est assurée par l'AWS Nitro System, la couche de sécurité fondamentale des instances Amazon EC2. Nitro empêche même le personnel d'AWS d'accéder aux données des clients au sein des machines virtuelles.

Contrairement aux systèmes cloud traditionnels, Nitro a été conçu dès l'origine pour éliminer tout accès opérateur : il n'existe donc aucune porte dérobée ni privilège administratif permettant de consulter ou de récupérer le contenu des clients. Ce modèle de sécurité unique a été validé de manière indépendante lors d'un audit réalisé en 2023 par le NCC Group, confirmant que Nitro ne fournit aucun mécanisme d'accès aux données pour les employés d'AWS sur les hôtes concernés.

En déployant HSI sur une infrastructure basée sur Nitro, Philips garantit que les données des clients sont protégées contre les menaces externes et internes, y compris celles émanant du fournisseur cloud lui-même. Cette couche de protection supplémentaire est particulièrement précieuse pour les établissements de santé soucieux de la confidentialité des données sensibles, leur offrant l'assurance qu'aucun accès non autorisé n'est possible, y compris pendant leur traitement.

Analyse de sécurité proactive

Pour identifier et limiter de manière proactive les vulnérabilités, HSI intègre des outils d'analyse de sécurité avancés. Ces services évaluent régulièrement l'environnement à la recherche de configurations incorrectes, de dérives de conformité et de menaces potentielles. Les alertes sont hiérarchisées et consolidées afin de faciliter une correction rapide. Ces évaluations automatisées viennent compléter les contrôles manuels et contribuent à une surveillance continue de la sécurité.

Détection et réponse aux incidents sur les terminaux (EDR)

La solution Détection et réponse aux incidents sur les terminaux (EDR) de Trend Micro renforce la sécurité des terminaux sur les instances EC2. L'EDR offre des capacités de surveillance en temps réel, de détection des menaces et de réponse rapide sur l'ensemble du parc informatique. Les systèmes hébergeant les composants PACS font ainsi l'objet d'une surveillance constante afin d'identifier tout comportement anormal, permettant la mise en œuvre immédiate de mesures correctives en cas de suspicion de compromission. Enfin, le Centre d'Opérations de Sécurité (SOC) de Philips assure une surveillance continue de l'infrastructure, 24 heures sur 24 et 7 jours sur 7.

Résilience des données

Amazon S3 permet la restauration des versions antérieures des objets, protégeant ainsi les données contre les pertes liées aux suppressions ou aux écrasements accidentels. Parallèlement, la fonctionnalité Object Lock applique une politique WORM (Write Once, Read Many : écriture unique, lecture multiple), garantissant que les données d'imagerie médicale ne peuvent être ni modifiées ni supprimées durant la période de conservation définie. Ces mécanismes de protection sont activés par défaut pour l'ensemble des données d'imagerie archivées, offrant une stratégie d'archivage à la fois fiable et immuable.

Durabilité des données

HSI exploite la durabilité de 99,999999999 % (11 neuf) d'Amazon S3 pour garantir la conservation pérenne des données. Afin d'assurer cette résilience, Amazon S3 stocke les informations de manière redondante sur plusieurs zones de disponibilité au sein d'une même région AWS. Le logiciel PACS sélectionne intelligemment la classe de stockage la plus appropriée selon les profils d'accès. Cette approche permet d'optimiser les coûts tout en assurant un accès rapide aux examens, qu'ils soient récents ou historiques.

Sécurité générale des produits

Tous les services du portefeuille HealthSuite Imaging sont développés selon le cadre de sécurité complet établi pour les solutions Philips Radiology Informatics. Pour en savoir plus sur ce cadre de sécurité, nous vous invitons à consulter le livre blanc "Cybersecurity in Radiology Informatics". Ce livre blanc présente de manière détaillée l'approche de Philips en matière de sécurité, notamment :

- Normes industrielles et conformité
- Sécurité des tiers et de la chaîne d'approvisionnement logicielle
- Protection contre les logiciels malveillants et gestion des correctifs OS
- Durcissement des systèmes et sécurité des données
- Sécurité applicative
- Accès distant sécurisé
- Gestion des utilisateurs
- Continuité d'activité et reprise après sinistre
- Surveillance des menaces et réponse aux incidents

Nous vous invitons à consulter l'intégralité du livre blanc

Gestion des identités et des accès (IAM)

AWS IAM permet de contrôler avec précision qui ou quoi peut accéder à quelles ressources, et dans quelles conditions. Chaque service, compte et utilisateur est soumis au principe du moindre privilège, garantissant que les personnes comme les systèmes ne disposent que des autorisations strictement nécessaires à l'exécution de leurs fonctions. Le contrôle d'accès basé sur les rôles (RBAC) est largement utilisé pour définir des périmètres d'accès clairs entre les différents types d'utilisateurs (administrateurs, radiologues, opérateurs informatiques et partenaires d'intégration) offrant ainsi à la fois un haut niveau de sécurité et une clarté opérationnelle.

