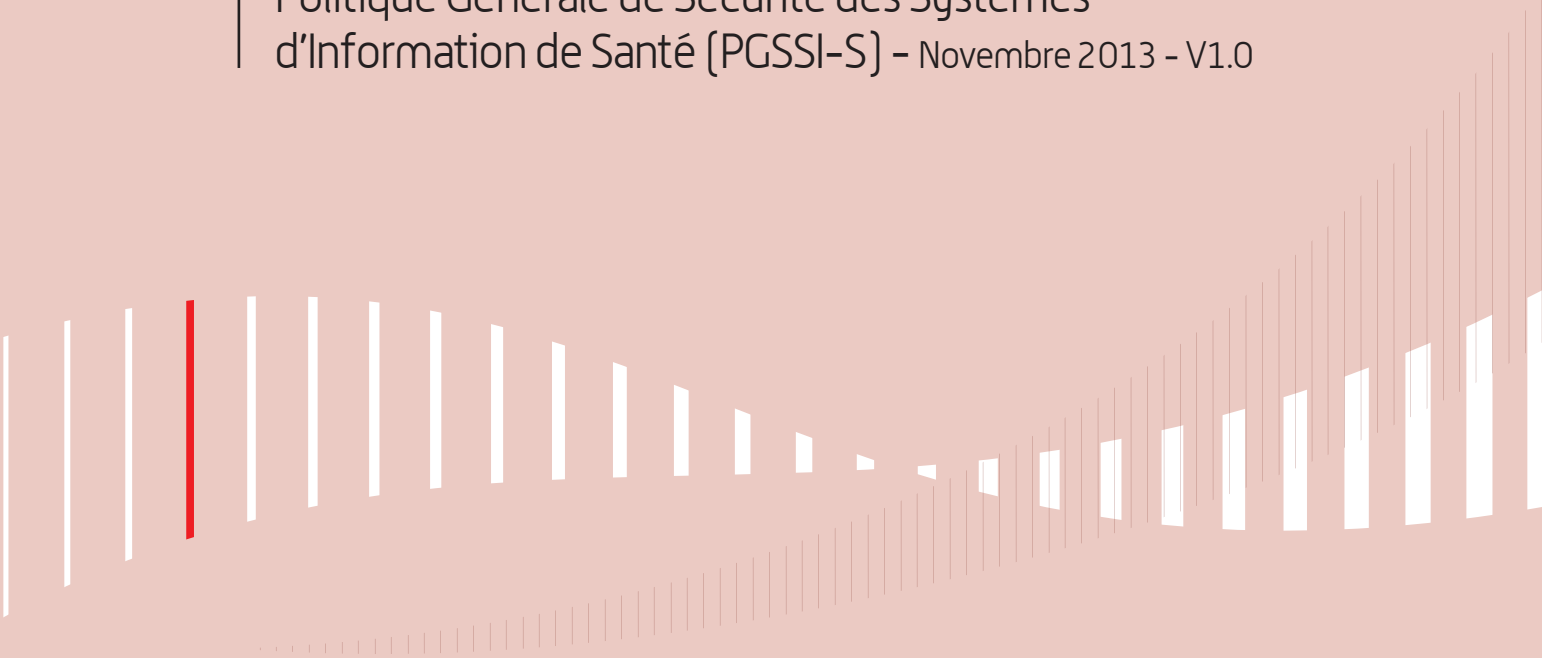
Mémento de sécurité informatique pour les professionnels de santé en exercice libéral

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. PRÉAMBULE

Professionnels de Santé, prenez quelques minutes pour lire ce mémento si :

- Vous utilisez un poste informatique (fixe, portable, tablette, …) contenant des données professionnelles, et en particulier des données de santé à caractère personnel de patients.
- Les moyens informatiques que vous utilisez sont connectés à Internet.
- Vous utilisez une carte de professionnel de santé (CPS) par exemple pour accéder au dossier médical personnel (DMP) de patients ou envoyer des feuilles de soins électroniques.
- Vous utilisez une messagerie électronique à des fins professionnelles et/ou vous échangez des données de santé à caractère personnel de patients pour la coordination des parcours de soins.
- Vous gérez votre agenda, comportant en particulier les noms de vos patients, sous format électronique.

Les données concernant vos patients doivent être protégées, qu'il s'agisse de données personnelles ou de données de santé à caractère personnel, ces dernières bénéficiant d'une protection renforcée au regard de leur sensibilité : leur dématérialisation nécessite la prise en compte des risques inhérents aux nouvelles technologies.
Le mémento a pour objectif de vous aider à respecter vos obligations légales, dont celles portant sur le secret professionnel. Il vous permet aussi d'éviter de nombreux écueils pouvant aller jusqu'à la perte de vos moyens informatiques et des données de santé à caractère personnel qu'ils contiennent.

« Admis dans l'intimité des personnes, je tairai les secrets qui me seront confiés. Reçu à l'intérieur des maisons, je respecterai les secrets des foyers et ma conduite ne servira pas à corrompre les mœurs »[1].

Le cadre législatif et réglementaire impose le respect de règles précises dès lors que sont traitées informatiquement des données à caractère personnel. Ces règles sont d'autant plus contraignantes que ces données ont trait à la santé d'un patient et sont ainsi soumises au secret professionnel.
Ce mémento vous accompagne dans une utilisation et une protection adéquates de vos moyens informatiques au regard de ces obligations.
Ce document méthodologique fait partie du corpus documentaire de la PGSSI-S, cité dans les documents de référence.
Il appartient à chaque professionnel de santé de s'approprier les différentes préconisations proposées, de les adapter à sa propre organisation et de se reporter autant que de besoin aux documents de référence.

1. Extrait de la version actualisée du serment d'Hippocrate.

2. POURQUOI PROTÉGER LES DONNÉES DE VOS PATIENTS ?

La prise en charge d'un patient nécessite le recueil de données à caractère personnel et tout particulièrement des données de santé. Ces données peuvent être partagées entre professionnels de santé ou provenir d'autres sources (DMP, autres professionnels de santé, institutions ou structures médicalisées, …) dans le respect du secret professionnel.
La prise en charge d'un patient est d'autant plus efficace qu'elle est réalisée sur la base d'informations disponibles mais aussi vérifiées, à jour, précises et cohérentes. Elle nécessite des moyens informatiques performants et garantissant la continuité du service.

