RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

l'Assurance Maladie
Agir ensemble, protéger chacun

RGPD

WEBINAIRE DE SENSIBILISATION À DESTINATION DES CPTS

5 mars 2024

sesan Groupement d'Intérêt Public eSanté

FCPTS Fédération Nationale

SOMMAIRE

LES RÈGLES JURIDIQUES RELATIVES AU RGPD

LES MESURES DE SÉCURITÉ POUR PROTÉGER LES DONNÉES

LES OUTILS NUMÉRIQUES POUR LA SÉCURITÉ DES ÉCHANGES

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

l'Assurance Maladie
Agir ensemble, protéger chacun

sesan
Groupement d'Intérêt Public eSanté

FCPTS
Fédération Nationale

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

Agence Régionale de Santé Île-de-France

Session de formation
Protection des données personnelles

CPTS
5 mars 2024

Ordre du jour

- De quoi parle-t-on concrètement ?
- Les grands principes de la protection des données personnelles
- Le RGPD appliqué aux CPTS
- Temps d’échange : questions/réponses

1. De quoi parle-t-on concrètement ?

1. De quoi parle-t-on concrètement ?

Qu’est-ce que le RGPD ?

= Règlement Général sur la Protection des Données (ou en anglais GDPR, Général Data Protection Régulation)

=> **une réglementation européenne, entrée en vigueur le 25/05/2018** qui fixe les modalités applicables aux traitements de données à caractère personnel sur tout le territoire de l’Union Européenne de manière homogène.

En droit interne, la Loi informatique et libertés est applicable depuis déjà 40 ans !

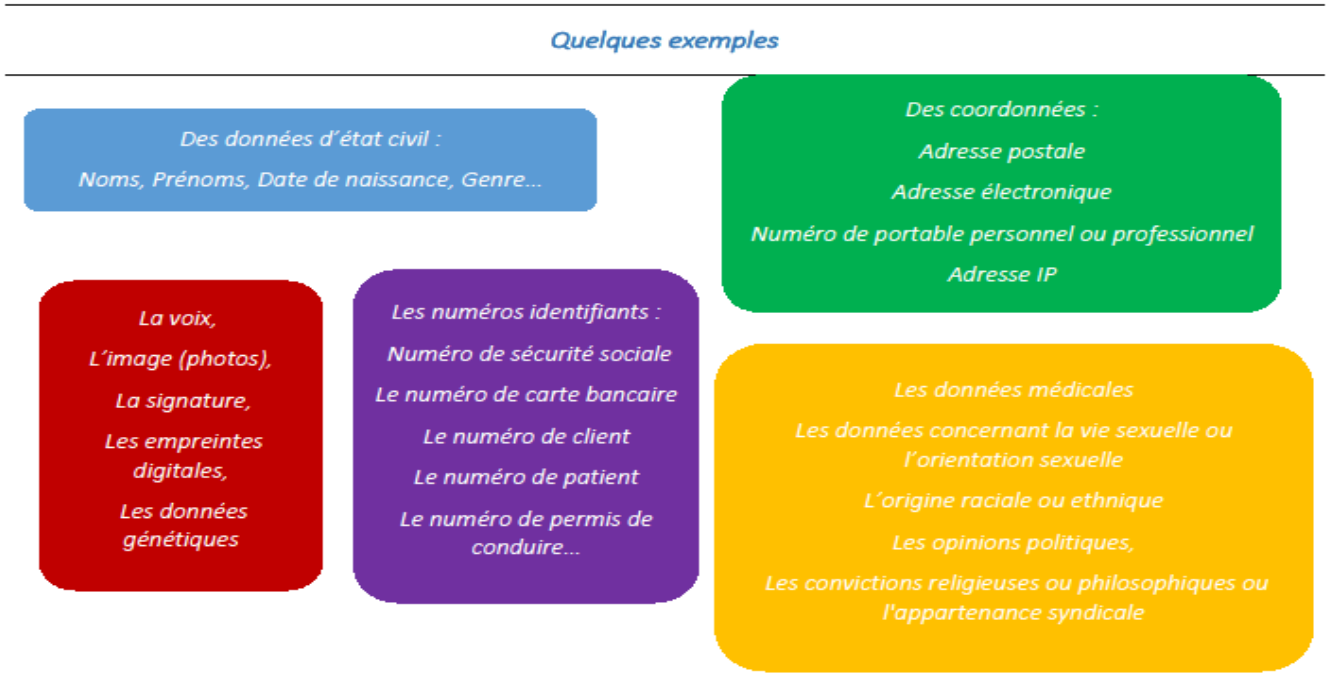
Elle a fait l’objet de plusieurs modifications récemment pour intégrer les évolutions du RGPD.

1. De quoi parle-t-on concrètement ?

Qu’est-ce qu’une donnée personnelle ?

= « *toute information se rapportant à une **personne physique** identifiée ou identifiable* »

=> Est réputée être une «*personne physique identifiable*» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale » (article 4 du RGPD).



1. De quoi parle-t-on concrètement ?

Qu’est-ce qu’une donnée personnelle ?

∆ *A la donnée prétendument anonyme qui échappe à l’application du RGPD*

On ne peut affirmer que des données sont anonymes que lorsque la ré-identification des personnes concernées **est impossible par quelque moyen que ce soit et de manière irréversible**.

L’anonymisation requiert l’utilisation de techniques particulières décrites dans l’avis du 10/04/2014 G29 (actuel Comité européen de la protection des données CEPD).

Généralement, les traitements mis en œuvre par l’Agence sont pseudonymisés c’est-à-dire qu’il est possible de ré-identifier les personnes concernées en ayant recours à des informations complémentaires. **Le RGPD s’applique aux données pseudonymisées**.

1. De quoi parle-t-on concrètement ?

Qu’est-ce qu’une donnée personnelle sensible ?

= une donnée personnelle **dont l’utilisation est en principe interdite** et qui porte sur / ou révèle :

- l’origine raciale ou ethnique,
- les opinions politiques,
- les convictions religieuses ou philosophiques,
- l’appartenance syndicale,
- les données génétiques,
- les données biométriques,
- les **données de santé**,
- les données concernant la vie sexuelle ou l'orientation sexuelle d’une personne physique.

Il s’agit également des données relatives aux **condamnations pénales, infractions** et mesures de sûreté connexes qui font l’objet d’un encadrement particulier tout comme le **numéro de sécurité sociale** ou NIR, son utilisation étant encadrée par un texte spécifique.

1. De quoi parle-t-on concrètement ?

Qu’est ce qu’une donnée personnelle de santé ?

= **L'ensemble des données se rapportant à l'état de santé d'une personne physique qui révèle des informations sur son état de santé** physique ou mentale passé, présent ou futur.

*« les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique**, y compris la prestation de services de soins de santé**, qui révèlent des informations sur l'état de santé de cette personne; »* Article 4 du RGPD

Cela comprend *« un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé; des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques; et toute information concernant, par exemple, une **maladie, un handicap**, un risque de maladie, les **antécédents médicaux, un traitement** clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro. »* considérant 35 du RGPD

1. De quoi parle-t-on concrètement ?

Quelques exemples de données de santé

« l'information relative à la résidence en établissement de personnes âgées dépendantes, la nature des actes et médicaments ou produits de santé et leurs codages détaillés, ***l'existence d'une grossesse ou d'une affection de longue durée*** *et les éléments du protocole relatif à cette affection, les informations relatives à l'appareillage, à une cure thermale ou à une prestation soumise à accord préalable,* ***l'existence d'une hospitalisation, ses dates le numéro d'établissement****, la discipline médico-tarifaire et le groupe homogène de séjour, le descriptif médical, les résultats des examens complémentaires et les traitements en cours en rapport avec une pathologie à l'origine d'une demande de prestation) » Délibération de la CNIL n° 2014-430 du 23 octobre 2014 portant avis sur un projet de décret en Conseil d'Etat autorisant les traitements de données à caractère personnel mis en œuvre par les organismes gestionnaires des régimes obligatoires de base de l'assurance maladie pour l'accomplissement des missions de leurs services médicaux (demande d'avis n° 14021842)*

1. De quoi parle-t-on concrètement ?

Quelques exemples de données de santé

*« le poids, la taille, les antécédents médicaux, les diagnostics médicaux, la thérapie suivie, les traitements prescrits, la **nature des actes effectués**, les résultats d'examens, des renseignements d'ordre biologique, physiologique et pathologique propres à influencer la réaction du patient à sa prise en charge médicale et tout élément de nature à caractériser la santé du patient et considéré comme pertinent par le professionnel de santé) » extrait du Référentiel relatif aux traitement de données personnelles pour les cabinets médicaux et paramédicaux*

1. De quoi parle-t-on concrètement ?

Qu’est-ce qu’un traitement de données ?

