Erwann Picart

Doctorant au Laboratoire IODE (UMR CNRS 6262) ; Faculté de droit de l'Université de Rennes 1

erwann.picart@univ-rennes1.fr

Tirés à part : E. Picart

Le règlement général européen sur la protection des données personnelles et la relation médecin-patient

Résumé

Le médecin est au cœur de la récolte et du traitement des données de santé. De ce fait, le nouveau règlement général sur la protection des données personnelles lui est applicable. D'un côté, le médecin est soumis à des obligations concernant le traitement des données de santé, alors que de l'autre, le patient détient des droits sur celles-ci.

• **Mots clés**
données à caractère personnel ; protection des données.

Abstract. The general European regulation on the protection of personal data and the doctor-patient relationship

The doctor is at the heart of harvesting and processing health data. As a result, the new general regulation on the protection of personal data is applicable to it. On the one hand, the doctor is subject to obligations concerning the processing of health data, while on the other hand, the patient has rights over them.

• ***Key words***
personnaly identifiable; cyber security.

DOI: 10.1684/med.2018.382

D'un contrôle a priori à un contrôle a posteriori

Le règlement général relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après RGPD) est entré en vigueur le 25 mai dernier[1]. Bien que ce règlement soit d'application directe devant les juridictions françaises, le législateur a dû modifier la loi informatique et liberté, d'une part car ce règlement met en place une nouvelle façon de penser la protection des données personnelles, et d'autre part car il laisse aux États quelques marges de manœuvre.

Dans un premier temps, le règlement change le paradigme classique de la protection des données personnelles. La loi informatique et libertés [1] et la directive de 1995 [2] avaient opté pour une logique de contrôle a priori : le responsable devait déclarer le traitement à la Commission Informatique et Liberté (CNIL) avant de le mettre en œuvre. Cette obligation de déclaration préalable a été supprimée pour laisser place à un principe « d'accountability » [3], soit un principe de responsabilisation des détenteurs de traitement. C'est désormais au responsable de mettre en œuvre les obligations découlant du règlement. D'un contrôle a priori, l'autorité de contrôle exerce dorénavant un contrôle a posteriori et peut, à tout moment, demander au responsable de démontrer qu'il respecte ces obligations. Ce régime s'applique dès lors qu'un responsable met en œuvre un traitement de données à caractère personnel.

Pour être considéré comme responsable de traitement, il faut mettre en œuvre un traitement de données à caractère personnel. La définition retenue par le RGPD est vaste. Ainsi, « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel [. . .]* » [4] est un traitement de données à caractère personnel. Par conséquent, le responsable de traitement est la personne physique ou morale qui détermine l'objectif et les moyens du traitement [5]. En application de ces textes, le médecin est donc considéré comme un responsable de traitement dès lors qu'il collecte, enregistre, utilise et stocke des données relatives aux patients.

Dans un second temps, le règlement laisse aux États quelques marges de manœuvre [6]. Les données de santé en font partie. Toutefois, le choix effectué par le législateur français d'utiliser cette marge de manœuvre n'a

[1] Tous les textes législatifs cités sont disponibles sur www.legifrance.gouv.fr, ou également, pour la loi Informatique et libertés et le RGPD sur : www.cnil.fr.

pas abouti à un régime entièrement spécifique aux données de santé du patient.

La donnée de santé : une catégorie particulière de donnée personnelle

Le règlement européen retient une définition extensive de la donnée à caractère personnel. Synthétiquement, une donnée personnelle est toute information qui se rapporte ou peut-être rapportée directement ou indirectement à une personne physique. Le RGPD donne des illustrations allant du plus proche au plus éloigné de la personne [7]. Aux côtés de cette définition générale de la donnée personnelle, le règlement réserve un régime spécifique à certaines catégories de données dites sensibles.

