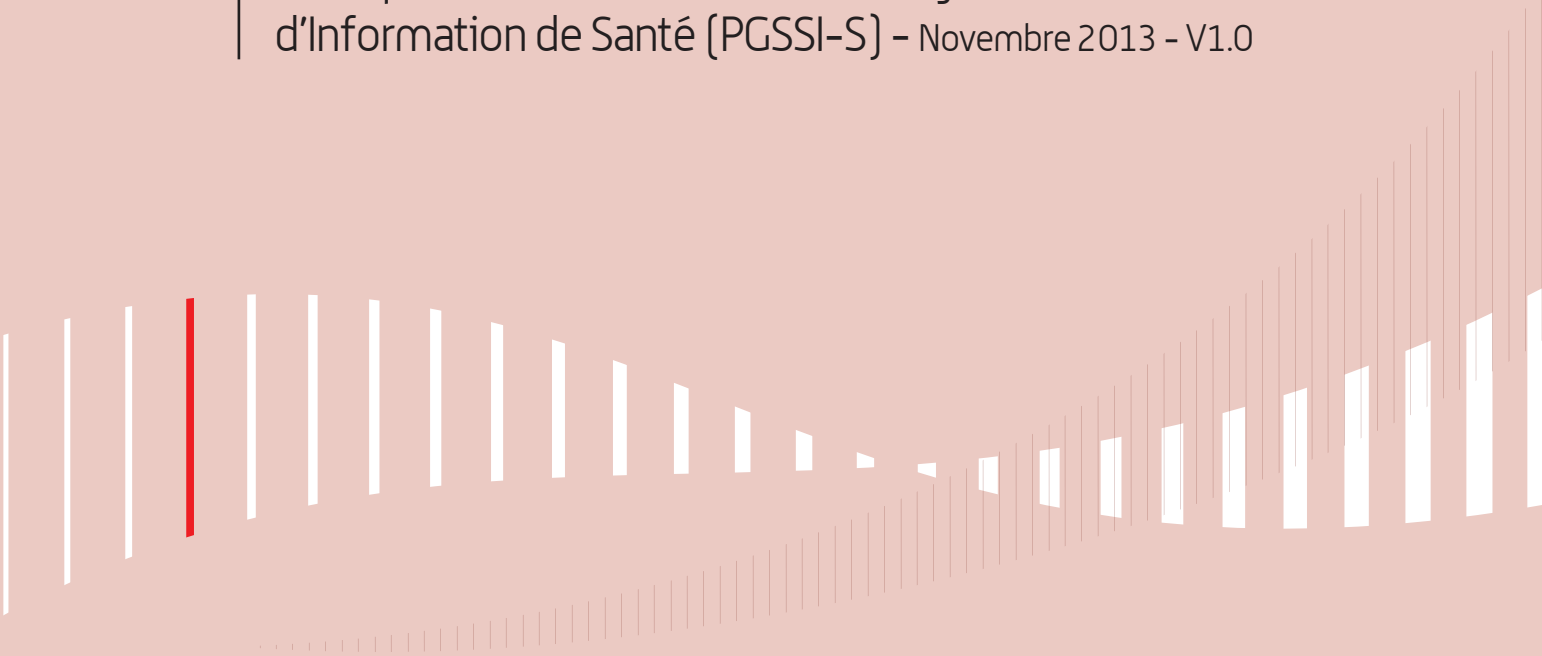
Guide Pratique
Règles pour les dispositifs connectés d'un Système d'Information de Santé

Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) - Novembre 2013 - V1.0



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES AFFAIRES SOCIALES
ET DE LA SANTÉ

asipsanté
AGENCE DES SYSTÈMES
D'INFORMATION
PARTAGÉS DE SANTÉ

Le présent document a été élaboré dans le cadre d'un processus collaboratif avec les principaux acteurs du secteur (institutionnels, utilisateurs et industriels) et le grand public.

La Délégation à la Stratégie des Systèmes d'Information de Santé (DSSIS) et l'Agence des Systèmes d'Information Partagés de Santé (ASIP Santé) remercient l'ensemble des personnes et organisations qui ont apporté leur contribution à son élaboration et à sa relecture.