= « *toute opération ou tout ensemble d'opérations effectuées* ***ou non*** *à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel* » (article 4 RGPD)

Δ Le RGPD s’applique au traitement de données automatisés mais aussi « papier ».

Au sens large = **tout acte qui porte sur des DP**

1. De quoi parle-t-on concrètement ?

Qu’est-ce qu’un traitement de données ?

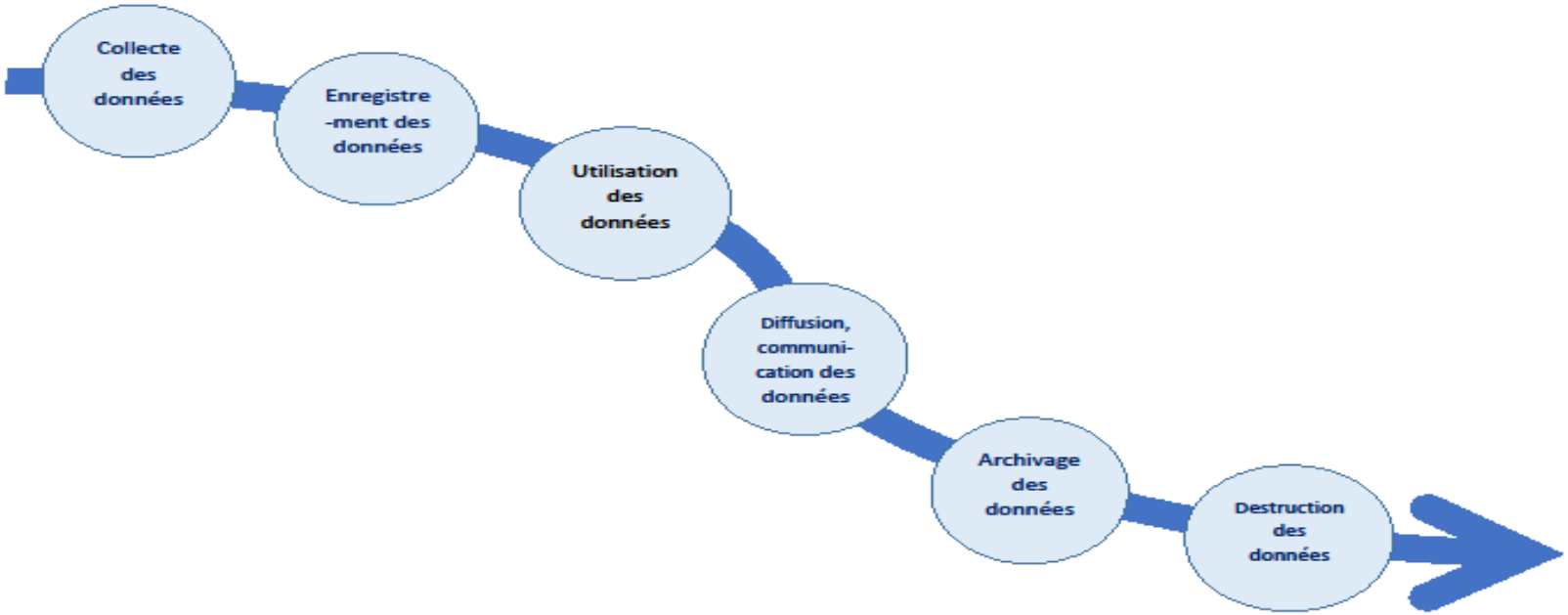
Quelques exemples :

collecte de DP, enregistrement de DP dans un fichier, extraction de DP, consultation de DP, communication de DP par transmission, diffusion de DP, rapprochement ou interconnexion de DP, effacement ou destruction de DP et plus concrètement, le fait de tenir un fichier Excel avec des DP, de collecter des DP via un questionnaire, d’adresser un mail d’invitation à plusieurs personnes physiques, de prendre en photo des personnes, de communiquer / diffuser une liste de DP…

1. De quoi parle-t-on concrètement ?

Qu’est-ce qu’un traitement de données ?

Dans la pratique, un traitement de données comprend plusieurs opérations de traitement :



1. De quoi parle-t-on concrètement ?

Qu’est-ce qu’un responsable de traitement ?

= « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* » (article 4 RGPD)

Plus exactement = la ou les personnes qui déterminent les finalités et les éléments essentiels des moyens du traitement (type de données collectées, nom des destinataires des données, durée de conservation…), les moyens techniques et organisationnels pouvant être délégués.

Le RGPD rend possible la responsabilité conjointe d’un TD (partage de responsabilités dorénavant possible)

☞ Pour les personnes morales, le RT = son représentant légal

1. De quoi parle-t-on concrètement ?

Qu’est-ce qu’un registre des activités de traitement de données personnelles ?

Le registre des activités de traitement permet de recenser toutes les activités de traitement de données mises en œuvre par une structure/organisation/un responsable de traitement.

Concrètement = la liste de tous les traitements de données mis en œuvre par une structure.

Il est prévu par l’article 30 du RGPD.

1. De quoi parle-t-on concrètement ?

Qu’est-ce qu’un registre des traitements ?

D’après l’article 30 du RGPD, le registre doit comporter toutes les informations suivantes **pour chaque activité de traitement** :

- le nom et les coordonnées du responsable du traitement avec le nom de son représentant légal
- Le nom et les coordonnées du délégué à la protection des données s’il existe
- les finalités/objectifs du traitement (à quoi il sert et pourquoi il est mis en œuvre)
- les catégories de personnes concernées
- les catégories de données à caractère personnel traitées;
- les catégories des destinataires auxquels les données à caractère personnel ont été ou seront communiquées,
- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale avec identification de ce pays tiers ou de l’organisation internationale avec les documents attestant de l'existence de garanties appropriées;
- dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.

1. De quoi parle-t-on concrètement ?

Qu’est-ce qu’un Délégué à la Protection des Données personnelles (DPD) ou DPO (Data Protection Officer) ?

= la personne responsable de la protection des données personnelles traitées au sein d’un organisme/une structure.

La fonction de DPD/DPO est réglementée et définie avec précision dans les articles 37 à 39 du RGPD.

Le DPO a un rôle de **conseil, d’accompagnement et d’information** : il apporte son expertise auprès de la direction afin que celle-ci puisse assurer la conformité des traitements et diffuse la culture et les règles de la protection des données auprès de toutes les personnes qui traitent des données personnelles au sein de son organisme. Il a également une **mission de contrôle** du respect du RGPD (audit).

Le DPO est enfin le **point de contact/l’interlocuteur privilégié de la CNIL et des personnes concernées** par les traitements de données personnelles mis en œuvre par la structure.

2. Les grands principes de la protection des données personnelles

2. Les grands principes de la protection des données personnelles

1- Le principe de licéité

Pour le RGPD, un **TD n'est licite** que dans 6 hypothèses :

①la personne concernée **a consenti** au traitement,

②le TD est nécessaire à **l'exécution d'un contrat** auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles,

③Le TD est nécessaire au respect d'une **obligation légale** à laquelle le RT est soumis;

④le TD est nécessaire à la **sauvegarde des intérêts vitaux** de la personne concernée ou d'une autre personne physique;

⑤ le TD est nécessaire à l'exécution d'une **mission d'intérêt public** ou relevant de l'exercice de l'autorité publique dont est investi le RT;

⑥ le TD est nécessaire aux fins des **intérêts légitimes** poursuivis par le RT ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

2. Les grands principes de la protection des données personnelles

2- Principe de limitation des finalités

Les **finalités du traitement doivent être déterminées, explicites et légitimes**.

Les données collectées pour un traitement ne doivent pas être ultérieurement traitées pour d'autres finalités.

▲ aux détournements de finalités : le fait, par toute personne détentrice de DP à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende (article 226-21 du code pénal).

2. Les grands principes de la protection des données personnelles

3- Principe de minimisation et d'exactitude des données

Les DP collectées doivent être **adéquates, pertinentes et limitées** à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

☞ **Limiter le traitement aux seules DP indispensables**. Par exemple, ne pas collecter la date de naissance complète si l'année de naissance (âge) de la personne concernée peut suffire.

Elles doivent également être **exactes et, si nécessaire, tenues à jour.**

2. Les grands principes de la protection des données personnelles

4- Principe de limitation de la durée de conservation des données

Les DP ne peuvent être conservées que pendant **une durée limitée et définie en amont** en fonction de la finalité du traitement.

La durée d'un TD peut être prévue par **un texte** (par exemple pour les traitements mis en œuvre dans le cadre de la gestion de la paie la durée de conservation des DP est fixée à 5 ans par l'article L 3243-4 du code du travail) et peut ne pas être définie en mois ou année mais correspondre à la période du traitement, par exemple, le temps de la collaboration professionnelle.

