UNIVERSITE DE STRASBOURG
FACULTE DE CHIRURGIE DENTAIRE

Année 2019 N°74

THESE

Présentée pour le Diplôme d'Etat de Docteur en Chirurgie Dentaire
le 05 décembre 2019

par

RAYNAUD Caroline
Née le 10 mai 1994 à COLMAR

REGLEMENT GENERAL DE LA PROTECTION DES DONNEES : APPLICATION EN MEDECINE BUCCO-DENTAIRE

Président : Professeur Anne-Marie MUSSET

Assesseurs : Docteur Etienne WALTMANN

Docteur Florence FIORETTI

Docteur Damien OFFNER

Table des matières

INTRODUCTION

Au lendemain de la mise en application du Règlement Général sur la Protection des Données (RGPD) les professionnels de santé, eux-aussi concernés par ce texte, ont l'obligation de se mettre aux normes de la nouvelle réglementation applicable depuis le 25 mai 2018, c'est-à-dire *: « assurer une protection optimale des données de leurs patients et être en mesure de le démontrer en documentant leur conformité »*

Pour rappel, le Règlement Européen N°2016/679 du 27 avril 2016 vise à renforcer les droits des citoyens et donc des patients européens vis-à-vis de la protection de leurs données personnelles, dans un environnement numérique croissant et mondialisé.

Dans une première partie, il s'agira de reprendre l'historique concernant le secret médical et la mise en place de la confidentialité.

Dans la deuxième partie, un état des lieux sur les réglementations en vigueur jusqu'à l'application du RGPD sera présenté.

Enfin, il sera abordé en détail le Règlement Européen N°2016/679 du 27 avril 2016 ainsi que les conséquences de cette nouvelle réglementation pour l'exercice du chirurgien-dentiste.

Cette thèse a pour objectif de faire un état des lieux des exigences requises par la nouvelle règlementation et de guider les professionnels de santé afin qu'ils adaptent leurs procédures.

CHAPITRE 1 : CONFIDENTIALITE DES DONNEES A CARACTERE PERSONNEL ET SECRET MEDICAL

1. Définitions

1.1. Donnée à caractère personnel

Une donnée à caractère personnel, couramment appelé « donnée personnelle » correspond en droit français à toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement. Ainsi, le nom, le prénom, l'adresse postale, l'adresse mail, le numéro de sécurité sociale, sont des données personnelles, que ces données soient publiques ou confidentielles. (1–3)

1.2. Traitement des données personnelles

Un traitement des données personnelles correspond à toute opération portant sur des données personnelles, quel que soit le procédé utilisé. C'est-à-dire, l'enregistrement, l'organisation, la conservation, la modification, la transmission, etc. des données personnelles.

Un traitement ne correspond pas uniquement à un fichier ou une base de données. Il peut s'agir par exemple d'une installation de vidéosurveillance ou d'un système de paiement par carte bancaire.

Le dossier patient dans lequel sont regroupées les informations d'identité du patient, qu'il soit numérique ou papier, est donc un traitement de données personnelles. De la même façon que les échanges avec les professionnels de santé (prothésiste, laboratoire de biologie médicale, médecin généraliste etc.), la réalisation d'actes de télémédecine est un traitement de données personnelles.

Le chirurgien-dentiste doit assurer la protection des données personnelles de ses patients et doit à tout moment pouvoir prouver sa mise en conformité par rapport à la réglementation en vigueur.(2)

1.3. Le dossier patient

Le dossier du patient regroupe les informations administratives, médicales et paramédicales, formalisées et actualisées de chaque patient. Ces informations sont enregistrées pour tout patient accueilli, à quelque titre que ce soit, dans un établissement de santé. Il permet d'assurer la continuité des soins et leur traçabilité. (4,5)

Chaque praticien va créer pour chaque nouveau patient un dossier médical, celui-ci est enrichi lors du parcours de soin du patient, « Le dossier est une mémoire écrite des informations cliniques, biologiques, diagnostiques et thérapeutiques d'un malade, à la fois individuelle et collective constamment mise à jour » comme l'affirme FH Roger-France, médecin belge.

1.4. Secret médical

Caractéristique du domaine de la santé et perçu comme un mode de protection du patient, le « secret médical » est l'interdiction faite aux professionnels de santé de divulguer « tout ce qui a été vu, entendu ou compris » au sujet de leurs patients dans le cadre de leur exercice professionnel, conformément à la loi, sous peine de sanction pénales.(6)

2. Naissance du secret médical

2.1. Antiquité

Le secret médical est l'une des règles les plus anciennes de la pratique médicale. Il apparaît dès le siècle de Périclès vers 400 avant J.-C., au moment où la médecine s'émancipe, Hippocrate affirme dans son serment traduit par Littré :(7,8)

« Je jure par Apollon, médecin, par Esculape, par Hygie et Panacée, par tous les dieux et toutes les déesses, les prenant à témoin que (…) quoi que je voie ou entende dans la société pendant l'exercice ou même hors de l'exercice de ma

profession, je tairai ce qui n'a jamais besoin d'être divulgué, regardant la discrétion comme un devoir en pareil cas.»(9)

Le serment d'Hippocrate marque l'apparition de la notion de secret médical dans l'éthique médicale. (10,11)

Avec Hippocrate, pour bien soigner, l'examen du malade se fait désormais sur un examen de l'environnement et de l'intérieur des habitations du malade. « Sous le toit et dans la chambre à coucher » dira Cicéron, écrivain latin (106 av J.-C – 43 av J.-C). Le médecin doit surtout porter son attention sur la personne malade, l'interroger de façon indiscrète et si nécessaire en l'examinant au plus intime de son corps. Ces examens peuvent être tellement poussés qu'à l'époque, il est recommandé, d'éviter de les réaliser, autant que faire se peut, devant des tiers, proches ou même assistant du médecin afin de respecter la dignité des personnes examinées. Ainsi, l'examen touche à la vie privée des individus, le plus souvent mais pas toujours avec leur accord. Le fait de s'introduire dans l'intimité est reconnu comme indispensable à l'acte de soins, ce droit particulier est dérogatoire du droit commun. « En somme, 'il n'y a pas de soins de qualité sans confidences, pas de confidences sans confiances, pas de confiance sans secret »(8)

Dans l'Antiquité, le secret médical n'a pas d'existence juridique, voilà pourquoi les documents à ce sujet sont rares. (12)

Etymologiquement, le mot serment en français provient du latin *sacramentum,* issu du verbe « consacrer, rendre sacré » et de l'adjectif *sacer*, « sacré ». Dès l'origine, il y a une dimension sacrée à ce serment (13). Le serment d'Hippocrate est un engagement public, moral et à caractère religieux.

2.2. Moyen Age

Rares sont les manuscrits latins faisant part d'une nécessaire discrétion au Moyen-Âge. Et pour cause, la médecine se pratiquait dans les monastères depuis les invasions barbares. A cette époque, les soins sont donnés par des moines et des

clercs. Les notions d'individus et de vie privée ne sont pas celles que nous connaissons aujourd'hui. (11,13).

Selon l'historien, Mirko Gmerk (1924-2000) « C'est construire une légende que d'affirmer comme on le fait, qu'il existe une tradition ininterrompue du secret depuis Hippocrate jusqu'au Code Napoléon ». Ainsi, il n'y a pas assez de preuves pour affirmer une telle continuité morale de la profession.(11,12)

Les recherches de Mirko Grmek notifient que le secret médical n'est pas mentionné dans les textes juridiques importants, ni dans les ouvrages médicaux de l'époque. Pour exemple, l'école de médecine de Salerne, première école de médecine fondée en Europe au Moyen-Âge vers le IXème siècle, n'exprime rien au sujet du secret médical dans ses traités, y compris ceux donnant aux médecins des conseils sur la façon de se conduire, comme le « *De adventu medici ad aegrotum »*. On ne retrouve pas d'avantage la notion de secret dans les ouvrages arabes, comme celui d'Ishaq ibn Ali al-Ruhawi, médecin arabe. Et la prière de Maimonide (1138-1204), médecin juif, n'y fait aucune allusion. (11,14)

Les allusions faites au secret médical au Moyen-Age, sont rares mais existent. Dans une lettre adressée par Saint-Jérôme (347-420) à Népotien, neveu d'Héliodore, nous retrouvons une référence au serment d'Hippocrate « Hippocrate adjure ses disciples avant de les instruire, puis les forces à répéter son propre serment. Il exige qu'ils gardent le silence ; leur langage ; leurs attitudes ; leurs mœurs, il décrit tout avec soins »(12)

On retrouve aussi une référence au serment hippocratique et son secret avec le « serment » d'Assaph de Tibériade, médecin juif au VI^{e} siècle : « Vous ne divulguerez aucun des secrets qu'on vous a confiés et n'accepterez à aucun prix de nuire ou de détruire. »*(13). Mirko Gmerk mentionne également un médecin persan du Xe siècle, Ali ibn Abbas, qui dit que le médecin ne doit révéler aucun secret relatif à la maladie et au traitement. D'autres médecins arabes, comme Mahomet al-Gafiqi, (XI^{e} siècle) recommandent une discrétion rigoureuse. (11,12)

Aux XIII^{e} siècle, deux grands médecins, Lanfranc chirurgien italien (1250-1306) et Yperman chirurgien flamand (1260-1331), ont rédigé, des règles de conduite pour les chirurgiens. On ne retrouve rien sur le secret médical dans ces manuscrits historiques.

