Guide pratique spécifique pour la mise en place d'un accès Wifi

Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S)- Mai 2014 - V1.0

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES AFFAIRES SOCIALES
ET DE LA SANTÉ

asipsanté
AGENCE DES SYSTÈMES
D'INFORMATION
PARTAGÉS DE SANTÉ

SOMMAIRE

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.

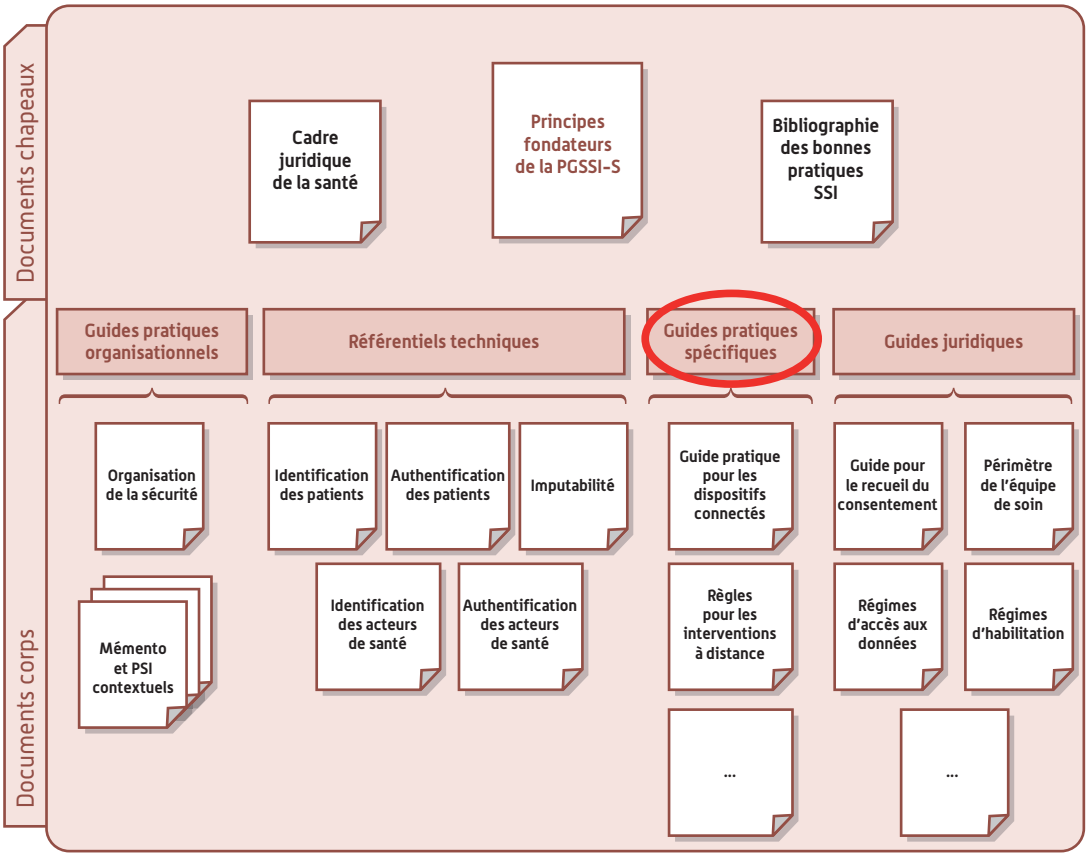
1. INTRODUCTION

1.1. Objet du document

Le présent document définit les règles de sécurité relatives à la mise en place d'un accès Wifi dans un Système d'Information de Santé (SIS).

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

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



Ce guide pratique exprime les règles de sécurité auxquelles doivent se conformer les responsables de Systèmes d'Information de Santé.

Les règles correspondent aux conditions requises et exposées dans les référentiels cités en référence pour que les risques sur la sécurité d'un SIS et les informations traitées restent acceptables lorsqu'un accès Wifi est mis en place dans ce système.

La mise en place d'un accès Wifi peut répondre à trois types de besoins :

1. Rendre possibles les accès sans fil, par des acteurs de santé, aux ressources informatiques.
   Ce besoin est principalement celui de professionnels de santé qui souhaitent s'affranchir de connexions filaires sur leur lieu d'exercice ou qui interviennent de manière intermittente sur divers lieux d'exercice.
   Ce cas est désigné par « accès PS » dans la suite du document.
2. Permettre à des équipements techniques du SIS de se connecter au réseau en mode Wifi.
   Ce besoin est principalement celui d'équipements connectés qui, pour des raisons d'usage en mobilité par exemple, tendent à privilégier progressivement la connectivité sans fil.
   Ce cas est désigné par « accès technique ».