Pour plus d'informations : https://www.cnil.fr/fr/passer-laction/les-durees-de-conservation-des-donnees

Et notamment les référentiels suivants :

Référentiel des durées de conservation dans le domaine de la santé hors recherche

Référentiel des durées de conservation dans le domaine de la recherche en santé

Référentiel durées de conservation social et médico-social

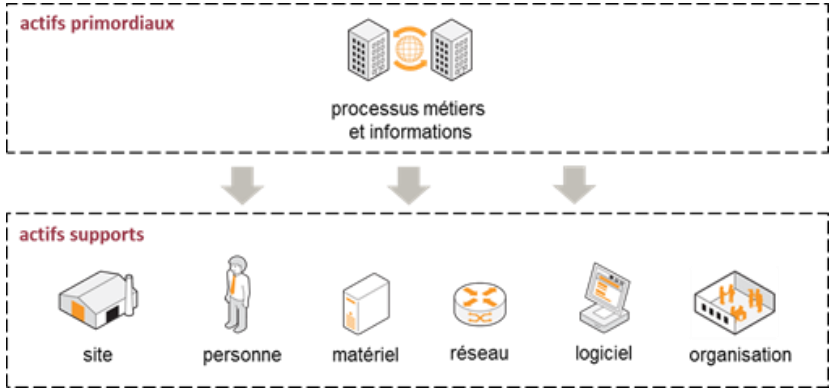
2. Les grands principes de la protection des données personnelles

5- Principe de sécurité : disponibilité, intégrité, confidentialité

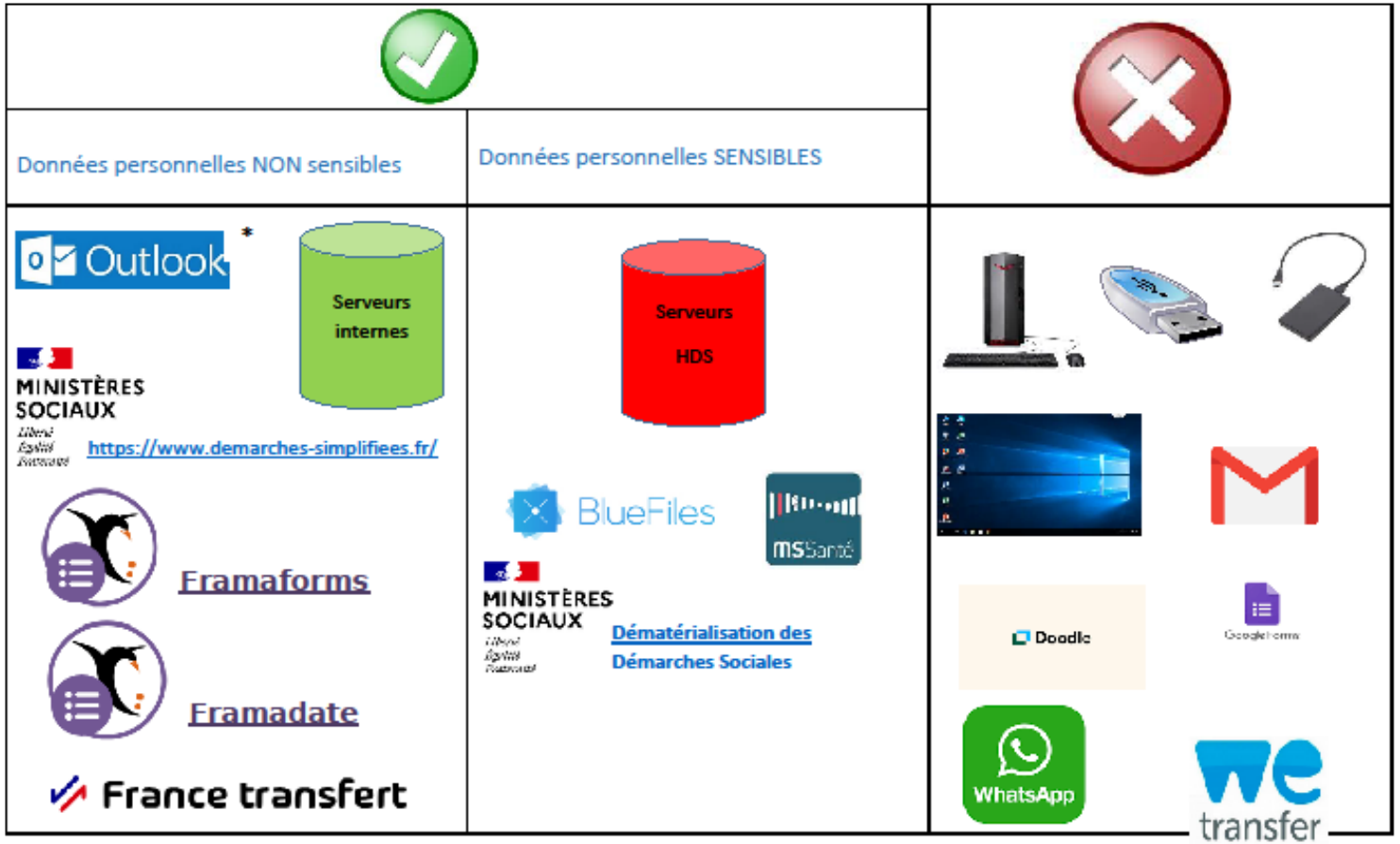
Article 5 et 32 du RGPD :

- Les données doivent être traitées de façon à **garantir la sécurité des données à caractère personnel traitées à l'aide de mesures techniques ou organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ainsi qu'au type de donnée traitée.**

  - **Le RT doit garantir la sécurité des systèmes d'information de l'agence** c'est-à-dire de l'ensemble des moyens humains et matériels (techniques et organisationnels) permettant à l'agence de fonctionner et donc de collecter, traiter, conserver, échanger/partager et diffuser des informations en interne et à l'externe.



2. Les grands principes de la protection des données personnelles



* Pour la CNIL, « Sans mesure complémentaire, les canaux de transmission de données grand public (ex. : messagerie électronique, messagerie instantanée, plateforme de dépôt de fichiers) constituent rarement un moyen de communication sûr pour transmettre des données personnelles » : https://www.cnil.fr/fr/securite-securiser-les-echanges-avec-dautres-organismes

2. Les grands principes de la protection des données personnelles

5- Principe de sécurité : disponibilité, intégrité, confidentialité

Article 5 et 32 du RGPD :

- **Sécurité « physique » :**
  - Accès aux locaux uniquement par badges;
  - En votre absence, ne pas laisser sur les espaces de travail des documents « papier » contenant des données personnelles et a fortiori des données sensibles => prévoir des armoires ou tiroirs fermés à clefs;
  - Prévoir des poubelles dédiées à la destruction de documents « papier » contenant des données personnelles ou des broyeurs

2. Les grands principes de la protection des données personnelles

5- Principe de sécurité : disponibilité, intégrité, confidentialité

Article 5 et 32 du RGPD :

Les données doivent être traitées de façon à garantir également la confidentialité des données à caractère personnel.

- seules les personnes autorisées à obtenir communication de données enregistrées dans un fichier ou un traitement en raison de leurs fonctions peuvent accéder aux données.
- Il faut donc déterminer quelles vont être les personnes autorisées/les destinataires des données **et s'assurer que seuls ces destinataires y auront accès.**

2. Les grands principes de la protection des données personnelles

5- Principe de sécurité : disponibilité, intégrité, confidentialité

Article 5 et 32 du RGPD :

Le principe de sécurité et de confidentialité impose enfin au responsable de traitement d'encadrer ses relations contractuelles avec ses sous-traitants en insérant dans les conventions (contrat d'achat, marchés publics…) des clauses relatives à la protection des données conformes à l'article 28 du RGPD.

2. Les grands principes de la protection des données personnelles

6- Principe de transparence

Les données personnelles doivent être traitées de **manière loyale et transparente** :

- Obligation d'information à la charge du RT dès la collecte des DP **portant sur les caractéristiques du TD** mis en œuvre (information complète, accessible et adaptée à chacun portant sur l'identité du RT, la finalité poursuivie, base juridique du TD, destinataires des données, durée de conservation…)

- Respect des droits des personnes dont les données sont traitées (droit d'accès aux données, droit de rectification, droit d'opposition, droit à l'effacement + nouveaux droits issus du RGPD droit à la limitation du traitement (gel temporaire des données), droit à la portabilité des données (récupération des données et transmission à un autre RT), droit de ne pas faire l'objet d'une décision individuelle exclusivement fondée sur un traitement automatisé (profilage).

3. Le RGPD appliqué aux CPTS

3. Le RGPD appliqué aux CPTS

1. Les CPTS doivent-elles désigner un DPO/DPD ?

- Selon l'article 37 du RGPD, la désignation d'un DPD est obligatoire pour :
  - les autorités ou les organismes publics,
  - Toutes les structures dont les activités principales les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle ;
  - Toutes les structures dont les activités de base les amènent à traiter à grande échelle des données sensibles (donc de santé) ou relatives à des condamnations pénales et infractions.

