# RGPD : Conseils aux professionnels de la santé

**Ce document a pour visée de préciser les principes directeurs et les obligations auxquels les professionnels de la santé sont soumis en vertu de la nouvelle réglementation européenne entrée en vigueur le 25 mai 2018 et d'en donner quelques exemples de mesures concrètes.**

Préalablement, 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 »**[1]. 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 coutumiers du respect du secret professionnel respectaient déjà la LVP, la mise en conformité avec le nouveau RGPD ne devrait *a priori* pas être trop « compliquée ».

L'entrée en vigueur de cette nouvelle réglementation peut être vue par les professionnels de la santé comme **l'opportunité d'être critique sur leurs politiques de protection des données afin de partager et de diffuser une culture de la protection de données personnelles.**

Le présent document a été produit en collaboration par l'un des collaborateurs d'e-santé Wallonie, le **Dr Thierry DEFOUR**, médecin spécialiste en gestion de données de santé et DPO hospitalier et par **Emeraude CAMBERLIN**, juriste spécialisée en droit des nouvelles technologies de l'information et de la communication. Dans la mesure où il a pour seule vocation de donner un conseil pratique non exhaustif aux acteurs de soins de santé sur les exigences du RGPD, il n'engage nullement la responsabilité de ses auteurs.

[1] La LVP est aujourd'hui intégralement remplacée par une **nouvelle loi belge du 30 juillet 2018** relative à la protection de la vie privée. Cette nouvelle loi belge a été publiée au Moniteur belge le 5 septembre 2018. Dans la mesure où elle ne répète ou n'infirme nullement les exigences du RGPD, elle constitue **un complément à la réglementation européenne** déjà en vigueur. En effet, le RGPD laissait une marge de manoeuvre au législateur belge à certains égards pour édicter des règles complémentaires ou créer certaines exceptions.

| Réf. | Cadre légal | En pratique |
|---|---|---|
| **CHAMP D'APPLICATION**<br>**Cfr. Art. 2 et 4** | Les médecins et acteurs de soins traitent des données de santé qui sont des **données à caractère personnel sensibles** qu'il convient de protéger à ce titre.<br><br>Le but du RGPD est d'**assurer une culture de protection de ces données**. | Dès lors qu'ils possèdent dans leurs dossiers patients des données signalétiques et médicales, les médecins et acteurs de soins sont individuellement **soumis aux exigences du RGPD**.<br><br>Ils sont chacun **responsable du traitement** des données personnelles qu'ils traitent dans le cadre de leur activité. |
| | Remarque : Il n'y a **pas lieu de confondre le « traitement des données de santé » avec le « traitement médical »** ***sensu stricto***. La notion de « traitement » au sens du RGPD s'entend largement comme « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés, telles que l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification* ». | |
| **TRAITEMENT LEGITIME DES DONNEES DE SANTE**<br>**Art. 9** | En principe, **le traitement des données sensibles est interdit** sauf si une exception de **l'article 9.2** est rencontrée. En l'espèce, les médecins et acteurs de soins peuvent invoqués **l'exception h).** Ainsi, ils sont bien autorisés à traiter des données de santé pour établir des diagnostics médicaux. Par ailleurs, **l'article 9.3** précise que les données de santé 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 dans l'exercice de leur mission de soin.<br><br>⇨ **Aucun consentement explicite** du patient n'est requis pour le traitement des données de santé aux fins d'un traitement médical *sensu stricto*. |
| **PRINCIPES**<br>**Art. 5** | Le cœur du RGPD se retrouve en son **article 5.** Cet article reprend les **principes directeurs** à respecter pour réaliser la protection des données à caractère personnel : **licéité, loyauté et transparence ; limitation des finalités ; minimisation des données ; exactitude ; limitation de la conservation ; intégrité et confidentialité et responsabilité**. 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.<br><br>Précisons que ces principes sont des principes qu'il convient de mettre en œuvre en tant que **bon père de famille**. Le RGPD fait en effet appel à une obligation de moyens plutôt quà une obligation de résultat. Les médecins et acteurs de soins doivent ainsi mettre en place tous les **moyens raisonnables** pour atteindre l'effectivité de ces principes. | |