Authentification multifacteur (MFA)

Pour sécuriser les points d'accès sensibles, l'accès administratif à l'infrastructure cloud requiert une authentification multifacteur (MFA). En imposant un second facteur, tel qu'un jeton de sécurité ou une confirmation biométrique, la MFA ajoute une couche de protection essentielle contre la compromission des identifiants. Cette exigence est particulièrement critique dans le secteur de la santé, où l'intégrité des données médicales et la disponibilité des systèmes sont impératives.

Le déploiement intégral sur le cloud de la solution HSI s'intègre aux systèmes de gestion des identités hospitaliers via SAML, permettant une gestion des accès centralisée et sécurisée. La prise en charge d'OpenID Connect est prévue pour des évolutions futures, afin d'élargir les capacités de fédération des identités.

Pour les configurations hybrides, le portail web de visualisation Enterprise assure la sécurité par MFA via un mot de passe à usage unique.

Architecture de sécurité à vérification systématique ("Zero Trust")

L'approche de sécurité Zero Trust de HSI repose sur le principe qu'aucun utilisateur ni système n'est intrinsèquement fiable, qu'il se situe à l'intérieur ou à l'extérieur du périmètre cloud. Chaque point d'accès fait l'objet d'une vérification systématique, où la confiance est établie de manière dynamique selon la posture de l'appareil, l'emplacement réseau et la robustesse des identifiants. Cette stratégie complète la segmentation et les contrôles d'accès existants, réduisant ainsi significativement le risque de mouvements latéraux en cas de compromission.

Journalisation centralisée et journaux d'audit immuables

La journalisation et la surveillance complètes de HSI facilitent la supervision opérationnelle ainsi que la préparation aux investigations numériques (forensic). L'ensemble des activités est enregistré via AWS CloudTrail et centralisé dans un référentiel de journaux sécurisé. Ces journaux sont protégés contre toute altération et permettent la constitution de pistes d'audit détaillées, essentielles dans les contextes réglementaires et lors des opérations de réponse aux incidents. L'immutabilité optionnelle des journaux peut être activée afin de garantir une protection de type WORM (Write Once Read Many), améliorant ainsi la capacité de mise en conformité.

Cycle de vie et suppression sécurisés des données

De l'ingestion de données à l'archivage, jusqu'à la suppression finale, HSI régit les flux de données par des politiques garantissant à la fois leur disponibilité et leur conformité. Lorsque les données atteignent le terme de leur période de conservation, des programmes de suppression assurent leur élimination de manière sécurisée et irréversible.

Sécurité opérationnelle

L'équipe Philips en charge de l'entretien et de l'exploitation utilise des méthodes avancées en conformité avec l'ITIL (Information Technology Infrastructure Library). Les risques en matière de sécurité et de confidentialité font l'objet d'une évaluation continue, et des contrôles sont mis en œuvre lors des phases de maintenance afin de limiter les risques et d'assurer une disponibilité maximale.

Journalisation des événements, audit et surveillance

La réglementation impose aux établissements de journaliser toutes les activités relatives aux informations de santé protégées (PHI). Chaque événement consigné peut inclure les avertissements et les échecs, la nature de l'opération, l'identité de l'utilisateur, l'emplacement d'origine (y compris l'adresse IP du client) ainsi que les données concernées (notamment l'identifiant unique de l'instance d'étude ou SOP Instance UID).

Une piste d'audit est un journal d'événements qui répertorie les actions et événements critiques du système afin de permettre le suivi et l'investigation des activités passées. Il s'agit d'une table en écriture unique / lecture seule (write-once/read-only), ce qui signifie que Philips peut uniquement y consigner des données puis les consulter. Une fois créé, un enregistrement ne peut être ni modifié, ni supprimé.

Les journaux et pistes d'audit sont fondamentaux en cybersécurité : ils fournissent un historique détaillé des activités du système, facilitant ainsi la détection d'incidents, l'enquête sur des événements suspects, la conformité réglementaire et l'analyse des données historiques pour renforcer la posture de sécurité et les stratégies de réponse.

Philips propose des journaux d'audit détaillés conformes au profil IHE ATNA, couvrant les connexions ainsi que la consultation et la modification des données cliniques.