Pour répondre aux enjeux liés à une bonne prise en charge des patients, il est nécessaire d'assurer :

- la **disponibilité des données de santé** des patients et des moyens informatiques pour limiter le risque de perte de chance ;
- la **confidentialité des données de santé** des patients pour préserver le secret professionnel ;
- l'**exactitude des données de santé** des patients pour un diagnostic rapide et juste ;
- le **partage maîtrisé des données de santé** des patients pour permettre la coordination des soins ;
- la **traçabilité** des actes médicaux dont les prescriptions médicales, des produits de santé dispensés ou administrés, des produits de santé utilisés ou implantés lors d'un acte chirurgical et la conservation de l'historique des antécédents médicaux, afin de conserver la mémoire des actions réalisées dans le cadre de la prise en charge du patient.

2.1. Le besoin de sécurité

Les moyens informatiques, devenus essentiels à la qualité des soins, se trouvent confrontés à des sources de menaces qui croissent en nature et en nombre. Cette informatisation rapide nécessite de tenir compte de nouveaux risques par rapport aux systèmes d'information papier.

De nombreux exemples ont récemment mis en lumière ces menaces et la fragilité de moyens informatiques insuffisamment protégés :

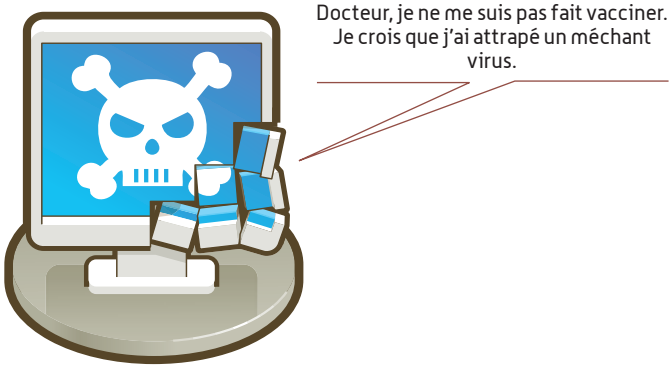
- Certains virus détruisent très rapidement des volumes considérables de données ou mettent hors-service un ordinateur. Ces situations conduisent parfois à devoir réinstaller tout le parc informatique et à reconstituer les données, et ce avec un coût élevé pour un résultat souvent très partiel.
- Les vols de matériels informatiques se multiplient et conduisent trop souvent à la perte de volumes conséquents de données de santé. Les conséquences financières, de temps passé et de gêne professionnelle sont élevées et très comparables à celles évoquées dans le point précédent.
- Des altérations (effacement par erreur, modifications indues…) de données, parfois essentielles aux professionnels de santé, se produisent régulièrement, par exemple dans le cas de suivi médical à partir d'informations issues de dispositifs implantés. Elles peuvent impacter très significativement la qualité du suivi des soins et des diagnostics.
- Des dossiers de patients peuvent se retrouver accessibles sur Internet, par de simples requêtes à travers des moteurs de recherche tels que Google, Yahoo, Bing… Ils sont souvent publiés sur Internet soit par erreur, soit après avoir été confiés à des fournisseurs de services d'hébergement de données dont la sécurité est défaillante. Ces incidents se traduisent par une médiatisation dommageable pour l'ensemble du secteur de la Santé, mais aussi des poursuites pénales engagées par les patients qui en sont victimes.

Adhérer à la démarche sécurité permet de prévenir les incidents liés aux moyens informatiques et de limiter leurs impacts sur les données de santé des patients qu'ils peuvent contenir.

Les menaces qui pèsent sur les moyens informatiques sont de nature technique, organisationnelle ou humaine. Elles peuvent résulter d'une volonté manifeste ou être fortuites.

2.2. La diversité des menaces informatiques

Un équipement informatique, matériel ou logiciel, peut présenter une panne, une défaillance ou être infecté par un programme malveillant. Ces programmes malveillants, notamment certains virus, peuvent entrainer la destruction totale d'un ordinateur et de ses données.



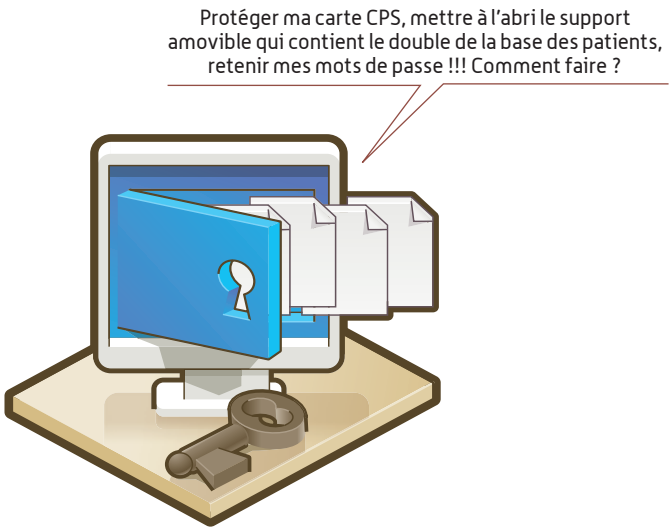
2.3. La recrudescence des actes de malveillance

Les vols d'équipements informatiques sur les lieux d'exercice sont fréquemment constatés. Ils alimentent un véritable marché noir des nouvelles technologies (tablettes, ordinateurs portables, téléphones, …). Ils contribuent aussi à des faits d'exploitation frauduleuse des données de santé à caractère personnel qu'ils contiennent, par exemple pour alimenter des campagnes ciblées de courriers électroniques de vente de médicaments d'origine douteuse.

Les données de santé peuvent aussi être extorquées par le biais d'attaques informatiques.

2.4. La multiplication des risques liés aux mauvais usages

Prêter son mot de passe, envoyer par courrier électronique des informations confidentielles non protégées, ne pas sauvegarder quotidiennement ses données… nombreux sont les écarts potentiels dont les conséquences peuvent être graves.
L'organisation définie au sein du lieu d'exercice doit considérer tous les aspects liés à l'utilisation ou à la gestion des moyens informatiques. Elle doit préciser les règles d'usage à respecter.