SOMMAIRE

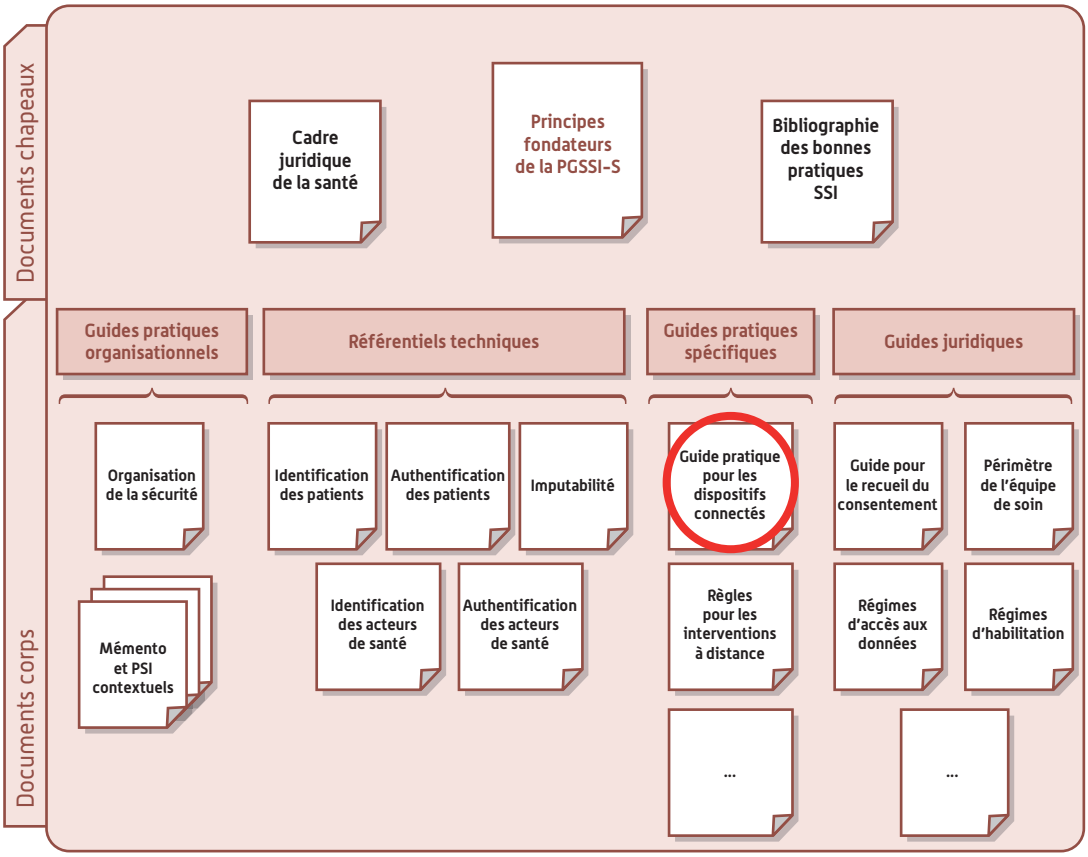
1. INTRODUCTION

1.1. Objet du document

Le présent document définit les règles et les recommandations de sécurité relatives aux dispositifs connectés à un Système d'Information de Santé (SIS, système d'informations traitant de données de santé).

Il fait partie des guides spécifiques de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S).

FIGURE 1 : PLACE DU GUIDE DANS LE CORPUS DOCUMENTAIRE DE LA PGSSI-S



Ce guide spécifique exprime les règles de sécurité auxquelles doivent se conformer **les fabricants d'équipements médicaux connectés**.
Les règles correspondent aux conditions requises pour que l'équipement fourni soit conforme aux standards de sécurité du domaine et puisse être intégré dans un Système d'Information de Santé avec un niveau de risques qui puisse être réduit à un niveau acceptable par les responsable du traitement et le responsable de la structure au sein de laquelle le dispositif est installé. Elles ne traitent pas de la formation des utilisateurs du matériel qui est du ressort de l'industriel qui le fournit.

En conséquence, le document s'adresse :

- aux fournisseurs déclinés
  - aux fabricants qui conçoivent et proposent des équipements médicaux,
  - aux fournisseurs qui vendent les produits en rapport avec les dispositifs connectés,
  - aux intégrateurs qui assurent l'intégration du dispositif connecté au sein du SIS ;
- aux acteurs relevant de la personne responsable d'une structure, qui interviennent dans le processus d'acquisition des équipements, de leurs composantes informatiques ou des prestations d'exploitation et de maintenance associées. (par exemple ingénieurs biomédicaux, RSSI, ...).

Pour des raisons de facilité de lecture, dans la suite du document, le terme générique « Responsable » est utilisé pour identifier toute personne impliquée dans la mise en œuvre des règles présentées dans le document, que celle-ci soit la personne responsable de la structure ou une personne agissant sous sa responsabilité. Le rôle de Responsable est à distinguer de celui de responsable de traitement tel que défini dans la loi Informatique et Liberté nº 78-17 du 6 janvier 1978 modifiée bien que ces rôles puissent être tenus par une même personne.