| | | |
|---|---|---|
| **Art 5.1** | **1.** Les données doivent être traitées de manière **licite, loyale et transparence** – ajout du RGPD !<br><br>Avant, dans la LVP n'y figurait que le mot loyal. A présent, dans le RGPD, il est ajouté « de manière transparente ». Le RGPD veut ainsi accentuer cette exigence de transparence.<br><br>- Le principe de transparence : c'est le droit à l'auto-détermination informationnelle. La personne concernée doit savoir le pourquoi de la collecte et le devenir de ses données personnelles.<br>- 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, il ne doit pas y avoir de traitement caché ou secret de données personnelles. Il faut annoncer aux personnes concernées ce que l'on fait de leurs données et faire uniquement ce qui a été dit et pas autre chose.<br>- Licitement, cela veut dire qu'il faut aussi respecter les autres législations, par exemple l'obligation de respecter le secret professionnel. | Il est conseillé aux professionnels de la santé d'**informer explicitement leurs patients**, par exemple au moyen d'une **affiche apposée en salle d'attente** qui rappelle qu'ils tiennent un dossier médical informatisé.<br><br>Il est par ailleurs conseillé aux cabinets de groupe de communiquer clairement les règles de collaboration applicables, notamment en ce qui concerne le partage des dossiers entre collaborateurs.<br><br>Téléchargez ces deux affiches sur www.e-santewallonie.be. |
| **Art. 5.2** | **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 :<br><br>- 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.<br><br>- Deuxièmement, les finalités de la collecte doivent être **légitimes**. Cela signifie que le but poursuivi ne peut pas induire une atteinte disproportionnée aux intérêts des personnes. Il importe de faire une balance des intérêts pour vérifier si la finalité de la collecte est bien légitime. | Dans le cadre des soins de santé, tous les renseignements personnels sont exploités à des fins de **gestion du dossier médical**.<br><br>⇨ **Finalité = gestion du dossier médical.** |

| | | |
|---|---|---|
| **Art. 5.3** | **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 LVP : c'est-à-dire qu'on ne peut pas porter atteinte de manière disproportionnée aux droits et libertés des personnes concernées.<br><br>Ce principe est relativement important dans la mesure où il requiert de ne pas récolter trop de données à caractère personnel, mais bien de collecter seulement les données qui sont strictement nécessaires pour répondre à la finalité du traitement. | Les acteurs de soins doivent **se limiter au recueil des données strictement nécessaires** suivant les missions de soins des différents acteurs. |
| **Art. 5.4** | **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.<br><br>Un parallèle doit être fait avec la loi sur les droits du patient du 22 août 2002 dans laquelle il est précisé que le dossier médical du patient doit être soigneusement tenu à jour et conservé en lieu sûr. Au vu de l'évolution moderne dans laquelle nous vivons et compte tenu de la mission impartie aux acteurs de soins, à savoir la tenue à jour du DMG (qui se concrétise dans le DMI), il convient de **vérifier l'exactitude des données qui y sont inscrites.** | ⇨ **vérifier l'exactitude des données inscrites dans les « SUMEHR » en collaboration directe avec le patient.** |
| **Art. 5.5** | **5.** En vertu de la réglementation, il existe un **principe de limitation de la conservation**. Ce dernier exige que chaque acteur ne conserve 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.<br><br>A noter que la réglementation, propre au secteur médical, impose que les données du dossier médical soient conservées **30 ans** après le dernier contact avec le patient. Ainsi, la loi sur la conservation des données médicales l'emporte sur le principe de minimisation des données tel qu'il est inscrit dans le RGPD. | ⇨ Conservation limitée à **30 ans.** |