Si les données personnelles « ordinaires » peuvent faire l'objet d'un traitement respectant les obligations issues du règlement, il en va autrement des données sensibles. Le traitement de ces données fait l'objet d'une interdiction de principe en raison du risque accru pour les droits et libertés de la personne que représentent ces données. Selon l'article 9, une donnée sensible est une donnée qui « *révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique* ».

L'interdiction de principe est assortie de multiples exceptions. Les données sensibles pourront notamment être traitées avec le consentement explicite de la personne [8], ou si « *le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique [. . .]* » [9].

Autre exception, et non des moindres, les données sensibles, notamment de santé, pourront faire l'objet d'un traitement par un professionnel de la santé soumis au secret professionnel aux fins de diagnostics médicaux ou de la gestion des systèmes et services de soins de santé [10].

Le médecin, puisqu'il est soumis au secret médical en application de l'article R4127-2 du Code de la santé publique [11], s'inscrit donc dans les exceptions au principe d'interdiction de traitement des données sensibles.

Ce constat n'est pas altéré par la lecture de la nouvelle loi informatique et liberté [12]. Si le législateur français a effectivement opté pour un régime spécifique concernant les traitements de données à caractère personnel dans le domaine de la santé, l'article 53 de la loi exclut d'emblée de ce régime spécifique certains traitements de données sensibles, notamment ceux aux fins de diagnostics médicaux ou de la gestion des systèmes et services de soins de santé. L'exception à l'exception nous ramenant au principe, le médecin est bien un responsable de traitement de données sensibles.

À l'occasion de ce traitement, deux acteurs émergent. D'un côté le médecin, en tant que responsable de traitement doit respecter les principes du RGPD (I) tandis que de l'autre le patient détient des droits sur ses données (II).

Les obligations du médecin responsable du traitement de données sensibles

Nous examinerons les obligations du médecin en matière de protection des données à caractère personnel d'un point de vue chronologique. De cette manière, un nouvel acteur va apparaître : le sous-traitant. Voyons d'une part le traitement antérieur à la consultation (A), puis le traitement qui découle de la consultation (B).

Le traitement précédant la consultation

Aux côtés des solutions traditionnelles de la prise de rendez-vous via un secrétariat, se développent des solutions décentralisées. Si ces solutions proposées par des start-up font miroiter un gain de temps et d'argent [13], celles-ci ne sont pas sans conséquences sur la protection des données personnelles. En confiant la gestion des rendez-vous, de l'agenda et de toute autre fonction à un tiers, le médecin fait apparaître un autre acteur au sein du régime de protection des données personnelles : le sous-traitant.

Le sous-traitant est défini par le RGPD comme la personne physique ou morale qui traite des données à caractère personnel pour le compte du responsable [14]. Le texte est sans équivoque : le sous-traitant rend compte au responsable de la gestion des données personnelles. Les données récoltées par le sous-traitant dans le cadre de la prise de rendez-vous sont non seulement considérées comme des données personnelles, mais peuvent également, suivant le niveau de précision demandé sur leur site, être considérées comme des données sensibles. S'il revient au sous-traitant de respecter les obligations issues du règlement, le médecin doit également y être attentif car il sera responsable de toute défaillance dans le traitement et la protection des données de ses patients.

La question de l'hébergement et du traitement des données de santé par des prestataires de services fait l'objet d'une attention particulière depuis la loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé. L'article L1111-8 du Code de la santé publique exigeait déjà de l'hébergeur des données de santé qu'il soit « agréé à cet effet » [15]. La version actuelle diffère sur deux points :

– *Le premier réside dans le consentement du patient*. En effet, ce dernier devait être recueilli avant d'organiser le transfert de ses données de santé hors de l'établissement. Les réformes successives ont achevé de supprimer la condition de consentement pour la remplacer par une obligation d'information assortie d'un droit d'opposition du patient pour motif légitime [16].