1.2. Champ d'application du guide

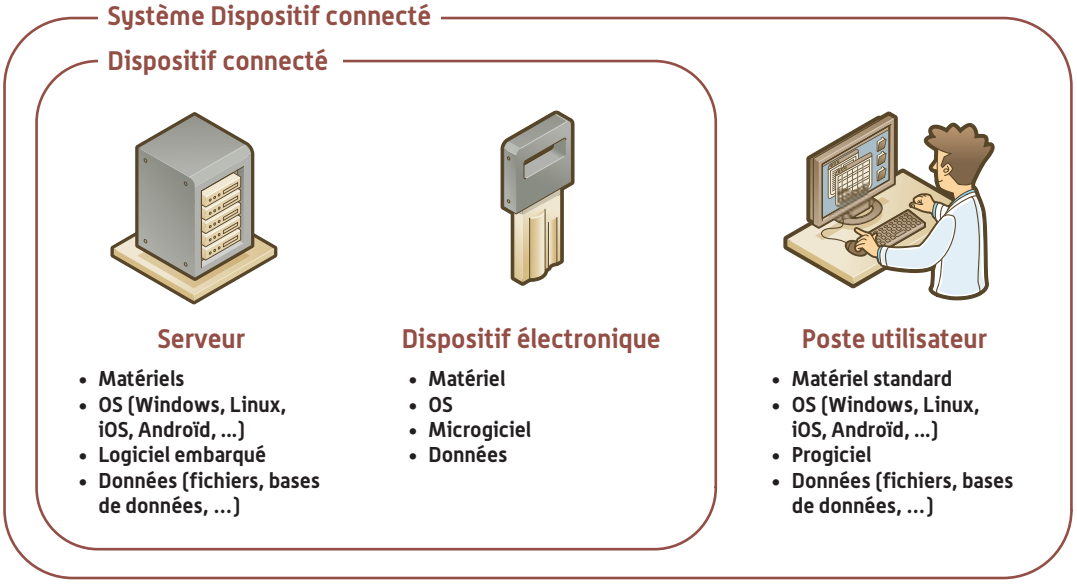
Définition des dispositifs connectés

Code de la santé publique (articles L 5211-1 et R 5211-1) : *« On entend par **dispositif médical** tout instrument, appareil, équipement, matière, produit, à l'exception des produits d'origine humaine, ou tout autre article utilisé seul ou en association, y compris les accessoires et logiciels intervenant dans son fonctionnement, destiné par le fabricant à être utilisé chez l'homme à des fins médicales et dont l'action principale voulue n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens ».*

Dans le cadre de ce document, un dispositif connecté est un dispositif médical particulier connecté à un SIS directement ou à distance (par exemple via Internet). Ce dispositif intègre des matériels (serveur, périphériques, dispositif électronique spécifique, …), des logiciels (systèmes d'exploitation, logiciel embarqué, microgiciel) et des données (fichiers, bases de données, …) et qui assure, dans un processus de soin, une fonction de traitement médical, d'analyse médicale, de surveillance médicale, de diagnostic ou de supervision.

Ce dispositif connecté est piloté à partir d'un poste de travail livré par le fournisseur du dispositif connecté ou d'un poste de travail banalisé du SIS. Ce poste de travail s'appuie sur un système d'exploitation standard (Windows, Linux, iOS, Android…) et peut comporter des progiciels et des données (fichiers, bases de données, …) spécifiques pour la gestion du dispositif connecté.
L'ensemble du dispositif connecté et de son (ses) poste(s) utilisateur est dénommé « Système dispositif connecté » dans la suite du document.

Cette configuration de base peut être déclinée selon des architectures plus complexes comportant par exemple un serveur externe. A titre d'illustration, plusieurs configurations type sont présentées en Annexe 1.



À titre illustratif, les catégories d'équipements suivantes sont concernées par le présent document :

- automate de laboratoire et poste de pilotage ;
- modalité d'imagerie (scanner, échographe, IRM, ...) et poste de pilotage / d'interprétation ;
- système d'archivage et de transmission d'images (PACS[1]) ;
- armoire à pharmacie (automate de dispensation nominative de type EURAF, armoire sécurisée à digicode, …) ;
- station de monitoring anesthésie ;
- accélérateur de radiothérapie ;
- système d'acquisition d'images (microscopes, angiographes, fond d'œil) ;
- électrocardiographe (ECG) connecté ;
- appareils servant à la prise de constantes (TA, SAT, FC) ;
- moniteurs de surveillance (respiratoire, cardiaque, multiparamétriques, …) ;
- Dispositifs de télésurveillance (appareil respironix, surveillance de la glycémie, fréquence cardiaque, …).

Équipements non concernés : les dispositifs implantables

Les équipements médicaux actifs ou non actifs qui ont vocation à être physiquement implantés, sur ou dans le corps du patient, n'entrent pas dans le champ d'application de ce guide.

1.3. Enjeux relatifs aux dispositifs connectés

Les systèmes et équipements utilisés aujourd'hui n'ont pas été conçus pour faire face aux nouvelles menaces que les possibilités technologiques ont fait apparaitre, en particulier dans le domaine des malveillances informatiques.

Dans le secteur de la santé plus qu'ailleurs, l'exploitation des vulnérabilités de ces dispositifs peut avoir des conséquences néfastes pour les SIS auxquels les équipements sont connectés, voire impacter la santé des patients.
Par exemple, la modification, qu'elle soit volontaire ou non, des paramètres d'un équipement de radiologie peut avoir des effets désastreux sur la santé du patient ou celle du personnel de santé.

Pour les Responsables, il devient donc nécessaire d'intégrer la sécurisation de ces équipements dans une réflexion générale de sécurité et notamment de prendre en compte ce critère dans le choix des équipements ou de leurs composantes et dans la mise en place de leur exploitation et de leur maintenance.

En conséquence et afin de répondre aux besoins de sécurité des Systèmes d'Information de Santé, les règles édictées dans le présent document visent à permettre en pratique :

- aux fabricants ou fournisseurs d'équipements connectés ou de prestations associées de déterminer et d'exprimer leur engagement à l'égard de la sécurité des produits et services fournis ;
- aux Responsables de vérifier que les risques représentés par les équipements connectés existants ou dont l'intégration au Système d'Information de Santé est projetée sont acceptables pour la personne responsable de la structure au sein de laquelle le dispositif est installé.

1. PACS : Picture Archiving and Communication System.

2. FONDEMENTS DU GUIDE

Le guide « Maîtriser la SSI pour les systèmes industriels »

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a publié un guide relatif à la SSI dans les systèmes industriels.
Ce guide souligne l'importance de la sécurité dans les systèmes spécifiques employés dans les activités de production. Il précise les vulnérabilités propres à ces systèmes, évoque les attaques et les négligences auxquelles ils sont exposés et indique les impacts d'incidents réels : dommages matériels / corporels ; perte de chiffre d'affaires ; impact sur l'environnement ; vol de données ; responsabilité civile / pénale ; image et notoriété.