| | | |
|---|---|---|
| **Art. 5.6** | **6.** Les **principes d'intégrité et de confidentialité** que l'on retrouvait 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. | **Exemples de mesures concrètes** :<br>- Utilisation d'un mot de passe, correctement géré, pour la protection de l'ordinateur.<br>- Utilisation d'antivirus et protection « firewall » en cas de connexion à Internet.<br>- Bonne gestion des backups en fréquence et endroits de stockage. Si utilisation du cloud : avoir les garanties de rester sur le territoire EU.<br>- Pour l'échange de données de santé, n'utiliser que des messageries sécurises-cryptées e-Hbox<br>- Partage de données via des réseaux de santé reconnus et adaptés (HUBs MétaHub). Ex. RSW |
| **Art. 5.7** | **7.** Enfin, le dernier principe est tout nouveau. Il s'agit du **principe d'accountability**.<br><br>La traduction en français qui fait penser à la responsabilité juridique (civile ou pénale) n'est pas juste. Au sens du RGPD, le principe « accountability » signifie que le responsable du traitement des données doit garantir le respect des autres principes énoncés ci-dessus et être à même de démontrer que son traitement est en conformité avec ces principes. C'est une approche très anglo-saxonne. Il s'agit **de pouvoir prouver qu'on a mis tout en œuvre pour pouvoir contrôler le respect de la législation**. C'est l'idée d'une responsabilisation accrue des acteurs.<br><br>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.<br><br>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, des contrats de sous-traitance… | C'est aux acteurs de soins de prouver qu'ils sont **pro-actifs** dans la protection des données de leurs patients.<br><br>⇨ **Plus de responsabilité pour une protection des données plus effective.** |

| | | |
|---|---|---|
| **OBLIGATIONS** | Après avoir rappelé les différents principes directeurs du RGPD, précisons quelques **obligations** auxquelles le RGDP soumet les acteurs de soins. A nouveau, le non respect de ces obligations peut être sanctionné lourdement. | |
| **Art. 30** | **1. Obligation de tenir un registre interne des activités de traitement.**<br><br>L'obligation de notification préalable des traitements à l'autorité de contrôle disparaît au profit d'une obligation générale de tenir un registre des traitements.<br><br>Ce registre est obligatoire pour les structures comportant 250 employés. Toutefois, cette obligation est requise lorsque le traitement mis en œuvre porte notamment sur des données sensibles.<br><br>L'article 30 du RGPD fournit toutes les informations qui doivent être reprises dans ce registre (description de chaque traitement) : finalité, indication du responsable du traitement, catégories de données, destinataires, mesures de sécurité, etc. A noter que ce document doit être mis à la disposition de l'autorité de contrôle et n'est pas destiné à être mis à la disposition du public, en ce compris le patient et sa famille. | Les médecins et acteurs de soins **sont visés par cette obligation** dès lors qu'ils traitent des données sensibles, à savoir les données de santé de leurs patients.<br><br>⇨ **Obligation de tenir un registre des traitements**<br><br>A venir, un exemple de registre des activités de traitement sur www.e-santewallonie.be. |
| **Art. 35-36**<br><br>**Pour plus de détails : Cfr. Guidelines du G29** | **2. Obligation de réaliser une analyse d'impact relative à la protection des données (AIPD).**<br><br>En sus de l'obligation de tenir un registre de traitement, le RGPD prévoit dans certains cas une obligation de réaliser une **AIPD**. Le but d'une AIPD est d'identifier l'ensemble des risques mais aussi d'essayer d'y répondre<br><br>Quels sont les risques ?<br>- Destruction : écoulement d'eau, des problèmes de sécurité dans les bâtiments.<br>- Perte : de nos jours c'est très fréquent au vu du nombre de données sauvegardées sur des supports mobiles.<br>- Altération : modification des données.<br>- Divulgation non autorisée.<br>- Accès non autorisé aux données. | Si les médecins et acteurs de soins viennent à perdre leur matériel informatique et si ce dernier est correctement protégé, l'accès non autorisé aux données médicales est évité. La récupération des données perdues peut alors être assurée par un bon back up.<br><br>⇨ Il importe de **se protéger contre la perte ou la diffusion inadéquate des données à caractère personnel telles que les données de santé**. |