– *Le deuxième réside dans la procédure à suivre qui est désormais une procédure de certification et non plus d'agrément.* Alors que l'agrément répondait à une procédure déclarative, la certification est désormais dans les mains d'un organisme certificateur accrédité [17]. Ce certificat devrait, à terme, renforcer la sécurité autour de l'hébergement des données de santé. Une fois certifié, le sous-traitant sera considéré comme un professionnel intervenant dans le système de santé. Il sera alors soumis à la règle du secret [18]. Toutefois, la certification ne signifie pas une exonération de responsabilité ni du sous-traitant, ni du médecin. En raison du contrat qui doit le lier à l'hébergeur, ainsi que de la qualité de responsable de traitement, le médecin sera tenu responsable en cas de traitement non conforme [19].

Illustration : Lorsqu'un médecin généraliste décide de faire gérer la prise de rendez-vous par un service en ligne tel que « Doctolib.fr » ou « Rdvmédicaux.com », il doit s'assurer de la bonne utilisation et de la bonne gestion des données de santé. En l'occurrence, les entreprises citées font appel à des hébergeurs qui ont obtenu l'agrément.

Avant d'examiner les obligations du médecin en matière de protection des données personnelles, il nous faut tout de même évoquer le contexte numérique dans lequel se déroule cette prise de rendez-vous en ligne.

De façon simpliste, on pourrait voir ici une relation à trois personnes entre le patient, le médecin et l'intermédiaire. Mais sur Internet, les apparences sont parfois trompeuses et des tiers s'interposent à travers diverses techniques (cookies et autres trackers). Cette multiplication d'acteurs va de pair avec la logique lucrative qui sous-tend l'offre de service. Sans en développer tous les aspects, il nous semble que la présence de ces acteurs est un point non négligeable pouvant mettre à mal le régime de protection des données de santé. De prime abord, le caractère anodin des informations renseignées lors de la prise de rendez-vous acquiert une tout autre dimension lorsque l'acteur qui les intercepte est en mesure de les recouper avec d'autres informations. Pour exemple, on peut penser à un utilisateur du navigateur Chrome (propriété de Google), utilisant le même moteur de recherche avant de prendre rendez-vous en ligne avec un médecin. L'entreprise aura alors un ensemble de données qui pourrait être qualifié de données sensibles sans pour autant qu'il ne soit soumis à aucune certification, ni aucune règle du secret. C'est ce contexte numérique, brossé à grands traits, qui pourrait poser problème s'il n'était pas pris en compte dans l'élaboration du régime de protection des données de santé.

Les obligations auxquelles doit répondre le traitement sont identiques lorsqu'il a lieu précédemment à la consultation ou lorsqu'il en est issu.

Le traitement issu de la consultation

Les obligations relatives au traitement de données personnelles s'imposent à chaque responsable de traitement. Le médecin doit donc veiller à ce que le traitement qu'il opère soit conforme aux obligations du RGPD.

La spécificité du traitement opéré par le médecin sur les données de santé réside dans la forme qu'il adopte : le dossier patient ou dossier médical. Ce dossier n'est mentionné dans le Code de la santé publique que dans la partie réglementaire. L'article R1112-2 énonce qu'un « *dossier médical est constitué pour chaque patient hospitalisé dans un établissement de santé public ou privé* ». Les praticiens libéraux ne sont pas visés par ce texte. En revanche, le Code de déontologie médicale, dans son article 45 énonce qu'« *Indépendamment du dossier médical prévu par la loi, le médecin tient pour chaque patient une fiche d'observation qui lui est personnelle ; cette fiche est confidentielle et comporte les éléments actualisés, nécessaires aux décisions diagnostiques et thérapeutiques* ». Pis, l'absence d'établissement de fiche d'observation est considérée par le Conseil national de l'ordre des médecins (CNOM) comme une faute [20]. Le terme de « dossier médical » n'est pas non plus expressément visé. Toutefois, le CNOM commente cet article en indiquant clairement que ces fiches d'observations, si elles n'ont aucun cadre formel, sont effectivement considérées comme des dossiers professionnels [21]. Par la même, ce dossier tenu par les médecins doit répondre aux principes inscrits dans le RGPD.