Le guide recommande aux entreprises une démarche globale de sécurité pour leurs systèmes industriels et l'accompagne de bonnes pratiques.

D'un point de vue de la sécurité des systèmes d'information, un dispositif connecté s'apparente à un système industriel. L'usage d'un dispositif connecté s'inscrit principalement dans des activités de production de soins. L'équipement réalise le plus souvent des fonctions spécifiques de supervision, de contrôle, de mesure, d'acquisition de données, de pilotage d'actionneurs.
Le guide de l'ANSSI est utile à la prise en compte de la sécurité des équipements connectés lors de leur intégration dans un SIS.

Les « Exigences de sécurité des Systèmes d'Information pour les équipements biomédicaux des établissements de santé »

Un collectif de RSSI et d'ingénieurs biomédicaux issus d'instituts et de centres hospitaliers (cf Référence n° 1) a défini des exigences de sécurité liées à l'intégration d'équipements biomédicaux dans un SIH, avec le support du Fonctionnaire de la Sécurité des Systèmes d'information (FSSI), de l'ANAP et de la DGOS, répondant ainsi à une demande formulée par le ministère de la santé.
Les exigences de sécurité ont été déterminées sur la base de textes juridiques, de bonnes pratiques et de retours d'expérience en matière d'incidents de sécurité.
La liste des exigences et la grille d'évaluation associée permettent aux Responsables de définir et mettre à jour la politique de SSI à appliquer aux équipements biomédicaux dans leur établissement, et de préciser leurs attentes détaillées en matière de sécurité dans le cadre de l'acquisition de nouveaux équipements biomédicaux.

Les « Exigences de sécurité des Systèmes d'Information pour les équipements biomédicaux des établissements de santé » ont été retenues comme document de référence pour constituer le présent guide.
Leur champ d'application est étendu à celui des équipements médicaux connectés au SIS de tout type de structure juridique[2].

Les principales menaces induites par l'intégration de dispositifs connectés dans un SIS

Les exigences du guide ont été déterminées à partir de menaces spécifiques et de difficultés rencontrées en établissement hospitalier pour y faire face.

Les menaces sont les suivantes :

- l'attaque logique de l'équipement, notamment par exploitation de vulnérabilités de ses logiciels ;
- l'introduction ou l'activation de codes malveillants dans l'équipement ;
- la perturbation de fonctionnement de l'équipement à partir du SIS ou de son réseau ;
- la perturbation de fonctionnement de l'équipement due aux rayonnements électromagnétiques ;
- la capture ou la modification de données sur la liaison entre l'équipement et le SIS ;
- l'accès illicite à l'équipement, et l'introduction ou l'extraction de ses données ;
- le mésusage de l'équipement par une personne autorisée ;
- la modification non autorisée des logiciels de l'équipement.

2. Dans l'énoncé des exigences le terme « établissement » désigne la structure juridique rencontrée ; à l'origine il s'agissait de l'établissement de santé.

3. UTILISATION DU GUIDE

Les exigences identifiées sont applicables quel que soit le contexte d'utilisation des équipements par les industriels ou les fournisseurs de dispositifs connectés et de prestations associées.

Le guide préconise aux industriels et aux fournisseurs d'indiquer par écrit, dans toute offre effectuée auprès d'un Responsable, leur engagement de conformité (ou déclaration d'applicabilité) vis-à-vis de ces exigences.
Pour rappel, la loi impose aussi aux industriels de signaler à la personne publique les vulnérabilités qui sont détectées dans les logiciels des équipements fournis et dont l'exploitation fortuite ou malveillante, lorsqu'elle est possible, peut mettre la vie de personnes physiques en danger.
Ce signalement s'inscrit dans le cadre du guide d'organisation de la sécurité de la PGSSI-S.

Le guide permet également aux Responsables, dans le cadre de l'intégration d'un nouveau dispositif connecté dans leur SIS, de choisir les offres d'équipements et de prestations relatives aux dispositifs connectés en fonction des engagements produits.

Par ailleurs, des règles complémentaires détaillées selon les contextes (établissement hospitalier, exercice libéral, …) peuvent être définies en cas de besoin dans les politiques contextuelles.

Il est du ressort des Responsables d'estimer et de traiter les risques de sécurité induits par toutes les exigences non satisfaites liées à l'équipement lui-même ou à son contexte d'utilisation.

Le traitement d'un risque de sécurité peut consister à adopter une ou plusieurs des options suivantes vis-à-vis de ce risque :
- le réduire, par des mesures de protection ou de prévention ;
- l'accepter tel quel ;
- l'éviter ;
- le transférer vers un tiers dans le cadre d'un contrat.

4. LISTE DES EXIGENCES DE SÉCURITÉ

Deux paliers sont définis pour la mise en œuvre des exigences de sécurité applicables aux dispositifs connectés : un palier intermédiaire (Palier 1), porteur des exigences prioritaires, et un palier supérieur (Palier 2) reprenant les exigences prioritaires et les complétant afin d'offrir un meilleur niveau de sécurité.

