GDPR : CONSEILS AUX PROFESSIONNELS DE LA SANTE.

Tout d'abord, il est nécessaire de rappeler que le nouveau Règlement général sur la protection des données, ci-après RGPD, s'inscrit dans la continuité de la loi sur la vie privée de 1992 (ci-après LVP). Les principes directeurs du RGPD sont, à quelques exceptions près, pour la plupart identiques à ceux de la LVP. Ainsi, si les médecins et acteurs de soins respectaient déjà la LVP, la mise en conformité avec le nouveau RGPD ne devrait a priori pas être trop compliquée.

Réf.	Cadre légal	En pratique
Art. 9	En principe, **le traitement des données sensibles* est interdit** sauf si une exception du point 2 dudit article est rencontrée. En l'espèce, les médecins et acteurs de soins peuvent invoqués **l'exception h**) de l'article mentionné. Ainsi, ils sont bien autorisés à traiter des données de santé pour établir des diagnostics médicaux. Par ailleurs, **le point 3 de l'article 9** précise que les données en question doivent être traitées sous la surveillance et la responsabilité d'un professionnel de la santé qui est soumis à une obligation de secret professionnel.	Les médecins et acteurs de soins sont **autorisés** à traiter les données à caractère personnel.
	Les médecins et acteurs de soins traitent des données de santé qui sont des données à caractère personnel, sensibles. Le but du RGPD est d'**assurer une culture de protection de ces données**.	Les médecins et acteurs de soins sont **soumis aux exigences du RGPD**.
Art. 5	Le cœur de ce RGPD se retrouve en son **article 5** qui instaure les **principes directeurs** à respecter. Il est primordial de se conformer à ces principes car la sanction s'avère particulièrement lourde… Le RGPD parle de **4%** du chiffre d'affaire.	Respecter ces principes directeurs en **bon père de famille**. Quelques mesures concrètes.
Art 5.1	1. Les données doivent être traitées de manière **licite, loyale et transparence** – ajout du RGPD ! Avant il n'y avait que le mot loyal mais maintenant on a rajouté « de manière transparente ». On veut accentuer cette exigence. - Le principe de transparence : c'est le droit à l'auto-détermination informationnelle. - Le principe de loyauté évoque la transparence des opérations propres au traitement des données à caractère personnel. A moins que la loi ne l'autorise,	**Informations conseillées au patient** - Avertissement de la tenue d'un DMI ou DPI par un affichage en salle d'attente. - Communication claire des règles de collaboration applicables aux cabinets de groupe, notamment en ce qui concerne le partage des dossiers entre collaborants.

	il ne doit pas y avoir de traitement caché ou secret de données personnelles. Il faut annoncer aux gens ce que l'on fait, faire ce que l'on a dit et pas autre chose, et on ne peut pas faire de récoltes secrètes. - Licitement, cela veut dire qu'il faut aussi respecter les autres législations, par exemple l'obligation de respecter le secret professionnel.	
Art. 5.2	Ensuite, un traitement de données personnelles doit toujours poursuivre une **finalité spécifique**. <!> Le principe de finalité est la pierre angulaire de la protection. Il y a deux grandes parties à ce principe : - Premièrement, les données à caractère personnel doivent être collectées pour des finalités **déterminées** (précises) et **explicites** (pas secrètes). On ne peut donc pas poursuivre un but imprécis et on ne peut pas annoncer quelque chose et faire autre chose. La collecte à des fins explicites est liée au principe de loyauté. - Les finalités de la collecte doivent aussi être **légitimes**. Cela signifie que le but poursuivi ne peut pas induire une atteinte disproportionnée aux intérêts des personnes. Il faut faire une balance des intérêts pour vérifier si la finalité de la collecte est légitime. Dans le cadre des soins de santé, tous les renseignements personnels sont exploités à des fins de **gestion du dossier médical** de manière générale.	**Finalité = gestion du dossier médical**
Art. 5.3	Le troisième principe du RGPD est le **principe de minimisation des données**. Ce principe de minimisation des données est une traduction du principe de proportionnalité que l'on retrouvait initialement dans la loi de 1992 : c'est-à-dire qu'on ne peut pas porter atteinte de manière disproportionnée aux droits et libertés des personnes. Ce principe est relativement important dans la mesure où il requiert de ne pas récolter trop de données à caractère personnel, mais que les données qui sont strictement nécessaires pour répondre à la finalité du traitement.	**Se limiter au recueil des données strictement nécessaires** suivant les missions de soins des différents acteurs.
Art. 5.4	Les données doivent être exactes et si nécessaires mises à jour. Ce principe d'exactitude n'appelle pas beaucoup de commentaires. C'est une question de bonne pratique. Le conseil que l'on pourrait donner aux praticiens c'est qu'au vu de l'évolution moderne dans laquelle nous vivons et compte tenu de la	Exemple de bonne pratique : Dans le cadre du DMI (DMG), **vérifier l'exactitude des « SUMEHR »** en collaboration directe avec le patient.