3. COMMENT PROTÉGER LES DONNÉES DE VOS PATIENTS ?

Les incontournables pour la sécurité des données de vos patients

La prise en charge d'un patient nécessite le recueil de données à caractère personnel, notamment des données de santé. Ces données peuvent être partagées entre professionnels de santé ou provenir d'autres sources (DMP, autres professionnels de santé, institutions ou structures médicalisées, …) dans le respect du secret professionnel.
La prise en charge d'un patient est d'autant plus efficace qu'elle est réalisée sur la base d'informations disponibles mais aussi vérifiées, à jour, précises, et cohérentes. Elle nécessite des moyens informatiques performants et garantissant la continuité du service.

La sécurisation des données et des moyens informatiques est une manière de répondre aux enjeux liés à une bonne prise en charge d'un patient et aux obligations de secret professionnel.
Dans un contexte marqué par la recrudescence des malveillances informatiques et des vols de matériels sur les lieux d'exercice, les principes suivants sont essentiels :

Le lieu d'exercice

- Une affiche de sensibilisation (affiche fournie par l'ASIP Santé) relative aux principes de fonctionnement du DMP et aux dimensions de sécurité associées, ainsi qu'une affiche relative à la protection des données personnelles fournie par la CNIL
- Une protection renforcée des ouvertures permettant l'accès au lieu d'exercice (portes et fenêtres) et si possible un système d'alarme.
- La fermeture à clé du local contenant des moyens informatiques (poste de travail, clé USB, disque dur amovible, tablette…) lors de votre absence et un câble antivol pour votre ordinateur portable.

Les équipements informatiques

- Un mot de passe non trivial, de 10 caractères (mêlant chiffres, lettres et caractères spéciaux) ou plus et renouvelé tous les 90 jours.
- Un verrouillage de session (déverrouillable par mot de passe) automatique au bout d'un temps d'inactivité, généralement de l'ordre de 30 minutes mais à adapter à vos contraintes.
- Un antivirus à jour, un pare-feu (firewall) et une application systématique des correctifs de sécurité du système informatique et des logiciels.

Les données de vos patients

- La pratique de sauvegardes régulières des systèmes et des données de vos patients (sauvegarde au minimum hebdomadaire, avec une conservation des sauvegardes mensuelles sur 12 mois glissants et annuelles) et leur conservation sur un lieu différent du lieu d'exercice.
- Le chiffrement des données avec un logiciel adapté, d'autant plus lorsqu'elles sont échangées par email ou encore stockées sur un support amovible.
- Pour réduire les risques d'attaques informatiques, ne connecter sur le réseau du lieu d'exercice que des matériels informatiques à usage professionnel.
- Le respect des formalités préalables généralement simplifiées pour les professionnels de santé. Les procédures de déclaration sont accessibles dans la rubrique réservée aux professionnels sur le site Internet de la CNIL (www.cnil.fr).

La Carte de Professionnel de Santé (CPS)

- Le respect du caractère personnel et strictement incessible des CPS.
- La préservation de la confidentialité totale des codes secrets de la CPS (PIN et PUK).
- Le rappel des mêmes principes aux porteurs de Cartes de Professionnels d'Etablissements (CPE) au sein du lieu d'exercice.

Que faire en cas d'incident ?

Un incident est considéré comme grave si la confidentialité de données de santé à caractère personnel est atteinte ou si des données de santé essentielles à la prise en charge de patients sont détruites. Un incident peut être, par exemple, la conséquence du vol de matériel informatique ou d'une intrusion informatique.

1) Si vous avez un doute, contactez en premier lieu votre prestataire de services informatiques pour vous aider au diagnostic. N'interagissez plus avec vos moyens informatiques si l'incident suspecté est grave pour permettre une éventuelle copie des données à valeur juridique (certaines situations peuvent nécessiter une mise sous séquestre).
2) Rendez-vous sur le site de l'Agence Nationale de la Sécurité des Systèmes d'Information - www.ssi.gouv.fr - et consultez la rubrique « Que faire en cas d'incident ».
3) Si l'incident est avéré et la conséquence d'une malveillance, faites une déclaration auprès des services de police ou de gendarmerie. Cette déclaration est indispensable en cas de vol de matériel informatique ayant contenu des données de Santé de vos patients.
4) Pour les signalements d'incidents, cette fiche sera complétée en fonction des travaux du Groupe de Travail « Organisation de la sécurité » de la PGSSI-S.

Détail des règles de protection des données de vos patients par thématique

Ce paragraphe a pour objectif de faciliter l'appréhension des thématiques de sécurité qui suivent. Il présente notamment les critères qui vous permettent d'organiser le recours à un tiers pour répondre aux obligations de sécurité et de mieux percevoir les limites de votre responsabilité en fonction de votre contexte d'exercice.

Les cas présentés ci-dessous ne considèrent que les moyens informatiques et ne préjugent pas du contexte de l'exercice, c'est-à-dire qu'ils peuvent s'appliquer :

- **à un professionnel de santé exerçant seul et qui est intégralement responsable des moyens informatiques qu'il utilise ; dans ce cas, le professionnel de santé est le responsable du traitement des données à caractère personnel.**
- **à un professionnel de santé exerçant dans un contexte collectif (cabinet de groupe, EHPAD, laboratoire, réseau de soins, pôle de santé, …) et qui utilise dans ce cadre des moyens informatiques mutualisés ou mis à disposition par un tiers, avec une responsabilité limitée à celle relevant de l'utilisation de ces moyens.**

Les moyens informatiques que vous utilisez se composent :

- au moins d'un poste de travail disposant d'un lecteur de cartes pour votre carte CPS et les cartes Vitale des patients, d'un terminal de paiement, d'une imprimante, d'un scanner, …
- d'un accès à Internet, qui relève d'un abonnement de type « particulier » ou « professionnel » ;
- d'un logiciel métier pour la gestion des dossiers de vos patients (exemple : Logiciel de Gestion de Cabinet, Logiciel de gestion d'Officine, Logiciel d'Aide à la Prescription, …).

Vous renseignez vous-même les dossiers patients. Dans le cadre de votre organisation interne, vous pouvez confier certaines activités de gestion des dossiers patients au personnel autorisé (secrétaire médicale par exemple) qui intervient sous votre responsabilité et qui est tenu au secret professionnel.