Les premiers statuts de la Faculté de Médecine de Paris, qui datent de 1270 ne parlent pas du secret médical.(11,12) Il faut attendre l'année 1598 pour lire dans les statuts rénovés : « Que personne ne divulgue les secrets (*arcana*) des malades, ni ce qu'il a vu, entendu ou compris ». (11,13)

Au Moyen-Âge, le secret n'est pas du domaine de la loi, il est d'ordre moral et individuel.(12)

La tradition hippocratique a survécu jusqu'à notre époque en grande partie grâce à la médecine arabe. (11,12)

2.3. Renaissance

A la Renaissance, on redécouvre un esprit plus individualiste, une promotion de la personne, qui entraîne davantage de respect pour la vie privée.

D'autre part, l'invention de l'imprimerie en 1454, a permis aussi de faciliter les échanges mais surtout elle a permis la conservation de nombreux documents.(12)

Le secret médical est mentionné dans plusieurs ouvrages en l'Europe. En Italie avec Gabriele Zerbi (1445-1505) anatomiste italien dans son traité « "*Opus perutile de cautelis medicorum »* (1495). Plus tard, avec Alessandro Benedetti (1452-1512) médecin italien, et son traité « De medici et aegri officio libellus » (1505). Et également dans les écrits de Codronchi, médecin italien, (1547-1628). En Espagne, dans le livre de Lobera de Avila médecin (?-1551). En France, dans les ouvrages de François Ranchin (1560-1641), chancelier de l'école de médecine de Montpellier. (11)

Nous pouvons citer Ahasverus Fritsch (1629-1701), avocat allemand, qui en 1684 explique que « Le médecin est en faute s'il ne se garde pas de ne pas propager les défauts secrets des malades » Nous notons une différence entre les auteurs

allemands et ceux de contrées latines.(11) En effet, le médecin Français François Ranchin dans son *Traité de la Peste* précise que les médecins doivent faire un rapport des malades tous les jours aux Supérieurs pour des raisons de santé publique.

Pour François Ranchin, le secret du médecin est toujours assimilé à celui du prêtre. Le médecin doit se taire parce qu'il est le « confesseur des maladies du corps ». Les théologiens font une distinction entre le secret médical d'ordre *naturel* et le secret du prêtre d'ordre *sacramental.* Cependant, le médecin baigne dans une atmosphère religieuse. Mêmes si les universités sont laïques, elles restent sous la coupe de l'Eglise. (12)

Le document le plus intéressant de l'époque est sans doute le « serment » du médecin juif Amatus Lusitanus (1511-1561). Dans ce document, traduit par les historiens Marcel Simon et Yeshayahou Leibowitz dans la Revue d'histoire de la médecine hébraïque, Amatus Lusitanus évoque très clairement le secret médical « *Je n'ai jamais divulgué à quiconque le secret qui m'a été confié* » et fait référence au serment d'Hippocrate : « Je me suis toujours proposé, comme exemple à imiter, Hippocrate et Galien, les pères de la médecine »(14)

A la Renaissance, le secret médical a pris un caractère religieux, il est comparé au secret de la confession. (11) Dans son exercice professionnel, le médecin a des obligations religieuses et le secret médical en est une.(12)

2.4. XVII^{e} et XVIII^{e} siècle

Durant cette période, le secret médical a gardé son caractère religieux mais des auteurs, petit à petit, en parleront dans des termes plus juridiques. On commence à voir naitre une morale professionnelle et laïque.

Deux médecins Français, Jean Bernier (1622-1698), et Jean Verdier (1735-1820), ont laissé des ouvrages traitant du secret.

En effet, Jean Bernier fut l'un des premiers auteurs à faire de véritables éloges du secret médical. Avec lui, le secret professionnel est vigoureusement défendu. Le

secret médical est « l'âme de la médecine » et il est d'une extrême importance : « Voici, dit-il l'âme de la médecine », parce que le médecin doit être l'ami fidèle du malade. « Le secret est le lien entre malade et médecin ». Bernier précise que les noms et qualités des malades doivent être cachés dans les publications scientifiques. Il professe une doctrine catholique du secret médical ; sa conception est celle du *secret absolu* (« même en jugement ») ; il admet toutefois une dérogation pour la déclaration des maladies contagieuses. (11,12,15,16)

Jean Verdier, avec sa double compétence de docteur en médecine et d'avocat à la Cour du Parlement de Paris était bien placé pour établir un tableau fidèle de la jurisprudence médicale en France de son temps. Il exprime une conception très absolue du secret médical. « *Les secrets qui sont confiés aux médecins sont des dépôts sacrés qui ne leur appartiennent point. La raison, la religion et les statuts leur enjoignent de garder sur eux un silence inviolable ; et les Cours Souveraines ont puni très rigoureusement ceux qui ont trahi leur ministère par des indiscrétions criminelles. L'obligation du secret est si forte chez eux, que la plus saine partie des théologiens, canonistes, jurisconsultes et médecins, disent qu'un médecin ne peut être tenu par le commandement d'aucun Supérieur à rendre compte de ce que son ministère lui a fait connaître* ».

En 1598, dans les statuts de la faculté de médecine de Paris, le secret devient une règle formelle. Le règlement de la confrérie des chirurgiens en 1699 contient « Vous jurez de garder le secret dans les choses de votre art qui vous seront confiées ». Il n'y a pas de doute, au XVII^{e} siècle, le secret professionnel est une notion officielle.

A partir de 1761, on imprime sur toutes les thèses de médecine à Paris comme à Montpellier la vieille formule agrée par le parlement : *Aegrorum arcana, visa, audita, intellecta, eliminet nemo* « Que personne ne divulgue les secrets des malades ni ce qu'il a vu, entendu et compris ».

Les premiers textes « déontologiques » dignes de cette appellation commencent à apparaitre au XVIIIe siècle, notamment en Angleterre avec John Gregory (1721-1773) médecin du roi. Il insiste sur le secret médical : « Un médecin

qui se veut gentleman doit être discret, secret et honnête » Thomas Percival (1740-1804) médecin à Londres s'intéresse aussi au secret médical et recommande aux médecins d'interroger les malades à voix basse ou sans témoins. Il ne remet cependant pas en doute que le médecin doit témoigner en justice, s'il est cité.

On retrouve dans de multiples ordonnances et édits une dérogation au secret. Les médecins sont tenus de dénoncer leur malade, on peut lire dans un texte de 1721 « Tous les médecins, chirurgiens, apothicaires, et autres personnes suivant des malades, qui s'apercevront de quelques signes de mal contagieux, seront tenus, à peine de vie, de l'aller déclarer dans le moment même aux maires, consuls, et autres officiers municipaux » Dans l'ordonnance de police de Paris du 4 novembre 1778, il est imposé aux maitres chirurgiens et à tout personne exerçant la chirurgie d'écrire les noms, qualité et demeure des blessés qui seront pansés ainsi que la qualité et les circonstances de ces blessures sous 24 heures sous peines d'amende et d'interdiction de l'exercice.

Ainsi, un médecin pouvait être condamné, du moins par certains tribunaux, pour avoir négligé de dénoncer ou refusé de témoigner. Il risquait beaucoup moins de l'être pour la violation du secret. Les archives à ce sujet sont pauvres. Mirko Gmerk, à la suite de Jean Verdier n'a relevé que quatre ou cinq procès instruits pour ce motif avant notre Code pénal. Le 8 novembre 1747, le parlement de Rouen condamnait à 10 livres d'amende et six années d'interdiction un médecin, qui avait mentionné l'affection vénérienne de son patient dans une réclamation d'honoraires impayés. Mais en regardant de près le jugement, l'accusation retenue n'était pas la violation du secret mais la déclaration d'injures et de calomnies. (12,15)

2.5. La Révolution

La Révolution a accentué les divergences entre le pouvoir exécutif et le corps médical. Les exigences de la police se sont agrandies et de l'autre côté, l'idée de la liberté personnelle et professionnelle s'affirme puissamment.

C’est à cette époque qu’est rédigé le Serment de Montpellier : « Admis dans l’intérieur des maisons, mes yeux ne verront pas ce qui s’y passe : ma langue taira les secrets qui me seront confiés »(15)

Le secret médical est finalement accepté par le Législateur et la France devient ainsi le premier pays au monde à introduire la protection du secret professionnel des médecins dans le Code pénal.

Le secret médical prend naissance juridiquement en 1810 avec l’article 378 du Code Pénal, alors appelé « Code des délits et des peines français ». « Les médecins chirurgiens et autres officiers de Santé, ainsi que les pharmaciens et autres officiers de Santé, les sages-femmes et toutes autres personnes dépositaires, par état ou profession, par fonctions temporaires ou permanentes, des secrets qu’on leur confie, qui hors les cas où la loi les oblige à se porter dénonciateurs, auront révélé ces secrets, seront punis d’un emprisonnement d’un mois à six mois, et d’une amende de 100 francs à 500 francs »

L’article 378 a un double intérêt : privé et public. Privé car c’est la protection de l’intimité des personnes, de leur pudeur, de la paix des familles ; le secret est une condition de la confiance de chaque malade, et la violation du secret est un abus de confiance. Un intérêt public : il importe à l’ordre public que tous les médecins soient discrets, que l’on puisse compter sur cette discrétion, que tout le monde puisse se confier à un médecin, et que nul n’hésite à recevoir des soins par peur d’être trahi. La violation du secret est aussi un délit de droit public.

