Services Vue Cloud de Philips – Sécurité de l'Information et protection des Données de Santé à Caractère Personnel (DSCP)

Les services cloud Philips Vue sont régis par un système de gestion de la sécurité de l'information (Information Security Management System = ISMS), couvert par les certifications suivantes délivrées par la BSI (suivez les liens pour valider et télécharger les certificats depuis les pages web de la BSI) :

Le certificat ISO/IEC 27001 EST 728705 ;
Certificat ISO/IEC 27018 PII 719405 ;
Certificat HDS 722501.

La norme HDS (Hébergeur des Donnes de Santé) s'appuie sur la norme internationale ISO/IEC 27001 en ajoutant 31 exigences spécifiques, avec un accent particulier sur les exigences contractuelles, la souveraineté des données et la représentation transparente des garanties liées à la Protection des Données de Santé à Caractère Personnel (DSCP).

Activités HDS pour les services VueCloud

L'hébergement des données de santé personnelles au format numérique effectué par Vue Cloud Services de Philips (le sous-traitant) pour le compte des clients Vue Cloud (les responsables de traitement) comprend les 6 activités décrites dans [HDS-ACCR] « Référentiel d'accréditation HDS », à savoir :

1. La mise à disposition et le maintien en condition opérationnelle de sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé ;
2. La mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé ;
3. La mise à disposition et le maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé ;
4. La mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information ;
5. L'administration et l'exploitation du système d'information contenant les données de santé ;
6. La sauvegarde des données de santé.

Moyens et processus de traitement des DSCP

Les activités ci-dessus incluent les moyens et processus suivants liés au traitement des données de santé à caractère personnel :

- Ingestion de DSCP (démographie et imagerie) issues de modalités d'imagerie en utilisant le protocole DICOM standard.
- Alignement des DSCP (démographie, imagerie, ordres, résultats) avec d'autres systèmes d'information via des interfaces standard (HL7, DICOM).
- Archivage sécurisé et sauvegarde de multiples copies des DSCP sur l'infrastructure des centres de données.
- Présentation des DSCP pour interprétation et création de compte rendu de radiologie.
- Accès externe pour les professionnels de santé à distance.
- Accès externe pour les patients via le portail patient.

- Partage des DSCP avec d'autres départements autorisés au sein de l'établissement de santé.
- Partage des DSCP avec d'autres établissements de santé dans le cadre d'un accord mutuel de partage des données.
- Contrôle d'accès basé sur les rôles basé sur le principe d'accès minimum pour les utilisateurs clients, les utilisateurs privilégiés du service et les patients.
- Transmission bidirectionnelle sécurisée des données entre le réseau client et les centres de données
- Accès à distance sécurisé pour des fins de service.
- Conservation des DSCP, y compris les activités visant à respecter les droits des personnes concernées.
- Retour et suppression des DSCP lors de la déconnexion des clients cloud, conformément aux réglementations applicables.

Toutes les communications en production se font de manière sécurisée grâce au chiffrement lors du transfert sur le réseau. Le transfert de supports d'information matérielle peut être envisagé exclusivement lors de connexion ou de la déconnexion du client, lorsque le transfert de données massives d'imagerie diagnostique de plusieurs années de production n'est pas réalisable sur un réseau étendu. Dans ce cas, un système de stockage NAS mettant en œuvre la technologie SED (Self Encrypting Drive) peut être utilisé.

Objectifs de sécurité de l'ISMS

L'ISMS certifié s'appuie sur des mesures organisationnelles et techniques avec les objectifs suivants :

- Les risques liés à la sécurité de l'information sont compris et traités comme acceptables par l'organisation.
- La confidentialité des données des patients, des informations clients, du développement produit et des plans marketing est protégée.
- L'intégrité des données des patients et des dossiers comptables est préservée.
- Les données des patients et les informations clients sont disponibles et utilisables pour toute personne autorisée.
- La conformité aux réglementations de chaque pays concernant la protection des informations personnelles identifiables (PII) et des données de santé à caractère personnel est assurée.

Autres références

Pour plus d'informations sur la politique de Philips en matière de protection des données personnelles, veuillez consulter la politique de confidentialité de Philips au lien suivant https://www.philips.com/a-w/privacy.html.

Plus d'informations sur la politique de Philips en matière de sécurité des produits sont disponibles au lien suivant https://www.philips.com/a-w/security/product-security.html.

Représentation des garanties

Le tableau ci-dessous offre une transparence sur les garanties fournies par Philips en tant qu'Hébergeur des Donnes de Santé aux clients adoptant les services VueCloud, en particulier en ce qui concerne la souveraineté et la protection des données de santé à caractère personnel (DSCP), conformément aux exigences de la certification HDS.

Raison sociale de l'acteur	Rôle dans le cadre de la prestation d'hébergement (Hébergeur/soustraitant de l'Hébergeur)	Certifié HDS (oui / non / exempté)	Qualifié SecNumCloud 3.2	Activités d'hébergement sur laquelle l'acteur intervient	Accès aux données de santé à caractère personnel depuis des pays tiers à l'Espace Economique Européen, par l'Hébergeur ou l'un de ses sous-traitants (exigence n°29 du référentiel HDS)	Hébergeur ou sous-traitants soumis à un risque d'accès aux données de santé à caractère personnel depuis des pays tiers à l'Espace Economique Européen, imposé par la législation d'un pays tiers en violation du droit de l'Union (exigence n° 30 du référentiel HDS)
Philips France	Hébergeur	Oui	Non	1,2,3,4,5,6	Oui. Le service d'assistance du niveau 0 au niveau 2 est entièrement assuré au sein de l'Espace Economique Européen. Seulement occasionnellement et exclusivement en cas d'escalade nécessaire, un service d'assistance de niveau 3 peut être fourni depuis des pays tiers à l'Espace Économique Européen. L'accès des pays concernés est fondé sur une décision d'adéquation de la Commission Européenne adoptée vertu de l'article 45 du RGPD.	Non
FreePro (centre de données)	Sous-traitant	Oui	En cours	1	Non	Non
SFR (Centre de données)	Sous-traitant	Oui	Non	1	Non	Non