Pour la protection de vos outils professionnels et des données qu'ils contiennent, plusieurs cas sont possibles :

Cas 1 : Vous êtes totalement autonome quant à la gestion de votre système informatique. Vous êtes responsable de vos matériels et outils informatiques et administrateur de votre poste de travail.

➜ Vous devez mettre en œuvre et respecter toutes les exigences du présent document.

Cas 2 : Vous avez recours à un (ou plusieurs[22]) prestataire(s) pour vous aider dans la gestion de votre système informatique

Option A : La maintenance des moyens informatiques fait l'objet d'un contrat de service avec un prestataire, qui peut également être en charge de la fourniture du matériel.

➜ L'exécution des règles correspondant à cette option A peut être confiée à votre fournisseurs dans le cadre du contrat portant sur cette prestation d'hébergement.
L'annotation A identifiant ce type de règles est positionnée devant chaque règle dans un cartouche.
Exemple : | A | |

Option B : vous accédez par internet à l'application métier. Celle-ci est gérée par une société qui héberge des données de santé de vos patients.

➜ L'exécution des règles correspondant à cette option B peut être confiée à votre fournisseur dans le cadre du contrat portant sur cette prestation d'hébergement.
L'annotation B identifiant ce type de règles est positionnée devant chaque règle dans un cartouche.
Exemple : | | B |

Les options A et B ne sont pas exclusives l'une de l'autre. Le professionnel de santé peut y avoir recours simultanément.

2. Pour faciliter la lecture, la formulation au singulier est retenue pour la suite. Si vous avez plusieurs prestataires, considérez que l'application des règles peut être exigée de chacun dans la limite des travaux qui leur sont confiés.

Exemple

Je suis professionnel de santé en exercice libéral en cabinet individuel. J'ai passé un contrat de maintenance avec un prestataire qui vient régulièrement s'assurer du bon fonctionnement de mes matériels informatiques (imprimante, ordinateur, etc.).

J'accède via internet à l'application de gestion de mes patients. Pour cela, j'ai souscrit à une solution d'entreprise qui héberge les données de mes patients.

Je peux confier contractuellement:
- l'application et la mise en œuvre des règles annotées avec un **A** au tiers s'occupant de la prestation de maintenance, l'application et la mise en œuvre des règles annotées avec un **B** à la société propriétaire de l'application de gestion de mes patients,
- l'application et la mise en œuvre des règles annotées avec un **A** et un **B** au tiers s'occupant de la prestation de maintenance et à la société propriétaire de l'application de gestion des patients.

L'ensemble des règles applicables est présenté ci-après. Ces règles doivent permettre une mise en œuvre opérationnelle de la sécurité.

Elles sont organisées en thématiques homogènes :
- le rappel des obligations légales ;
- la promotion de la sécurité, que ce soit vis-à-vis de son personnel ou du patient ;
- la sécurité physique du lieu d'exercice ;
- la protection des équipements informatiques ;
- la maîtrise des accès aux informations ;
- la gestion des incidents de sécurité.

Thématique 1 : Répondre aux obligations légales

L'obligation de secret professionnel doit être respectée quel que soit le support de l'information médicale, papier ou informatique. Chaque professionnel doit assurer aux informations médicales dématérialisées le même niveau de protection et de confidentialité que celui qu'il donne aux informations dont il a connaissance ou qu'il conserve sous forme papier

À titre d'exemple, conditionner l'accès à un ordinateur par un mot de passe est comparable à la mise sous clé des dossiers médicaux sous format papier.

1.1. Respecter les règles d'échange et de partage de données de santé à caractère personnel

1.1.1. Respecter les règles d'échange des données de santé à caractère personnel

L'échange de données, c'est la communication d'informations à un (des) destinataire(s) clairement identifié(s) par un émetteur connu. L'utilisation d'une messagerie sécurisée en constitue un exemple.

- L'échange de données doit être précédé d'une information claire, afin de laisser au patient la possibilité d'exercer son droit d'opposition.
- L'échange de données de santé entre deux ou plusieurs professionnels de santé est subordonné à deux conditions cumulatives :
  - les professionnels de santé doivent tous intervenir dans la prise en charge du patient dont les données de santé sont échangées
  - l'échange de données doit être limité aux données utiles pour la continuité des soins ou la détermination de la meilleure prise en charge sanitaire du patient.

1.1.2. Respecter les règles de partage des données de santé à caractère personnel

Le partage des données de santé à caractère personnel permet de mettre à la disposition de plusieurs professionnels fondés à en connaître des informations utiles à la coordination et à la continuité des soins ou l'intérêt de la personne.
Les conditions de partage de données de santé sont fortement dépendantes du mode d'exercice du professionnel de santé.

Un professionnel de santé en exercice libéral peut ainsi être confronté aux situations suivantes:

Partage de données de santé au sein d'une maison ou d'un centre de santé

- Le partage de données doit être précédé d'une information et d'un consentement exprès des patients avec une possibilité de retrait du consentement à tout moment.
- Les professionnels de santé de la maison ou du centre de santé peuvent accéder à toutes les informations concernant la personne prise en charge.

Partage de données de santé au sein d'un établissement de santé

- Le patient dispose du droit de s'opposer, pour des motifs légitimes à l'accès à ses données de santé.
- Les données de santé sont partagées au sein de l'équipe de soin constituée des professionnels de santé qui participent à la prise en charge sanitaire du patient.

Partage de données de santé dans le cadre d'un « dossier médical partagé »
(Dossier Médical Personnel (DMP), Dossier Pharmaceutique (DP), dispositif de télémédecine, réseaux de santé, etc.)

- Le professionnel de santé doit s'enquérir pour chaque service des conditions spécifiques applicables.
- Limiter l'accès aux données de santé de vos patients aux stricts besoins liés à la prise en charge des soins.

1.2. Respecter les principes de la protection des données de santé à caractère personnel

La loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés définit les principes à respecter lors de la collecte, du traitement et de la conservation des données à caractère personnel.

Ces principes sont au nombre de cinq :

- **la finalité du traitement**
  Les données à caractère personnel ne peuvent être collectées et traitées que pour une finalité déterminée, explicite et légitime. Elles ne peuvent être utilisées ultérieurement de manière incompatible avec cette finalité. Le détournement de finalité est pénalement sanctionné.