Problème : le RGPD ne définit pas la notion de grande échelle…

Les textes européens ne donnent pas d'informations précises sur le nombre ou la nature de données traitées, sur la zone géographique que doit concerner le fichier ou sur la durée de conservation des données. **Pour la CNIL, il revient à chaque responsable du traitement de décider de la qualification de son traitement de "traitement à grande échelle".**

3. Le RGPD appliqué aux CPTS

1. Les CPTS doivent-elles désigner un DPO/DPD ?

Le considérant 91 du RGPD donne quelques précisions sur la notion de « grande échelle »

Il s'agit des traitements qui visent à traiter *« un **volume considérable de données personnelles** au niveau régional, national ou supranational, qui peuvent affecter un nombre important de personnes concernées et qui sont susceptibles d'engendrer un risque élevé »*

Exemples de "traitements à grande échelle"	Exemples de traitements ne constituant pas un "traitement à grande échelle"
- Traitement des données de patients par un hôpital dans le cadre du déroulement normal de ses activités. (cf. guide DPO de la CNIL) : https://www.cnil.fr/sites/cnil/files/atoms/files/guide_pratique_rgpd_-_deleques_a_la_protection_des_donnees.pdf - La CNIL estime que la désignation d'un DPO devrait être nécessaire pour les professionnels de santé qui, exerçant **en cabinet groupé, partagent un système d'information commun, à partir d'un seuil annuel de 10 000 patients** (cf. le référentiel de la CNIL pour les cabinets médicaux et paramédicaux : https://www.cnil.fr/sites/cnil/files/atoms/files/referentiel_-_cabinet.pdf	- Traitement, par un médecin exerçant à titre individuel, des données de ses patients (considérant 91 du RGPD)

3. Le RGPD appliqué aux CPTS

1. Les CPTS doivent-elles désigner un DPO/DPD ?

En dehors des trois cas précités, la **désignation d'un DPO est fortement recommandée** par la CNIL et le CEPD. Cela permet de confier à un expert l'identification et la coordination des actions à mener en matière de protection des données personnelles et c'est toujours valorisant en termes d'image pour la structure et encore plus si ladite structure traite au quotidien des données sensibles,

Les organismes peuvent désigner un **DPO en interne ou externe à leur structure (sous-traitant) et sous certaines conditions, le DPO peut être mutualisé.**

3. Le RGPD appliqué aux CPTS

2. Les CPTS ont-elles l'obligation de tenir un registre des traitements de données ?

Article 30 du RGPD : « *Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité.* »

- L'obligation de tenir un registre des traitements **concerne tous les organismes, publics comme privés et quelle que soit leur taille,** dès lors qu'ils traitent des données personnelles.

MAIS il existe des exceptions : les dispositions de l'article 30 du RGPD *« **ne s'appliquent pas à une entreprise ou à une organisation comptant moins de 250 employés**,*

sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et des libertés des personnes concernées,

s'il n'est pas occasionnel ou

s'il porte notamment sur les catégories particulières de données visées à l'article 9, paragraphe 1, ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10. »

3. Le RGPD appliqué aux CPTS

2. Les CPTS ont-elles l'obligation de tenir un registre des traitements de données ?

Les CPTS ont peu d'employés ou elles en ont moins de 250 le plus souvent **MAIS** elles mettent potentiellement en œuvre des traitements de données qui ne sont pas occasionnels :

Ex :

- Echanges réguliers avec des interlocuteurs identifiés par mail ou téléphone,
- Animent des réunions avec des interlocuteurs identifiés
- Gestion et paiement des salaires de ses employés
- Signent des conventions avec des partenaires identifiés, procèdent à des achats…

Ou qui portent sur des données de santé (ex. les CPTS trouvent des médecins traitants pour des patients qui n'en ont pas et priorisent en fonction de la situation des patients)

➢ **Le registre est obligatoire**

3. Le RGPD appliqué aux CPTS

FOCUS les missions des CPTS et les catégories de données potentiellement traitées

1/ **Mission concernant les patients sans médecin traitant** : *« une procédure de recensement des patients à la recherche d'un médecin traitant, **d'analyse de leur niveau de priorité au regard de leur situation de santé** et mettre en œuvre une organisation pour leur proposer un médecin traitant parmi les médecins de la communauté. » (cf. l'accord conventionnel interprofessionnel en faveur du développement de l'exercice coordonné et du déploiement des CPTS (ACI*

2/ **Mission concernant les SNP** *: les CTPS doivent « proposer **une organisation** visant à permettre la prise en charge le jour même ou dans les 24 heures de la demande d'un patient du territoire en situation d'urgence non vitale » et « définir des solutions d'organisation à mettre en place en fonction des besoins identifiés lors du diagnostic territorial ». « Le recours à un outil numérique ou relevant d'une autre forme de régulation, permettant notamment **le partage d'agenda, l'orientation des patients et le partage d'information sur la prise en charge facilite la réalisation de la mission**. En outre, les communautés professionnelles ont la possibilité de mettre en place un **dispositif de traitement et d'orientation des demandes de soins non programmés.** Celui-ci doit comprendre a minima une orientation téléphonique par un personnel formé pour apprécier si la demande relève bien des soins non programmés, la prioriser par rapport aux autres demandes et mettre en contact le patient avec le professionnel de santé disponible et le plus proche. Cette organisation peut être mutualisée entre plusieurs communautés professionnelles. Dans le cas où une telle organisation est mise en place, la communauté professionnelle reçoit un financement dédié spécifiquement à cette mission (cf. article 8 de l'accord) »*

3. Le RGPD appliqué aux CPTS

FOCUS les missions des CPTS et les catégories de données potentiellement traitées

3/ **développer le recours à la télémédecine** en constituant « *un cadre particulièrement porteur pour favoriser le développement des téléconsultations dans le respect du parcours de soins*. »

4/ **permettre l'organisation des parcours des patients** en vue d'assurer une meilleure coordination entre les acteurs, d'éviter les ruptures de parcours et de favoriser autant que possible le maintien à domicile des patients, via **une gestion coordonnée renforcée entre tous les acteurs de santé intervenant autour du même patient (mise en place d'annuaires des acteurs de santé, réunions pluriprofessionnelles régulières, outils de partage autour des patients, etc.).**

5**/ Promotion des actions de préventions**

⇒ Tous les éléments ci-dessus sont issues de :

- ⇒ Articles L 1434-12-2 et suivants et D1434-44du CSP
- ⇒ Instruction n° DGOS/DIR/CNAM/2019/218 du 9 octobre 2019 portant dispositions et modalités d'accompagnement à proposer aux porteurs de projets des communautés professionnelles territoriales de santé
- ⇒ Extraits de l'accord conventionnel interprofessionnel en faveur du développement de l'exercice coordonné et du déploiement des CPTS (ACI)
- ⇒ Ou du site https://www.ameli.fr/val-d-oise/exercice-coordonne/actualites/communautes-professionnelles-territoriales-de-sante-decryptage-de-l-accord-signe-et-des-2-avenants

CERTAINES DES MISSIONS PRÉCITÉES IMPLIQUENT NÉCESSAIREMENT LE TRAITEMENT DE DONNÉES DE SANTÉ DES PATIENTS PAR LES CPTS (RECHERCHE DE MT EN PRIORISANT SELON L'ÉTAT DE SANTÉ). => LES CPTS TRAITENT DONC NÉCESSAIREMENT DES DONNÉES DE SANTÉ DE PATIENTS

3. Le RGPD appliqué aux CPTS

FOCUS le principe de confidentialité et le secret médical

- Rappel : Article 5 et 32 du RGPD : Les données doivent être traitées de façon à garantir également la confidentialité des données à caractère personnel et seules les personnes autorisées à obtenir communication de données enregistrées dans un fichier ou un traitement en raison de leurs fonctions peuvent accéder aux données.