4.1. Gestion des configurations

N°	Exigence	Niveau d'exigibilité
Gestion des configurations [G]		
[G1]	Le fournisseur et/ou le fabricant doit identifier dans sa documentation (accessible par exemple au travers d'un espace client sur Internet) l'ensemble des composants matériels (serveur s, périphériques, …) et logiciels (versions des logiciels, systèmes d'exploitation, bases de données, …) informatiques standards constituant le dispositif connecté ainsi que leurs principales caractéristiques.	Palier 1
[G2]	Le fournisseur et/ou le fabricant doit identifier dans sa documentation l'ensemble des spécifications portant sur le poste d'administration/ utilisation du dispositif connecté (caractéristiques matérielles du poste, version du système d'exploitation, middleware et pilotes, services activés, périphériques, …).	Palier 1
[G3]	Le système dispositif connecté doit fournir une interface permettant à un système de management des configurations (CMDB) d'un SIS ou à un service de télémaintenance (par exemple pour un Professionnel de Santé en exercice libéral) d'obtenir automatiquement la configuration du système dispositif connecté	Palier 2

4.2. Sécurité physique

N°	Exigence	Niveau d'exigibilité
Sécurité physique [S]		
[S1]	Le fournisseur et/ou le fabricant doit identifier dans sa documentation l'ensemble des mesures de sécurité physique (sécurité des locaux, clés du coffret protégeant le dispositif connecté, contraintes d'environnement notamment compatibilité électromagnétique (réseau WiFi, téléphone mobile), sécurité des câblages…) préconisées pour la mise en œuvre du système dispositif connecté au sein du SIS.	Palier 1
[S2]	Le dispositif connecté doit mettre en œuvre des moyens de sécurité physique permettant de détecter toute tentative d'accès physique aux composants internes sensibles (disque dur, interfaces internes, paramétrages matériels par cavaliers par exemple, …).	Palier 2

3. CMDB : Configuration Management DataBase, ou base de données de gestion de configuration

4.3. Exploitation et communications

N°	Exigence	Niveau d'exigibilité
Exploitation et communications [E]		
Vérification du bon fonctionnement		
[E1]	Les dispositifs connectés doivent disposer d'une fonction permettant de garantir l'intégrité des logiciels et des données sensibles du dispositif au démarrage du dispositif et lors de son fonctionnement. La date de dernière modification des logiciels et des données sensibles dont celles inhérentes à l'appareil est présentée lors de la connexion des utilisateurs.	Palier 1
Mise à jour des dispositifs		
[E2]	Les dispositifs connectés et les logiciels des postes utilisateurs doivent disposer d'une fonction de mise à jour sécurisée des logiciels (logiciels, microgiciel, …) permettant de garantir l'origine et l'intégrité des mises à jour.	Palier 1
[E3]	Les dispositifs connectés doivent vérifier la bonne installation d'une mise à jour logicielle avec une possibilité de retour arrière en cas de dysfonctionnement détecté.	Palier 1
[E4]	Les dispositifs connectés et les logiciels des postes utilisateur doivent disposer d'une fonction de mise à jour sécurisée avec notification automatique de l'existence d'une mise à jour des logiciels (logiciels, microgiciel, …).	Palier 2
Protection contre les codes malveillants		
[E5]	Les dispositifs connectés doivent comporter des moyens de sécurité permettant de détecter et de répondre aux menaces liées aux codes malveillants notamment dans le cas d'utilisation de supports amovibles. Si le dispositif ne comporte pas de solution de type antivirale l'utilisation de support externe est interdite.	Palier 1
[E6]	Les postes utilisateurs des dispositifs connectés doivent s'adapter ou comporter des moyens de sécurité permettant de détecter et de répondre aux menaces liées aux codes malveillants. Dans ce sens, les logiciels spécifiques à la gestion des dispositifs connectés installés sur les postes utilisateurs sont compatibles avec des solutions de sécurité contre les codes malveillants. Le fabricant doit fournir la liste des outils avec lesquels ses logiciels et matériels sont compatibles.	Palier 1
Sécurité des réseaux		
[E7]	La documentation du dispositif connecté (accessible par exemple au travers d'un espace client sur Internet) doit comporter une matrice des flux réseau (types de protocoles, origine/destination des flux, plan d'adressage…) exhaustive.	Palier 1
[E8]	Les dispositifs connectés doivent comporter des moyens de sécurité permettant de filtrer les données échangées sur les réseaux (types de protocoles, origine/destination des flux, …).	Palier 2
[E9]	Les postes utilisateurs des dispositifs connectés doivent comporter des moyens de sécurité permettant de filtrer les données échangées sur les réseaux (types de protocoles, origine/destination des flux, …). Dans ce sens, les logiciels spécifiques à la gestion des dispositifs connectés, installés sur les postes de travail, sont compatibles avec les solutions de sécurité de filtrage réseaux de type firewall personnel.	Palier 1
[E10]	En cas de mise en œuvre de communications sans fil, le dispositif connecté doit être conforme aux exigences en vigueur dans les bonnes pratiques. Concernant le mode WiFi, se référer aux documents de référence dans le domaine[4].	Palier 1

4. Par exemple : Sécurité des réseaux sans fil Bluetooth – 2007 : http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-003/index.html
http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-technologies-sans-contact/guide-securite-des-technologies-sans-contact-pour-le-controle-des-acces.html
http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-liaisons-sans-fil/recommandations-de-securite-relatives-aux-reseaux-wifi.html