Illustration : Les informations inscrites sur les fiches personnelles servant à suivre les patients dans l'ordinateur du praticien, quelle que soit leur forme, (fichier Word, dossier spécifique…) seront qualifiées de données à caractère personnel.

Les principes entourant le traitement de données sont listés à l'article 5 du RGPD. Le traitement doit être loyal, licite et transparent. Il doit répondre à une finalité déterminée et la collecte doit être proportionnelle à cette finalité. Détaillons-les.

– *Tout d'abord, la notion de loyauté* n'est présente qu'à l'article 5 et n'est ni détaillée, ni expliquée. On peut la rapprocher de celle juridique de bonne foi dans l'exécution du contrat qui lie le médecin au patient [22]. Au-delà de la relation contractuelle, on peut retrouver des notions connexes au sein du Code de déontologie médicale avec les principes de moralité, de dévouement, de probité [23], ou encore avec le respect du secret [24].

– *Ensuite, la licéité* se rapporte au fondement sur lequel repose le traitement. L'article 6 du RGPD liste ainsi six conditions suivant lesquelles le traitement sera licite. Sans les détailler une à une, il nous semble que la matière médicale et la protection des données personnelles ont cela de commun que le consentement de la personne en est un point central [25]. Pour être valable, le consentement devra alors être libre, spécifique à un traitement, éclairé par les informations fournies par le médecin et univoque [26].

– *La transparence,* quant à elle, est liée aux informations concernant le traitement. Ces dernières doivent être accessibles, aisément compréhensibles et formulées dans des termes clairs et simples [27]. La CNOM et la CNIL ont d'ailleurs établi un exemple de notice d'information pour la gestion d'un cabinet médical [28].

– *La finalité du traitement* lorsqu'il s'agit de données de santé est circonscrite par le texte européen. En effet, du fait de l'interdiction de principe, le traitement des données de santé par le médecin devra être nécessaire « *aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale* » [29]. De manière plus pragmatique, les traitements de données qui permettent l'édition d'ordonnance et l'établissement des feuilles de soin sont considérés comme nécessaires [30].

Pour finir, la collecte des données doit être proportionnelle à cette finalité. Selon le principe de minimisation des données [31], le praticien ne devra collecter que ce qui est nécessaire aux finalités précitées. Conjointement, le CNOM et la CNIL estiment que la collecte des données d'identification (nom, prénom, date de naissance, adresse et numéro de téléphone) et du numéro de sécurité sociale est nécessaire. En revanche, la collecte des informations familiales et professionnelles, ainsi que celles relatives habitudes de vie, dépendra du contexte [32].

Le non-respect de ces principes est assorti de sanctions

En la matière, le texte européen accroît le montant des sanctions possibles. Au maximum, le responsable d'un traitement non conforme pourra subir une amende administrative de 20 000 000 d'euros ou 4 % du chiffre d'affaires mondial. Les cibles de telles sanctions sont aisément identifiables et il semble peu probable que la CNIL inflige de telles sanctions à une personne physique isolée. L'article 83 du RGPD énonce d'ailleurs qu'il reviendra à la CNIL d'adapter la sanction pour qu'elle soit « *effective, proportionnée et dissuasive* ». A nouveau, en qualité de responsable de traitement, le médecin peut être sanctionné alors même qu'un sous-traitant est en charge de la conservation des données de santé. C'est au médecin de s'assurer que toutes les mesures sont prises pour que le traitement soit conforme, notamment en termes de sécurité [33].

Aux côtés du médecin, et le cas échéant du sous-traitant, l'autre protagoniste en matière de donnée de santé est le patient.