Il est temps à présent de venir à une époque plus contemporaine en matière de protection de donnée à caractère personnel.

3. Naissance de la protection des données personnelles

Dans les années 1970, avec l’arrivée de l’informatique en France, on assiste à une accélération du traitement des informations. Le projet SAFARI imaginé par l’Etat, prévoyant de mettre en relation les informations administratives des usagers afin de faciliter les échanges, est dévoilé par le journal Le Monde en 1974. Les Français s’y

opposent, y voyant un fichage de leur donnée. De là est né une commission indépendante permettant d'évaluer et d'assurer que le développement de l'informatique se fera toujours dans le respect des libertés individuelles.

Cette commission aboutie à la « Loi Informatique et Liberté » et à la création de la Commission Nationale d'Informatique et des Libertés (CNIL)

Depuis, les avancées technologiques et les transformations numériques ont beaucoup influé sur la quantité et la sensibilité des données collectées, ne cessant d'augmenter (réseaux sociaux, smartphones, objets connectés.

En 2013, Edward Snowden alerte l'opinion en révélant que des données personnelles d'individus du monde entier sont collectées et exploitées par les services de renseignement américain. C'est dans ce contexte qu'est né le Règlement Général de la Protection des Données (RGPD).

CHAPITRE 2 : REGLEMENTATIONS EN VIGUEUR JUSQU'A LA MISE EN PLACE DU RGPD

1. Fondement juridique du secret médical et de la protection des données

Il n'existe pas de sources juridiques internationales au sujet du secret médical, il fait cependant l'objet de paragraphes spécifiques dans les textes de loi français.

1.1. Le Code Pénal

Article 226-13 du Code Pénal :

« *La 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, est punie d'un an d'emprisonnement et de 15 000 euros d'amende* »

Avec cet article, le Code Pénal ne désigne plus uniquement le secret médical, il désigne le secret professionnel en général. Celui-ci s'applique alors à toute profession dépositaire du secret d'autrui.

1.2. Le Code de la Santé Publique

Article R4127-206 du CSP

« Le secret professionnel s'impose à tout chirurgien-dentiste, sauf dérogations prévues par la loi. Le secret couvre tout ce qui est venu à la connaissance du chirurgien-dentiste dans l'exercice de sa profession, c'est-à-dire non seulement ce qui lui a été confié, mais aussi ce qu'il a vu, entendu ou compris. »

L'article R4127-207 du CSP concerne le personnel médical :

« *Le chirurgien-dentiste doit veiller à ce que les personnes qui l'assistent dans son travail soient instruites de leurs obligations en matière de secret professionnel et s'y conforment. »*

L’article R4127-208 du CSP fait référence aux documents médicaux :

« En vue de respecter le secret professionnel, tout chirurgien-dentiste doit veiller à la protection contre toute indiscrétion des fiches cliniques, des documents et des supports informatiques qu'il peut détenir ou utiliser concernant des patients.

Lorsqu'il utilise ses observations médicales pour des publications scientifiques, il doit faire en sorte que l'identification des patients soit impossible »

L’Article R4127-255 du CSP s’adresse aux chirurgiens-dentistes chargés de contrôles :

« Le chirurgien-dentiste chargé du contrôle est tenu au secret professionnel vis-à-vis de l'administration ou de l'organisme qui l'emploie.

Les conclusions qu'il lui fournit ne doivent être que d'ordre administratif sans indiquer les raisons d'ordre médical qui les motivent.

Les renseignements d'ordre médical contenus dans les dossiers établis par le praticien ne peuvent être communiqués ni aux personnes étrangères au service médical ni à une autre administration. »

L’Article R4127-263 du CSP concerne les témoignages dans le cadre d’une instruction, et précise que le secret professionnel doit être maintenu :

« Dans tous les cas où ils sont appelés à témoigner en matière disciplinaire, les chirurgiens-dentistes sont, dans la mesure compatible avec le respect du secret professionnel, tenus de révéler tous les faits utiles à l'instruction parvenus à leur connaissance »

L’article R4127-235 donne une dérogation au secret médical dans le cadre de sévices sur mineurs.

« Lorsqu'un chirurgien-dentiste discerne, dans le cadre de son exercice, qu'un mineur paraît être victime de sévices ou de privations, il doit, en faisant preuve de

prudence et de circonspection, mettre en œuvre les moyens les plus adéquats pour le protéger et, le cas échéant, alerter les autorités compétentes s'il s'agit d'un mineur de quinze ans, conformément aux dispositions du code pénal relatives au secret professionnel. »

Article L.1110-4 du Code de la Santé Publique

« *Toute personne prise en charge par un professionnel, un établissement, un réseau de santé, ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et du secret des informations le concernant* »

1.2.1. Le Code de Déontologie Médicale

Toutes les professions réglementées sont soumises à un Code régissant leur mode d'exercice selon le respect de principes déontologiques : c'est le Code de déontologie, le code de déontologie médicale appartient au code de la santé publique.

Le Code de déontologie des chirurgiens-dentistes a été incorporé au code de la santé publique (CSP) par le décret n° 2004-802 du 29 juillet 2004.

Le Code de déontologie des chirurgiens-dentistes est un ensemble de droits et de devoirs s'appliquant à la profession, à la conduite des chirurgiens-dentistes ainsi qu'aux relations entre patients et praticiens

1.3. Le Code de la Sécurité Sociale

Article L.162-2 :

« *Dans l'intérêt des assurés sociaux et de la santé publique, le respect de la liberté d'exercice et de l'indépendance professionnelle et morale des médecins est assuré conformément aux principes déontologiques fondamentaux que sont le libre choix, la liberté de prescription, le secret professionnel, le paiement direct des honoraires par le malade, la liberté d'installation…* »

1.4. Partage du secret

Il existe des situations dans lesquelles le partage du secret médical est autorisé entre professionnels de santé, notamment afin d'assurer la continuité des soins et la meilleure prise en charge du patient et conformément à l'article L. 1110-4 du Code de la santé publique :

« Toute personne prise en charge par un professionnel, un établissement, un réseau de santé ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et du secret des informations la concernant.

Excepté dans les cas de dérogation, expressément prévus par la loi, ce secret couvre l'ensemble des informations concernant la personne venue à la connaissance du professionnel de santé, de tout membre du personnel de ces établissements ou organismes et de toute autre personne en relation de par ses activités avec ces établissements ou organismes. Il s'impose à tout professionnel de santé ainsi qu'à tous les professionnels intervenant dans le système de santé.

Deux ou plusieurs professionnels de santé peuvent toutefois sauf opposition de la personne dûment avertie, échanger des informations relatives à une même personne prise en charge, afin d'assurer la continuité des soins ou de déterminer la meilleure prise en charge sanitaire possible. Lorsque la personne est prise en charge par une équipe de soins dans un établissement de santé, les informations la concernant sont réputées confiées par le malade à l'ensemble de l'équipe.

Les informations concernant une personne prise en charge par un professionnel de santé au sein d'une maison ou d'un centre de santé sont réputées confiées par la personne aux autres professionnels de santé de la structure qui la prennent en charge, sous réserve :

1° du recueil de son consentement exprès, par tout moyen, y compris sous forme dématérialisée. Ce consentement est valable tant qu'il n'a pas été retiré selon les mêmes formes ;

2° de l'adhésion des professionnels concernés au projet de santé mentionné aux articles L.6323-1 et L.6323-3.

La personne, dûment informée, peut refuser à tout moment que soient communiquées des informations la concernant à un ou plusieurs professionnels de santé.

Afin de garantir la confidentialité des informations médicales mentionnées aux alinéas précédents, leur conservation sur support informatique, comme leur transmission par voie électronique entre professionnels sont soumises à des règles définies par décret en Conseil d'Etat pris après avis public et motivé de la Commission nationale de l'informatique et des libertés. Ce décret détermine les cas où l'utilisation de la carte professionnelle de santé mentionnée au dernier alinéa de l'article L.161-33 du code de sécurité sociale est obligatoire. La carte de professionnel de santé et les dispositifs équivalents agréés sont utilisés par les professionnels de santé, les établissements de santé, les réseaux de santé ou tout autre organisme participant à la prévention et aux soins.

Le fait d'obtenir ou de tenter d'obtenir la communication de ces informations en violation du présent article est puni d'un an d'emprisonnement et de 15 000 € d'amende.

En cas de diagnostic ou de pronostic grave, le secret médical ne s'oppose pas à ce que la famille, les proches de la personne malade ou la personne de confiance définie à l'article L.1111-6 reçoivent les informations nécessaires destinées à leur permettre d'apporter un soutien direct à celles-ci sauf opposition de sa part. Seul un médecin est habilité à délivrer, ou à faire délivrer sous sa responsabilité, ces informations.