	mission impartie aux médecins, à savoir la tenue du DMG (qui se concrétise dans le DMI), il convient de vérifier l'exactitude des données en collaboration directe avec le patient.	
Art. 5.5	Il y a un **principe de limitation de la conservation**, c'est-à-dire que l'on ne peut conserver les données que le temps nécessaire au traitement des données. Dès que la finalité a été atteinte, il n'y a plus de raison de conserver la donnée. Mais la loi, propre au secteur, sur la conservation des données médicales l'emporte. Ainsi les données médicales doivent être conservées **30 ans** après le dernier contact pour les données du dossier médical.	Conservation limitée à **30 ans**
Art. 5.6	Les **principes d'intégrité et de confidentialité** que l'on retrouvaient déjà dans la LVP, restent des principes majeurs. Il est primordial de savoir utiliser son ordinateur en tant que bon père de famille. Cela implique plusieurs mesures concrètes.	**Mesures concrètes** : - Utilisation d'un mot de passe, correctement géré, pour la protection de l'ordinateur. - Utilisation d'antivirus et protection « firewall » en cas de connexion à Internet. - Bonne gestion des backups en fréquence et endroits de stockage. Si utilisation du cloud : avoir les garanties de rester sur le territoire EU. - Pour l'échange de données de santé, n'utiliser que des messageries sécurises-cryptées ex e-Hbox - Partage de données via des réseaux de santé reconnus et adaptés (HUBs MétaHub). Ex RSW
Art. 5.7	Enfin, le dernier principe est tout nouveau. C'est **le principe d'accountability**. Le mot n'est pas bon en français parce qu'on pense à la responsabilité juridique (civile ou pénale) mais c'est l'accountability qui veut dire le fait de devoir garantir le respect des autres principes énoncés ci-dessus. C'est une approche très anglo-saxonne = **Obliger de pouvoir prouver qu'on a mis tout en œuvre pour pouvoir contrôler le respect de la législation**. C'est une idée de responsabilisation des acteurs. Ce principe est sans aucun doute, celui qui sera le plus difficile à mettre en œuvre dans la mesure où il impose en pratique de tenir une documentation afin de prouver le respect de ces différents principes. Pour respecter ce principe en due et bonne forme, il est intéressant de veiller à la conformité légale des contrats de maintenance, veiller à avoir des clauses de confidentialité…	C'est au responsable des traitements de données de santé de prouver qu'il est **pro-actif** dans la protection des données au sens du RGDP.