3. Rendre possible des accès invités à des ressources tel l'accès Internet.
   Offrir à des patients (hospitalisés dans une structure de soins) ou encore des visiteurs (tous types d'organisation) la possibilité d'accéder à Internet avec des équipements Wifi sans risque supplémentaire pour le réseau du SIS.
   Ce cas est désigné par « accès invité ».
   Les employés d'une structure utilisant un « accès invité » sont considérés comme des utilisateurs externes dans le périmètre de cet accès. Le cas échéant, la charte d'utilisation des ressources de la structure peut limiter ou interdire l'utilisation de « l'accès invité » par les employés.

Ce document s'adresse :
- aux responsables de structure mettant en œuvre des accès Wifi ;
- aux personnes agissant sous leur responsabilité ; en particulier celles impliquées dans :
  - les processus d'acquisition des équipements et de leurs composantes informatiques,
  - les prestations d'exploitation,
  - les prestations de maintenances associées,
  - la mise en œuvre de la sécurité.

1.2. Champ d'application du document

Le document est applicable quels que soient les contextes de SIS rencontrés ou prévus et la structure juridique qui en est responsable, au sens des « Principes fondateurs de la PGSSI-S ».

Le cartouche ci-après présente de manière synthétique le périmètre d'application du document.

Santé						Médico Social
Production des soins	Fonctions supports à la production de soins	Coordination des soins	Veille sanitaire	Etudes et recherche	Dépistage et prévention	
✓	✓	✓	✓	✓	✓	✓
Commentaire						

Les équipements suivants (liste non exhaustive) font partie du périmètre d'application du document :

Catégories	Exemples de ressources informatiques
Borne d'accès Wifi	Routeur/modem Wifi, points d'accès sans fil
Poste de travail	Ordinateur portable, tablette, …
Equipement éditique	Imprimante, photocopieur, scanner, …
Equipement téléphonique	Smartphone, téléphone portable, …
Equipement biomédical[1]	Appareil d'imagerie médicale, dispositif biomédical connecté, …

Limites du champ d'application :
Les dispositifs implantables[2] et les dispositifs autonomes[3] ne sont pas traités par le présent document. Il est toutefois possible de s'inspirer des règles présentées dans ce guide dans le cadre de la mise en œuvre de fonctionnalités sans fil de ce genre de dispositif.

Les accès wifi invité correspondant à des prestations commerciales offertes par des tiers et sans contact avec le SI de la structure ne sont pas traités dans le présent document. Il appartient au responsable de chacune de ces offres de sécuriser ces accès.

1. Au sens du Code de la Santé Publique (articles L 5211-1 et R 5211-1).
2. Dispositif médicaux destinés à être implantés en totalité ou partiellement dans le corps humain, de manière définitive ou pendant une période d'au moins 30 jours.
3. Équipements médicaux autonomes, c'est-à-dire dont l'usage et l'exploitation s'effectuent indépendamment de tout SIS.

1.3. Enjeux principaux relatifs aux accès Wifi

L'utilisation de réseaux Wifi procure un réel confort à l'utilisateur, puisqu'il permet de s'affranchir de la connexion physique des équipements au réseau local du SIS et ainsi répondre prioritairement aux besoins de mobilité.

En contrepartie, la mise en œuvre d'un tel réseau nécessite l'implémentation de mesures spécifiques de sécurité, car elle génère des risques de sécurité accrus sur le SIS.

En effet, l'installation d'un réseau sans fil sans mesure de sécurité spécifique peut permettre à des personnes non autorisées d'écouter et d'accéder au réseau interne du SIS qui contient des données de santé à caractère personnel.

En outre, la mise en place d'un accès Wifi ouvert aux invités (de type hot-spots) impose de respecter les règles relatives à la protection de la vie privée des utilisateurs de réseaux et services de communications électroniques explicitées dans les documents cités en référence de la PGSSI-S.

Des règles spécifiques peuvent s'appliquer aux bornes Wifi ouvertes au public, en particulier l'obligation de conservation des données de connexion (article L34-1 du code des postes et communications électroniques)[4].

Il est donc essentiel de définir des mesures de sécurité pour garantir :
- la confidentialité des données transmises sur la liaison Wifi ;
- le contrôle d'accès au SIS via l'accès Wifi ;
- le cloisonnement strict de l'accès invités vis-à-vis du SIS ;
- le respect de la réglementation en matière d'accès à Internet ouvert au public.

