Journée européenne de la

Protection des Données

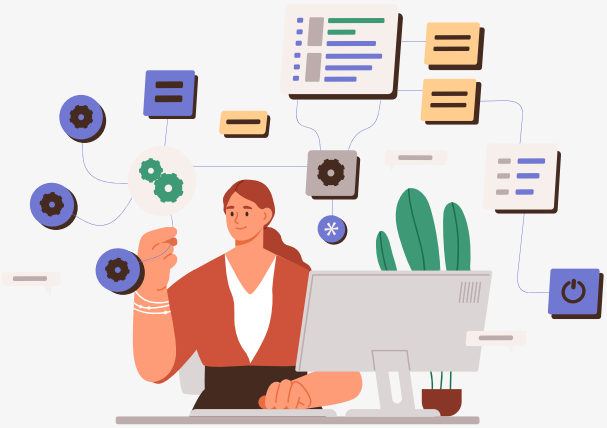
Cyberattaques, on parle de quoi ?

MES DONNÉES PARTAGÉES, EN SÉCURITÉ ?

Nos données de santé sont partagées à de nombreux endroits et pour différentes raisons

OÙ SONT MES DONNÉES “SÉCURISÉES” ?

- **Dans l’ordinateur de votre soignant, en ville ou à l’hôpital, pour vous soigner**
- **Dans les serveurs de l’Assurance maladie pour vous rembourser**
- **Dans Mon Espace Santé, le carnet de santé numérique pour vous et votre équipe de soins**
- **Dans les bases de données pour la recherche, qui rassemblent les données de remboursement et les dossiers médicaux**



TOUS SUR LA MÊME LONGUEUR D’ONDE ?

En parallèle de l’implication des acteurs publics dans le numérique en santé, une politique complète a été élaborée. L’Agence du Numérique en Santé pilote ainsi **la Politique générale de sécurité des systèmes d’information de santé (PGSSIS)**.

Cette politique s’enrichit continuellement de différents documents :

- des **référentiels dits “opposables”** et qui ont donc un caractère contraignant, obligatoire
- des **guides pratiques** pour accompagner les acteurs et sensibiliser chacun à la sécurité des données

Une partie de ces documents sont inscrits dans un cadre législatif ou réglementaire.

Différents domaines sont couverts par cette politique comme :

- **la bonne identification numérique du patient**, pour les bons soins au bon patient : réception de documents de santé, éviter les doublons ou les pertes d’information, etc.
- **la bonne identification numérique du professionnel de santé**, pour tracer les actions informatiques de chacun : envoi d’une ordonnance numérique, signature d’un document de santé, etc.

France Assos Santé
La voix des usagers

Journée européenne de la

Protection des Données

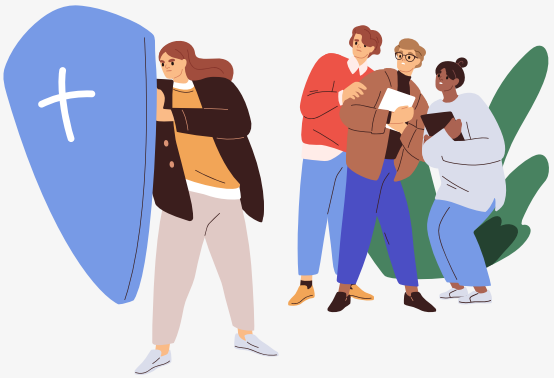
Cybersécurité, on parle de quoi ?

MES DONNÉES PARTAGÉES, EN SÉCURITÉ ?

Nos données de santé sont partagées à de nombreux endroits et pour différentes raisons

LE RISQUE ZÉRO EXISTE-T IL ?

- **Que ce soit sur l'ordinateur de votre médecin, sur le serveur d'une base de donnée à l'hôpital ou même sur votre téléphone portable, le risque zéro n'existe pas.**
- **Intrusion forcée, virus caché, erreur humaine, il existe de nombreuses façons de compromettre un appareil numérique et les données qu'il contient**



UNE SOLUTION POUR TOUS ?

Les données de santé étant des données personnelles de haute sensibilité, tous les acteurs amenés à manipuler des données de santé doivent recourir à des outils ou service sécurisés. La certification "Hébergeur Données de Santé" (HDS) a donc été créée et est imposée à l'ensemble de ces services.

Imposée par la loi, cette exigence prend la forme d'une certification, délivrée pour 3 ans et qui donne lieu chaque année à un audit de surveillance.