N°	Exigence	Niveau d'exigibilité
Sécurité des données		
E11]	Afin de garantir la confidentialité des données médicales personnelles stockées localement, le dispositif connecté doit embarquer un dispositif de chiffrement des données. Le fournisseur et/ou le fabricant pourra se référer au Référentiel Général de Sécurité (RGS) qui comporte une annexe décrivant les exigences relatives à la fonction de sécurité « confidentialité »[5].	**Palier 2**
[E12]	Afin de garantir l'intégrité des données, le dispositif connecté doit mettre en œuvre des protocoles de transmission adaptés permettant de vérifier l'équivalence des données reçues à celles émises.	**Palier 1**
[E13]	Lors de la numérisation et de la compression des images (imagerie médicale), des procédures normalisées doivent être mises en œuvre afin de garantir l'intégrité de ces données.	**Palier 1**
[E14]	Les échanges de données du dispositif connecté doivent être conformes aux exigences de sécurité (notamment authentification et chiffrement) identifiées dans le Cadre d'Interopérabilité des SIS publié par l'ASIP Santé.	**Palier 1**
[E15]	Les échanges de données entre le dispositif connecté et les postes utilisateurs doivent être protégés en confidentialité et intégrité.	**Palier 2**
[E16]	L'accès aux fonctions d'export de données du dispositif connecté doit être limité à des personnes dûment habilitées.	**Palier 1**
Gestion des supports amovibles		
[E17]	La fonction de démarrage du dispositif connecté à partir d'un support amovible doit être désactivée en fonctionnement nominal.	**Palier 1**
Surveillance		
[E18]	Le dispositif connecté doit comporter une fonction d'alerte locale permettant de surveiller le bon fonctionnement, et tout événement pouvant avoir un impact critique sur son fonctionnement.	**Palier 1**
[E19]	Le dispositif connecté doit comporter une fonction d'alerte s'appuyant sur des mécanismes standards permettant au SIS de surveiller le bon fonctionnement, le contrôle des connexions au dispositif, et tout événement pouvant avoir un impact critique sur son fonctionnement (mise à jour du logiciel, modification de paramètre critiques, …).	**Palier 2**
Journalisation		
[E20]	Le dispositif connecté doit comporter une fonction de journalisation locale permettant de conserver une trace des accès au dispositif connecté et de tout événement pouvant avoir un impact critique sur son fonctionnement en particulier les événements identifiés par la règle E18. Le fabricant doit indiquer dans sa documentation les modalités de mise en œuvre de la journalisation en particulier les capacités de stockage de journaux du dispositif connecté et les recommandations en matière de sauvegarde des journaux.	**Palier 1**
[E21]	Le dispositif connecté doit comporter une fonction de gestion des traces s'appuyant sur des mécanismes standards permettant au SIS de conserver des enregistrements de tout événement pouvant avoir un impact critique sur le fonctionnement du dispositif connecté avec une garantie d'imputabilité pour l'ensemble des opérations effectuées sur ce dispositif. Ces journaux doivent permettre l'analyse ultérieure des causes des dysfonctionnements.	**Palier 2**
Sauvegardes		
[E22]	Le dispositif connecté doit comporter une fonction de sauvegarde conforme aux exigences en vigueur dans les bonnes pratiques.	**Palier 1**
Règles de destruction de données lors du transfert de matériels informatiques		
[E23]	Le fournisseur doit mettre en œuvre des fonctions de sécurité d'effacement des données conformes aux exigences en vigueur dans les bonnes pratiques.	**Palier 1**

5. Lien du site de l'ANSSI :
http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/liste-des-documents-constitutifs-du-rgs-v1-0.html

4.4. Maîtrise des accès

N°	Exigence	Niveau d'exigibilité
Maîtrise des accès [A]		
Contrôle d'accès au réseau		
[A1]	Le dispositif connecté doit comporter une fonction standard d'identification et d'authentification réseau du matériel, par exemple par l'utilisation du protocole 802.1X.	Palier 2
Authentification des utilisateurs		
[A2]	Le dispositif connecté doit comporter une fonction d'authentification des utilisateurs sur la base de comptes nominatifs et au minimum de mots de passe modifiables par les utilisateurs. Les mots de passe par défaut doivent être changés lors de l'installation ou de la première connexion d'un utilisateur et être spécifiques à chaque client.	Palier 1
[A3]	Le dispositif connecté doit comporter une fonction d'authentification forte des utilisateurs pour certains profils (administration, maintenance, …).	Palier 2
[A4]	Le dispositif connecté doit permettre d'imposer une politique de mots de passe (période de renouvellement, règles de constitution des mots de passe, réutilisation d'anciens mots de passe, …)	Palier 2
[A5]	Tout accès au système dispositif connecté nécessite une authentification préalable.	Palier 1
[A6]	La date de dernière connexion au système dispositif connecté doit être présentée lors de la connexion d'un utilisateur.	Palier 1
[A7]	Les logiciels du système dispositif connecté doivent offrir des fonctionnalités de verrouillage automatique en cas d'inactivité prolongée et de blocage de comptes en cas de tentative d'accès non autorisé répétée.	Palier 1
Droits d'accès		
[A8]	Les droits d'accès des utilisateurs doivent être organisés selon des rôles.	Palier 1
[A9]	L'accès aux fonctions de mise à jour des logiciels ou de modification des paramètres sensibles nécessite une authentification forte des utilisateurs. Toute action de validation dans ces contextes nécessite une double confirmation (ex.la validation d'une demande de modification de paramètres sensibles ouvre une fenêtre de dialogue rappelant l'impact d'une telle modification et demandant la confirmation de la demande).	Palier 2

