AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

Mise en place d'un accès wifi

Guide pratique technique PGSSI-S

Publication : août 2022 | *Classification : Publique* | *Version : v1.1*

Agence du Numérique en Santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

SOMMAIRE

1. PREAMBULE

1.1. Objet du guide

Le présent guide propose un ensemble de règles de sécurité relatives à la mise en place d'un accès wifi (ou « Wi-Fi ») dans un Système d'Information de Santé (SIS).

L'objet de ces règles est de répondre aux conditions requises et exposées dans les référentiels sur lesquels s'appuie le guide pour que les risques pesant sur la sécurité d'un SIS et sur les informations traitées restent acceptables lorsqu'un accès wifi est mis en place. Les documents de référence utilisés sont présentés en Annexe 1 « Fondements du guide ».

Ce document fait partie des guides pratiques techniques de la Politique Générale de Sécurité des Systèmes d'Information de Santé [PGSSI-S].

Ce document s'adresse :

- Aux responsables de structure mettant en œuvre des accès wifi ;
- Aux personnes agissant sous leur responsabilité, et 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.

Pour des raisons de facilité de lecture, dans la suite du document, le terme « responsable du SIS » est utilisé pour désigner toute personne en charge dans la mise en œuvre de tout ou partie des règles, qu'elle soit la personne responsable de la structure ou une personne agissant sous sa responsabilité.

1.2. Périmètre d'application du guide

Le périmètre d'application de ce guide est celui fixé à l'article L1470-1 du code de la santé publique [CSP-L1470] : est concerné l'ensemble des services numériques en santé, les systèmes d'information (SI) ou les services ou outils numériques mis en œuvre par des personnes physiques ou morales de droit public ou de droit privé, y compris les organismes d'assurance maladie, proposés par voie électronique, qui concourent à des activités de prévention, de diagnostic, de soin ou de suivi médical ou médico-social, ou à des interventions nécessaires à la coordination de plusieurs de ces activités.

Au sein de ce périmètre, le présent guide décrit les règles qui s'appliquent à la mise en place de tout accès wifi par la structure, qu'il s'agisse d'accès destinés à la connexion d'équipements utilisés par le personnel de la structure ou d'accès destinés à la connexion d'équipements utilisés par des tiers (*comme par exemple des patients, des visiteurs…*), alors spécifiquement désignés sous le terme d'« **accès wifi invité** » ou d'« **accès invité** ».

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…

Catégories	Exemples de ressources informatiques
Equipement téléphonique	Smartphone, téléphone portable…
Equipement biomédical[1]	Appareil d'imagerie médicale, dispositif biomédical connecté…

1.3. Limites du périmètre d'application du guide

Dispositifs implantables et dispositifs autonomes

Les dispositifs implantables[2] et les dispositifs autonomes[3] ne sont pas traités par le présent guide. Il est toutefois possible de s'inspirer des règles présentées dans ce guide pour la mise en œuvre de fonctionnalités sans fil de ce type de dispositif.

Accès wifi « invité » gérés par des tiers

Les accès wifi « invité » qui correspondent à des prestations commerciales offertes au sein de la structure par des tiers et sans interconnexion avec le SI de la structure[4] ne sont pas traités dans ce guide. Il appartient au responsable de chacune de ces offres de sécuriser ces accès.

[1] *Au sens « Equipement faisant partie d'un dispositif médical ou d'un accessoire de dispositif médical tels que définis par les articles L5211-1 et R5211-1 du Code de la Santé Publique ».*

[2] *Dispositifs médicaux destinés à être introduits partiellement dans le corps humain par une intervention clinique et à demeurer en place après l'intervention pendant une période d'au moins trente jours*

[3] *Dispositifs médicaux dont l'usage et l'exploitation s'effectuent indépendamment de tout SIS.*

[4] *Hors partie du SI éventuellement accessible publiquement depuis Internet.*

2. ENJEUX PRINCIPAUX RELATIFS AUX ACCES WIFI

De façon générale, l'utilisation de réseaux wifi apporte un réel confort à l'utilisateur, puisqu'il lui permet de s'affranchir de la connexion physique de ses équipements au réseau local du SIS. Elle répond prioritairement aux besoins de mobilité des utilisateurs et des équipements à l'intérieur des locaux de la structure.

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

1. Rendre possibles les accès sans fil, par des acteurs de santé, aux ressources informatiques interne ou externes. 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, par exemple pour des raisons d'usage en mobilité dans les locaux de la structure, tendent à privilégier progressivement la connectivité sans fil.
   Ce cas est désigné par « accès technique ».