| | | |
|---|---|---|
| **Art. 37-39** | **3. <u>Obligation de désigner un délégué à la protection des données (« DPO »).</u>**<br><br>Le RGPD prévoit dans certains cas la désignation d'un délégué à la protection des données, mieux connu sous l'abréviation anglaise « DPO » pour « Data Protection Officer ». Le DPO peut être un membre du personnel ou un tiers prestant dans le cadre d'un contrat de services.<br><br>A noter que la désignation d'un DPO n'est requise que lorsque les activités du responsable du traitement ou du sous-traitant consistent en des opérations de traitement, qui, du fait de leur nature, de leur portée et/ou de leurs finalités exigent un suivi régulier et systématique <u>à grande échelle</u> de données sensibles. | **La désignation d'un DPO n'est pas de mise dans ce contexte.**<br><br>Nonobstant, la désignation d'une personne référente pour la protection des données est vivement encouragée. Cette personne serait en charge d'assurer la mise en conformité réglementaire du RGPD et aurait notamment pour mission de veiller à sensibiliser l'équipe de soins et les autres membres du cabinet à la protection des données, à tenir et à mettre à jour le registre des activités de traitement, à être la personne de référence pour toutes questions relatives à la protection des données et à être la personne de référence pour centraliser les fuites de données et en faire rapport à l'autorité de protection des données. |
| **Art. 25** | **4. <u>Obligation d'intégrer dans ses démarches les principes « *privacy by design* » et « *privacy by default* ».</u>**<br><br>Il s'agit de deux concepts juridiques conçus pour les technologies de traitement des données personnelles, y compris celles relatives à la santé du patient, qui trouvent leur consécration à l'article 25 du RGPD.<br><br>Pour aller à l'essentiel :<br><br>- <u>Le principe du « privacy by design »</u> (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 d'information qui fonctionne en respectant la législation).<br><br>- <u>Le principe du « privacy by default »</u> (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. | ⇨ **Il importe de garantir contractuellement par les concepteurs de logiciels** les mesures associées à la qualité et à la conformité RGDP de l'outil de gestion des données de santé . |

| | | |
|---|---|---|
| **Art. 32** | **5. <u>Obligation de sécurité et confidentialité</u>.**<br><br>Il faut prendre des mesures techniques et organisationnelles appropriées pour protéger les données en tenant compte :<br><br>- De l'état de l'art/état des connaissances<br>- Des coûts de la mise en œuvre<br>- Des risques<br>- De la nature des données : pour un hôpital on va mettre la barre de la sécurité plus hautes.<br>- De la portée, du contexte et des finalités du traitement<br><br>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. | Les acteurs de soins doivent **assurer une certaine sécurité et confidentialité des données traitées** (Cfr. les mesures concrètes du principe de l'article 5.6).<br><br>En cas de recours à de la sous-traitance, des garanties de confidentialité à mettre en place contractuellement. |
| **Art. 44 et s.** | **6. <u>Pas de transfert hors de l'Union européenne.</u>**<br><br>A l'heure actuelle, l'Union européenne bénéficie du meilleur système juridique en termes de protection des 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. | Les acteurs de soins doivent **être attentifs à cette obligation lors de l'utilisation de « Cloud » et lors de la participation à des études cliniques**. |
| **Art 33 et 55** | **7. <u>Obligation de notification en cas de fuites de données :</u>** les acteurs de soins sont dans l'obligation de signaler toute obligation ou fuite de données à l'autorité de contrôle (= l'Autorité de Protection des Données, ex Commission Vie Privée) dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle doit être accompagnée des motifs du retard. **Une fuite de données va de la perte d'une clé USB contenant les fiches de salaires ou des données patients à une demande de rançon suite à un piratage informatique.** | **<u>Procédure de notification des fuites de données</u>** :<br><br>1) Identifier une fuite de données<br><br>2) Evaluation de la nature/gravité de l'incident<br><br>3) Notification à l'Autorité de protection des données (sans retard inutile et, si possible, dans un délai de 72 heures à compter de la découverte de la fuite de données)<br><br>4) Limiter l'impact de la fuite |