4.5. Développement et maintenance des logiciels

N°	Exigence	Niveau d'exigibilité
Développement et maintenance des logiciels [D]		
[D1]	Le fournisseur et/ou le fabricant s'engage à n'installer que les seuls logiciels nécessaires au fonctionnement du dispositif connecté. Le fournisseur et/ou le fabricant s'engage à n'activer que les seuls services nécessaires au fonctionnement du dispositif connecté.	Palier 1
[D2]	L'architecture générale du système dispositif connecté et des logiciels développés doit être sans adhérence avec les briques système standards utilisées, en vue de faciliter les migrations de versions de logiciels. A défaut, le fournisseur doit assurer la compatibilité ascendante avec les évolutions des briques adhérentes.	Palier 1
[D3]	Le processus de développement doit prévoir la gestion des exceptions (débordement de plages de valeurs, erreurs internes des composants, …).	Palier 1
[D4]	Le fournisseur et/ou le fabricant doit implémenter une fonction permettant de vérifier l'intégrité des logiciels lors de leur démarrage ou lors de leur mise à jour.	Palier 1
[D5]	Le fournisseur du dispositif connecté doit assurer un suivi permanent des incidents liés aux dispositifs connectés et met à disposition de ses clients, les correctifs nécessaires. Ce suivi s'inscrit dans le cadre du guide d'organisation de la sécurité de la PGSSI-S.	Palier 1
[D6]	Le fournisseur du dispositif connecté doit assurer un suivi permanent des vulnérabilités liées aux technologies mises en œuvre dans ses produits et met à disposition de ses clients les correctifs nécessaires. Ce suivi s'inscrit dans le cadre du guide d'organisation de la sécurité de la PGSSI-S.	Palier 1
[D7]	Les fonctionnalités de télémaintenance du dispositif connecté doivent être conformes au guide PGSSI-S – Règles pour les interventions à distance sur les SIS.	Palier 1
[D8]	Les modes de tests et de maintenance du dispositif connecté doivent être exclusifs du mode opérationnel.	Palier 1
[D9]	Le dispositif connecté doit disposer d'un mode dégradé (sécurisé) permettant son fonctionnement déconnecté du SIS avec une fonction de reprise des données lors du retour en mode nominal.	Palier 1
[D10]	Le fabricant doit mener des tests de la robustesse des dispositifs connectés (tests aux limites, injection de données malformées, …)	Palier 1
[D11]	Le fournisseur et/ou le fabricant doit proposer des solutions de restitution des données permettant une reprise de celles-ci par le client notamment en cas de changement d'équipement, dans un format réutilisable par le client.	Palier 1
[D12]	Le fournisseur et/ou le fabricant doit réaliser des tests de non régression à chaque évolution du logiciel ou matériel du dispositif connecté.	Palier 1

4.6. Conformité

N°	Exigence	Niveau d'exigibilité
Conformité [C]		
[C1]	Il est du ressort du fournisseur d'acquérir et de concéder au client l'ensemble des licences d'utilisation nécessaires au fonctionnement du dispositif connecté sauf condition spécifique du client. Ceci concerne les droits d'usage des progiciels, des matériels et de l'ensemble des couches logiques utilisées (Système d'exploitation, algorithme, progiciels sécuritaires, progiciels réseaux, progiciels de base de données, progiciels systèmes, progiciels de transfert et de prise de main à distance, progiciels applicatifs, etc.).	Palier 1
[C2]	Le fournisseur et/ou le fabricant doit réaliser une analyse de risques[6] du système dispositif connecté et doit adapter les mesures de sécurité à mettre en œuvre dans ses produits au regard des risques résiduels. Il doit informer le client de la méthode d'analyse de risques retenue, des risques couverts et des risques résiduels qui seront portés par le client. Il peut en outre préconiser des mesures de sécurité à mettre en œuvre par le client afin de réduire les risques résiduels identifiés dans le cadre des précautions d'usage du dispositif.	Palier 1

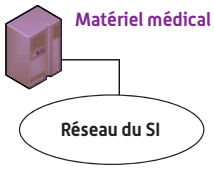
6. Exemple de méthode d'analyse des risques : EBIOS de l'ANSSI http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite.html

5. ANNEXES

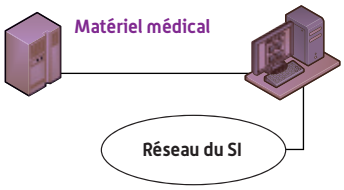
5.1. Annexe 1 : Configuration type de systèmes dispositifs connectés

Dans la figure ci-dessous, la partie en « violet » représente, dans chaque schéma, ce qui est livré par le « fournisseur ».