- En parallèle, il existe des dispositions dans le CSP qui instaurent en principe l'obligation de respecter le secret médical :

Alinéa 1 de l'article L1110-4 du CSP « *I.-**Toute personne prise en charge par** un professionnel de santé, un établissement ou service, un professionnel ou **organisme concourant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le présent code**, le service de santé des armées, un professionnel du secteur médico-social ou social ou un établissement ou service social et médico-social mentionné au I de l'article L. 312-1 du code de l'action sociale et des familles **a droit au respect de sa vie privée et du secret des informations la concernant. »***

3. Le RGPD appliqué aux CPTS

FOCUS le principe de confidentialité et le secret médical

Mais des exceptions sont possibles dès lors qu'elles sont prévues expressément par un texte (Certificats d'état civil, MDO, Soins psychiatriques sans consentement…) :

Alinéa 2 de l'article L1110-4 du CSP « ***Excepté dans les cas de dérogation expressément prévus par la loi****, ce secret couvre l'ensemble des informations concernant la personne venues à la connaissance du professionnel, de tout membre du personnel de ces établissements, services ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes. Il s'impose à tous les professionnels intervenant dans le système de santé… »*

3. Le RGPD appliqué aux CPTS

FOCUS le principe de confidentialité et le secret médical

Parmi les nombreuses exceptions prévues par les textes, figure le **SECRET MÉDICAL PARTAGÉ entre professionnels visé aux aliénas suivants de l'article L1110-4 précité.**

Ce secret médical partagé peut se matérialiser par :

- **un échange d'informations** : l'échange de documents comportant des données de santé consiste dans un flux de données visant à communiquer des données de santé à un (des) destinataire(s) clairement identifié(s) - Exemple: envoi d'un mail par messagerie sécurisée de santé, envoi par fax, appel téléphonique.
- **un partage d'informations** : le partage vise à mettre à la disposition de plusieurs professionnels fondés à les connaître, des données de santé utiles à la coordination et à la continuité des soins, dans l'intérêt de la personne prise en charge –

Exemple: informations disponibles dans le Dossier Pharmaceutique, Dossier Médical Partagé, ou les dossiers de réseaux de santé.

Il est par ailleurs rendu possible que SI TROIS CONDITIONS CUMULATIVES SONT REMPLIES.

3. Le RGPD appliqué aux CPTS

FOCUS le principe de confidentialité et le secret médical

Une première condition, qui en réalité est une double condition, **tient à la catégorie de professionnel concerné** souhaitant échanger ou partager des informations médicales :

- Article R1110-2 CSP « ***Les professionnels susceptibles d'échanger ou de partager des informations relatives à la même personne prise en charge <u>APPARTIENNENT AUX DEUX CATÉGORIES SUIVANTES</u> :***

1° Les professionnels de santé mentionnés à la quatrième partie du présent code, quel que soit leur mode d'exercice (Médecins, Chirurgiens-dentistes, Sages-Femmes, Pharmaciens, Préparateurs en pharmacie et préparateurs en pharmacie hospitalière, Physicien médical, Infirmiers, Masseur- kinésithérapeute, Pédicure-podologue, Ergothérapeute, Psychomotricien, Orthophoniste, Orthoptiste, Manipulateur d'électroradiologie, Technicien de laboratoire médical, Opticien-lunetier, Audioprothésiste, Prothésiste et orthésiste pour l'appareillage des personnes handicapées, Diététicien, Aides-soignants**)**

*2° **Les professionnels relevant des sous-catégories suivantes** :*

a) Assistants de service social mentionnés à l'article L. 411-1 du code de l'action sociale et des familles;

b) Ostéopathes, chiropracteurs, psychologues et psychothérapeutes non professionnels de santé par ailleurs, aides médico-psychologiques et accompagnants éducatifs et sociaux ;

c) Assistants maternels et assistants familiaux mentionnés au titre II du livre IV du code de l'action sociale et des familles;

d) Educateurs et aides familiaux, personnels pédagogiques occasionnels des accueils collectifs de mineurs, permanents des lieux de vie mentionnés au titre III du livre IV du même code ;

3. Le RGPD appliqué aux CPTS

FOCUS le principe de confidentialité et le secret médical

e) Particuliers accueillant des personnes âgées ou handicapées mentionnés au titre IV du livre IV du même code ;

f) Mandataires judiciaires à la protection des majeurs et délégués aux prestations familiales mentionnés au titre VII du livre IV du même code ;

g) Non-professionnels de santé salariés des établissements et services et lieux de vie et d'accueil mentionnés aux articles L. 312-1, L. 321-1 et L. 322-1 du même code, ou y exerçant à titre libéral en vertu d'une convention; h) (Abrogé) ;

i) Non-professionnels de santé membres de l'équipe médico-sociale compétente pour l'instruction des demandes d'allocation personnalisée d'autonomie mentionnée aux articles L. 232-3 et L. 232-6 du même code, ou contribuant à cette instruction en vertu d'une convention.

j) Personnels des dispositifs d'appui à la coordination des parcours de santé complexes mentionnés à l'article L. 6327-1, des dispositifs spécifiques régionaux mentionnés à l'article L. 6327-6 et des dispositifs d'appui mentionnés au II de l'article 23 de la loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé intervenant dans le cadre de leur mission de coordination du parcours de santé de la personne concernée et spécialement habilités par les représentants légaux de ces dispositifs ;

k) Etudiants en troisième cycle mentionnés aux articles R. 6153-1, R. 6153-2 et R. 6153-93 du présent code.

⇒ **Tout échange ou partage d'informations entre un professionnel appartenant à l'une des deux catégories et un professionnel n'appartenant pas à l'une de ces deux catégories est exclu et donc potentiellement constitutif d'une violation du secret médical.**

➢ **Les professionnels susceptibles d'échanger ou de partager des informations relatives à la même personne DOIVENT EN OUTRE NÉCESSAIREMENT PARTICIPER À SA PRISE EN CHARGE.**

3. Le RGPD appliqué aux CPTS

FOCUS le principe de confidentialité et le secret médical

➢ **La seconde condition cumulative tient <u>AUX FINALITÉS DE L'ÉCHANGE OU DU PARTAGE DE DONNÉES MÉDICALES</u>** : l'échange et le partage d'informations ne peuvent porter que sur des informations *strictement* ***nécessaires à :***

- ***la coordination des soins;***
- ***la continuité des soins,***
- ***la prévention***
- ***au suivi médico-social de la personne,***

➢**La 3ème et dernière condition cumulative tient à la nature des informations échangées ou partagées :** L'échange et le partage de données entre professionnels ne peuvent porter que **<u>SUR DES INFORMATIONS RELEVANT DU PÉRIMÈTRE DE LEURS MISSIONS.</u>**

3. Le RGPD appliqué aux CPTS

FOCUS le principe de confidentialité et le secret médical

Si les trois conditions précitées sont remplies alors l'échange ou le partage de données médicales peut avoir lieu **SOUS RÉSERVE DE RESPECTER LES OBLIGATIONS SUIVANTES qui vont varier selon que le professionnel souhaite échanger ou partager des données médicales :**

1 / Dans le cas d'un échange de données => simple obligation d'information : *« I. — Le professionnel […] souhaitant échanger des informations relatives à une personne prise en charge […] informe préalablement la personne concernée, d'une part, de la nature des informations devant faire l'objet de l'échange, d'autre part, soit de l'identité du destinataire et de la catégorie dont il relève, soit de sa qualité au sein d'une structure précisément définie. » (Article R1110-3 csp)*

Concernant les modalités pratiques de l'information, l'article R 1110-3-5 du csp précise que : « *L'information préalable de la personne est attestée par la remise à celle-ci, par le professionnel, d'un support écrit reprenant cette information. Ce support indique les modalités effectives d'exercice de ses droits en application du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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. »*

3. Le RGPD appliqué aux CPTS

FOCUS le principe de confidentialité et le secret médical

2 / Dans le cas d'un partage de données => Les obligations diffèrent selon que les professionnels souhaitant partager des données médicales appartiennent ou non à la même équipe de soins au sens de l'article L1110-12 du CSP :

*2. a) : « II. — **Lorsqu'ils sont membres d'une même équipe de soins,** les professionnels relevant d'une des catégories mentionnées à l'article R. 1110-2, partagent, avec ceux qui relèvent de l'autre catégorie, les informations relatives à une personne prise en charge dans les strictes limites de l'article R. 1110-1 et **en informent préalablement la personne concernée**. Ils tiennent compte, pour la mise en œuvre de ce partage, des recommandations élaborées par la Haute Autorité de santé avec le concours des ordres professionnels, en particulier pour ce qui concerne les catégories d'informations qui leur sont accessibles. »*

=> SIMPLE OBLIGATION D'INFORMATION

3. Le RGPD appliqué aux CPTS

FOCUS le principe de confidentialité et le secret médical

2. b) : « *Lorsqu'une personne est prise en charge par un professionnel relevant des catégories de professionnels mentionnées à l'article R. 1110-2 et* ***ne faisant pas partie de l'équipe de soins*** *au sens de l'article L. 1110-12,* ***ce professionnel recueille le consentement de la personne concernée pour partager ces données dans le respect des conditions suivantes :***

1° La ***personne et, le cas échéant, son représentant légal, est dûment informée****, en tenant compte de ses capacités, avant d'exprimer son consentement,* ***des catégories d'informations ayant vocation à être partagées, des catégories de professionnels fondés à en connaître, de la nature des supports utilisés pour les partager et des mesures prises pour préserver leur sécurité, notamment les restrictions d'accès ;***

2° Le consentement préalable de la personne, ou de son représentant légal, est recueilli ***par tout moyen, y compris de façon dématérialisée****, après qu'elle a reçu les informations prévues au 1°.* » (Article D1110-3-1 du csp)

=> OBLIGATION D'INFORMATION + OBLIGATION DE RECUEIL DE CONSENTEMENT

3. Le RGPD appliqué aux CPTS

FOCUS le principe de confidentialité et le secret médical

Concernant le consentement, l'article D1110-3-3 du csp précise que :

« Le consentement est recueilli par chaque professionnel mentionné à l'article D. 1110-3-1, par tout moyen, y compris sous forme dématérialisée, sauf en cas d'impossibilité ou d'urgence. Dans ce cas, il procède au recueil du consentement lorsque la personne est de nouveau en capacité ou en situation de consentir au partage d'informations la concernant. Il en est fait mention dans le dossier médical de la personne.