Le secret ne fait pas obstacle à ce que les informations concernant une personne décédée soient délivrées à ses ayants droit, dans la mesure où elles leur sont nécessaires pour leur permettre de connaître les causes de la mort, de défendre la mémoire du défunt, ou de faire valoir leurs droits, sauf volonté contraire exprimée par la personne avant son décès »

1.5. Dérogations

Le professionnel de santé n'est pas propriétaire du secret, il en est dépositaire. De ce fait, il ne peut en disposer librement. Les seules conditions exceptionnelles, dans lesquelles le secret médical n'est pas applicable, dans l'intérêt du patient ou de la santé publique, sont également précisément définies à l'article 226-14 modifié par la Loi n°2015-1402 du 5 novembre 2015 - art. 1 du Code pénal :

« *L'article 226-13 n'est pas applicable dans les cas où la loi impose ou autorise la révélation du secret. En outre, il n'est pas applicable :*

1° A celui qui informe les autorités judiciaires, médicales ou administratives de privations ou de sévices, y compris lorsqu'il s'agit d'atteintes ou mutilations sexuelles, dont il a eu connaissance et qui ont été infligées à un mineur ou à une personne qui n'est pas en mesure de se protéger en raison de son âge ou de son incapacité physique ou psychique ;

2° Au médecin ou à tout autre professionnel de santé qui, avec l'accord de la victime, porte à la connaissance du procureur de la République ou de la cellule de recueil, de traitement et d'évaluation des informations préoccupantes relatives aux mineurs en danger ou qui risquent de l'être, mentionnée au deuxième alinéa de l'article L. 226-3 du code de l'action sociale et des familles, les sévices ou privations qu'il a constatés, sur le plan physique ou psychique, dans l'exercice de sa profession et qui lui permettent de présumer que des violences physiques, sexuelles ou psychiques de toute nature ont été commises. Lorsque la victime est un mineur ou une personne qui n'est pas en mesure de se protéger en raison de son âge ou de son incapacité physique ou psychique, son accord n'est pas nécessaire ;

3° Aux professionnels de la santé ou de l'action sociale qui informent le préfet et, à Paris, le préfet de police du caractère dangereux pour elles-mêmes ou pour autrui des personnes qui les consultent et dont ils savent qu'elles détiennent une arme ou qu'elles ont manifesté leur intention d'en acquérir une.

Le signalement aux autorités compétentes effectué dans les conditions prévues au présent article ne peut engager la responsabilité civile, pénale ou disciplinaire de son auteur, sauf s'il est établi qu'il n'a pas agi de bonne foi. »

D'autre part, selon l'article R.11 et L.3113-3 du Code de santé publique, « les maladies vénériennes et contagieuses » doivent être obligatoirement déclarés.

Dans les cas de pathologies graves, l'article 35 du Code de déontologie médicale prévoit qu'un pronostic fatal ne doit être révélé qu'avec circonspection, mais les proches doivent en être prévenus sauf exception ou si le malade a préalablement interdit cette révélation ou désigné les tiers auxquels elle doit être faite.

Tableau 1 Dérogations légales au secret médical (7)

Obligatoires	Facultatives/autorisées par la loi
• Naissance • Décès • Maladies contagieuses graves • Soins psychiatriques : sur demande d'un tiers ou d'un représentant de l'État • Sauvegarde de justice • Accidents du travail et maladies professionnelles • Pensions civiles et militaire de retraite • Indemnisation de personnes victime d'un dommage • Dopage • Sécurité, veille, alerte sanitaire	• Sévices ou privations infligés à un mineur ou à une personne incapable de se protéger • Sévices permettant de présumer de violences sexuelles, etc. • Recherches dans le domaine de la santé • Evaluation de l'activité des établissements de santé • Dangerosité d'un patient détenteur d'une arme à feu

Ainsi, dans le cadre de l'exercice du chirurgien-dentiste, le secret médical peut-être partagé qu'avec :

- D'autres professionnels de santé et seulement dans l'intérêt thérapeutique du patient
- La famille, les proches du patient ou la personne de confiance, seulement en cas de diagnostic ou de pronostic grave

Quoi qu'il en soit, le partage de ce secret est systématiquement subordonné à l'absence d'opposition du patient.

1.6. Loi n°78-17 du 6 janvier 1978 :

Plus couramment appelée « Loi Informatique et Liberté », ce texte vise à protéger et réglementer la liberté de traitement des données personnelles « c'est-à-dire la liberté de ficher les personnes humaines ».

Cette loi a été modifiée profondément en 1995, transposée en droit Français par la loi du 6 aout 2004, modifiant notamment la notion d « informations nominatives » par « données à caractère personnel » permettant d'embrasser le plus de situations possibles. Cette transposition renforce le pouvoir d'enquête et de sanction de la CNIL.

Les notions importantes sont, entre autres, le droit d'information, le droit d'opposition, le droit d'accès et le droit de rectification.(3)

2. Dossier patient

2.1. Décret n° 2002 -637 du 29 avril 2002

L'obligation de la constitution d'un dossier hospitalier par les professionnels de santé et en particulier par les médecins n'est pas récente, elle est régulièrement rappelée par les textes législatifs et réglementaires. Le décret n° 2002-637 du 29 avril 2002 confirme dans son article 9 l'obligation de constituer un dossier pour tout patient hospitalisé ou consultant dans un établissement de santé public ou privé. Le décret n° 2003-462 du 21 mai 2003 reprend cette obligation dans son article R. 1112-2.

CHAPITRE 3 : LE REGLEMENT GENERAL DE LA PROTECTION DES DONNEES

1. Encadrement légal

1.1. Le Règlement Général de la Protection des Données

1.1.1. Définition

Le Règlement Général de la Protection des Données encadre le traitement des données personnelles sur le territoire de l'Union Européenne. Ce nouveau règlement européen s'inscrit dans la continuité de la Loi française Informatique et Libertés de 1978 et renforce le contrôle par les citoyens de l'utilisation qui peut être faites des données les concernant. Il harmonise les règles en Europe en offrant un cadre juridique unique aux professionnels. Il permet de développer leurs activités numériques au sein de l'UE.

1.1.2. Le texte

Après quatre années de négociations législatives, le texte a été définitivement adopté le 14 avril 2016 par le Parlement européen. Le règlement a été promu le 27 avril 2016, entrée en vigueur le 24 mai 2018 et applicable depuis le 28 mai 2018, dans les 28 Etats membres de l'Union Européenne.

Le RGPD abroge la Directive 95/46/CE sur la protection des données personnelles adoptée en 1995. Elle constituait jusqu'alors le texte de référence européen en matière de protection des données à caractère personnel.

1.2. Loi Informatique et Liberté

Le Règlement général sur la Protection des Données (RGPD) est entré en application le 25 mai 2018. La loi française Informatique et Libertés a été adaptée en conséquence par la loi sur la protection des données personnelles. La loi n° 2018-493 du 20 juin 2018 a été promulguée le 21 juin 2018, elle permet de mettre en conformité le droit national avec le cadre juridique européen. Ces deux textes constituent désormais le socle de la nouvelle réglementation sur la protection des données personnelles.

La nouvelle loi Informatique et Libertés permet l'application effective des textes européens, qui représentent un progrès majeur pour la protection des données personnelles des citoyens et la sécurité juridique des acteurs économiques.

Elle dote notamment la CNIL des pouvoirs nécessaires à l'exercice de ses missions, dans un contexte marqué par la reconnaissance de nouveaux droits aux citoyens et le renforcement de la responsabilité des opérateurs.

Elle organise l'articulation nécessaire des procédures internes de la CNIL aux nouveaux mécanismes de coopération européenne.

Elle exerce certaines des « marges de manœuvre nationales » autorisées par le RGPD, transpose en droit français la Directive « police-justice » et modifie certaines de ses dispositions pour les rapprocher de la lettre du RGPD.

La bonne compréhension du cadre juridique suppose de combiner désormais les deux niveaux, européen et national. Le RGPD s'applique directement en droit français : il remplace sur de nombreux points (droits des personnes, bases légales des traitements, mesures de sécurité à mettre en œuvre, transferts, etc.) la loi nationale.

1.3. Le chirurgien-dentiste et les données personnelles

Le chirurgien-dentiste dans sa pratique, collecte des données d'identification des patients, comme le nom, prénom, adresse, numéro de téléphone, information sur la vie personnelle du patient, sa couverture sociale pour tenir son dossier patient. Ces dossiers contiennent nécessairement des données personnelles sur les patients, ainsi le chirurgien-dentiste est concerné par le RGPD.

2. Mise en conformité : outils et moyens en pratique

2.1. Tenue du dossier patient

Comme dit plus haut, le chirurgien-dentiste doit assurer que l'usage des dossiers « patients » respecte les principes fondamentaux de la protection des données personnelles.(17)

2.1.1. Finalité du dossier médical

Les informations collectées dans les « dossiers patients » sont utilisées afin de permettre le bon déroulement de l'activité du chirurgien-dentiste. Elles sont indispensables à une activité de prévention, de diagnostic et de soins. Elles permettent d'assurer la prise en charge la plus idéale du patient. Ces informations permettent entre autres de :

- Gérer les rendez-vous
- Gérer les dossiers médicaux
- Editer des ordonnances
- Envoyer des courriers aux confrères
- Etablir et télétransmettre des feuilles de soins

Toute autre utilisation des informations collectées par le chirurgien-dentiste doit être réalisé avec précaution. Plus particulièrement, une utilisation personnelle ou commerciale des dossiers « patients » du chirurgien-dentiste est totalement prohibée.

2.1.2. Pertinence des données collectées

Les informations collectées par le chirurgien-dentiste doivent être adéquates, pertinentes et limitées à ce qui est nécessaire à la prise en charge du patient au titre des activités de prévention, de diagnostic et de soins.

Toutes les informations délivrées par le patient, dans le cadre des échanges entre le patient et le praticien, ne doivent pas nécessairement être intégrées dans le

dossier du patient. Seules celles ayant une utilité au suivi du patient peuvent être enregistrées et conservées.