Par ailleurs, la disponibilité des communications Wifi doit être prise en compte. En effet, ce type de communications est particulièrement sensible à des attaques de type « déni de service », en particulier par brouillage des bandes de fréquence utilisées.

Il convient donc de prévoir un mode dégradé permettant de garantir la continuité des activités, notamment de production de soins, en cas de dysfonctionnement des communications Wifi.

4. En application de l'article L34-1 du Code des Postes et des Communications Électroniques, *« les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article. »*

2. FONDEMENTS DU GUIDE

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a publié plusieurs notes concernant les réseaux Wifi sur lesquelles s'appuie le présent document :

- une note technique « Recommandations de sécurité relatives aux réseaux Wifi »[5] ;
- une Fiche Technique sur l'utilisation du Wifi (Portail de la sécurité informatique du 20 décembre 2007) ;
- une recommandation CERTA sur la sécurité des réseaux Wifi (21 novembre 2008 N° CERTA-2002-REC-002).

Les recommandations de ces documents sont reprises dans leurs principes par le présent document.

3. UTILISATION DU GUIDE

Les responsables identifiés au chapitre 1.1 sont en charge :

- de mettre en œuvre les règles prescrites ou de les faire appliquer par leurs sous-traitants ;
- d'estimer et de traiter les risques de sécurité induits par les règles non appliquées.

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, notamment si le risque est jugé mineur par le responsable du SIS ;
- l'éviter, par exemple par le choix d'une connexion filaire plutôt que Wifi ;
- le transférer vers un tiers dans le cadre d'un contrat, étant précisé que cela n'exonère pas de toute responsabilité le responsable du SIS.

L'utilisation du guide s'effectue à partir de la liste des règles du chapitre suivant.

5. http://www.ssi.gouv.fr/IMG/pdf/NP_WIFI_NoteTech.pdf

4. RÈGLES POUR LA MISE EN PLACE D'UN ACCÈS WIFI

La totalité des règles ci-après est applicable dès la mise en œuvre d'un accès wifi. Il n'y a donc pas nécessité de distinguer des paliers de mise en œuvre.

N°	Règle	Applicabilité accès Wifi Invité
Installation et configuration d'un point d'accès Wifi		
[C1]	Seul le personnel ou les sociétés désignées par le responsable du SIS, ou leurs délégataires en charge de la gestion des réseaux informatiques, peuvent mettre en place et gérer un point d'accès Wifi. Une procédure d'installation et de sécurisation des points d'accès doit être formalisée. Elle doit être mise en œuvre lors de chaque installation d'un nouvel équipement.	X
[C2]	Le point d'accès Wifi doit être compatible avec la norme IEEE 802.11. Le choix des canaux de transmission du Wifi doit être effectué de manière à ne pas créer d'interférences avec d'autres équipements ou entre les différents réseaux wifi mis en œuvre (accès PS, accès technique et accès invité).	X
[C3]	Pour prévenir toute interférence potentielle, les recommandations des fournisseurs d'équipements de santé installés à portée du point d'accès Wifi doivent être respectées. Une étude doit être menée dans ce sens avant toute mise en œuvre de point d'accès Wifi.	X
[C4]	Le nombre de bornes, leur positionnement ainsi que la puissance du signal Wifi doivent être adaptés à la superficie de la zone à couvrir.	X
[C5]	Il convient de prévoir, pour les équipements connectés par Wifi un mode dégradé permettant de garantir la continuité des activités, en cas de dysfonctionnement des communications Wifi.	X
[C6]	Comme tous les équipements connectés au réseau, les équipements Wifi (bornes, câbles d'accès…) doivent, autant que faire se peut, être protégés et non accessibles au public afin d'éviter : • un accès direct au réseau interne du SIS, par exemple en déconnectant le câble de connexion et en l'utilisant directement sur son matériel ; • ou une réinitialisation non contrôlée de l'équipement. Cette protection peut être mise en œuvre par une combinaison de disposition physique et de configuration du matériel par exemple routeur wifi dans une boite fermée à clef, routeur wifi positionnée dans le champ de vision du personnel, désactivation des connecteurs RJ45 femelles non utilisés, authentification du routeur sur le réseau filaire…	X
[C7]	L'identifiant du réseau Wifi (SSID) doit être anonymisé afin d'éviter de faire apparaitre le nom de l'opérateur internet et de donner toute information qui permettrait à une personne mal intentionnée de se connecter au réseau. Il peut également être rendu invisible, nécessitant ainsi, lors de sa première connexion, que l'utilisateur entre manuellement les informations du SSID au lieu de la sélectionner dans la liste des réseaux. Il est cependant à noter que cette mesure n'est pas suffisante pour sécuriser l'accès au wifi, elle peut cependant réduire le nombre de tentatives de connexions frauduleuses.	X
[C8]	Un contrôle d'accès des équipements connectés au réseau interne du SIS via le Wifi doit être effectué. Il doit être réalisé en priorité par l'utilisation du protocole 802.1X[6]. Les réseaux Wifi et internes du SIS doivent être cloisonnés au moyen d'un dispositif de filtrage (firewall) n'autorisant que les services, les protocoles et les ports de communication nécessaires aux flux métiers prévus.	