Le consentement est valable tant qu'il n'a pas été retiré par tout moyen, y compris sous forme dématérialisée. Il est strictement limité à la durée de la prise en charge de la personne. La prise en charge peut nécessiter une ou plusieurs interventions successives du professionnel.

La matérialisation du recueil des modifications ou du retrait du consentement est faite selon les modalités décrites à l'article D. 1110-3-2. »

3. Le RGPD appliqué aux CPTS

FOCUS le principe de confidentialité et le secret médical

L'article D 1110-3-2 du csp précise que *« L'information préalable de la personne est attestée par la remise à celle-ci, par le professionnel qui a recueilli le consentement, d'un support écrit, qui peut être un écrit sous forme électronique, reprenant cette information. Ce support indique les modalités effectives d'exercice de ses droits par la personne ainsi que de ceux qui s'attachent aux traitements opérés sur l'information recueillie, en application de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. »*

Enfin et pour terminer à noter que les textes ne prévoient rien pour :

- les échanges entre professionnels relevant d'une même catégorie listée à l'article R. 1110-2 (l'information est prévue que lorsqu'ils ne relèvent pas de la même catégorie)
- Les partages de données médicales entre professionnels relevant d'une même catégorie listée à l'article R. 1110-2 et faisant partie d'une même équipe de soins (l'information n'est prévue que lorsque les professionnels relèvent d'une catégorie différente et font partie d'une même équipe de soins).

3. Le RGPD appliqué aux CPTS

FOCUS le principe de confidentialité et le secret médical

Pour résumer :

	Obligation préalable d'information du patient	Obligation de recueillir le consentement du patient
Echange d'informations entre un professionnel relevant d'une des catégories de l'article R. 1110-2 et un professionnel relevant de l'autre catégorie de l'article R. 1110-2	OUI, L'information doit porter sur la nature des informations échangées, l'identité des destinataires et sur la possibilité pour les personnes concernées d'exercer leur droit d'opposition (L 1110-4 IV. Et R1110-3 I. du CSP)	NON
Echange d'informations entre professionnels relevant d'une même catégorie mentionnée à l'article R. 1110-2 soit la 1° soit la 2°	? Le CSP ne prévoit rien mais d'après le RGPD : OUI	?
Partage d'informations médicales entre professionnels relevant d'une des catégories mentionnées à l'article R. 1110-2 avec ceux qui relèvent de l'autre catégorie, et qui sont tous membres d'une même équipe de soins	OUI, L'information doit porter sur l'existence du partage et sur la possibilité pour les personnes concernées d'exercer leur droit d'opposition. (L 1110-4 IV. Et R 1110-3 II.) (En attente des recommandations élaborées par la HAS avec le concours des ordres professionnels)	NON
Partage d'informations entre professionnels relevant d'une même catégorie mentionnée à l'article R. 1110-2 soit la 1° soit la 2° et faisant partie de la même équipe de soins	? Le CSP ne prévoit rien mais d'après le RGPD : OUI	?
Partage d'informations médicales avec un professionnel, relevant des catégories prévues à l'article R 1110-2 du CSP, ne faisant pas partie de l'équipe de soins (Article D1110-3-1 csp)	OUI, nécessité d'un support écrit même sous forme électronique. L'information porte les catégories des informations échangées, catégories des destinataires, nature des supports utilisés pour le partage, les mesures prises pour préserver leur sécurité notamment les restrictions d'accès et sur la possibilité pour les personnes concernées d'exercer leur droit d'opposition et plus généralement les modalités effectives d'exercice de leurs droits	OUI, Consentement recueilli par tout moyen y compris sous forme dématérialisée

3. Le RGPD appliqué aux CPTS

FOCUS le principe de confidentialité et le secret médical

Article L1110-12 csp sur la notion d'équipe de soins : «*Pour l'application du présent titre,* ***l'équipe de soins est un ensemble de professionnels qui participent directement au profit d'un même patient à la réalisation d'un acte diagnostique, thérapeutique, de compensation du handicap, de soulagement de la douleur ou de prévention de perte d'autonomie, ou aux actions nécessaires à la coordination de plusieurs de ces actes, et qui :***

1° Soit exercent dans le même établissement de santé, au sein du service de santé des armées, dans le même établissement ou service social ou médico-social mentionné au I de l'article L. 312-1 du code de l'action sociale et des familles ou dans le cadre d'une structure de coopération, d'exercice partagé ou de coordination sanitaire ou médico-sociale figurant sur une liste fixée par décret ;

2° Soit se sont vu reconnaître la qualité de membre de l'équipe de soins par le patient qui s'adresse à eux pour la réalisation des consultations et des actes prescrits par un médecin auquel il a confié sa prise en charge ;

3° Soit exercent dans un ensemble, comprenant au moins un professionnel de santé, présentant une organisation formalisée et des pratiques conformes à un cahier des charges fixé par un arrêté du ministre chargé de la santé. »

3. Le RGPD appliqué aux CPTS

FOCUS le principe de confidentialité et le secret médical

Sachant que d'après l'article D1110-3-4 du csp : « *Les structures de coopération, d'exercice partagé ou de coordination sanitaire ou médico-sociale mentionnées au 1° de l'article L. 1110-12 sont les suivantes :*

1° Les groupements hospitaliers de territoire ;

2° Les fédérations médicales inter-hospitalières ;

3° Lorsqu'ils ont pour objet la prise en charge médicale coordonnée de personnes, les groupements de coopération sanitaire et les groupements de coopération sociaux et médico-sociaux, ainsi que les groupements d'intérêt public et les groupements d'intérêt économique ;

4° Les maisons et les centres de santé ;

5° Les sociétés d'exercice libéral et toute autre personne morale associant des professionnels de santé libéraux, lorsqu'elles ont pour objet la prise en charge médicale coordonnée de personnes ;

6° Les organisations mises en œuvre dans le cadre des protocoles de coopération prévus aux articles L. 4011-1 à L. 4011-3 ;

7° Les équipes pluridisciplinaires prévues à l'article L. 146-8 du code de l'action sociale et des familles et les équipes médico-sociales intervenant au titre de l'allocation personnalisée d'autonomie prévue à l'article L. 232-6 du même code ;

8° Les dispositifs d'appui à la coordination mentionnés à l'article L. 6327-2 ;

9° Les dispositifs spécifiques régionaux mentionnés à l'article L. 6327-6. »

3. Le RGPD appliqué aux CPTS

FOCUS le principe de confidentialité et le secret médical

Point de vigilance rappelé dernièrement pas la CNIL :

Entre 2020 et 2024, la CNIL a procédé à 13 contrôles auprès d'établissements de santé et a mis en demeure plusieurs d'entre eux de prendre les mesures permettant d'assurer la sécurité et la confidentialité de leur dossier patient informatisé et a rappelé que les données de santé des patients ne doivent être accessibles qu'aux personnes **justifiant du besoin d'en connaître.**

Un des constats opérés = Politique de gestion des habilitations inadaptée voire inexistante.

Les CPTS doivent dans la gestion de leurs « dossiers patient » appliquer les recommandations de la CNIL en la matière.