- **la pertinence et la proportionnalité des données**
  Les données collectées et traitées doivent être adéquates, pertinentes et non excessives au regard de la finalité poursuivie.
  Certaines catégories de données font l'objet d'une protection légale particulière, en particulier les données dites « sensibles » dont font partie les données de santé (art. 8).

- **la conservation limitée des données**
  Les données ne peuvent être conservées dans les fichiers au-delà de la durée nécessaire à la réalisation de la finalité poursuivie.

- **la sécurité et la confidentialité des données**
  Le responsable du traitement doit veiller à ce que les données ne soient pas déformées, endommagées et que des tiers non autorisés ne puissent y avoir accès.
  Les mesures de sécurité physique et logique doivent être adaptées à la nature des données et aux risques présentés par le traitement.

- **le respect des droits des personnes**
  - le droit à l'information
  - le droit d'opposition
  - le droit d'accès
  - le droit de rectification

L'exercice de ces droits est soumis à certaines conditions fixées par la loi informatique et libertés et son décret d'application (Décret nº 2005-1309 du 20 octobre 2005).
En outre, tout responsable de traitement ne peut mettre en œuvre un traitement automatisé contenant des données à caractère personnel qu'après s'être assuré du respect des formalités préalables applicables, le cas échéant, à la mise en œuvre du traitement.

Pour les cabinets médicaux, les pharmacies, les laboratoires d'analyses médicales ou encore les centres d'optiques, les formalités ont été simplifiées (normes simplifiées nº 50, 52, 53, 54). Dès lors que le traitement est conforme au contenu des normes de référence un simple engagement de conformité à la norme suffit. Les procédures de déclaration sont accessibles dans la rubrique réservée aux professionnels sur le site internet de la CNIL (www.cnil.fr).

1.3. Définir l'objet des prestations et les limites d'engagement dans les relations contractuelles avec des tiers fournisseurs de service

1.3.1. Définir précisément dans le contrat le contenu des prestations confiées au tiers fournisseur de service pour répondre aux obligations de sécurité

- Le contrat va permettre par la description du contenu des prestations confiées au tiers fournisseur de service par le professionnel de santé d'apprécier la répartition des responsabilités entre le fournisseur de service et le professionnel de santé. Le professionnel de santé peut avoir recours à des prestataires de services spécialisés qui établissent fréquemment des prestations et des contrats standards à signer par le client et fixant *de facto* un certain mode de traitement

standardisé des données à caractère personnel. **Le professionnel de santé, en sa qualité de responsable du traitement de données à caractère personnel reste libre d'accepter ou non les clauses contractuelles. Il lui appartient de veiller à ne pas accepter de clauses et conditions contractuelles qui seraient contraires à la législation sur la protection des données.**

- Le contrat prévoit que le tiers fournisseur de service s'engage à respecter les éléments du Mémento et les référentiels cités en référence qui le concernent.
- Les prestations qui peuvent être confiées à un tiers fournisseur pour remplir les obligations de sécurité sont identifiées par les lettres A et B.

1.3.2. Exercer sereinement dans des environnements maîtrisés par un tiers

- Dans de nombreuses situations d'exercice, les professionnels de santé libéraux ne sont pas maîtres des moyens de travail, qui sont mis à leur disposition par un tiers qui en assument la responsabilité. Ce peut être le cas par exemple pour les professionnels de santé libéraux qui exercent en EHPAD, en établissement de santé, au sein de sociétés civiles organisant la mise en commun de moyens. Cette situation peut également concerner des professionnels de santé réalisant des remplacements. Pour vous prémunir du risque juridique inhérent à cette situation, vous pouvez inclure dans le contrat qui organise vos relations avec le tiers mettant à disposition les moyens informatiques, une clause l'engageant à garantir que ces moyens informatiques respectent les principes du présent Mémento et des référentiels cités en référence.
- En cas de manquement manifeste aux obligations de sécurité mis en évidence à l'occasion de l'utilisation des moyens informatiques mis à sa disposition, le professionnel de santé devra le signaler aux autorités compétentes.

1.3.3. Respecter les règles relatives à l'hébergement de données de santé à caractère personnel

- Si vous confiez les données de vos patients à un tiers (par exemple dans le cadre d'une prestation de fourniture d'un outil en ligne de gestion de vos patients), assurez-vous que ce tiers dispose d'un agrément en tant qu'hébergeur de données de santé à caractère personnel.

1.4. Répondre aux obligations de conservation et de restitution des données

1.4.1. Fixer une durée de conservation des données de santé à caractère personnel

- Le dossier médical constitué pour chaque patient hospitalisé doit être conservé par les établissements de santé, publics et privés, pendant une durée de vingt ans à compter de la date du dernier séjour de son titulaire dans l'établissement ou de la dernière consultation externe en son sein […] (Cf. article R1112-7 du code de la santé publique). Cette durée couvre selon la doctrine de la CNIL la durée de conservation des archives dites actives et également la durée des archives intermédiaires[33]. Le même niveau de protection (ex. droit d'accès, sauvegarde…) doit être assurée quel que soit le statut de la donnée archivée (archive active ou intermédiaire). Les modalités pratiques permettant la protection de ces données peuvent être en revanche différentes, les données qualifiées d'archive intermédiaire n'étant plus considérées comme « vivantes » (i.e. susceptibles d'être modifié).
  En l'absence de règles propres au dossier constitué par le professionnel libéral pour le suivi de ses patients, il est d'usage d'adopter la même durée de conservation.

1.4.2. S'assurer de la capacité de restitution des données de santé à caractère personnel

- Lors de recours à une prestation comprenant de l'hébergement des données de santé à caractère personnel, le contrat doit prévoir que lorsqu'il sera mis fin à l'hébergement, l'hébergeur lui restituera les données, sans en garder de copie. Le support sur lequel seront restituées les données devra permettre au professionnel de santé de poursuivre son activité et, le cas échéant, de recourir à un autre prestataire pour les héberger.

3. Au-delà de cette durée, les règles qui s'appliquent sont celles fixées par le code du patrimoine.

Thématique 2 : Promouvoir la sécurité

2.1. Connaître et faire connaître les principes essentiels de sécurité

2.1.1. Maîtriser les recommandations de sécurité

- Prendre connaissance de ce mémento.
- Compléter vos connaissances par la réalisation du module d'autoformation « Principes essentiels de la sécurité informatique » et du test associé, proposés sur le site dédié de l'Agence Nationale de la Sécurité des Systèmes d'Information[44].