3. Rendre possible, pour des personnes qui n'appartient pas à la structure, l'accès à des ressources mises à leur disposition par la structure ou à Internet.
   Il s'agit d'offrir à des patients (hospitalisés dans une structure de soins) ou encore à des visiteurs (dans tous types d'organisation) la possibilité d'accéder à Internet ou à des applications spécifiques (*par exemple pour le choix du menu de restauration interne*) avec des équipements raccordés de façon temporaire en wifi, depuis des terminaux qui leur appartiennent le cas échéant (*smartphone, tablette*…), 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 cadre 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.

En contrepartie de cette facilité d'usage accrue, la mise en œuvre d'un tel réseau nécessite l'application 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, lequel traite notamment des données de santé à caractère personnel.

En outre, la mise en place d'un accès wifi ouvert aux invités (de type « hotspot ») impose de respecter les règles relatives à la protection de la vie privée des utilisateurs de réseaux et services de communications électroniques et à la protection de leurs données à caractère personnel.

Des règles spécifiques peuvent également s'appliquer aux bornes wifi ouvertes au public, en particulier l'obligation de conservation des données de connexion[5].

Il est dès lors essentiel de définir les mesures de sécurité adéquates pour garantir :

- La confidentialité des données transmises sur les liaisons wifi ;
- Le contrôle d'accès au réseau via l'accès wifi ;

[5] Article L34-1 du Code des Postes et des Communications Electroniques : *« II. - […] 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. […] »*, l'intégralité de l'article étant de ce fait applicable.

- Le cloisonnement strict des accès invités entre eux et vis-à-vis du SIS ;
- Le respect de la réglementation en matière d'accès à Internet ouvert au public et de protection des données à caractère personnel.

Par ailleurs, les spécificités des communications wifi en matière de disponibilité doivent être prises 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, selon les usages faits des réseaux wifi, de prévoir un mode dégradé permettant de garantir la continuité des activités, notamment de production de soins, en cas de dysfonctionnement des communications wifi.

3. UTILISATION DU GUIDE

La totalité des règles formulées au chapitre suivant 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.

Dans le cas d'un accès wifi « invité » destiné à être utilisé par des tiers (patients, visiteurs…), par opposition à un accès wifi destiné au personnel ou aux équipements de la structure, une croix (**X**) dans la colonne « Applicable aux accès wifi invité » des tableaux ci-après indique si la règle doit être respectée pour cet accès wifi.

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, à la lumière de l'analyse de risque menée pour le SI et l'environnement d'utilisation concernés ;
- D'estimer et de traiter les risques de sécurité induits par les règles non appliquées**.**

Les documents sur lesquels se base ce guide ou qui sont cités en référence sous la forme [REF] sont listés en Annexe 2 « Documents cités en référence ».

4. REGLES DE SECURITE APPLICABLES A LA MISE EN PLACE D'UN ACCES WIFI

4.1. Installation et configuration d'un point d'accès wifi

N°	Règle	Applicable aux accès wifi invité
[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.	**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 étudié 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 de leur 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, en cohérences avec les exigences de continuité de fonctionnement applicables à ces équipements.	**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, obtenu par exemple en déconnectant le câble de connexion réseau de l'équipement 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 dispositions physiques et de configuration du matériel (*par exemple ; routeur wifi dans une boite fermée à clef, routeur wifi positionné dans le champ de vision du personnel, désactivation des prises réseau RJ45 non utilisées, 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 du fournisseur de cet accès wifi (*établissement de santé, opérateur Internet*…) et de donner toute information qui permettrait à une personne mal intentionnée de se connecter au réseau. L'identifiant peut également être rendu invisible, nécessitant ainsi que l'utilisateur, lors de sa première connexion, entre manuellement les informations du SSID au lieu de sélectionner le réseau souhaité dans la liste des réseaux visibles. Il faut cependant noter que cette mesure n'est pas suffisante pour sécuriser l'accès au wifi, mais qu'elle peut contribuer à réduire le nombre de tentatives de connexions frauduleuses.	**X**