La CNIL a estimé légitime la collecte de certaines catégories de données personnelles notamment :

- Les données d'identification : nom, prénom, date de naissance, adresse, numéro de téléphone ;
- Le numéro de sécurité sociale : uniquement pour l'édition des feuilles de soins et la télétransmission aux caisses d'assurances maladie ;
- Selon les contextes, la situation familiale : situation matrimoniale, nombre d'enfants ;
- Selon les contextes, la vie professionnelle : profession, conditions de travail ;
- La santé : historique médical, historique des soins, diagnostics médicaux traitements prescrits, natures des actes effectués, résultats d'examens de biologie médicale et tout élément de nature à caractériser la santé du patient et considéré comme pertinent par le praticien
- Informations relatives aux habitudes de vie :si collectées avec l'accord du patient et sans la stricte mesure où elles sont nécessaires au diagnostic et aux soins ;

A noter que si le praticien juge que d'autres informations paraissent pertinentes et nécessaire à son activité, il peut la collecter (ex : origine ethnique ayant une influence sur une pathologie déterminée ou un traitement médical etc.). En revanche, toutes informations sans lien avec l'objet de la consultation, non indispensable à la prise en charge doit être exclue. A titre d'exemple, d'autres informations sur la vie privée du patient (religion, orientation sexuelle) ne doivent pas figurer sur le dossier du patient.

2.1.3. Durée de conservation des dossiers patients

Un communiqué de L'ANAES sorti en 2000 préconisait une conservation des dossiers patients pour une durée de 30ans. Plus récemment, le Conseil National de l'Ordre des Chirurgiens-dentistes préconise, en l'absence de dispositions spécifiques

portant sur la durée de conservation des dossiers professionnels exerçant en libéral comme le guide de l'Agence de système informatique partagé de Santé (Asip Santé) un alignement de la durée de conservation en cabinet de ville sur celle prévue pour les établissements de santé (5,18–21):

- 20 ans à compter de la date de la dernière date de consultation du patient
- Si le patient est mineur et que ce délai de 20 expire avant son 28ème anniversaire, la conservation des informations le concernant doit être prolongée jusqu'à cette date ;
- Dans tous les cas, si le patient décède moins de 10 ans après sa dernière consultation, les informations le concernant doivent être conservées pendant 10 ans à compter de la date du décès
- En cas d'action tenant à mettre en cause la responsabilité du médecin, il convient de suspendre ces délais de conservation.

Les doubles des feuilles de soins doivent être conservé 3 mois.

2.1.4. Information des patients de la collecte de données

Les personnes dont les données de santé sont collectées, c'est-à-dire, ici les patients, disposent de droit, dont celui d'être informées. C'est une obligation prévue par le Règlement Général sur la Protection des Données (RGPD). Ainsi, dans notre cas, le chirurgien-dentiste est le responsable du traitement des données en conséquence, il est tenu de prendre les mesures appropriées pour informer les patients.(22)

L'information doit être délivrée de façon concise, transparente, compréhensible et aisément accessible. Elle doit pouvoir être abordable par le « grand public ».

Il faut aller à l'essentiel tout en faisant figurer l'ensemble des mentions obligatoires dans le document d'information. Le support de l'information doit être le plus intelligente possible (affiches avec des pictogrammes visuels, surlignage des informations essentielles…)

L'information délivrée doit être adaptée aux capacités cognitives de la personne.

Le contenu de l'information à délivrer varie selon deux hypothèses : les données de santé ont été collectées directement auprès de la personne concernée ou non (collecte indirecte des données)

Le support d'information est libre : par oral, par écrit ou par tout autre moyen (affichage dans les lieux de soins, dans les secrétariats, remise de documents écrits d'informations, etc.) (2)

L'information doit comporter impérativement les éléments suivants :

- Nom et coordonnées du praticien
- La finalité et la base juridique du traitement, y compris la finalité ultérieure
- Les destinataires des données ;
- La durée de conservation
- Les droits de la personne : accès, rectification, à certaines conditions effacement, limitation, opposition, introduction d'une réclamation auprès de la CNIL ;
- Caractère obligatoire des données fournies et des conséquences éventuelles d'un défaut de réponse ;
- Le cas échéant, utilisation ultérieure des données pour une finalité autre que celle pour laquelle les données ont été collectées (ex si un médecin souhaite utiliser ultérieurement les données à des fins de recherche)

Les patients disposent de droits et ils peuvent (23–36)

- Accéder aux données les concernant ;
- Rectifier ces données en cas d'erreur ;
- S'opposer au traitement pour des raisons tenant à leur situation particulière ;
- Effacer les données, dans certaines situations particulières (dossier patient conservé trop longtemps, données non adéquates, par ex)

Les demandes des patients portant sur leurs droits doivent être examinés dans un délai raisonnable. Ce délai est fixé à 8 jours et porté à 2 mois pour les informations datant de plus de 5 ans. (37)

2.1.5. Protection des données collectées

Il est impératif de mettre en place toutes les précautions utiles pour empêcher que des tiers non autorisés aient accès aux données de santé.

Seules certaines personnes sont autorisées à accéder aux données de santé des patients.

En pratique, il sera important de veiller au respect des règles relatives à l'échange et au partage de données entre professionnels. Par exemple, pour le personnel administratif, l'accès au dossier « patient » doit être limité.

En cas de recours à un prestataire de service pour assurer la maintenance d'un logiciel gérant les dossiers des patients, celui-ci n'est pas censé accéder aux données de santé à caractère personnel. Son rôle est purement technique. Les données doivent, en principe être chiffrées afin de permettre au technicien d'assurer ses missions sans pouvoir lire ces données.

En cas de stockage de dossier « patient » à un prestataire chargé d'en assurer la conservation, dans des serveurs à distance, celui-ci doit être un hébergeur agrée au certifié pour l'hébergement, le stockage, la conservation des données de santé conformément aux dispositions de l'article L. 1111-8 du Code de la Santé publique.

Il est impératif de réaliser un contrat de sous traitance dès que le praticien sollicite un prestataire (société de maintenance, hébergeur de donnée de santé agréé ou certifié). Ce contrat mentionne que le prestataire en tant que sous-traitant : (38)

- Ne traite les données à caractère personnel que sur votre instruction ;
- Veille à la signature d'engagements de confidentialité par le personnel ;
- Prend toutes les mesures de sécurité requises ;
- Ne recrute pas de sous-traitant sans votre autorisation écrite préalable ;

- Coopère avec vous pour le respect de vos obligations en tant que responsable de traitement notamment lorsque des patients ont des demandes concernant leur données ;
- Supprimer ou vous renvoie l'ensemble des données à caractère personnel à l'issue des prestations ;
- Collabore dans le cadre d'audits

2.1.6. Sécuriser l'accès aux données personnelles

Il est impératif pour le praticien de respecter les mesures prévues par les référentiels de sécurité et d'interopérabilité des données de santé (38–41)

2.1.6.1. Sécurisation du système informatique

Concernant la sécurisation du système informatique, le praticien devra respecter les grands principes suivants :

- Utilisation d'un mot de passe conforme aux recommandations de la CNIL, 12 caractères (chiffres, lettre majuscules et minuscules, caractères spéciaux), renouvelé régulièrement ;
- Verrouillage de la session informatique du praticien automatiquement après 30 minutes d'inactivité ;
- Antivirus à jour, pare-feu, application systématique des correctifs de sécurité du système informatique et des logiciels ;
- Sauvegardes régulières des données (sauvegarde au minimum hebdomadaire, avec conservation des sauvegardes mensuelles sur 12 mois glissants) et leurs conservations dans un lieu différent que le cabinet) ;
- Chiffrement des données avec un logiciel adapté ;
- Absence ou minimisation des connexions d'appareils non professionnels sur le réseau ;
- Authentification du praticien via la Carte Professionnel de Santé (CPS) ou tout moyen alternatif d'authentification forte.

La CPS doit rester strictement personnelle. En aucun cas, le code secret ne peut être communiqué au personnel (ex : assistante dentaire). Le praticien peut mettre en place une authentification forte pour son personnel au moyen d'un mot de passe à usage unique par exemple (identifiant, mot de passe et envoi d'un code à chaque connexion) ou au moyen d'une Carte de personnel d'établissement (CPE) à demander à la Caisse primaire d'assurance maladie.

Si le praticien utilise un logiciel gérant les dossiers « patients », et que celui-ci est accessible à distance et est hébergé par un prestataire, il doit s'assurer que ce tiers ou son sous-traitant est agréé ou certifié pour l'hébergement des données de santé conformément à l'article L 1111-8 du Code de la Santé Publique.

Si le praticien utilise des dossiers « patients » sous format papier, celui-ci doit s'assurer de leur sécurité (locaux sécurisés à l'abri du feu et de l'eau, armoire contenant les dossiers fermée à clé). En installant, par exemple des moyens spécifiques : système anti-incendie dédiée, surélévation contre d'éventuelles inondations, redondance d'alimentation électrique et/ou climatisation etc.

Afin de garantir une sécurité physique optimale, l'accès aux locaux doit être sécuriser, par exemple, une alarme anti-intrusion peut être installée. Les zones du cabinet peuvent être répertoriés en fonction de leurs risques.