2.1.2. Sensibiliser votre personnel

- Diffuser les recommandations générales de sécurité présentes dans ce document.
- Connaître et faire connaître les aspects légaux qui encadrent la gestion des données de santé à caractère personnel, accessibles sur le site de la CNIL : www.cnil.fr.

2.2. Informer vos patients

2.2.1. Informer vos patients des conditions de traitement informatique de leurs données, en particulier dans le cadre du DMP

- Apposer une affiche d'information relative aux traitements des données des patients (modèles proposés par la CNIL[5]) à la vue des patients dans votre lieu d'exercice.
- Mettre en évidence sur le lieu d'exercice une affiche de sensibilisation (affiche fournie par l'ASIP Santé[6]) relative aux principes de fonctionnement du DMP et aux conditions de sécurité associées.
- Partager toute l'information nécessaire avec vos patients en amont d'opérations liées au cycle de vie de leur DMP et conditionnées à leur accord (ouverture, transmission de droits, suppression de contenus et éventuellement fermeture ou suspension).

4. www.securite-informatique.gouv.fr/gp_article676.html
5. http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_professionnels_de_sante.pdf
6. http://www.dmp.gouv.fr/e-doc-sts

Thématique 3 : Assurer la sécurité physique du lieu d'exercice

3.1. Maîtriser l'accès aux équipements qui sont nécessaires à votre activité

A 3.1.1. Assurer la protection physique de vos équipements, qui contiennent des données de santé à caractère personnel et qui ne sont pas sous votre surveillance

- Assurer une protection renforcée des ouvertures permettant l'accès au lieu d'exercice (portes et fenêtres) et si possible mettre en place un système d'alarme.
- Placer vos équipements informatiques dans un lieu qui n'est pas facilement accessible par le public (patients, accompagnants, …) et protéger votre ordinateur du vol (par exemple : portable avec un câble antivol, coffre, …) pendant les heures de travail et en dehors.
- Sélectionner un lieu qui ne présente pas de risques environnementaux ou majeurs (dégâts des eaux, incendie, installation électrique défaillante, …).
- Veiller à relier électriquement vos équipements à un équipement qui prévient les différences de tension (multiprises avec dispositif anti surtension, onduleur…).

A 3.1.2. Assurer la protection physique de vos équipements amovibles, qui contiennent des données de santé à caractère personnel et qui ne sont pas sous votre surveillance

- Placer vos équipements amovibles (disques durs externes, CD ou DVD, etc.) dans un coffre ou une armoire qui ferme à clé.
- Procéder à la destruction physique des équipements supports intégrant un espace de stockage de données non effaçable (exemples : CD, DVD, carte de mémoire flash endommagée, …).
- Assurer l'effacement des données avant de procéder à l'échange standard ou au remplacement des équipements supports intégrant un espace de stockage de données (disque dur, carte de mémoire flash, …).

Thématique 4 : Protéger vos équipements informatiques

4.1. Gérer la connexion Internet

A 4.1.1. Paramétrer correctement votre connexion Internet accessible depuis un boîtier intégrant des options de sécurité

- Utiliser les options de sécurité offertes par votre fournisseur d'accès. Ces options sont proposées et présentées dans le guide d'installation.

4.2. Gérer le réseau local

A 4.1.2. Protéger correctement votre réseau local

- Vérifier fréquemment que seuls vos équipements informatiques professionnels sont connectés au réseau.
- Configurer le réseau WIFI, s'il est utilisé au sein de votre lieu d'exercice, avec la technologie WPA2 pour en protéger l'accès.
- Ne jamais utiliser simultanément une double connexion filaire et Wifi au réseau.
- Désactiver les fonctions Wifi ou Bluetooth si elles ne sont pas utilisées.

4.3. Adopter les bons réflexes pour protéger l'accès à votre système

Exemple de mot de passe	
Mot de passe non robuste	Mot de passe robuste
28011968 Date de naissance	**1Ax5b=5Ab!** Mot de passe robuste et mémorisable

A B 4.3.1. Gérer les mots de passe pour qu'ils présentent une robustesse appropriée (cf. guide ANSSI – Recommandations de sécurité relative aux mots de passe).

- Fixer à au moins 10 caractères la longueur du mot de passe et éviter qu'il soit prédictible.
- Imposer la combinaison de caractères alphanumériques et de caractères spéciaux (# » !-…).
- Procéder au renouvellement périodique de vos mots de passe.
- Interdire la réutilisation des 3 mots de passe précédents.
- Interdire un mot de passe identique au nom du compte.
- Adopter une approche mnémotechnique pour vous souvenir de vos mots de passe, sans jamais les inscrire sur un support accessible par un tiers.
- Refuser systématiquement la mémorisation de vos mots de passe lorsqu'elle vous est proposée par votre navigateur Internet.

A 4.3.2. Protéger l'accès à votre poste de travail en votre absence

- Activer la mise en veille automatique de votre poste de travail après une durée compatible avec votre activité (des durées de 30 minutes sont généralement adaptées).
- Penser à mettre manuellement en veille votre poste de travail lorsque vous vous en éloignez (par exemple sous Windows, le raccourci clavier pour ce faire est le suivant : Touche Windows + L).
- Imposer le déverrouillage de l'écran de veille par usage du mot de passe du compte.

A B 4.3.3. Assurer la protection logique de vos équipements et supports informatiques, qui contiennent des données de santé à caractère personnel

- Mettre en place un antivirus sur votre poste de travail et le maintenir à jour.
- Installer un pare-feu sur votre poste de travail et le maintenir à jour.
- Recourir à un logiciel de chiffrement pour protéger votre poste de travail, serveur, clé USB, disque dur amovible ou encore smartphone ; les outils préconisés sont ceux qui bénéficient d'un référencement sur le site de l'ANSSI (www.ssi.gouv.fr).

A B 4.3.4. Procéder à une mise à niveau régulière de vos moyens informatiques

- Vérifier que les logiciels et le système d'exploitation sont toujours maintenus et mis à jour par les industriels pour anticiper notamment les évolutions de versions.
- Appliquer l'ensemble des correctifs de sécurité du système informatique et des logiciels.

A B 4.3.5. Vérifier l'authenticité des logiciels

- N'utiliser que des logiciels originaux à l'exclusion de toute copie.