Le patient, détenteur de droits sur ses données

On peut déceler une similitude entre la matière médicale et celle de la protection des données. D'un individu soumis à une autorité paternaliste, le médecin d'un côté, et la CNIL de l'autre, les modèles ont évolué vers un accroissement des droits de la personne. Ainsi, si la plupart des droits du patient sur ses données sont présents dans notre système juridique depuis la loi informatique et liberté de 1978 (A), de nouveaux droits ont été ajoutés par le texte européen (B).

Les droits classiques du patient sur ses données

Dès la loi de 1978, l'individu avait des droits sur ses données. Les articles 39 et 40 indiquent que l'individu a un droit d'accès, de modification, rectification et de suppression sur ses données. Toutefois, ces droits sont conditionnés. En effet, la rectification est conditionnée à des données inexactes, incomplètes ou équivoques. De même, la suppression n'est possible que lorsque les données ne sont plus utiles aux finalités affichées, ou lorsque ces finalités ont été accomplies. Ce droit ne sera donc pas effectif lorsqu'une disposition légale impose la conservation des données au-delà des finalités originelles. L'élément central de ce dispositif reste donc le droit d'accès de l'individu sur ses données. En quelque sorte, ce droit d'accès conditionne tous les autres. C'est un préalable à leur exercice.

De la même manière, le Code de la santé publique donne à toute personne un droit d'accès aux informations concernant sa santé [34]. Il faut lire cette disposition conjointement à l'article R1112-2 du Code de la santé publique qui impose aux établissements de santé public ou privé l'ouverture d'un dossier médical. Vingt éléments doivent être répertoriés dans ce dossier [35]. En résumé, « *tout document inclus physiquement dans le dossier médical en vue d'y être conservé doit être communiqué, quelle que soit la forme sous laquelle il se présente* » [36].

Une question demeure néanmoins. Modifié par un décret de 2012 [37], l'article 45 du Code de déontologie énonce que « *les notes personnelles du médecin ne sont ni transmissibles, ni accessibles au patient et aux tiers* ». À l'inverse, l'article L1111-7 du Code de la santé publique précise que le droit d'accès s'exerce sur toute information concernant la santé du patient. Il semble ici y avoir une contradiction entre l'article 45 du Code de déontologie et l'article L1111-7 du Code de la santé publique. Les notes personnelles du médecin sont nécessairement liées à la

santé du patient et devraient donc pouvoir être communiquées au patient. Ce même article 45, en son second paragraphe, puisqu'elles n'en sont pas expressément exclues, va dans le sens d'une communicabilité des notes personnelles lorsqu'elles le sont à un second médecin en charge de la continuité des soins.

Quid alors de leur communicabilité au patient ? À regarder la jurisprudence, l'article L1111-7 du Code de la santé publique semble prévaloir. Antérieurement au décret de 2012, la Cour administrative d'appel [38] ainsi que la Commission d'accès aux documents administratifs [39] ont estimé que les documents manuscrits font partie du dossier médical et sont donc communicables de plein droit. Si certains voient dans l'article 45 du Code de déontologie médicale la solution à ce conflit [40], d'autres (et c'est notre cas) voient dans la hiérarchie des normes la solution. Le règlement étant inférieur à la loi, le Code de déontologie devrait céder devant l'article L1111-7 du Code de la santé publique, voire être modifié [41].

La loi informatique et liberté nous semble également aller dans ce sens. Le droit d'accès de l'article 39 s'applique à toute information détenue par le responsable pouvant être reliée directement ou indirectement à une personne physique. Les notes personnelles du médecin, dès lors qu'elles sont appelées à figurer dans un fichier en lien avec l'individu, sont considérées comme des données à caractère personnel. S'il en fait la demande, le patient devrait donc avoir accès à ces données.

Illustration : Si un patient exerce son droit d'accès, le médecin devra lui communiquer toutes les informations inscrites dans son dossier médical ainsi que les notes personnelles qu'il a pu rédiger.

Aux côtés de ces droits classiques, de nouveaux droits ont été intégrés au sein de la protection des données personnelles.