	Précisons que ces principes sont bien des principes qu'il convient de mettre en œuvre en bon père de famille, il n'y a pas d'obligation de résultat à la lecture portée sur ce règlement mais ce sont des **obligations de moyens**.	Les médecins et acteurs de soins mettront en place les **moyens raisonnables** pour atteindre l'effectivité de ces principes.
	Après avoir rappelé ces différents principes directeurs, précisons quelques **obligations** auxquelles le RGDP soumet les acteurs de soins.	
Art. 30	1. La **tenue d'un registre interne des activités de traitement** : ce registre est obligatoire pour les structures avec 250 salariés. Même si les médecins et acteurs de soins n'entrent pas dans cette catégorie, ils **sont visés par cette obligation** dès lors qu'ils traitent des données sensibles pouvant comporter un risque pour les droits et les libertés des personnes concernées, à savoir les patients. L'article 30 du RGPD donne toutes les informations qui doivent être reprises dans ce registre (Description de chaque traitement) : finalité, responsable, catégories de données, destinataires, mesures de sécurité, etc.	**Obligation de tenue d'un registre** Modèle standard : https://www.cnil.fr/sites/default/files/atoms/files/registre-reglement-publie.xlsx
Art. 35-36 Pour plus de détails : Cfr. Guidelines du groupe de l'article 29.	2. **Une analyse d'impact des risques** (PIA). Le but d'une PIA c'est d'identifier les risques mais aussi d'essayer d'y répondre. Quels sont les risques ? - Destruction : écoulement d'eau, des problèmes de sécurité dans les bâtiments. - Perte : de nos jours c'est très fréquent au vu du nombre de données sauvegardées sur des supports mobiles. - Altération : modification des données. - Divulgation non autorisée. - Accès non autorisé aux données. Si les médecins et acteurs de soins perdent leur matériel, si ce dernier est protégé, on évitera l'accès non autorisé aux données médicales. La récupération des données perdues est assurée par un bon back up.	Mesures concrètes de la gestion des risques : **se protéger contre la perte ou la diffusion inadéquate des données à caractère personnel comme les données de santé**
Art. 37-39	3. **Désignation d'un délégué à la protection des données (DPO)**. Les acteurs	**La désignation d'un DPO n'est pas de mise dans ce**

	de soins qui comptent moins de 250 employés ne doivent pas désigner un DPO (data personnal officer)	**contexte.**
	4. **Privacy By Design et By Default** - Le principe du « privacy by design » ou protection dès la conception impose au responsable de traitement de façonner son traitement de manière à assurer la protection la plus effective possible des droits des personnes concernées. = Système qui fonctionne en respectant la législation. - Le principe du « privacy by default » ou protection par défaut met l'accent sur l'adoption de mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées.	**Garantir contractuellement par les concepteurs de logiciels** les mesures associées à la qualité et à la compliance RGDP de l'outil de gestion des données de santé .
Art. 32	5. **Sécurité et confidentialité** Il faut prendre des mesures techniques et organisationnelles appropriées pour protéger les données en tenant compte : - De l'état de l'art/état des connaissances - Des coûts de la mise en oeuvre - Des risques - De la nature des données : pour un hôpital on va mettre la barre de la sécurité plus hautes. - De la portée, du contexte et des finalités du traitement En cas de recours à un sous-traitant, le sous-traitant traite uniquement les données à caractère personnel pour l'exécution de ses obligations en conformité avec le Contrat de Traitement des Données et les instructions écrites du responsable du traitement.	**Assurer une certaine sécurité et confidentialité des données traitées**. Cfr. Principe de l'article 5.6. Sous-traitance : garanties de confidentialité à mettre en place contractuellement.
Art. 44 et s.	6. **Pas de transfert hors de l'UE.** A l'heure actuelle, l'union européenne bénéficie de la meilleure protection en termes de données à caractère personnel. Si des radios, des diagnostics ou encore des études médicales sont envoyées hors de l'Union européenne, il convient de s'assurer que le pays destinataire offre des garanties équivalentes à celles instaurées dans le RGPD par le biais d'une clause contractuelle notamment.	**Être attentif à cette obligation lors de l'utilisation de « Cloud » et lors de la participation à des études cliniques**.