N°	Règle	Applicable aux accès wifi invité
[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 les uns vis-à-vis des autres au moyen de dispositifs de filtrage (firewall…) n'autorisant que les services, les protocoles et les ports de communication strictement nécessaires aux flux métiers et aux flux d'administration des équipements informatique.	
[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]	Les mots de passe par défaut du compte administrateur et, de manière générale, de tout compte privilégié de la borne wifi doit être modifié. Des mots de passe non triviaux de 12 caractères au minimum (recours à la fois de caractères alphabétiques, numériques, spéciaux et non triviaux) doivent être utilisés. Il est recommandé que ces mots de passe soient générés de manière aléatoire et aient une longueur d'au moins 16 caractères. Il est recommandé qu'ils soient stockés dans un porte-clé électronique sécurisé dédié ou intégré au logiciel d'administration réseau utilisé. Les mots de passe doivent être gérés de façon cohérente avec les autres mots de passe techniques utilisés au sein du SIS. Il est recommandé qu'ils soient renouvelés au moins tous les deux ans.	**X**
[C11]	Au niveau de la borne wifi et des éventuels autres équipements associés, 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 être désactivé quand le parc d'équipement ne nécessite pas de reconfiguration fréquente.	**X**
[C12]	L'authentification des utilisateurs et la confidentialité des données transmises 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. Un document [WIFI] de l'ANSSI décrit ces différents mécanismes. A 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 reconnue par les postes clients.	
[C14]	Lorsque des mécanismes d'authentification robuste (802.1X) ne peuvent pas 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. En outre, ce mot de passe ou « passphrase » doit avoir une longueur d'au moins 20 caractères.	**X**
[C15]	Les fonctions de simplification de l'authentification de type WPS (Wifi Protected Setup) doivent être désactivées.	**X**

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

N°	Règle	Applicable aux accès wifi invité
[C16]	Un filtrage de l'accès aux sites web doit être mis en place conformément à la charte d'utilisation d'accès réseau et d'usage du SIS de la structure.	X
[C17]	La 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 d'accès.	X

4.2. Exploitation d'un point d'accès wifi

N°	Règle	Applicable aux accès wifi invité
[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 exclusivement des protocoles sécurisés (*ex : HTTPS, SSH, autres protocoles encapsulés dans TLS*…). Les interfaces d'administration du point d'accès wifi ne doivent pas être accessibles 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, notamment en ce qui concerne le contrôle d'accès à ces traces, leur durée de conservation…	
[E5]	Le réseau du SIS ne doit pas accueillir de bornes wifi non gérées par le responsable du SIS (*bornes wifi « pirates »*). Des contrôles doivent être menés régulièrement pour s'assurer de ce point.	X

4.3. Mise en place d'un accès wifi invité

N°	Règle	Applicable aux accès wifi invité
[M1]	Le SIS interne et les réseaux wifi à usage interne doivent être strictement cloisonnés vis-à-vis du réseau wifi mis à disposition des invités pour interdire 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. A défaut, un cloisonnement logique doit être mis en œuvre et vérifié régulièrement.	X
[M2]	L'accès au réseau 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 (*à l'accueil par exemple*), soit par un enregistrement auprès d'un serveur portail 802.1X ou d'un portail captif.	X
[M3]	Dans le cas où un code personnel ou le passage par un portail web est nécessaire pour utiliser l'accès wifi Invité, la procédure doit comporter l'approbation par l'invité des conditions d'utilisation	X