3. Le RGPD appliqué aux CPTS

FOCUS le principe de confidentialité et le secret médical

Parmi les recommandations, la CNIL a notamment exigé que chaque professionnel de santé ou agent de l'établissement n'accède qu'aux dossiers dont il a à connaître => mise en place d'une politique d'habilitation qui doit être élaborée en **tenant compte notamment du métier exercé :**

Exemple donné : « *un agent responsable de l'accueil des patients dans la structure ne doit accéder qu'au dossier administratif du patient et non aux données médicales, alors qu'un médecin accèdera également aux données médicales ».*

Pour plus d'informations : https://www.cnil.fr/fr/donnees-de-sante-la-cnil-rappelle-les-mesures-de-securite-et-de-confidentialite-pour-lacces-au

4. Temps d’échange : questions/réponses

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

Agence Régionale de Santé Île-de-France

Merci de votre attention

Secrétariat Général

Les mesures de sécurité

Charlotte CABALION – ***Référente SI CPTS***

Tania MAC-LUCKIE – ***Consultante en cyber sécurité***

TOUS CYBER VIGILANTS

sesan
Groupement d'Intérêt Public eSanté

Les mesures de sécurité

Prendre en compte toutes les dimensions de la sécurité des données

Organisationelles

Techniques

Physiques

Les mesures de sécurité

La sécurité physique

Risques à prévenir : Vol, intrusion, incendie
Origine du risque : malveillance ou accident

- **Protection des zones:**
  - **Clé,**
  - **Badge,**
  - **Contrôle d'accès**

- **Protection des équipements:**
  - **Système de vidéo protection,**
  - **Sécurité des câblages,**
  - **….**

Les mesures de sécurité

La sécurité logique

Risques à prévenir : Indisponibilité de l'information, intrusion sur le SI, vol de données.
Origine du risque : malveillance

- **Protection antivirale**

- **Messagerie sécurisée et outils de chiffrement**

- **Protection du réseau interne (wifi invité, …)**

Les mesures de sécurité

La sécurité organisationnelle

Risques à prévenir : Mauvaise usage des outils numériques
Origine du risque : Erreur ou méconnaissance

- **Sensibilisation des utilisateurs/salariés**

- **Charte d'usage des moyens informatiques**

- **Gestion des accès et revue des habilitations**

- **Politique de mot de passe renforcée**

Les mesures de sécurité

Points de vigilance

- **Mot de passe:**
  - Complexe
  - Changement régulier ou en cas de doute
  - Stockage : support sécurisé/ astuce mémo technique

- **Clé USB :**
  - Scan antivirus
  - Usage limité : transfert uniquement, interdiction,..

- **Phishing:**
  - identification,
  - Signalement

- **MAJ des logiciels**

TEMPS REQUIS POUR DÉCHIFFRER UN MDP

4 chiffres

Piratage

1

seconde

8 lettres majuscules & minuscules

Piratage

22

minutes

10 lettres majuscules & minuscules + chiffres

Piratage

7

mois

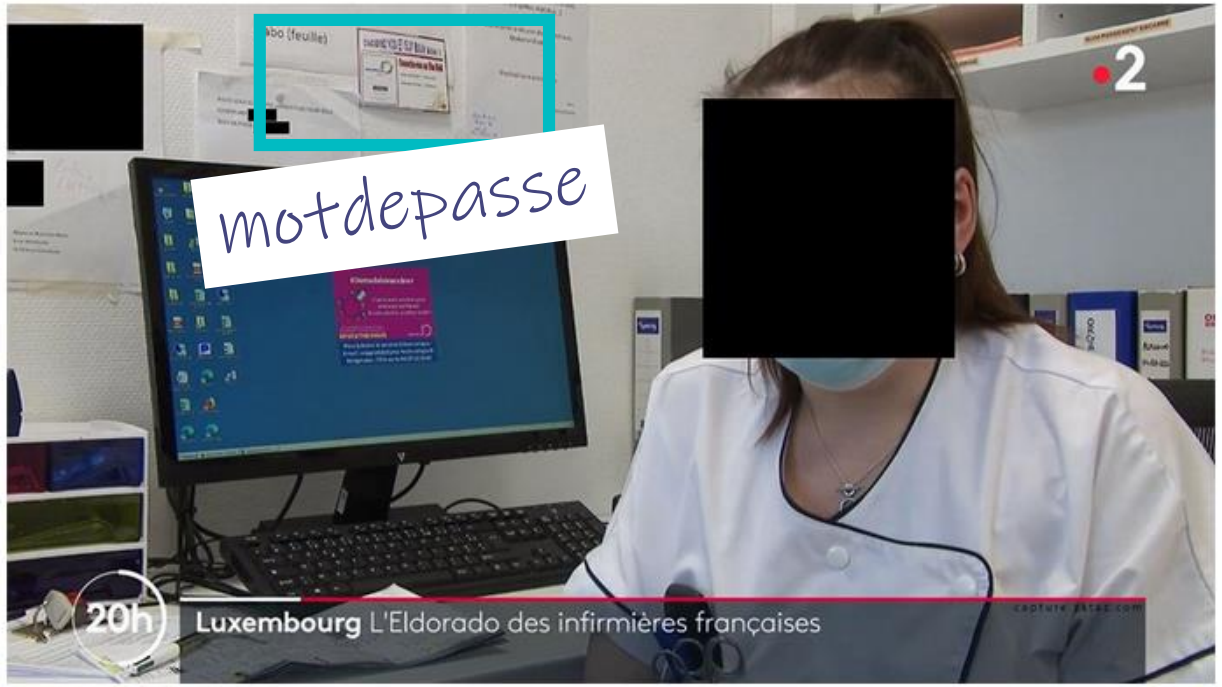
14 lettres majuscules & minuscules + chiffres + caractères spéciaux

Piratage

200 000 000

années

Fuite de mot de passe



« Quand un reportage TV sur la fuite des infirmières au Luxembourg fait fuiter un mot de passe d'un hôpital »
Zataz, 13 avril 2021

Indices d'un mail de phishing

Technique d'ingénierie sociale : urgence, importance, curiosité

Les fautes d'orthographe

ven. 06/11/2020 16:08

Ministère de l'économie et des finances <ministere@coom.site>

Communication importante : PRIME COVID-19

À Tania MAC-LUCKIE

Madame, Monsieur,

Vous êtes un professionnel hospitalier, d'un EHAPD ou d'un CENTRE MEDICO-SOCIAL ?

Vous pouvez bénéficier de la prime complémentaire COVID-19 d'un montant de 480 € !!!

Pour vous enregistrer et en bénéficier :

CLIQUEZ ICI POUR VOUS ENREGISTRER

La santé est l'affaire de tous, ensemble mettons en place les moyens de nous défendre contre le Coronavirus.

Ministère de l'économie et des finances

Liberté. Fraternité. Egalité

« coom.site » L'adresse mail est suspecte.

En survolant le bouton/le lien avec la souris **sans cliquer,** le lien réel va apparaitre, il est sans objet avec le mail et non légitime

Merci de votre attention

l'Assurance Maladie

Agir ensemble, protéger chacun

WEBINAIRE - SENSIBILISATION RGPD

Mardi 05 mars 2024

DCGDR Île-de-France

01

LE DMP

02

LA MSSANTE

03

LES TEXTES JURIDIQUES

01

LE DMP

LE DMP : LES RÈGLES DE PARTAGE ET D'INFORMATIONS DU PATIENTS

Qu'est ce que le DMP ?

Un carnet de santé numérique qui conserve et sécurise les informations de santé. Il peut être consulté et alimenté par différentes professions.

Pourquoi alimenter le DMP ?

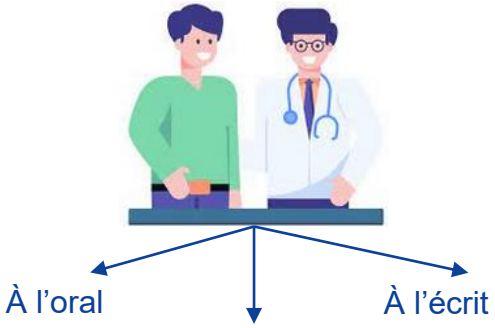
Selon l'article L,1111-15 du CSP : « *Chaque professionnel de santé, quels que soient son mode et son lieu d'exercice, doit reporter dans le DMP, à l'occasion de chaque acte ou consultation, les éléments diagnostiques et thérapeutiques nécessaires à la coordination des soins de la personne prise en charge, dont la liste est fixée par arrêté du ministre chargé de la santé* »

Cette liste est fixée par l'arrêté du 26 avril 2022, nous pouvons retrouver :

- Les comptes rendus : des examens de biologie médicale, des examens radio-diagnostiques, opératoire,
- Les prescriptions de produits de santé, d'examen de biologie médicale, les demandes d'examens de radiologie,

Mais aussi les autres certificats et déclarations, les lettres et courriers adressés à un professionnel de santé.