Ces journaux sont soit stockés localement sur le système (sous forme chiffrée), soit transférés vers un serveur Syslog centralisé. Grâce à l'outil Audit Log Viewer, les administrateurs hospitaliers peuvent superviser les événements stockés localement pour identifier toute activité système inhabituelle ou comportement utilisateur suspect. Ils ont également la possibilité de filtrer les enregistrements selon leurs besoins et de les exporter si nécessaire.

Réponse aux menaces de cybersécurité

La priorité absolue du Security Operations Center (SOC) de Philips, opérationnel 24/7, est de garantir la sécurité des actifs vitaux tels que les logiciels Vue PACS et Image Management. Notre stratégie multidimensionnelle intègre des mesures proactives, notamment la supervision continue et la détection des menaces, en s'appuyant sur des technologies de pointe.

En cas d'incident, le SOC de Philips Imaging Informatics applique des procédures rapides de triage et de confinement afin d'isoler immédiatement les systèmes touchés, d'atténuer les dommages et d'empêcher la propagation de la menace. Les analystes procèdent à une analyse forensique approfondie des preuves, des journaux d'événements et du trafic réseau pour appréhender les tactiques, techniques et objectifs de l'attaquant. Cette analyse granulaire oriente nos stratégies de réponse et renforce nos capacités de détection, nous permettant d'anticiper et de contrer plus efficacement les menaces futures.

Philips maintient des canaux de communication ouverts avec les parties prenantes internes, les partenaires externes et les organismes de réglementation afin d'informer toutes les parties concernées tout au long du processus de gestion d'incident. Cet esprit de collaboration s'étend à nos efforts de remédiation : nous travaillons sans relâche pour rétablir les systèmes affectés dans un état sécurisé. De la correction des vulnérabilités au déploiement des mises à jour de sécurité, en passant par la réinitialisation des identifiants compromis et la restauration des données à partir des sauvegardes, notre priorité demeure la protection des actifs critiques et le maintien de la continuité opérationnelle.

L'analyse post-incident fournit des enseignements précieux pour notre progression. Des évaluations approfondies permettent d'identifier les lacunes dans les contrôles de sécurité, les faiblesses des procédures de réponse aux incidents et les opportunités d'amélioration. L'engagement de Philips en faveur de l'amélioration continue inclut un investissement permanent dans la formation et le développement des compétences, garantissant que nos analystes restent à la pointe des meilleures pratiques en cybersécurité.

Conclusion

HealthSuite Imaging est spécifiquement conçue pour une imagerie diagnostique sécurisée, évolutive et haute performance sur le cloud. Son architecture intègre des technologies de sécurité avancées, une gouvernance solide et une approche sécurisée dès la conception, afin de protéger les données patient, de répondre aux exigences réglementaires et d'optimiser l'efficacité clinique. De la gestion et du cryptage des identités à la détection des menaces en continu, en passant par une réponse structurée aux incidents, chaque aspect de la plateforme est pensé avec la sécurité comme principe fondamental.

Philips adopte une approche proactive de la sécurité en intégrant des mises à jour régulières, des évaluations indépendantes et des certifications tierces pour s'assurer que HealthSuite Imaging s'adapte en fonction de l'évolution des menaces. Les contrôles de sécurité sont évalués en continu et sont alignés sur les normes de cybersécurité spécifiques au secteur de la santé.

Face à la complexité croissante des défis liés à la cybersécurité, Philips s'engage à maintenir la confiance des professionnels de santé et des patients en leur proposant des solutions sécurisées, résilientes et conformes aux exigences en vigueur.

Nous contacter

Vous souhaitez en savoir plus ?

Nous serions ravis de pouvoir vous présenter les avantages d'une collaboration par la mise en place de solutions et de services répondant à vos besoins spécifiques. N'hésitez pas à contacter votre interlocuteur Philips.

Vue PACS est un dispositif médical de classe IIa fabriqué par Philips et dont l'évaluation de la conformité a été réalisée par l'organisme notifié TUV Rheinland CE0197. Il est destiné à la visualisation et au stockage des images. Les actes effectués avec ce dispositif sont pris en charge par les organismes d'assurance maladie dans certaines situations. Lisez attentivement la notice d'utilisation.
Mai 2026

1 Neitzel E, vanSonnenberg E, Markovich D, Parris D, Tarrant J, Casola G, Mamlouk MD, Simeone JF, The New Normal or a Return to Normal: Nationwide Remote Radiology Reading Practices after Two Years of the COVID-19 Pandemic Journal of the American College of Radiology (2023), doi: https://doi.org/10.1016/j.jacr.2023.04.014.

00001167-00-00 * MAI 2026