N°	Règle	Applicable aux accès wifi invité
	de l'accès wifi invité, au moment de l'enregistrement de l'utilisateur s'il y a lieu ou lors de sa demande de connexion au réseau.	
[M4]	La connexion d'un invité au réseau wifi doit être temporaire. Sa durée maximale doit être explicitement indiquée lors de l'enregistrement ou de l'authentification au service. Dès que la durée maximale est dépassée, la connexion wifi doit être automatiquement interrompue.	**X**
[M5]	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. Le cas échéant, 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**
[M6]	Une trace technique de chaque connexion des utilisateurs au réseau wifi invité doit être enregistrée. Les article L34-1 et R10-13 du Code des Postes et des Communications Electroniques [CPCE] fixent les informations qui doivent être conservées dans cette trace. Les éléments suivants doivent notamment être enregistrés : ► Les informations d'identité et de contact de l'utilisateur, si elles ont été collectées (voir fiche CNIL [CONSERV]) ; ► Les informations permettant d'identifier le terminal utilisé (par exemple l'adresse MAC de son interface wifi) et la connexion au réseau wifi (*adresse IP attribuée, plage temporelle de la connexion*…). Ces traces doivent être conservée un an, puis supprimée. En outre, il doit être possible de générer des traces supplémentaires, uniquement dans le cadre d'une injonction émise par une autorité précisée par l'article L34-1 du [CPCE], enregistrant les informations suivantes : ► Les caractéristiques techniques (*protocole utilisé : http, https*…) ainsi que la date, l'horaire et la durée de chaque communication ; ► Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ; ► Les données permettant d'identifier le ou les destinataires de la communication (*adresse IP, nom DNS du site web consulté*…). Les traces enregistrées ne doivent en aucun cas porter sur le contenu des communications.	**X**
[M7]	Les utilisateurs doivent être informé, préalablement à l'accès au réseau wifi invité, de l'enregistrement de ces traces et du traitement de leurs données à caractère personnel correspondant. En particulier, l'ensemble des informations prévues à l'article 13 du Règlement général sur la protection des données [RGPD] doivent leur être communiquées, ainsi que leurs droits relatifs au traitement de leur données à caractère personnel fixés à l'article 15 du [RGPD].	**X**
[M8]	Des éléments de sensibilisation à la sécurité doivent être portés à la connaissance des utilisateurs du réseau wifi invité, notamment en ce qui concerne 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 associées (*rappel de l'engagement de sa responsabilité en cas de non-respect de la loi, existence éventuelle de mesure de filtrage*…). Ces éléments peuvent, par exemple, être intégrés aux supports d'informations diffusés aux usagers (*livret d'accueil, affiches en zone d'admission, dans les chambres et/ou dans les espaces patients interne*…) ou à la page d'accueil du portail d'accès au réseau wifi.	**X**

Annexe 1 : Fondements du guide

Les règles proposées par ce guide sont issues des bonnes pratiques en matière de SSI ainsi que des documents de référence suivants :

- Les recommandations publiées par l'ANSSI :
  - Recommandations de sécurité relatives aux réseaux WiFi [WIFI]
  - « Guide d'hygiène informatique », https://www.ssi.gouv.fr/entreprise/guide/guide-dhygiene-informatique/
- Les recommandations publiées par la CNIL :
  - Fiche pratique : « Conservation des données de trafic : hot-spots wifi, cybercafés, employeurs, quelles obligations ? » [CONSERV]
  - Guide de la sécurité des données personnelles – Fiche 7 : « Protéger le réseau informatique interne » [PROTEC]

Annexe 2 : Documents cités en référence

Réglementation

Renvoi	Document
[CPCE]	Code des Postes et des Communications Electroniques https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070987?etatTexte=VIGUEUR
[RGPD]	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (« règlement général sur la protection des données »), relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE et Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016
[CSP-L1470]	Articles L1470-1 à 1470-5 du code de la santé publique (issus de l'ordonnance n° 2021-581 du 12 mai 2021 relative à l'identification électronique des utilisateurs de services numériques en santé et des bénéficiaires de l'assurance maladie) https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043496464

Documents techniques

Renvoi	Document
[WIFI]	Recommandations de sécurité relatives aux réseaux WiFi (ANSSI, 09/09/2013) https://www.ssi.gouv.fr/entreprise/guide/recommandations-de-securite-relatives-aux-reseaux-wifi/
[CONSERV]	Fiche pratique : « Conservation des données de trafic : hot-spots wifi, cybercafés, employeurs, quelles obligations ? » (CNIL, 28/09/2010) https://www.cnil.fr/fr/conservation-des-donnees-de-trafic-hot-spots-wi-fi-cybercafes-employeurs-quelles-obligations
[PGSSI-S]	Politique générale de sécurité des systèmes d'information de santé https://esante.gouv.fr/produits-services/pgssi-s Corpus documentaire de la Politique générale de sécurité des systèmes d'information de santé https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire
[PROTEC]	Guide de la sécurité des données personnelles – Fiche 7 : « Protéger le réseau informatique » (CNIL) https://www.cnil.fr/fr/securite-proteger-le-reseau-informatique-interne

Annexe 3 : Glossaire

Sigle / Acronyme	Signification
AES	Advanced Encryption Standard
ANS	Agence du Numérique en Santé
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CNIL	Commission Nationale de l'Informatique et des Libertés
MAC	Media Access Control
PGSSI-S	Politique générale de sécurité des systèmes d'information de santé
PS	Personnel de Santé
SI	Systèmes d'Information
SIS	Systèmes d'Information de Santé
SSI	Sécurité des systèmes d'information
SSID	Service Set Identifier
TLS	Transport Layer Security
WPA2	Wifi Protected Access
WPS	Wifi Protected Setup