Le consentement de l'alimentation



Sur une plateforme en ligne

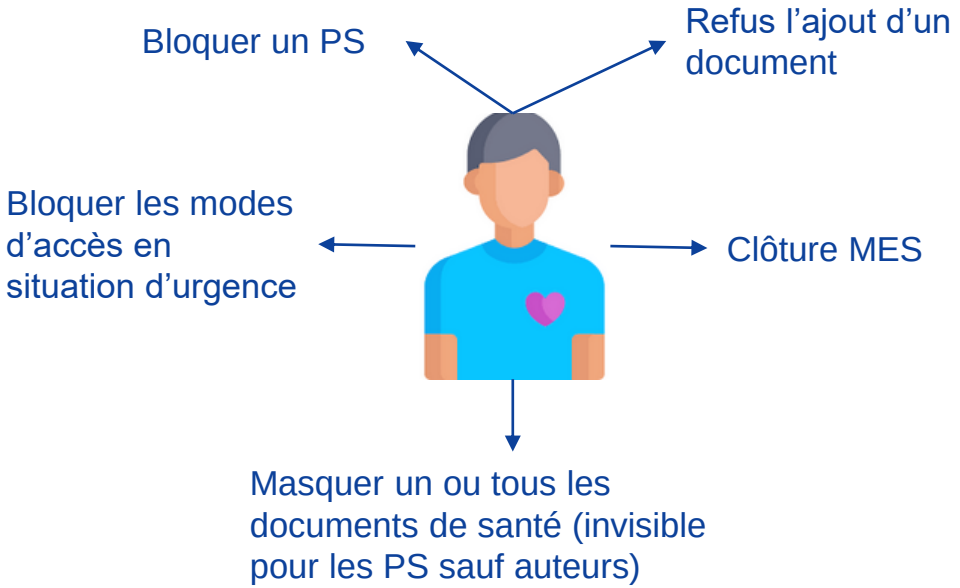
Il est possible de masquer des documents s'ils sont sensibles (attente consultation d'annonce ou actes auprès de mineurs).

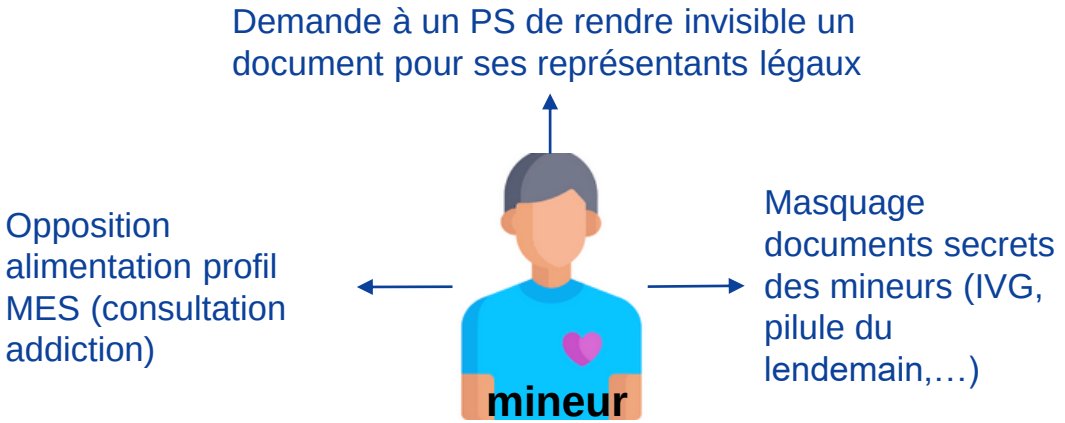
Plus de 68,4 millions (97%) de français disposent d'un profil Mon Espace santé ouvert

l'Assurance Maladie
Agir ensemble, protéger chacun

LE DMP ET MON ESPACE SANTE

L'usager peut accéder à tous ses documents versés dans son DMP. Aussi, toutes les actions réalisées par les professionnels de santé dans le DMP sont tracées et visibles par le patient.





02

LA MSSANTE

LA MSSANTE : LE CADRE ET SES APPLICATIONS

Qu'est ce que la MSSanté ?
Un ensemble de messageries sécurisées permettant d'échanger par mail des données de santé de manière dématérialisées et structurée dans un espace de confiance. Si l'utilisation d'une messagerie dans l'espace de confiance MSSanté n'est pas obligatoire en tant que tel, le professionnel doit respecter le cadre juridique (Articles L1110-4 CSP et L1111-8 CSP) de l'échange et l'hébergement des données de santé (loi informatique et libertés).

L'article L1111-15 du CSP dispose que « *Chaque professionnels doit également envoyer par messagerie sécurisée ces documents au médecin traitant, au médecin prescripteur s'il y a lieu, à tout professionnel dont l'intervention dans la prise en charge du patient lui paraît pertinente ainsi qu'au patient. ».* L'envoi au patient doit se faire via la messagerie sécurisée disponible au patient via son Espace Santé.

Critères de conformité

Différents opérateurs (industriel, ordre ou structures de santé)

MSSanté
Système de messageries sécurisées, données protégées.

Agence du numérique en santé

Le choix : nominative, organisationnelle ou applicative

~~Gmail~~ ~~Outlook.com~~ ~~Laposte.net~~ ~~orange~~ ~~SFR MAIL~~

l'Assurance Maladie
Agir ensemble, protéger chacun

03

LES TEXTES JURIDIQUES

LES TEXTES JURIDIQUES

L'article L1111-15 CSP :
https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038887045

L'arrêté du 26 avril 2022 fixant la liste des documents soumis à l'obligation prévue à l'article L1111-15 du CSP :
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045726627

L'article R1111-50 CSP :
https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043923258

La matrice d'habilitation DMP :
https://esante.gouv.fr/sites/default/files/media_entity/documents/M%C3%A9mo_D%C3%A9tail%20des%20droits%20et%20r%C3%A8gles%20d%27acc%C3%A8s%20Monespacesant%C3%A9_DMP.pptx%20%281%29.pdf

Le document d'informations concernant le DMP :
https://esante.gouv.fr/sites/default/files/media_entity/documents/M%C3%A9mo_D%C3%A9tail%20des%20droits%20et%20r%C3%A8gles%20d%27acc%C3%A8s%20Monespacesant%C3%A9_DMP.pptx%20%281%29.pdf

La MSSanté:
https://esante.gouv.fr/produits-services/mssante

Le numérique s'inscrit dans le cadre existant de responsabilité des professionnels de santé

Les règles relatives au secret professionnel, à la confidentialité et au respect de la vie privée des personnes s'appliquent pleinement à Mon espace santé.

- Ce n'est pas parce qu'un professionnel est tenu au secret médical qu'il peut accéder à des informations relatives à la santé d'une personne. La seule qualité de professionnel ne permet pas un accès au DMP d'une personne.
- Comme pour la pratique courante des soins, **l'accès aux données d'un patient n'est possible que dans le strict cadre de sa prise en charge pour assurer la prévention, la qualité, la continuité et la prise en charge coordonnée des soins**.

Quelle est la responsabilité du professionnel ?

Dans le cadre de la prise en charge d'un patient, **la responsabilité d'un professionnel peut être engagée :**

- **En cas de litige portant sur la non-connaissance d'une information visible et disponible dans le DMP** (l'article L. 1111-15 du CSP). La responsabilité du professionnel de santé doit être examinée au regard de sa situation conventionnelle. En effet, les professionnels de santé conventionnés ont l'obligation de consulter et d'alimenter le DMP de leurs patients (Al. 7 du L. 1111-14 du CSP).
- **En cas d'erreur de diagnostic du professionnel de santé malgré la consultation du DMP** (manquement manifeste du professionnel à l'obligation de dispenser des soins attentifs, consciencieux et conformes aux données acquises de la science). L'article L. 1142-1 du CSP précise que la responsabilité du professionnel de santé est engagée lorsque l'erreur de diagnostic constitue une faute de ce dernier. Le patient doit apporter les éléments de preuve permettant d'engager la responsabilité du professionnel.

A quels professionnels s'applique cette responsabilité ?

Cette responsabilité s'applique **à tout professionnel de santé, qu'il exerce en secteur libéral ou en établissement de santé.** Cependant, deux cas de figure existent et dépendent de **la situation conventionnelle** du professionnel.

- **Le professionnel de santé conventionné** est redevable d'une **double obligation** de consultation du DMP : d'abord vis-à-vis de son patient, au titre de sa responsabilité médicale mais également vis-à-vis de l'Assurance maladie, au titre de la convention à laquelle il a adhéré.
- **Le professionnel de santé non conventionné** n'est redevable de l'obligation de consultation du DMP que par rapport à son patient, dans le cadre de sa responsabilité médicale.

Des sanctions claires inscrites dans les textes

⚠ Ainsi, si un professionnel de santé venait à accéder et diffuser des données auxquelles il n'est pas habilité à accéder, cette consultation contrevient à ses obligations légales et déontologiques en matière de respect de la vie privée et de secret professionnel prévues aux articles L. 1110-4 et R.4127-4 du code de la santé publique.

En termes de **sanctions**, tout professionnel qui ne respecterait pas ces règles s'expose à :

- **1 an de prison et 15 000 euros d'amende** (violation du cercle de confiance en cas de révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire– articles L. 1110-4 V. et L. 1111-18 du CSP, article 226-13 du code pénal) ;
- **5 ans de prison et 150 000 euros d'amende** (accès frauduleux au DMP, système d'information mis en œuvre par l'Etat – Article 323-1 du code pénal), ainsi que plusieurs peines complémentaires possibles (article 323-5 du code pénal).
- des **sanctions ordinales** pourraient également être prises.