Les droits nouveaux du patient sur ses données

Parmi les nouveaux droits de la personne sur ses données, deux peuvent intéresser la matière médicale : le droit à la « portabilité des données » et le « droit à l'oubli ».

– *Le droit à la portabilité* est énoncé à l'article 20 du règlement européen. C'est un droit qui a pour but de redonner aux individus le contrôle sur leurs données une fois qu'elles ont été collectées par le responsable. Concrètement, l'individu pourra demander au responsable que les données qu'il a fournies lui soit communiquées dans un format réutilisable. De cette manière, les individus peuvent reprendre le contrôle de leurs données afin de quitter un service pour un autre sans que ces dernières ne soient perdues.

Ce droit n'est pas absolu et ne s'applique que sous deux conditions. La première réside dans le consentement de l'individu, la seconde dans le contrat qui lie les parties. Par conséquent, la portabilité des données n'est effective que si les données ont été récoltées suite au consentement de l'individu, ou suite à la conclusion d'un contrat entre le responsable et l'individu. La consultation faisant l'objet d'un contrat de prestation de service entre le patient et le médecin, s'il en fait la demande, la portabilité des données devrait alors être effective pour le patient. Cette lecture au prisme du règlement européen relatif à la protection des données personnelles peut, dans un premier temps, être mise en doute par la version française de ce droit. Dans un second temps, l'analyse du Code de la santé publique nous permettra de confirmer cette vision européenne.

D'un côté, la loi pour une république numérique, dite loi Lemaire [42], s'est inspirée du règlement européen pour créer un droit à la portabilité des données. Sauf que son champ d'application est extrêmement restreint. Il ne s'appliquera qu'aux relations entre les plateformes exerçant leurs activités sur internet et les individus. Ce droit a pour objectif de redonner aux individus le contrôle sur leurs données. Ils pourraient notamment quitter un service pour un autre sans perdre leurs données. Pourtant, loin d'être un texte général, la loi l'a intégré dans le Code de la consommation qui ne trouve à s'appliquer qu'entre un consommateur et un professionnel, en l'occurrence le « fournisseur d'un service de communication au public en ligne » [43]. Fort heureusement, le règlement étant d'application directe, on peut penser que le droit à la portabilité trouvera à s'appliquer dans d'autres situations.

De son côté, le Code de la santé publique était précurseur car il existait déjà un droit à la portabilité des données de santé inscrites dans le dossier médical. L'article R4127- 45 reprenant l'article 45 du Code de déontologie médicale énonce que le médecin doit « *transmettre aux médecins qui participent à sa prise en charge ou à ceux qu'il entend consulter, les informations et documents utiles à la continuité des soins* ». Cette portabilité des données de santé entre médecins se fonde sur un droit fondamental du patient : le droit de choisir son médecin [44]. À la demande du patient, le médecin devra donc lui confier les informations qu'il détient sur lui (exemple : le dossier médical) de manière à ce qu'il soit confié à un autre médecin.

Illustration : Si un patient exerce son droit à la portabilité, le médecin devra lui transmettre une copie de tous les documents qu'il détient sur le patient.

– *L'autre nouveau droit dont nous pouvons brièvement discuter est le « droit à l'oubli ».* Le droit à l'oubli numérique était l'objet de tous les espoirs. Avec la reconnaissance de ce droit, l'individu devait pouvoir demander à n'importe quel détenteur d'effacer ses données. La première brèche fut créée par la Cour de justice de l'union européenne qui a analysé ce droit comme un simple droit au déréférencement des moteurs de recherche si cela ne porte pas atteinte à un intérêt

supérieur [45]. La seconde brèche est présente dans l'intitulé même de l'article 17 du RGPD : « *Droit à l'effacement (« droit à l'oubli »)* ». Tout est dit. Loin d'être discrétionnaire, le droit à l'oubli est davantage un droit à l'effacement des données sous des conditions strictes. Par exemple, l'effacement des données sera requis lorsque le traitement n'est plus nécessaire aux finalités [46]. En plus de ces conditions, il existe des exceptions au droit à l'effacement. On y retrouve le cas du dossier médical.