6. Protocole standard lié à la sécurité des réseaux informatiques, il permet de contrôler l'accès aux équipements d'infrastructures réseau.

N°	Règle	Applicabilité accès Wifi Invité
[C9]	Les équipements utilisés pour se connecter (terminaux professionnels et équipements de santé) doivent être configurés, lors de leur installation, pour restreindre l'association automatique aux seuls réseaux Wifi légitimes et exigeant une authentification 802.1X dans le but d'éviter une connexion involontaire à un réseau malveillant qui se ferait passer pour un réseau légitime.	
[C10]	Le mot de passe par défaut du compte administrateur de la borne Wifi doit être modifié. Un mot de passe fort de 10 caractères au minimum (recours à la fois de caractères alphabétiques, numériques, spéciaux et non triviaux) doit être utilisé.	X
[C11]	Seuls les services, les protocoles et les ports de communication nécessaires au fonctionnement et à l'utilisation de la borne Wifi doivent être activés. Par exemple, le protocole DNS-SD doit notamment être désactivé quand le parc d'équipement ne nécessite pas de reconfiguration fréquente.	X
[C12]	L'authentification des utilisateurs et la confidentialité des données doivent être assurées par la mise en place de mécanismes s'appuyant sur la norme WPA2-entreprise (standard 802.1X et protocole EAP, idéalement EAP-TLS) avec utilisation de l'algorithme de chiffrement AES-CCMP. Le site de l'ANSSI décrit ces différents mécanismes (http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-liaisons-sans-fil/recommandations-de-securite-relatives-aux-reseaux-wifi.html). À défaut, le protocole PEAP/EAP-MSCHAPv2 peut être utilisé en lieu et place du protocole EAP-TLS.	
[C13]	Le certificat serveur présenté par le point d'accès Wifi configuré en WPA2-Entreprise doit être signé par une autorité de certification de confiance pour les postes clients.	
[C14]	Lorsque des mécanismes d'authentification robuste (802.1X) ne peuvent être utilisés, l'authentification des utilisateurs et la confidentialité des données doivent être assurées par le mode WPA2-PSK (WPA2-Personnel) avec utilisation de l'algorithme de chiffrement AES-CCMP. La clé de sécurité pour WPA2 doit être conforme aux règles d'élaboration de mots de passe non triviaux et changée dès l'installation puis régulièrement.	
[C15]	Les fonctions de simplification de l'authentification de type WPS (Wifi Protected Setup) doivent être désactivées.	X
[C16]	Un filtrage de l'accès aux sites web doit être mis en place conformément à la charte d'utilisation d'accès et d'usage du SIS de la structure.	X

