PHILIPS

IntelliSpace

PACS

Sécurité

# Confidentialité, intégrité, disponibilité

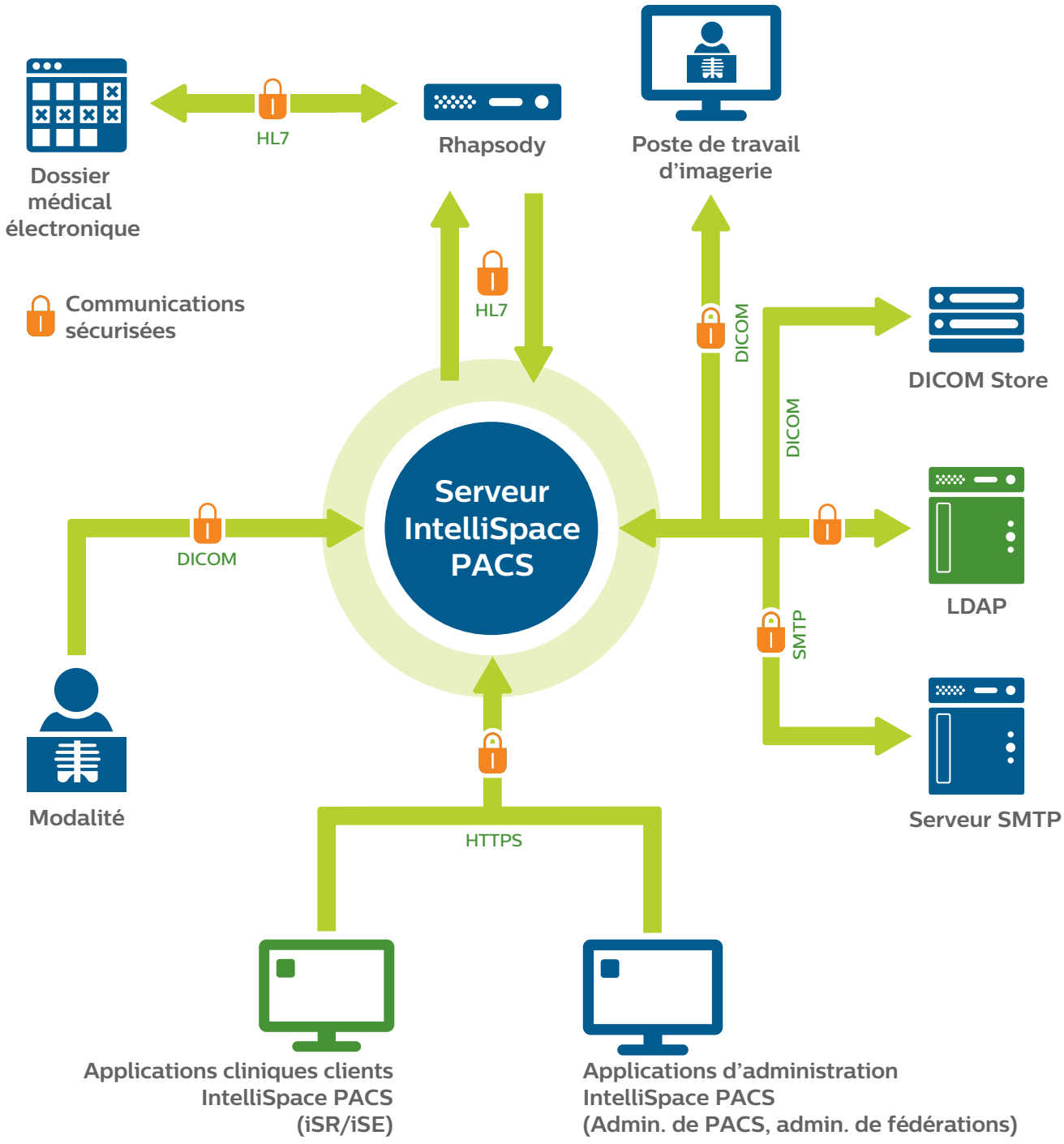
## Sécurité IntelliSpace PACS

Les failles de sécurité malveillantes ou involontaires compromettent la confidentialité des données de patients et exposent les entreprises de soins de santé à des risques financiers et juridiques. L'adoption de mesures de sécurité des systèmes permet d'atténuer ces vulnérabilités et de faciliter la disponibilité de l'information pour soutenir les décisions cliniques et la prestation des soins aux patients.

IntelliSpace PACS répond à ces préoccupations en matière de sécurité en respectant le cadre de gestion du risque du département américain de la Défense en ce qui a trait à trois aspects clés : **un environnement d'hébergement sécurisé, un cycle de vie de développement logiciel sécurisé et des logiciels d'application sécurisés**. Ces trois aspects liés à la sécurité sont à la base de la confidentialité, de l'intégrité et de la disponibilité des données de patients dans votre entreprise de soins de santé.

# Un environnement d'hébergement géré et sécurisé **assure la tranquillité d'esprit**

IntelliSpace PACS vous libère de nombreuses tâches de maintenance liées à la sécurité du système, tout en vous donnant l'assurance que vous utilisez les technologies les plus récentes. Notre plateforme de base de données Windows Server 2012 et SQL 2012* offre des fonctionnalités conformes aux normes de sécurité du National Institute of Standards and Technology (NIST). De plus, l'application logicielle IntelliSpace PACS hébergée sur le système d'exploitation Windows Server est sécurisée conformément aux guides techniques de mise en œuvre de la sécurité (STIG) de la Defense Information Systems Agency (DISA) du département américain de la Défense. En étant conformes aux normes du NIST et de la DISA, nous fournissons un système doté d'une approche de sécurité globale.