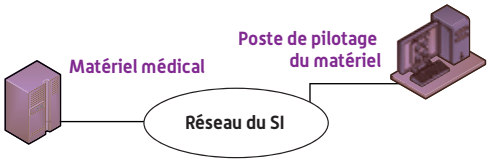
Exemple 1 : cabinet médical



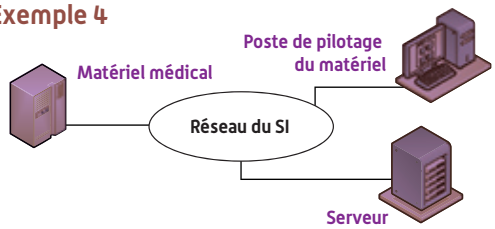
Exemple 2 : scanner, radiologie, automates



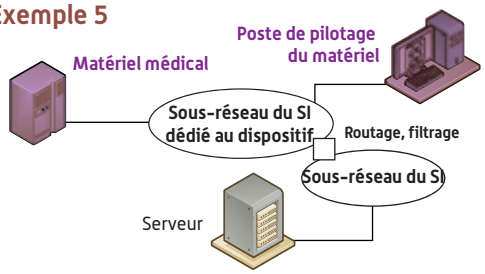
Exemple 3



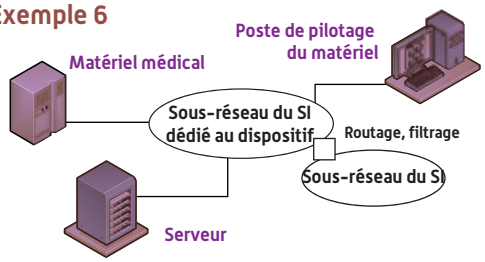
Exemple 4



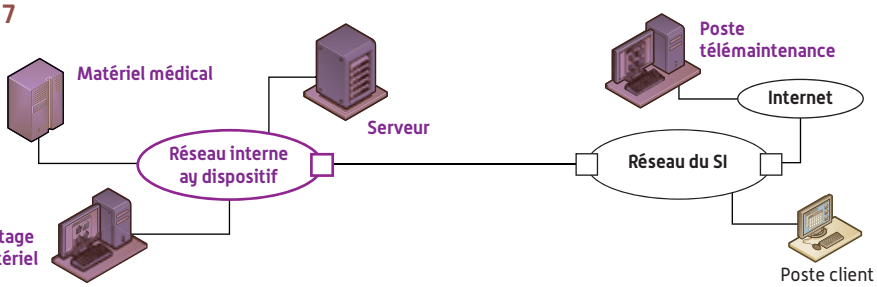
Exemple 5



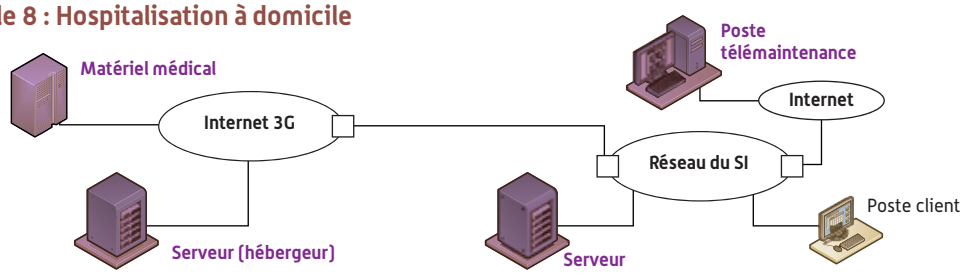
Exemple 6



Exemple 7



Exemple 8 : Hospitalisation à domicile



5.2. Annexe 2 : Glossaire

Sigle / Acronyme	Signification
ANAP	Agence Nationale d'Appui à la Performance des établissements de santé et médico-sociaux
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ASIP Santé	Agence des Systèmes d'Information Partagés de Santé
CMDB	Configuration Management Data Base
DGOS	Direction Générale de l'Offre de Soins
ECG	ElectroCardioGramme
ES	Etablissements de santé
FC	Fréquence Cardiaque
FSSI	Fonctionnaire de la Sécurité des Systèmes d'information
GT	Groupe de Travail
IRM	Imagerie par Résonnance Magnétique
OS	Operating System
PACS	Picture Archiving and Communication System
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé
PTS	Pôle Technique et Sécurité
RGS	Référentiel Général de Sécurité
RSSI	Responsable de la Sécurité des Système d'Informatique
SAT	Saturation
SIH	Système Informatique Hospitalier
SIS	Système d'Information de Santé
SSI	Sécurité des Systèmes d'Informations
TA	Tension Artérielle

5.3. Annexe 3 : Documents de référence

Référence n° 1 : Exigences de sécurité des Systèmes d'Information pour les équipements biomédicaux des ES (Collectif RSSI et ingénieurs biomédicaux des ES)

Référence n° 2 : La cybersécurité des systèmes industriels (ANSSI)

Référence n° 3 : Décret n° 2006-6 du 4 janvier 2006 – conditions d'agrément des hébergeurs de données de santé à caractère personnel

Référence n° 4 : Référentiel de constitution des dossiers de demande d'agrément des hébergeurs de données de santé à caractère personnel (ASIP)

Référence n° 5 : Recommandations de sécurité relatives aux ordiphones (ANSSI)

Référence n° 6 : Externalisation des systèmes d'information (ANSSI)

Référence n° 7 : Référentiel Général de Sécurité (ANSSI)

Référence n° 8 : Corpus documentaire de la PGSSI-S (référentiels et guides pratiques)

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES AFFAIRES SOCIALES
ET DE LA SANTÉ

asipsanté

Agence des systèmes d'information partagés de santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

RÉFÉRENTIELS / PGSSI-S – Guide Pratique : Règles pour les dispositifs
connectés d'un Système d'Information de Santé – Novembre 2013 – V1.0