2.1.6.2. Violation des données

En cas de violation des données (destruction, perte, altération, divulgation non autorisée de données à caractère personnel, accès non autorisé à de telles données), le praticien doit avoir les réflexes suivants :

- Analyser, dans la mesure du possible l'étendue du problème afin d'identifier les démarches à accomplir et éviter que cet incident se reproduise : qui a eu accès aux données ? quelle est l'origine du problème ? Les données ont-elles été envoyées à un tiers ? des données de santé sont-elles concernées ? Quelles mesures auraient pu empêcher l'événement ou quelles mesures peuvent en atténuer les conséquences ?

- S'il existe un risque pour les droits et libertés des personnes, notifier à la CNIL la violation de données. Cette notification détaillée contient les éléments suivants : nature de la violation, catégories et nombre approximatif de personnes concernées et d'enregistrements de données, nom et coordonnées du contact du cabinet, conséquences probables de la violation de données, mesures prises ou à prendre pour remédier à la violation, y compris, le cas échéant, mesures pour en atténuer les éventuelles conséquences négatives. Dans le cas d'une violation de données, un formulaire est à remplir sur le site de la CNIL « notifier une violation de données »
- Si la violation de données engendre un risque élevé pour les droits et libertés des personnes concernées, sur demande de la CNIL ou à l'initiative du praticien, celui-ci doit communiquer dans les meilleurs délais à la personne concernée cette violation exceptée si les données avaient été chiffrées rendant impossible leur lecture, ou si des mesure ultérieures prises garantissent que le risque élevé n'est plus susceptible de se matérialiser. Cette communication doit intervenir individuellement ou, si cela exige des efforts disproportionnés, par une communication publique. Elle contient à minima les éléments suivants : nom et coordonnées du contact du cabinet, conséquences probables, mesures prises ou à prendre pour remédier à la violation ; y compris le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.
- Inscrire cette violation de données à caractère personnel. Cette inscription peut se faire dans un registre spécifique, un tableau récapitulatif des incidents ou même au sein du registre des activités du traitement (sur le registre des activités de traitement)
- Le praticien doit contacter le plus rapidement possible son assurance et sa responsabilité professionnelle pour l'informer de l'incident.(40)

2.1.7. Sanctions

En cas de non-respect des obligations, le praticien s'expose à une sanction administrative de la CNIL, voire une sanction pénale.

La CNIL peut prononcer, en fonction de la gravité du non-respect de la réglementation, des amendes administratives allant jusqu'à 20 millions d'euros ou 4%

du chiffre d'affaires annuel. Les peines pénales maximales sont pour une personne physique, de 5 ans d'emprisonnement et de 300 000 euros d'amende, et pour une personne morale, de 1,5 millions d'euros d'amende.

Le praticien doit donc impérativement se mettre en conformité avec la réglementation et documenter cette conformité (registre des activités de traitement, traçabilité des violations de données, engagements de confidentialité du personnel, etc.)

Si la CNIL constate un défaut de conformité et met en demeure le praticien, celui-ci a encore la possibilité d'adopter les mesures nécessaires pour éviter une sanction.

Aussi, la CNIL a précisé que les contrôles réalisés dans les premiers mois d'application du RGPD, seront à visée pédagogique. L'essentiel est de pouvoir démontrer que le praticien s'engage dans une démarche de mise en conformité.

2.1.8. *Check list* des bonnes pratiques à respecter

- Limiter les informations collectées au nécessaire et utiliser les dossiers patients conformément aux finalités définies
- Tenir un registre à jour des « traitements »
- Supprimer les dossiers patients et de manière générale toute information ayant dépassé la durée de conversation préconisée
- Être en place les mesures appropriés de sécurité des dossiers « patients »
- Informer les patients et s'assurer du respect de leurs droits

2.2. Prise de rendez-vous électronique

Dans le cadre de son exercice, le chirurgien-dentiste peut être amener à faire appel à une plateforme de prise de rendez-vous en ligne ou à un prestataire de

permanence téléphonique. Ce tiers est amené à collecter des informations sur les patients prenant rendez-vous, notamment les éventuels motifs de consultation. (38,40)

2.2.1. Obligations du chirurgien-dentiste

Lorsque des rendez-vous sont pris, des données personnelles concernant les patients du chirurgien-dentiste sont collectées, enregistrées et utilisées, en particulier leur identité et leurs coordonnées personnelles.

Que la prise de rendez-vous soit assurée par le cabinet ou par un prestataire tiers de permanence téléphonique, ou une plateforme en ligne, le chirurgien-dentiste reste « responsable de traitement » des données d'identification des patients et des données de santé collectées lors de la prise de rendez-vous.

En tant que responsable de traitement, les obligations du chirurgien-dentiste sont identiques à celles applicables pour les dossiers « patients » : enregistrement des données strictement nécessaires, utilisation légitime des informations obtenues dans le cadre de la prise de rendez-vous, inscription dans le registre des activités de traitement, limitation des accès, sécurisation du planning et de son contenu, notification à la CNIL en cas de violation des données etc.

Si la consultation ne nécessite pas de préparation au préalable, les motifs de la consultation n'ont pas à être renseignés.

Contrairement aux dossiers « patients » qui ont une durée de conservation assez longue ; les données relatives à la prise de rendez-vous peuvent être supprimées lorsqu'elles ne sont plus nécessaires. Cette durée est à penser en fonction de l'activité du chirurgien-dentiste, tout en sachant que les dates des consultations médicales sont inscrites sur les dossiers des patients.

Le prestataire est également responsable de traitement des données relatives aux comptes créés par les patients et les professionnels de santé

Les droits des patients sont identiques à ceux précédemment évoqués pour les dossiers « patients ». Ils s'exercent auprès de vous de la même manière. Une information spécifique doit leur être délivrée.

2.2.2. Obligations du prestataire tiers gérant la prise de rendez-vous

Le prestataire tiers, que ce soit une plateforme de prise de rendez-vous en ligne ou un prestataire de permanence téléphonique, agit pour le compte du chirurgien-dentiste. Il est considéré comme sous-traitant en vertu de la réglementation. Il doit être guidé par la volonté de protéger au mieux les informations concernant les patients et de respecter la réglementions applicable. Il ne peut ainsi utiliser les informations concernant les patients que pour le strict accomplissement de ses missions.

Le prestataire doit notamment mettre en place des mesures techniques et organisationnelles nécessaires afin d'assurer la sécurité et la confidentialité des données confiées. Cela passe par la mise en place d'accès sécurisés, d'une politique d'habilitation (accès accordés aux personnes autorisées uniquement), d'un chiffrement des données (rendant impossible la lecture par un tiers ne possédant pas la clé de déchiffrement), d'une protection contre les attaques informatiques (anti-virus, etc.)

La relation avec le prestataire doit être formalisée par un contrat de sous-traitance. Le chirurgien-dentiste doit relire attentivement, avant toute signature, le contrat afin de vérifier que le prestataire (38)

- Ne traite les données à caractère personnel que sur son instruction ;
- Veille à la signature d'engagements de confidentialité par le personnel ;
- Prend toutes les mesures de sécurité requises ;
- Ne recrute pas de sous-traitant sans son autorisation écrite préalable ;
- Coopère avec lui pour le respect de ses obligations en tant que responsable de traitement, notamment lorsque des patients ont des demandes concernant leurs données ;
- Supprime ou lui renvoie l'ensemble des données à caractère personnel à l'issue des prestations ;
- Collabore dans le cadre d'audits ;

2.2.3. Sanctions

Les mêmes sanctions sont applicables en cas de non-respect de la réglementation dans le cadre de la prise de rendez-vous en ligne ainsi qu'en matière de gestion des dossiers « patients ».

2.2.4. *Check-list* de la bonne pratique

- Limiter les informations collectées par le prestataire et vérifie la conformité du prestataire avec la réglementation et notamment la présence des mentions obligatoires dans le contrat de sous traitance
- Tenir un registre à jour des « traitements »
- Informer les patients et s'assurer du respect de leurs droits
- Les praticiens ayant fait appel à une plateforme de prise de rendez-vous en ligne ou à un prestataire de permanence téléphonique sont tenus responsable des informations de leurs patients.

2.3. Messagerie électronique

Dans le cadre de son exercice, le chirurgien-dentiste est amené à échanger avec d'autres professionnels de santé et avec ses patients.

En tant que responsable de traitement et personne soumise au secret professionnel, vous devez assurer la protection des données que vous échangez. Cette protection nécessite le respect de règles particulières.

2.3.1. Système de messagerie sécurisée de santé

Le système de messagerie sécurisée de santé est un espace dématérialisé qui permet l'échange de données de santé en toute confiance entre professionnels de santé et, plus largement entre professionnels des secteurs sanitaire, social et médico-sociale. Il intègre également un annuaire commun et certifié de l'ensemble des professionnels habilités ou des structures au sein desquelles ils exercent.

De nombreux acteurs de la santé ont intégré ce système fondé, avant l'entré en application du RGPD, sur la réalisation d'un engagement de conformité à l'autorisation unique 037 (AU portant sur la mise en œuvre, par les professionnels et établissements de santé ainsi que par les professionnels du secteur médico-social habilités par une loi, de traitements de données de santé à travers un système de messagerie sécurisée).

Depuis l'entrée en application du RGPD, l'utilisation de la messagerie sécurisée est possible sans avoir à accomplir une formalité auprès de la CNIL. Pour autant, le traitement découlant de l'utilisation de la messagerie sécurise devra être inscrit sur votre registre des activités de traitement. A terme, il devra être conforme à un référentiel élaboré par la CNIL.

2.3.2. Mailiz :

Mailiz est une messagerie sécurisée proposée par les ordres de santé opérée par l'ASIP Santé et l'Assurance Maladie.