Thématique 5 : Maîtriser les accès aux informations

5.1. Maîtriser l'accès aux données de vos patients

5.1.1. Utiliser votre carte CPS en respectant les conditions générales d'utilisation et les consignes de sécurité

- Garder secret votre code PIN (en particulier détruire ou protéger les courriers relatifs au code PIN).
- Maintenir la CPS près de vous en période d'utilisation et dans un lieu sûr (pour éviter la perte ou le vol) lorsque vous ne travaillez pas.
- Conserver le code PUK[7] en lieu sûr (pour éviter l'utilisation frauduleuse de la CPS en cas de perte ou de vol).
- À la réception d'une nouvelle CPS, détruire l'ancienne CPS après vérification du bon fonctionnement de la nouvelle.

5.1.2. Dans le cas de la délivrance d'une Carte de Personnel d'Etablissement (CPE), les consignes de sécurité appliquées devront être les mêmes que pour la carte CPS

- Lorsqu'une carte CPE est confiée à une personne de votre lieu d'exercice, il convient de lui rappeler que la carte ne doit en aucun cas être laissée pour un usage « en libre-service ».
- Remettre au porteur de la carte une notice explicative relative aux conditions générales d'utilisation (accessible sur le site esante.gouv.fr).

5.2. Identifier des profils pour l'utilisation de votre système

A 5.2.1. Créer des comptes[8] qui respectent les bons usages

- Créer des comptes utilisateurs nominatifs pour vous et pour votre personnel autorisé. Les comptes utilisateurs ne doivent pas avoir les mêmes droits qu'un compte administrateur.
- Créer un compte administrateur, avec un mot de passe distinct du compte utilisateur Les comptes administrateurs peuvent concerner un environnement technique (poste de travail, système d'exploitation) ou un environnement applicatif (Logiciel de Gestion de Cabinet, Logiciel de Gestion d'Officine, Logiciel d'Aide à la Dispensation …).

A B 5.2.2. Utiliser les comptes de manière appropriée

- Réserver l'utilisation du compte administrateur aux actions d'administration (installation de logiciels par exemple).
- Mettre en place le verrouillage de compte pendant 5 minutes minimum après trois essais de mot de passe infructueux.
- Dans la mesure du possible, limiter l'usage des comptes utilisateurs aux seules applications auxquelles ils ont légitimement accès (logiciel métier, dossiers patients, logiciel de messagerie…).

5.3. Protéger les comptes informatiques les plus sensibles

A 5.3.1. Consigner le mot de passe du compte administrateur

- Mettre la feuille qui contient le mot de passe administrateur sous enveloppe cachetée.
- Placer cette enveloppe dans un endroit sûr (coffre-fort, armoire fermant à clé).

A 5.3.2. Créer un nouveau compte nominatif pour permettre à un nouveau professionnel de santé d'accéder aux environnements informatiques

- Créer un compte de travail avec des droits suffisants pour permettre une gestion normale des dossiers des patients.
- Désactiver temporairement ou définitivement votre compte de travail courant.
- En cas de cession de votre activité, s'assurer que votre successeur ou remplaçant est en mesure de modifier le mot de passe du compte d'administration.

7. Le code PUK permet de réactiver une CPS en cas de blocage consécutif à plusieurs saisies erronées de codes PIN via un appel au support CPS 0 825 85 2000. Ce code vous a été transmis par courrier lors de la remise de votre carte.
8. Un compte permet à un utilisateur d'accéder à un environnement de travail adapté à ses besoins et à ses droits.

5.3.3. Maîtriser la liste des comptes autorisés à se connecter à votre environnement informatique

- Désactiver temporairement ou définitivement le compte de votre personnel en cas d'absence prolongée ou de départ.
- Si votre personnel a pu avoir connaissance du mot de passe d'administrateur, changer ce mot de passe.

Thématique 6 : Limiter la survenue et les conséquences d'incidents de sécurité

6.1. Conserver les traces informatiques

A B 6.1.1. Tracer spécifiquement les actions réalisées sur les données de santé à caractère personnel

- Mettre en place et surtout activer la génération de traces de vos logiciels métiers. Contacter le support de votre logiciel, au besoin se référer au guide d'utilisation et d'administration mis à disposition par le fournisseur du logiciel.

A B 6.1.2. Tracer les événements informatiques

- Mettre en place et surtout activer la fonction de journalisation sur votre système d'exploitation (sur tous les équipements disposant d'un système d'exploitation autonome).
- Consigner les événements émanant de l'antivirus et du pare-feu en activant la journalisation des événements tel que précisé dans les guides d'utilisation.

6.2. Faire face à un incident de sécurité

A B 6.2.1. Anticiper la survenue d'un incident de sécurité

- Vérifier que les conditions (par exemple : sauvegarde des données, ordinateur portable équipé des logiciels nécessaires, accès de repli à Internet) sont réunies pour vous permettre de poursuivre vos activités de soin en cas de sinistre.

A B 6.2.2. Prendre les mesures pour gérer les incidents de sécurité

- Déconnecter du réseau le ou les équipements dont le fonctionnement est anormal et potentiellement utilisé par la personne malveillante, dans le cas d'une intrusion informatique.
- Révoquer les droits et les privilèges associés sur les équipements et les logiciels en cas de compromission (exemple : appeler le support CPS 0 825 85 2000 pour révoquer une carte CPS volée ou égarée).
- Se rendre sur le site de l'Agence Nationale de la Sécurité des Systèmes d'Information - www.ssi.gouv.fr - et consulter la rubrique « Que faire en cas d'incident ».
- Si l'incident est avéré et la conséquence d'une malveillance, faire une déclaration auprès des services de police ou de gendarmerie.

6.3. Sauvegarder vos données

A B 6.3.1. Procéder à des sauvegardes régulières

- Procéder à la sauvegarde de vos systèmes, avant toute nouvelle installation ou nouveau paramétrage de vos équipements (souvent une copie intégrale du système et des données sur un disque dur externe) pour pouvoir restaurer le système dans les meilleures conditions en cas de nécessité.
- Procéder fréquemment à la sauvegarde de vos données,
  - au moins chaque semaine, avec un support de sauvegarde différent chaque fois et
  - une réutilisation possible des supports par rotation sur 4 semaines et
  - en conservant une sauvegarde mensuelle sur 12 mois glissants.
- Conserver les sauvegardes au minimum dans un lieu sûr et de préférence **dans deux lieux sûrs différents**. Le recours à un service tiers est encouragé pour garantir la fiabilité et la pérennité des sauvegardes.
- Procéder à des tests de restauration des éléments sauvegardés, au moins trimestriellement, pour assurer le maintien en état d'utilisation des sauvegardes.
- Afin d'assurer la disponibilité des données en cas d'incident, les sauvegardes doivent être mises sous clé dans un format non chiffré.