Les données de **"Mon Espace Santé"**, le **"Dossier Pharmaceutique"** par exemple ont recours à des services certifiés "Hébergeur Données de Santé". Mais c'est aussi le cas des sociétés de **téléconsultations**, ou pour les **objets connectés** quand les données sont partagées ou rassemblées à des fins diagnostiques ou d'études.

Cette certification concerne aussi bien les **infrastructures** techniques du réseau informatique, que la **formation** des employés ou encore les **procédures** en cas d'incidents de cybersécurité.

France Assos Santé
La voix des usagers

Journée européenne de la

Protection des Données

Cybersécurité, on parle de quoi ?

MES DONNÉES PARTAGÉES, EN SÉCURITÉ ?

Un certain nombre de règles encadrent la sécurité des données personnelles de santé d'un point de vue informatique

LA TÊTE DANS LES NUAGES ?

Vos données peuvent être hébergées en ligne dans le "cloud" ("informatique dans les nuages"), et non sur votre disque dur d'ordinateur ou celui de votre médecin.

Exemple : les données de votre boite mail sont stockées en ligne, dans le "cloud", vous pouvez les retrouver en vous connectant depuis un autre ordinateur.

AVIS DE TEMPÊTE SUR MES DONNÉES ?

Vos données sont alors **plus facilement partagées à vos différents professionnels**, pas besoin de clés usb ou d'envois par mail. Le "cloud" est donc utilisé par de nombreux services numérique à destination des professionnels de santé ou pour les chercheurs.

VISA DE SÉCURITÉ – AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION – ANSSI

L'agence nationale de la cybersécurité (ANSSI) propose depuis 2016 un référentiel, régulièrement mis à jour pour, pour établir des standards de sécurité techniques, juridiques et opérationnels pour les services de "cloud" informatique.

Baptisé **"Sec Num Cloud"**, il permet pour les solutions numériques qui satisfont à ses critères après un contrôle indépendant, d'afficher un **label de confiance** pour 3 ans pour les utilisateurs et acheteurs de solutions, dans les hôpitaux par exemple.

France Assos Santé
La voix des usagers

Journée européenne de la

Protection des Données

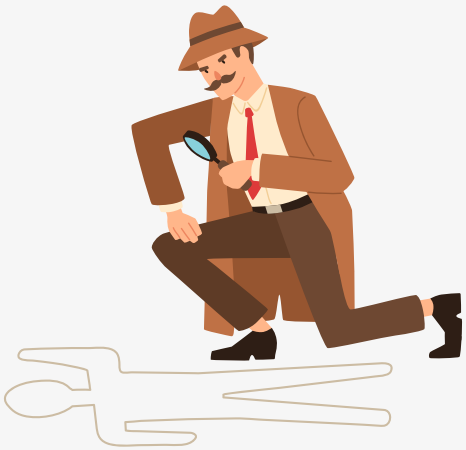
Cybersécurité, on parle de quoi ?

MES DONNÉES PARTAGÉES, EN SÉCURITÉ ?

Anonymes, pseudonymisées, identifiantes, toutes mes données font-elles l'objet de toutes les attentions ?

MES DONNÉES, TOUTES CONVOITÉES ?

- **Des bases de données qui réunissent collectivement des données de santé (remboursements, dossiers médicaux, etc.) existent et peuvent être utilisées pour l'intérêt public, c'est à dire pour la recherche scientifique, l'innovation ou le pilotage du système de santé.**
- **Les données de santé sont alors protégées par des normes techniques de cybersécurité, mais aussi par un regard éthique et juridique particulier pour les protéger.**



QUID DES DONNÉES NON IDENTIFIANTES ?

Une fois réunies, ces données sont délestées de l'identité des personnes, elles sont dites **"non-identifiantes"**. Elle peuvent être complétement "anonymes", ou bien "pseudonymisées". L'intérêt pour la recherche de ces données, n'est pas l'identité des personnes, mais les leçons à tirer de l'ensemble.

Contrairement aux données utilisées pour vous soigner, les données utilisées pour la recherche ne comportent donc **pas d'informations directes concernant votre identité** (nom, prénom, numéro de sécurité sociale, etc.) ou votre contact (téléphone, adresse, mail, etc.).

Or, les cyberpirates **utilisent des données personnelles** pour mener des actes malveillants, à partir des données d'identité et de contact (hameçonnage, usurpation d'identité, etc.).

Tenter de pirater une base de données pour la recherche n'est donc pas très rentable. Il faut **dépenser beaucoup d'énergie** pour essayer de retrouver l'identité d'une personne, quand cela est théoriquement possible. Sans information de contact, **les données obtenues ne sont pas réellement utilisables** pour réaliser les actes malveillants classiques.

France Assos Santé
La voix des usagers