<table>
<tr><td>DROITS DES PERSONNES CONCERNEES</td><td colspan="2">Il convient de ne pas perdre de vue les <u>droits</u> des patients !<br><br>< ! > Il importe de préciser que le RGPD est un corps législatif général qui ne tient pas compte du contexte spécifique des soins de santé. Ce pourquoi, il peut apparaître certaines contradictions entre ce que requiert ledit Règlement et ce qu'imposent les législations spécifiques des soins de santé. Dans la mesure où le RGPD constitue un tronc commun présentant des garanties effectives en termes de protection des données de santé, les dérogations expresses du droit national en ce qui concerne les données de santé priment sur les exigences du RGPD.</td></tr>
<tr><td>Art. 12-14</td><td>1. <u>Droit d'information</u> : lors de la collecte de données à caractère personnel, la personne concernée, à savoir le patient, doit recevoir les informations concernant le traitement de ses données, conformément aux articles 12.1, 12.5, 12.7, 13 et 14 du RGPD, par exemple par le biais d'un formulaire.</td><td><u>Informer le patient</u>. Le document de la tenue du DMI précisera les 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 réalisés.</td></tr>
<tr><td>Art. 15</td><td>2. <u>Droit d'accès</u> : 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.<br><br>Outre le droit de consultation directe de son dossier médical dans un délai de 15 jours maximum, le patient peut également 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. Au titre des exceptions figurent les annotations personnelles du professionnel de la santé ainsi que les données concernant des tiers. Comme le précise l'article 22 du Code de déontologie, le dossier médical est un outil de travail qui doit être à ce titre la propriété du praticien professionnel.</td><td>Prévoir la possibilité d'extraire du dossier médical les données relatives au patient pour lui en adresser une copie (la copie peut prendre différentes formes telles qu'une copie papier, une disquette, un message électronique <u>sécurisé</u> ou un document manuscrit).<br><br>Dans la mesure où les dossiers médicaux contiennent le plus souvent des notes personnelles qui ne peuvent pas être séparées des autres données concernant le patient en cas de demande de consultation ou de copie, tout DMI, hospitalier, de médecine générale ou paramédical devrait permettre que les notes personnelles, telles que les éléments concernant les tiers, les confidences du patient ou encore les hypothèses de diagnostiques, soient protégées, non transmissibles et non codifiables.</td></tr>
<tr><td>Art. 19</td><td>3. <u>Droit de rectification et d'effacement (droit à l'oubli)</u> : 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.</td><td><u>Droit de rectification</u> :<br><br>- Le prestataire/patient ne peuvent pendant cette durée de 30 ans retirer des éléments pertinents pour la tenue du dossier.</td></tr>
</table>

| | | |
|---|---|---|
| | A cette fin, le patient formule une demande à l'établissement de soins concerné. La rectification interviendra dans les deux mois de la demande.<br><br>**< ! >** En ce qui concerne le droit à l'effacement, ce dernier ne peut être pleinement efficace dans le cadre des soins de santé car le code de déontologie médicale précise en son article que les dossiers médicaux doivent être conservés pendant **30 ans** après le dernier contact avec son patient. Le droit à l'effacement ne s'applique qu'aux données à caractère personnel que le prestataire de soins ne peut plus traiter. | - Une rectification est possible sous la responsabilité du prestataire concerné.<br>- Toute rectification doit être réversible et dûment documentée.<br><br>**Pas de droit à l'effacement** : il est important d'informer le patient que son dossier médical est conservé jusqu'à 30 ans après l'interruption de la relation de soins. |
| **Art. 18** | **4. Droit à la limitation du traitement** : à nouveau, le droit à la limitation du traitement n'est pas absolu dans le contexte des soins de santé.<br><br>Le droit à la limitation s'applique uniquement aux données à caractère personnel dans les cas suivants :<br><br>- dans le cadre de l'exercice du **droit de rectification** pendant la période nécessaire au professionnel de la santé afin de contrôler l'exactitude des données.<br>- au titre **d'alternative à la suppression** des données à caractère personnel qui ont été traitées illicitement. | **Pas de droit absolu.** |
| **Art. 20** | **5. Droit à la portabilité des données** : le droit à la portabilité des données permet à la personne concernée 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.<br><br>L'article 20 du RGPD précise que la personne concernée, à savoir le patient, peut exercer son droit à la portabilité des données **lorsque cela est techniquement possible**. | **Droit à la portabilité des données si techniquement possible**. Mettre en place par exemple :<br><br>- une fonctionnalité pour extraire les informations pertinentes des bases de données<br>- un outil permettant la communication sécurisée 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,...) |

| | | |
|---|---|---|
| **Art. 21- 22** | **6. <u>Droit d'opposition</u>**: 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.<br><br>Toutefois, on remarquera que **la loi du 22 août 2002 relative aux droits du patient ne prévoit pas de droit d'opposition**. Pour le prestataire de soins, le dossier patient est surtout nécessaire dans l'optique d'offrir au patient une continuité des soins de qualité.<br><br>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. | **<u>Pas de droit de droit d'opposition</u>** à l'enregistrement et à la tenue à jour de données dans le dossier médical.<br><br>L'absence d'un dossier médical complet et tenu à jour comporte des risques. Il est clair qu'à l'égard des acteurs de soins, le dossier médical remplit une fonction médico-légale importante. |

Version mise à jour le 18 septembre 2018

Par Emeraude Camberlin, juriste