4. ANNEXES

4.1. Annexe 1 – Pour en savoir plus

L'information des patients à l'égard du traitement de leurs données	www.cnil.fr : Guide des professionnels de santé publié par la CNIL, Modèles d'affichettes d'information
L'exercice du droit d'accès, de rectification et de suppression des données par le patient	www.cnil.fr : Guide des professionnels de santé publié par la CNIL, Fiche n° 2 – Le droit d'accès au dossier médical
La déclaration du traitement de données à caractère personnel à la CNIL	www.cnil.fr : Guide des professionnels de santé publié par la CNIL, Fiche n° 20 – Comment déclarer auprès de la CNIL
La clause de confidentialité d'un contrat	www.cnil.fr : Guide des professionnels de santé publié par la CNIL, Annexe – Modèle de clause confidentialité en cas de sous-traitance
L'agrément des hébergeurs de données de santé	www.cnil.fr : Guide des professionnels de santé publié par la CNIL, Fiche n° 11 – Les hébergeurs de données de santé
	esante.gouv.fr : Liste des hébergeurs agréés
La sécurité des interventions à distance	PGSSI-S : Règles pour les interventions à distance sur les Systèmes d'Information de Santé
Les logiciels antivirus et antispyware	www.ssi.gouv.fr : Portail de la sécurité informatique de l'ANSSI
L'hygiène informatique	
Le choix des mots de passe	

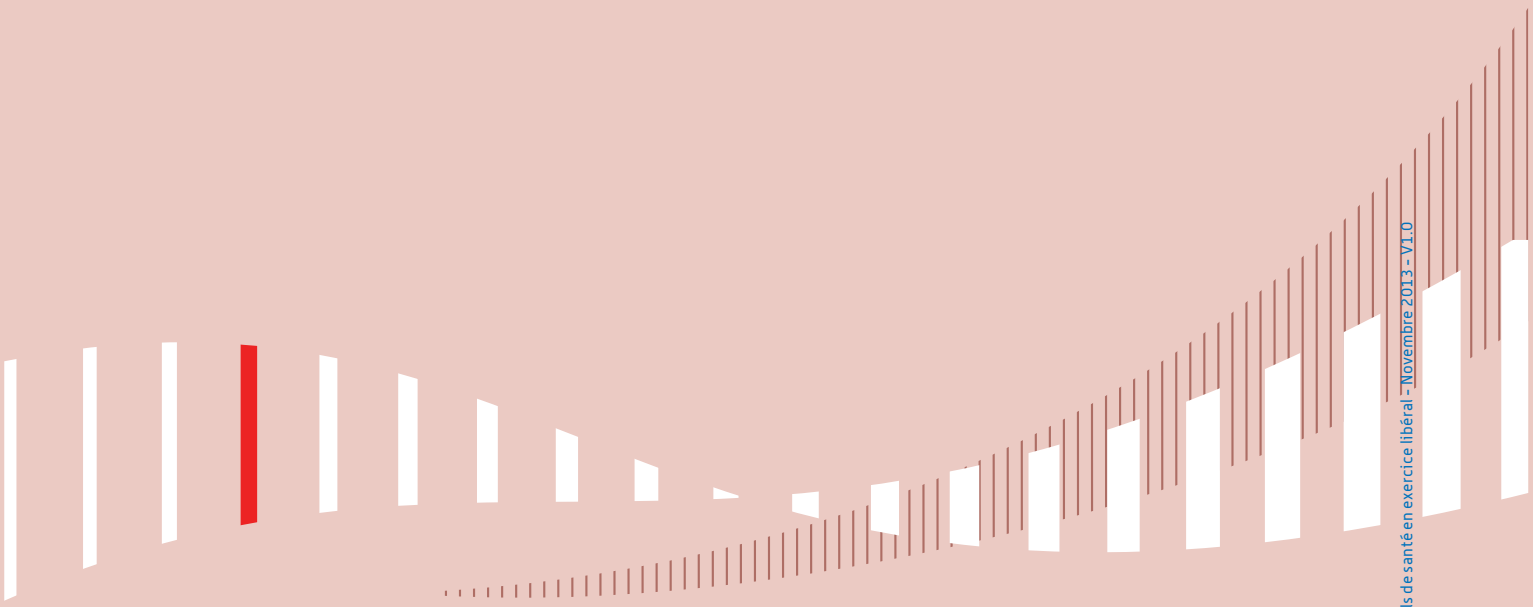
4.2. Annexe 2 – Glossaire

Sigle / Acronyme	Signification
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ASIP Santé	Agence des Systèmes d'Information Partagés de Santé
CD	Compact Disc
CNIL	Commission Nationale de l'Informatique et des Libertés
CPE	Carte de Personnel d'Etablissement
CPS	Carte de Professionnel de Santé
DMP	Dossier Médical Personnel
DP	Dossier Pharmaceutique
DVD	Digital Versatile Disc
EHPAD	Etablissement d'Hébergement pour Personnes Agées Dépendantes
GT	Groupe de Travail
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé
PIN	Personal Identification Number
PTS	Pôle Technique et Sécurité
PUK	PIN Unlock Key
USB	Universal Serial Bus
WPA2	Wi-Fi Protected Access

4.3. Annexe 3 – Documents de référence

Référence n° 1 : L'hygiène informatique en entreprise – Guide de l'ANSSI
Référence n° 2 : Guide des professionnels de santé publié par la CNIL
Référence n° 3 : Note ANSSI – Recommandations de sécurité relatives aux mots de passe
Référence n° 4 : Corpus documentaire constituant la PGSSI-S (référentiels et guides pratiques)

RÉFÉRENTIELS / PGSSI-S - Mémento de sécurité informatique pour les professionnels de santé en exercice libéral - Novembre 2013 - V1.0



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