En effet, on ne peut demander discrétionnairement l'effacement de son dossier médical. Le droit à l'effacement ne s'applique pas aux traitements qui sont nécessaires « *pour des motifs d'intérêt public dans le domaine de la santé* » [46]. Les médecins ont en effet une obligation de conservation des dossiers médicaux pendant une durée de 20 ans. Cette durée est celle conseillée par le CNOM afin de s'aligner sur la durée imposée aux établissements de santé par l'article R1112-7 du Code de la santé publique.

Illustration : Si un individu, demande la suppression de son dossier médical au praticien, ce dernier pourra refuser en invoquant l'obligation de conservation des dossiers médicaux (20 ans).

Points forts pour la pratique

- Faire attention à ce que le service en ligne (exemple : Doctolib®) soit habilité, lui-même ou ses partenaires, à traiter des données de santé.
- Le médecin est responsable du traitement des données quand bien même un prestataire de service serait chargé de l'hébergement desdites données.
- À l'issue de la consultation, le traitement des dossiers médicaux doit se faire loyalement selon les principes provenant du RGPD : finalité précise, conservation sécurisée...
- Les patients ont des droits sur leurs données, notamment un droit d'accès à celles-ci, de rectification si elles sont incorrectes. Leur suppression est limitée par l'obligation de conservation durant 20 ans des données de santé.
- Le RGPD met en place un nouveau droit : le droit à la portabilité, soit le droit du patient de récupérer ses données afin de les transmettre à un autre médecin.

La particularité des données de santé sur lesquelles l'individu détient de multiples droits issus de multiples sources trouve ici ses limites. Le droit à l'oubli n'en est qu'un exemple. À l'image de la protection des données personnelles qui s'inscrit à la croisée de multiples intérêts, la singularité de la relation médecin-patient émerge à nouveau. Les limites aux droits individuels rappellent ainsi l'utilité des données de santé pour la préservation de la santé publique.

Liens d'intérêts : l'auteur déclare n'avoir aucun lien d'intérêt en rapport avec l'article.

RÉFÉRENCES

1. Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
2. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016. Entré en vigueur le 25 mai 2018.
3. Maxwell W, Taieb S. L'accountability, symbole d'une influence américaine sur le règlement européen des données personnelles. Dalloz IP/IT 2016 : p. 123.
4. Art. 4.2 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016. Entré en vigueur le 25 mai 2018. Chapitre I- Dispositions générales. Définitions.
5. Art. 4.7 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016. Entré en vigueur le 25 mai 2018. Chapitre I- Dispositions générales. Définitions.
6. LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. Exposé des motifs.
7. Art. 4.1 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016. Entré en vigueur le 25 mai 2018. Chapitre I- Dispositions générales. Définitions.
8. Art. 9.2.a du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016. Entré en vigueur le 25 mai 2018. Chapitre II – Principes. Traitement portant sur des catégories particulières de données à caractère personnel.
9. Art. 9.2.c du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016. Entré en vigueur le 25 mai 2018. Chapitre II – Principes. Traitement portant sur des catégories particulières de données à caractère personnel.
10. Art. 9. 2.h & 3 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016. Entré en vigueur le 25 mai 2018. Chapitre II – Principes. Traitement portant sur des catégories particulières de données à caractère personnel.
11. Code de déontologie médicale intégré au Code de la santé publique. Articles R4127-1 à R4127-112.
12. Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, version modifiée du 20 juin 2018.
13. Site Doctolib. https://www.doctolib.fr/.
14. Art. 4.8 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016. Entré en vigueur le 25 mai 2018. Chapitre I- Dispositions générales. Définitions.
15. Légifrance. Art. L1111-8 du Code de la santé publique en vigueur au 5 mars 2002.
16. Art. L1111-8, al. 2 du Code de la santé publique.
17. Agence française de la santé numérique : http://esante.gouv.fr/services/hebergeurs-de-donnees-de-sante/procedures-pour-les-hebergeurs-de-donnees-de-sante.
18. Vacarie I. L'hébergement de données de santé : entre contrat et statut. RDSS 2002 : p.695.
19. CNOM, CNIL, Guide pratique sur la protection des données personnelles. Juin 2018 : p.13.
20. Philippe S. CDNOM 15 décembre 2011. n°10977.
21. CNOM. Dossier professionnel ou fiche d'observation, tenu par le médecin. Article 45.(article R.4127-45 du code de la santé publique).
22. Cornu G. Vocabulaire juridique 12e ed. Paris : PUF ;2018.
23. CNOM. Principes de moralité et de probité. Art. 3 du Code de déontologie médicale.
24. CNOM. Secret professionnel. Art. 4 du Code de déontologie médicale.
25. Lazaro C, Le Metayer D. Le consentement au traitement des données personnelles : une perspective comparative sur l'autonomie du sujet. *Rev. Jurid. Themis* 2015 ; 48 (3) : 765-815.
26. Art. 4. 11 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016. Entré en vigueur le 25 mai 2018. Chapitre I- Dispositions générales. Définitions.