Cette messagerie est un service gratuit et accessible à tous les professionnels de santé, exerçant en structure ou bien à titre libéral. La messagerie est accessible sur un webmail.

La messagerie peut stocker jusqu'à 2Go d'e-mails et permets d'échanger des pièces jointes de 10Mo maximum. La messagerie donne accès à un annuaire certifié de professionnels de santé.

La Mailiz est accessible avec une Carte de Professionnel de Santé (CPS).

2.3.3. Messagerie standard

Le chirurgien-dentiste a une obligation de sécurisation de ses échanges, en particulier en ce qui concerne les données de santé, le passage par une messagerie sécurisée est donc imposé. Cependant l'utilisation d'une telle messagerie n'est possible qu'entre professionnels de santé.

Pour les échanges avec d'autres professionnels de santé (médecin généraliste, oncologue, prothésiste dentaire etc.) ou avec les patients, l'envoi de données de santé via une messagerie standard implique de :

- Chiffrer les pièces sensibles à transmettre. A ce sujet, il convient de se référer aux préconisations de la CNIL.
- Utiliser un protocole garantissant la confidentialité et l'authentification du serveur destinataire pour les transferts e fichiers, par exemple SFTP ou HTTPS, en utilisant les versions les plus récents des protocoles ;
- Garantir le secret nécessaire à la lecture du fichier (ex : mot de passe) en utilisant un canal de nature différente (ex : téléphone, SMS, etc.)

Ainsi, l'utilisation d'une messagerie ne chiffrant pas les données et hébergeant les données dans un pays ou auprès d'un prestataire qui ne garantit pas la protection des données conformément aux règles européennes est à proscrire.

Si la messagerie ne garantit pas la confidentialité des messages, le chiffrement des pièces jointes s'impose.

2.3.4. *Check-list* de la bonne pratique

- Utiliser un service de messagerie sécurisée de santé pour les échanges avec d'autres professionnels de santé ;
- En cas d'utilisation de messagerie électronique standard ou de messageries instantanées, le chirurgien-dentiste doit s'assurer que ces messageries sont bien sécurisées et adaptées à son utilisation professionnelle ;
- Chiffrer les pièces jointes en cas d'utilisation de messagerie standard sur internet ne garantissant pas la confidentialité des messages.

2.4. Téléphones portables et tablettes

Dans le cadre de son exercice professionnel, le chirurgien-dentiste peut être amené à utiliser son téléphone portable ou sa tablette pour consulter des informations relatives à ses patients ou communiquer avec d'autres professionnels de santé avec les patients.

2.4.1. Téléphones portables, tablettes et accès aux dossiers « patients »

Le téléphone portable et la tablette du chirurgien-dentiste peuvent être utilisés, dans un contexte professionnel, à conditions de respecter les règles de sécurité.

Il est fortement déconseillé de conserver des informations d'ordre médical dans la mémoire interne du téléphone portable ou de la tablette (cela permet d'éviter de graves conséquences pour les patients en cas de vol ou de perte du matériel). Néanmoins, en pratique, si le chirurgien-dentiste est amené à passer outre ce conseil, la conservation des données doit s'effectuer a minima dans le respect des règles de la sécurité suivants : utilisation de mot de passe conforme aux recommandations de la CNIL (12 caractères comprenant des majuscules, des minuscules, des chiffres et des caractères spéciaux), verrouillage automatique après un court délai, chiffrement des données sensibles. D'une manière plus générale, le chirurgien-dentiste doit éviter de prêter son téléphone ou sa tablette et de les laisser sans surveillance.

Afin de garantir la qualité et la confidentialité des données de santé à caractère personnel et leur protection, l'accès à distance aux dossiers des patients du chirurgiens-dentistes doit se faire conformément aux référentiels d'interopérabilité et de sécurité élaborés par l'ASIP santé. Ces référentiels sont approuvés par arrêté du ministre chargé de la santé, pris après avis de la CNIL. Dans l'attente de la publication des textes réglementaires permettant l'entre en vigueur de ces dispositions, la CNIL demande que l'authentification des professionnels de santé intervienne au moyen d'une carte de professionnel de santé (CPS) ou d'un dispositif équivalent agréé par l'ASIP santé.

En cas de déplacement, le praticien doit toujours vérifier, lorsqu'il consulte des informations relatives à ses patients, que son écran soit à l'abri des regards indiscrets.

L'utilisation de supports mobiles (clé USB, disque dur externe) est fortement déconseillée. Si malgré tout, le chirurgien-dentiste les utilise, il convient de chiffrer les données sensibles qui y sont conservées.

2.4.2. Téléphones portables et moyen de communication

Le chirurgien-dentiste peut utiliser son téléphone portable comme moyen de communication avec ses patients, d'autres professionnels de santé ou son personnel. Il doit s'assurer tout de même, que la conversation de nature professionnelle ne soit pas entendue par des personnes à proximité.

Il faut proscrire l'utilisation de communications orales, de messageries instantanées ou chat, via des applications reliées à internet et non sécurisées. Seule une application présentant des garanties suffisantes de protection de données peut être utilisée dans le cadre de l'exercice professionnel du chirurgien-dentiste. A défaut, aucune information relative à un patient ou à un professionnel de santé intervenant dans sa prise en charge ne peut être échangée.

2.4.3. *Check-list* des bonnes pratiques à respecter

- Sécuriser l'accès à son téléphone ou à sa tablette et à son contenu (mot de passe, chiffrement, etc.) ;
- Ne pas stocker d'informations médicales relatives à ses patients sur son portable ou sa tablette ;
- S'assurer que l'accès à son logiciel de dossiers « patients » sur son téléphone portable ou la tablette soit sécurisé ;
- Consulter son logiciel de dossiers « patients » avec précaution

2.5. La recherche

2.5.1. Obligations du chirurgien-dentiste dans le cadre d'études internes

Dans le cadre d'étude interne, le praticien collecte des données relatives à ses patients, à partir de données de santé obtenues à l'occasion de leur suivi.

Dans la mesure où ces études sont réalisées par le chirurgien-dentiste lui-même et destiné à son usage exclusif, aucune autorisation de la CNIL n'est nécessaire. Seul un avis favorable du Comité de Protection des Personnes (CPP) doit être recueilli préalablement à la mise en œuvre de la recherche si celle-ci implique la personne humaine.

En revanche, le chirurgien-dentiste devra :

- Réaliser une analyse d'impact relative à chaque recherche ou à un ensemble de recherches similaires si le traitement de données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Une réflexion doit être menée sur l'utilisation qui va être faite des données personnelles dans le cadre de la recherche, sur les risques qui peuvent en résulter en ce qui concerne les droits et les libertés des personnes concernées et sur le niveau de protection nécessaire ai regard de ces risques. La CNIL a mis en place un outil simple permettant de réaliser une analyse d'impact, accessible sur son site internet.
- Renseigner son registre des activités de traitement pour indiquer la nouvelle utilisation des données et les modalités et informer les patients de la réalisation de ces études. Il suffit d'ajouter une mention dans l'affichette d'information de la salle d'attente

Les règles de sécurité sont les mêmes que celles des dossiers « patients »

Les droits des personnes doivent également être respectés.

2.5.2. Obligations du chirurgien-dentiste dans le cadre de recherches médicales en partenariat avec un tiers ou nécessitant un recueil de données supplémentaires

Si le praticien participe à des recherches médicales en partenariat avec un tiers ou nécessitant un recueil de données supplémentaires, que ce soit un institut de recherche ou un établissement de santé, que les données soient collectées dans le cadre de soins ou spécifiquement pour la recherche, un processus spécifique s'applique en amont de la recherche.

Le promoteur de la recherche, la personne à l'initiative et qui porte le projet de recherche (qui n'est pas forcément celui qui réalise en pratique la recherche ou qui contribue à la recherche), doit en tant que responsable de traitement, si une méthodologie de référence existe, procéder à une déclaration de conformité à cette méthodologie de référence. A défaut, il doit obtenir une autorisation de la CNIL.

Les formalités à accomplir auprès de la CNIL sont réalisées par le responsable de traitement.

Si la recherche implique la personne humaine, le promoteur de la recherche ou celui qui porte le projet devra également vérifier, que la recherche relève d'une méthodologie de référence ou d'une demande d'autorisation, d'un avis favorable du Comité de Protection des Personnes (CPP).

Si la recherche n'implique pas la personne humaine et seulement pour celles relevant d'une demande d'autorisation, le promoteur ou celui qui porte le projet doit également obtenir un avis du Comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé (CEREES). Le dossier doit être adressé à l'Institut national des données de santé (INDS) qui assure le guichet unique.

Le promoteur ou celui qui porte le projet de recherche, en tant que responsable de traitement, doit réaliser une analyse d'impact si le traitement de données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques et renseigner le registre des activités de traitement.

Les droits des personnes concernées devront être respectés. Ils devront être informés en amont de la recherche, de l'utilisation de leurs données pour cette recherche, de ses finalités, de leurs droits à cet égard. Ils disposent notamment d'un droit d'accès et d'un droit d'opposition. La note d'information doit être fournie au praticien par le promoteur de l'étude.