## Le cycle de vie de développement logiciel sécurisé assure la conformité en matière de sécurité

Le logiciel IntelliSpace PACS a été développé au moyen du processus de cycle de vie de développement logiciel sécurisé. Au cours du développement, nous passons en revue chacune des exigences à l'aide de notre modèle d'évaluation interne des risques liés à la sécurité pour détecter les vulnérabilités de sécurité potentielles. Les risques détectés sont classés par gravité et par probabilité d'occurrence, et les exigences sont mises à jour pour atténuer la vulnérabilité.


## Évaluations des risques liés à la sécurité

**ÉRSP + ÉFVP**
Évaluation des risques liés à la sécurité des produits (ÉRSP) et évaluation des facteurs relatifs à la vie privée (ÉFVP) fondées sur la norme NIST 800-53 R4

**Modélisation des menaces et examen de la conception**
Examen des menaces persistantes avancées actuelles et de leurs répercussions possibles, et modification ou contrôles de la conception pour atténuer les menaces

**Analyse de sécurité de code**
Analyse de code automatisée à chaque cycle de développement

**Tests de sécurité des applications**
Outils automatisés tels que HP Web Inspect et Nessus pour effectuer des constatations

**Tests de vulnérabilité et de pénétration**
Le Centre d'excellence en sécurité de Philips effectue des tests de pénétration sur le système et atténue les risques liés aux constatations effectuées

## Fonctionnalités qui favorisent un environnement d'hébergement sécurisé

- Serveur Web configuré en mode de communication sécurisé, disposant des dernières mises à jour de sécurité et utilisant des ports, protocoles et services sélectifs
- Logiciels antivirus et applications tierces, comme JAVA et SQL
- Mise en liste blanche des applications pour permettre l'exécution des applications autorisées seulement et pour empêcher les modifications non autorisées
- Coupe-feu réseau qui sépare le réseau interne de l'Internet et qui autorise seulement l'utilisation des ports de communication requis
- Cryptage des données en transit avec le protocole de sécurité de la couche transport (TLS) 1.2
- Algorithme de cryptage conforme à la norme Federal Information Processing Standards (FIPS) 140-2
- Prise en charge du protocole réseau IPv6 sur l'environnement d'hébergement
- Authentification basée sur les certificats
- Prise en charge de la carte de vérification d'identité personnelle / carte d'accès commun (CAC)

* Le logiciel d'application IntelliSpace PACS 4.4.550 prend en charge les environnements d'hébergement Windows Server 2008 et Windows Server 2012. L'environnement d'hébergement sécurisé est basé sur la plateforme de base de données Windows Server 2012 et SQL 2012.

## Le logiciel d'application sécurisé améliore la sécurité au niveau de l'application

IntelliSpace PACS fournit une sécurité au niveau de l'application, y compris l'authentification, la gestion de session, la gestion des mots de passe définis par l'utilisateur, le contrôle des accès au niveau des utilisateurs et des rôles, la vérification et les contrôles d'intégrité des données.

Les connexions client-serveur et serveur-serveur sécurisées protègent les renseignements des patients pendant la transmission. Les données de patients sont cryptées avant d'être transmises sur le réseau à l'aide d'un protocole cryptographique compatible entre les terminaux. Le serveur communique en mode sécurisé pour tous les protocoles pris en charge par le système, y compris le service Web, HL7, SMTP et DICOM.

En outre, les fonctionnalités de gestion de session vous permettent de configurer des règles de session pour améliorer la disponibilité ainsi que la sécurité des données. Vous pouvez limiter le nombre de sessions simultanées utilisées par un seul utilisateur, ainsi que le nombre de sessions simultanées par application et le nombre de sessions au niveau du système. Vous pouvez également déterminer quelles applications peuvent se joindre à une session et définir une limite de temps après laquelle les sessions inactives se terminent automatiquement.

### Fonctionnalités supplémentaires prenant en charge la sécurité au niveau de l'application

**La gestion des mots de passe,** qui offre des options configurables pour le verrouillage des comptes et la sécurité des mots de passe, et la possibilité d'utiliser la carte de vérification d'identité personnelle / carte d'accès commun (CAC), plutôt que le nom d'utilisateur et le mot de passe, pour accéder aux comptes

**Des pistes de vérification détaillées** vous permettent de suivre comment les personnes, les modalités, les services et les systèmes accèdent au système PACS

**Prise en charge** du protocole réseau IPv6 au niveau de l'application logicielle

**Validation des entrées** pour s'assurer que les données sont correctes et dans le format approprié

**Contrôle de l'accès des utilisateurs** permettant de limiter les données que les utilisateurs peuvent voir et ce qu'ils peuvent faire

Remarque : Le client est responsable de l'obtention et de l'administration des renouvellements des certificats de sécurité. Nous acceptons les protocoles TLS et SSL 3.0 et versions ultérieures.



www.philips.com

Imprimé aux Pays-Bas.
4522 991 21101 * AOÛT 2016