Art. 12-14 Art. 15 Art. 19 Art. 20 Art. 21 Art. 22 Art. 33	Droits des personnes concernées : • **Information** : lors de la collecte de données à caractère personnel, le patient reçoit les informations concernant le traitement de ses données à caractère personnel, conformément aux articles 12.1, 12.5, 12.7, 13 et 14 du RGPD, par exemple par le biais d'un formulaire. • **Accès** : le patient peut obtenir du responsable du traitement la confirmation du traitement ou non de ses données personnelles et, dans l'affirmative, il a un droit d'accès à ces données et aux informations fournies par l'article 15.1 du RGPD. Outre le droit de consultation directe dans un délai de 15 jours maximum de son dossier médical, le patient peut demander la copie de l'ensemble ou d'une partie de son dossier sous réserve des exceptions prévues par la loi du 22 août 2002. • **Rectification et effacement (droit à l'oubli)** : S'il apparaît que le traitement contient des données erronées, incomplètes ou ne répondant pas aux objectifs voulus, le patient a le droit d'en demander gratuitement la correction. A cette fin, le patient formule une demande à la Direction générale ou à la Direction médicale. La rectification interviendra dans les deux mois de la demande. En ce qui concerne le droit à l'effacement, ce dernier ne peut être pleinement efficace dans le cadre des soins de santé car l'AR. 3 mai 1999 relatif au dossier du patient à l'hôpital précise en son article 1 §3 que ce dossier doit être conservé pendant au moins **30 ans** dans l'hôpital. • **Portabilité des données** : le droit à la portabilité des données permet au patient de recevoir les données qu'elle a fourni au responsable du traitement dans un format couramment utilisé et lisible par une machine afin qu'il en reprenne le contrôle et puisse notamment les transmettre à un autre responsable du traitement. • **Opposition**: En vertu du RGPD, la personne concernée peut s'opposer au traitement de ses données pour des motifs liés à sa situation particulière, notamment lorsque les données sont traitées à des fins de profilage. Le responsable du traitement veillera à y répondre à	**Ne pas perdre de vue les droits du patient.** **Informer le patient.** **Le document de la tenue du DMI précisera l**es modalités de traitement, l'identité du responsable du traitement, la finalité poursuivie par le traitement, les destinataires des données, les droits des personnes concernées et les transferts de données. Cfr annexe. **Droit d'accès OUI:** prévoir la possibilité d'extraire du fichier les données relatives à la personne pour lui adresser une copie (la copie peut prendre différentes formes telles qu'une copie papier, une disquette, un message électronique sécurisé ou un document manuscrit). **Droit de rectification** : • Prestataire/patient, ne peuvent pendant cette durée retirer des éléments pertinents pour la tenue du dossier • Rectification possible sous la responsabilité du prestataire concerné • Toute rectification doit être réversible et documentée **Pas de droit à l'effacement** : informer le patient que le dossier patient est conservé jusqu'à 30 ans après l'interruption de la relation de soins. **Droit à la portabilité des données** : mettre en place par exemples:

	cette demande dans un délai de deux mois. Le responsable du traitement se réserve le droit de refuser à accorder ce droit d'opposition s'il justifie de l'existence de motifs impérieux et légitimes primant sur les intérêts et les droits et libertés de la personne. Toutefois, on remarquera que l'article 9 de la loi du 22 août 2002 relative aux droits du patient ne prévoit pas le droit d'opposition. En revanche, le patient dispose de la possibilité de faire joindre par le praticien professionnel des documents au dossier patient le concernant, à sa demande. Il convient de faire une distinction entre l'opposition à la communication de données médicales à des tiers et l'opposition à l'enregistrement et à la tenue à jour de données dans le dossier médical. L'absence d'un dossier médical complet et tenu à jour comporte des risques. Il est clair qu'à l'égard du médecin, le dossier remplit une fonction médico-légale importante. Pour le médecin, le dossier patient est surtout nécessaire dans l'optique d'offrir au patient une continuité des soins de qualité.	– une fonctionnalité pour extraire les informations pertinentes des bases de données – un outil permettant la communication sécurisé**e** des données extraites au RT destinataire ou à la personne concernée, un accord entre les RT sur la façon dont ils souhaitent réaliser cette portabilité (supports, standards,…) **Pas de droit d'opposition** à l'enregistrement et à la tenue à jour de données dans le dossier médical. Justification : offrir au patient une continuité des soins de qualité.

Document produit en collaboration par Emeraude Camberlin et Thierry Defour..