2.5.3. *Chek-list* des bonnes pratiques

- Réaliser une analyse d'impact avant la réalisation d'études internes sur les données des patients si le traitement donné est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques
- Dans le cadre de recherches en partenariat avec un tiers, s'assurer que les recherches sont menées conformément à la réglementation
- Tenir à jour le registre des activités de traitement
- Informer les patients et s'assurer du respect de leurs droits

2.6. Le Dossier Médical Partagé

2.6.1. Définition

Le Dossier Médical Partagé (DMP) est un carnet de santé informatisé propre à chaque patient. Il contient les informations de santé du patient : traitements, résultats d'examens, allergie, etc. Il contribue ainsi à la continuité et à la coordination des soins en ville et à l'hôpital.

Le DMP est gratuit, non obligatoire, ouvert à toute personne bénéficiaire de l'assurance maladie.

2.6.2. Le DMP et le RGPD

Ce dossier est confidentiel, sécurisé et conforme aux exigences de la règlementation en vigueur relative à la protection des données personnelles et en particulier de la loi du 6 janvier 1978 modifiée par la loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles.

Les données collectées dans le cadre du DMP sont exclusivement les données renseignées volontairement lors de l'utilisation des formulaires mis à disposition sur ce site.

Ces informations sont réservées à l'usage exclusif de la Cnam. Elles ne seront aucunement vendues à des tiers ou échangées.

Les patients disposent d'un droit d'accès et de rectification aux données qui les concernent. Ils disposent également d'un droit d'opposition, en conformité avec la loi informatique et libertés décrite plus haut. Ces droits s'exercent auprès du directeur de la Caisse de rattachement de la personne concernée.

L'hébergement de l'espace d'information et d'accès au DMP est assuré par la société Worldline. Worldline fait appel à l'hébergeur Santeos (société filiale de Worldline), qui bénéficie d'un agrément pour une prestation d'hébergement des données de santé à caractère personnel collectées dans le cadre du DMP.

Le DMP est en partie alimenté par l'Assurance Maladie. L'historique de soins des 24 derniers mois du patient est renseigné de façon automatique. Les antécédents médicaux du patient (pathologie, allergie…), les résultats d'examens (radios, analyses biologiques…), les comptes rendus d'hospitalisations, sont renseignés de cette façon.

CONCLUSIONS

La protection des données de nos patients est une préoccupation d'actualité. L'informatisation généralisée de toutes les données, dont les données personnelles, représente un enjeu de taille dans le domaine de la santé. Les textes de loi, français et européen, se font mis en place afin de protéger l'utilisation des données personnelles des citoyens. Dans sa pratique, le chirurgien-dentiste est amené à traité des données personnelles, pour cette raison, il est concerné par le nouveau texte encadrant le traitement des données personnelles : le Règlement Général de la Protection des Données.

Historiquement, les premières notions de protection des données et de confidentialité font apparition avec le secret médical. Tout d'abord, avec Hippocrate, le secret médical avait pour « vocation » de mieux soigner le malade. Le secret médical était alors un engagement moral.

En traversant les époques et les civilisations, le secret médical a partiellement demeuré. En effet, celui-ci n'a pas toujours été retrouvé dans les textes médicaux fondamentaux, notamment au Moyen-Âge.

A la Renaissance, le secret médical a fait sa réapparition, il est mentionné dans plusieurs ouvrages importants. Le secret médical est alors un devoir moral, d'ordre naturel et religieux. A cette époque, la notion de dérogation au secret médical fait son apparition pour des raisons de santé publique.

Au XVII^{e} siècle, des auteurs parlent du secret médical en des termes plus juridique, on commence à voir naître une morale professionnelle et laïque. Dans les statuts de la Faculté de médecine de Paris datant de 1598, le secret devient une règle formelle. Il faut finalement attendre 1810 pour que le secret médical prenne naissance juridiquement avec l'article 37 du Code Pénal.

De façon plus contemporaine, le secret médical est encadré juridiquement et apparait dans plusieurs paragraphes de texte de lois françaises. Il est ainsi retrouvé dans le code pénal, le code de la santé publique et le code de la sécurité sociale. Le chirurgien-dentiste, sous peine de sanction, est tenu de ne pas révéler, sauf dérogations, les informations confiées, vues ou entendues dans l'exercice de sa

profession. Le chirurgien-dentiste doit veiller à toute indiscrétion à l'égard des documents patients. Il existe des cas particuliers, toutefois encadrés par les textes de lois permettant le partage du secret médical.

Dans les années 1970, avec la venue de l'informatique, une commission indépendante est née pour veiller à la sécurité numérique des données individuelles : c'est la « Loi informatique et liberté ».

Des événements récents ont alerté les individus sur le niveau de protection de leurs données personnelles. C'est dans ce contexte qu'a été créé le RGPD, permettant de garantir à tout un chacun une protection optimale, à tout instant, de leurs données. Nous l'avons vu, le chirurgien-dentiste, dans sa pratique est amené à collecter et traiter des données personnelles, pour ses patients et pour son personnel.

Pour être en accord avec ce nouveau texte, le chirurgien-dentiste doit veiller à respecter différentes règles.

Ainsi, le dossier patient, que celui-ci soit informatique ou papier, doit avoir une finalité. Les informations qui y sont collectées doivent être pertinentes et les dossiers être conservés dans une durée limitée. Le chirurgien-dentiste doit assurer la protection et la sécurisation à l'accès de ces données. La prise de rendez-vous électroniques et les messageries électroniques sont également encadrées par ce texte. Les échanges doivent être protégés et sécurisés. Aussi, les effets personnels du chirurgien-dentiste, tels que le téléphone portables ou tablette, s'ils contiennent des données de patients doivent être sécurisés. Des registres de traitement des données doivent être réalisés et mis à jour régulièrement.

La notion de secret médical et de confidentialité ont évolué avec les époques, les cultures et les civilisations, s'adaptant aux demandes de santé publique et aux demandes des citoyens. Aujourd'hui plus que jamais, les données personnelles sont des données à protéger. Le chirurgien-dentiste pourra se mettre aux normes en respectant le protocole décrit et en se faisant aider auprès de la CNIL.

SIGNATURES

A insérer

BIBLIOGRAPHIE

1. ARTICLE 4 DU RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016.

2. Professionnel | CNIL [Internet]. [cité 26 avr 2019]. Disponible sur: https://www.cnil.fr/professionnel

3. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

4. dossier_du_patient_-_fascicule_1_reglementation_et_recommandations_-_2003.pdf [Internet]. [cité 12 févr 2019]. Disponible sur: https://www.has-sante.fr/portail/upload/docs/application/pdf/2009-08/dossier_du_patient_-_fascicule_1_reglementation_et_recommandations_-_2003.pdf

5. ANAES. Le Dossier du Patient en Odontologie. 2000 mai.

6. article R.4127-4 du Code de la Santé Publique.

7. TARDIVO D, CAMILLERI F. Prévention et gestion du risque contentieux en odontologie. CdP; 2015. 280 p. (JPIO).

8. Hoerni B. Principes et pratiques d'un secret : le secret médical. In: Secrets professionnels. Autrement. 1999. p. 170-89.

9. Littré E. Œuvres complètes d'Hippocrate Tome quatrième. Paris: J-B Baillière; 1844. p. 628-632.

10. Malicier D, Feuglet P, Devèze F. Le secret médical : le dossier médical, la communication des pièces, les informations du malade. ESKA; 2004.

11. Gmerk MD. Le secret médical I Aperçu historique dans Le Concours Médical 85. 1963;(n°26):4177.

12. Villey R. Histoire du Secret Médical. Edition SEGHERS. Paris; 1986.

13. Lécu A. Le secret médical - Vie et Mort. Les Editions du Cerf. 2016.

14. Simon I. Revue d'histoire de la médecine hébraïque. oct 1972;n°99.

15. Gmerk MD. Le secret médical II Du secret absolu au secret partagé dans Concours Médical. 1963;(n°27):4283.

16. Bernier J. Essais de médecine où il est traité de l'histoire de la médecine et des médecins. Du devoir des médecins à l'égard des malades, et de celui des malades à l'égard des médecins. Paris: Simon Langronne; 1689.

17. ARTICLE 5 DU RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016.

18. Code de la santé publique - Article R1112-7. Code de la santé publique.

19. Code de la santé publique - Article R1112-2. Code de la santé publique.

20. Dentistes ON des C. Actualités [Internet]. 2008 [cité 1 mai 2019]. Disponible sur: http://www.ordre-chirurgiens-dentistes.fr/actualites/annee-en-cours/actualites.html?tx_ttnews%5Btt_news%5D=459&cHash=1d05e33d0c5eb4ee3bdfa4a8970e53b2

21. Agence Nationale d'Accréditation et d'Evaluation en Santé (ANAES). Acta Endosc. avr 1998;28(2):151-5.

22. ARTICLE 13 DU RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016.

23. ARTICLE 15 DU RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016.

24. ARTICLE 16 DU RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016.

25. ARTICLE 17 DU RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016.

26. ARTICLE 18 DU RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016.

27. ARTICLE 19 DU RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016.

28. ARTICLE 20 DU RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016.

29. ARTICLE 21 DU RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016.

30. ARTICLE 22 DU RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016.

31. ARTICLE 23 DU RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016.

32. Article 39 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

33. Article 40 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

34. Article 41 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

35. Article 42 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

36. Article 43 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

37. Article L.1111-7 du Code de la Santé Publique.

38. ARTICLE 28 DU RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016.

39. Article L. 1110-4-1 du Code de la Santé Publique.

40. ARTICLE DU 33 RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016.

41. ARTICLE 34 DU RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016.