N°	Règle	Applicabilité accès Wifi Invité
Exploitation d'un point d'accès Wifi		
[E1]	L'administration d'un point d'accès Wifi doit être réalisée depuis le réseau filaire interne du SIS, de préférence à partir d'un réseau d'administration logiquement séparé et en utilisant un protocole sécurisé (ex : HTTPS). Les interfaces d'administration du point d'accès ne doivent pas être disponibles depuis le réseau Wifi.	X
[E2]	Le micrologiciel de chaque point d'accès Wifi doit être maintenu et mis à jour régulièrement.	X
[E3]	Pour s'assurer de la compatibilité des matériels utilisés pour la mise en œuvre d'un point d'accès Wifi, des tests préalables doivent être réalisés.	X
[E4]	La gestion des traces doit être activée sur les points d'accès Wifi. Les traces doivent être centralisées et analysées régulièrement pour identifier des anomalies potentielles dans les accès effectués (heures d'accès, volumes de données échangées…). Les traces des points d'accès Wifi doivent être gérées selon les mêmes modalités que les autres traces générées par le SIS (ex. droits d'accès, durée de conservation…).	
[E5]	Le réseau du SIS ne doit pas accueillir de bornes Wifi non gérées par le responsable du SIS (ex. bornes Wifi « pirates »). Des contrôles doivent être menés régulièrement pour s'en assurer.	X
Mise en place d'un accès Wifi Invité		
[M1]	Le SIS interne doit être strictement cloisonné du réseau Wifi mis à disposition des invités pour ne pas permettre l'accès aux ressources du SIS interne. Dans l'idéal, l'accès invité doit disposer d'une infrastructure dédiée à cet usage, et ne donnant accès à aucune ressource du SIS interne. À défaut, un cloisonnement logique doit être mis en œuvre.	X
[M2]	L'accès Wifi Invité doit être conditionné soit par un code d'accès disponible à l'intérieur des locaux et changé régulièrement soit par un code personnel attribué de manière individuelle suite à une procédure d'enregistrement (accueil par exemple) soit éventuellement après enregistrement auprès d'un serveur/portail 802.1X ou d'un portail captif.	X
[M3]	Dans le cas où un code personnel est nécessaire pour l'accès Wifi invité, la procédure d'enregistrement doit comporter l'approbation par l'invité des conditions d'utilisation de l'accès Wifi Invité ou l'acceptation obligatoire de ces éléments lors de sa demande de connexion au réseau. Elle peut comporter la vérification et la consignation de l'identité du demandeur.	X
[M4]	Une trace des connexions Wifi des utilisateurs doit comporter les éléments suivants s'ils sont disponibles : • les informations permettant d'identifier l'utilisateur ; • les données relatives aux équipements terminaux de communication utilisés (par exemple adresse MAC, type d'équipement, adresse IP attribuée…) ; • les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication (protocole utilisé http, https, …) ; • les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ; • les données permettant d'identifier le ou les destinataires de la communication (par exemple adresse IP ou nom DNS du site web consulté).	X
[M5]	La durée de connexion d'un invité doit être temporaire et sa durée explicitement indiquée lors de l'authentification au service. Dès lors que le délai est dépassé, la connexion wifi doit être automatiquement interrompue.	X

N°	Règle	Applicabilité accès Wifi Invité
[M6]	Des éléments de sensibilisation à la sécurité doivent être portés à la connaissance des « invités » utilisant le wifi notamment concernant le caractère public de l'accès mis à disposition, le fait qu'il n'est pas spécifiquement sécurisé par la structure hébergeant cet accès (ex. pas d'antivirus, pas de protection anti-intrusion des terminaux se connectant à l'accès wifi…) et les conditions d'usage (ex. engagement de sa responsabilité en cas de non-respect de la loi, existence éventuelle de mesure de filtrage et de trace des accès et des droits dont il dispose sur ce sujet…). Ces éléments peuvent par exemple être intégrée aux supports d'informations diffusés aux utilisateurs (ex. livret d'accueil, affiches en zone d'admission, dans les chambres et/ou dans les espaces patients internet, page d'accueil du portail d'accès au wifi…).	**X**
[M7]	Un filtrage doit être mis en place afin d'interdire l'accès aux sites web dont la consultation est interdite aux mineurs ou dont le contenu est illégal. Un filtrage plus contraignant peut être mis en place conformément à la charte d'utilisation d'accès et d'usage du SIS de la structure.	**X**

5. ANNEXES

5.1. Annexe 1 : Glossaire

Sigle / Acronyme	Signification
AES	Advanced Encryption Standard
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ASIP Santé	Agence des Systèmes d'Information Partagés de Santé
CERTA	Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques Informatiques
GT	Groupe de Travail
IPSec	Internet Protocol Security
MAC	Media Access Control
PGSSI-S	Politique générale de sécurité des systèmes d'information de santé
PS	Personnel de Santé
PTS	Pôle Technique et Sécurité
SIS	Systèmes d'Information de Santé
SSID	Service Set Identifier
TLS	Transport Layer Security
WPA2	Wifi Protected Access
WPS	Wifi Protected Setup

5.2. Annexe 2 : Documents de référence

Référence n° 1 : Recommandations de sécurité relatives aux réseaux Wifi, (Note technique ANSSI, 30/03/2013)

Référence n° 2 : Fiche Technique sur l'utilisation du Wifi (ANSSI, 20/12/2007)

Référence n° 3 : Recommandation CERTA sur la sécurité des réseaux Wifi – N° CERTA-2002-REC-002 (ANSSI, 21/11/2008)

Référence n° 4 : Corpus documentaire constituant la PGSSI-S (référentiels, guides pratiques et politiques contextuelles)

Référence n° 5 : Fiche pratique : « Conservation des données de trafic : hot-spots Wifi, cybercafés, employeurs, quelles obligations ? » (CNIL, 28/09/2010)

RÉFÉRENTIELS / PGSSI-S - Guide pratique spécifique pour la mise en place d'un accès Wifi – Mai 2014 – V1.0

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