27. Art. 39 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016. Entré en vigueur le 25 mai 2018. Chapitre IV- Responsable du traitement et sous-traitant. Missions du délégué à la protection des données.

28. CNOM, CNIL. Guide pratique sur la protection des données personnelles. Juin 2018 : p.27.

29. Art. 9.2.h du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016. Entré en vigueur le 25 mai 2018. Chapitre II- Principes. Traitement portant sur des catégories particulières de données à caractère personnel.

30. CNOM et CNIL. Guide pratique sur la protection des données personnelles, op. cit : p.6.

31. Art. 5.1.c du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016. Entré en vigueur le 25 mai 2018. Chapitre II- Principes. Principes relatifs au traitement des données à caractère personnel.

32. CNOM. Guide pratique sur la protection des données personnelles, op. cit., p.9.

33. Art. L1111-7 du Code de la santé publique.

34. Article R1112-2 du Code de la santé publique.

35. Viviana S, Winckler M. *Les droits du patient, 1e ed. 2007*. Paris : Fleurus, coll. Soigner ; 396 p.

36. Décret 2012-694 du 7 mai 2012 portant modification du code de déontologie médicale.

37. Cour Administrative d'Appel. Paris. 30 septembre 2004, n°03PA01769.

38. Cour Administrative d'Appel. Paris. 15 avril 2004, n°20041645.

39. Girer M, Mémeteau G. Cours de droit médical. LEH Edition ; 2016, n°972.

40. Saison J, Boughriet N. Les notes personnelles des médecins : un point d'incertitude dans la détermination du contenu transmissible du dossier. RGDM 2014 ; 53 :43-9.

41. Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

42. Art. 48 de la loi pour une République numérique.

43. Art. 1110-8 du Code de la santé publique.

44. Cour de Justice de l'Union Européenne (CJUE). Affaire Google Spain /c. AEPD ;n° C-131/12. 13 mai 2014.

45. Art. 17.1.a du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016. Entré en vigueur le 25 mai 2018. Chapitre III. Droits de la personne concernée. Droit à l'effacement.(« droit à l'oubli »).

46. Art. 17. 2. c du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016. Entré en vigueur le 25 mai 2018. Chapitre III. Droits de la personne concernée. Droit à l'effacement.(« droit à l'oubli »).

Réponses au test de lecture de novembre 2018 portant sur le n° 8 Volume 14, d'octobre 2018

Réponses exactes :

1. A. B, C, E. 2. B. 3. A, B, C. 4. B. 5. B, C D, E, G. 6. A, B, C.