La protection des données personnelles des patients face à la modernisation de notre système de santé

Valérie Siranyan

Version of Record: https://www.sciencedirect.com/science/article/pii/S1246739118300861
Manuscript_1baec8cf46321cf567df2f518a069001

Protection de la personne Exercice professionnel

La protection des données personnelles des patients face à la modernisation de notre système de santé

Data Protection and Healthcare

Valérie Siranyan (maître de conférences en droit de la santé, HDR),
Université Claude Bernard Lyon 1 (P2S 4129)
8, avenue Rockefeller, 69373 Lyon cedex 08, France

Résumé :
A l'ère de l'internet et du déploiement de l'intelligence artificielle, la collecte et le traitement de données personnelles deviennent un élément stratégique pour le développement de l'économie numérique. Une particulière attention devra être portée sur le respect des droits des personnes lors du recueil de renseignements touchant à la santé ou au corps.
Le RGPD (Réglement général sur la protection des données) est entré en vigueur le 25 mai 2018. L'exercice des professionnels de santé établis dans un État membre, sera impacté dans la mesure où il peut s'appuyer sur des éléments cliniques ou biologiques des patients.

Mots-clés :
Données personnelles, Secret professionnel (RGPD) , RGPD (Réglement général sur la protection des données),DPO

Abstract:
With the internet and the artificial intelligence, the collection of personal data is becoming a strategic element for the digital economy. The collection of information touching the health or the body must respect the patients' rights.
The GDPR came into effect on May 25th, 2018. The healthcare professionals who are established in a Member state, must be careful becausethey can base their exercise on clinical or biological elements of their patients.

Keyword:
Personal data , Professional secret, GPDR (Général data protection regulation) , Data protection officer

---

L'auteur déclare ne pas avoir de liens d'intérêts
Courriel : valerie.siranyan@univ-lyon1.fr

L'audition de Mark Zuckerberg, le 10 avril 2018 devant le Sénat des États-Unis a permis de mettre en exergue les risques liés à l'utilisation des réseaux sociaux au regard de la protection de la vie privée. En effet les données personnelles de millions d'internautes ont pu être collectées et exploitées à leur insu, par une société de conseil en communication[1]. Certains parlementairesaméricains ont alors pu souligner que la réglementation adoptée par les instances de l'Union européenne participait à une meilleure sécurisation des échanges.

[1] W. Audureau, « Ce qu'il faut savoir sur Cambridge Analytica, la société au cœur du scandale Facebook », Le Monde.fr, 22.03.2018, mis à jour le 16.05.2018.

Concernant plus particulièrement la France, la Commission Nationale de l'Informatique et des Libertés (CNIL) a le pouvoir de sanctionner les manquements à loi, en prononçant, à l'issue d'une procédure contradictoire, un avertissement, une amende, une injonction de cesser un traitement ou encore le retrait d'une autorisation[2]. A cet égard, la formation restreinte de la CNIL, par une délibération du 27 avril 2017, a prononcé une sanction financière de 150 000 euros à l'encontre des sociétés Facebook Inc. et Facebook Ireland, après la constatation de plusieurs atteintes aux droits des utilisateurs[3]. Il a notamment été reproché à ces deux compagnies, l'absence d'information explicite des internautes, puisqu'elles ne mentionnaient pas,ou de manière très imprécise, l'existence d'une collecte massive de renseignements personnels par des traceurs ou « *cookies* ». Dans ces conditions, le consentement des internautes n'apparaissait pas libre et éclairé.

Le recueil de données touchant à la santé physique ou mentale des personnes présente un risque élevé d'atteinte à la vie privée. Tout manquement à l'obligation d'assurer la sécurité et la confidentialité de fichiers ou d'enregistrements relatifs à des patients ou des consommateurs de produits de santé, sera donc susceptible d'être sanctionné. En l'espèce, une société spécialisée dans le commerce de détail d'optique n'avait pas pris suffisamment de précautions lors de la mise en œuvre de son site de vente sur internet. En effet des données sensibles telles que le NIR des clients, étaient librement accessibles par des tiers. Par une délibération du 7 mai 2018, la formation restreinte de la CNIL a donc prononcé une condamnation pécuniaire à hauteur de 250 000 euros[4].

L'ensemble des nouvelles technologies de communication, éventuellement combiné avec des logiciels de calculs logarithmiques, offre de nombreuses possibilités d'innovation pour la prise en charge et le suivi des patients, chroniques ou en situation de dépendance. Dans ce sens, un accord conventionnel a été signé les 14 et 15 juin 2018 par plusieurs syndicats de médecins en vue de participer au déploiement de la télémédecine, après dix ans d'expérimentation. En parallèle, l'utilisation de plateformes et de dispositifs médicaux interconnectés peut permettre d'optimiser l'accompagnement et la surveillance de patients souffrant notamment de diabète ou d'hypertension. Face à la modernisation de notre système

[2]E. Frago, « Les missions de la Cnil sont-elles nécessaires et efficaces ? », LPA 8 septembre 2017, n°179-180, p.101.

[3] Délibération de la formation restreinte SAN-2017-006 du 27 Avril 2017 prononçant une sanction pécuniaire à l'encontre des sociétés FACEBOOK INC. et FACEBOOK IRELAND, publiée sur Légifrance le 17 mai 2017.

[4] Délibération de la formation restreinte n° SAN-2018-002 du 7 mai 2018 prononçant une sanction pécuniaire à l'encontre de la société OPTICAL CENTER, publiée sur Légifrance le 7 juin 2018.

de santé, les professionnels de santé doivent néanmoins s'efforcer de rester fidèles à leur serment et protéger la vie privée de tous ceux qui ont recours à leur art.

1- Libre circulation et protection des données personnelles

A l'ère de l'internet et de l'intelligence artificielle, la collecte et le traitement de données personnelles deviennent un élément stratégique pour le développement de l'économie numérique. Une particulière attention devraêtre portée sur le respect des droits des personnes lors du recueil de renseignements touchant à la santé ou au corps. Dans un tel contexte, les normes adoptées par les instances de l'Union Européenne devront permettre d'atteindre un équilibre entre la sauvegarde des libertés fondamentales défendues par les traités et la préservation de l'intimité. Les dispositions communautaires devront aussi intégrer la multiplicité et la diversité des échanges électroniques entre les continents.

1-1 L'esprit du RGPD

Le règlement du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD) vise notamment l'atteinte d'un même niveau de protection de la vie privée au sein du marché intérieur européen[5]. Il s'appuie d'une part sur l'article 8 de la charte des droits fondamentaux dont le paragraphe 2 énonce en particulier que les données personnelles « doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondementlégitime prévu par la loi »[6] et d'autre part sur l'article 16 du traité sur le fonctionnement de l'UE. Il s'inscrit dans le prolongement des précédentes normes[7], en intégrant l'accroissement des flux électroniques et les pratiques liées à l'exploitation de grandes quantités de données, tout en favorisant l'harmonisation des politiques.

Le RGPD est entré en vigueur le 25 mai 2018. Il concerne les organismes publics, les entreprises, les associations et les particuliers, exploitant à titre professionnel des données relatives à des personnes se trouvant sur le territoire de l'UE[8]. Les compagnies américaines,

[5]Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE), JOCE 4.5.2016.

[6]Charte des droits fondamentaux de l'Union européenne (2000/C 364/01), JOCE 18. 12. 2000.

[7]Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JOCE 23. 11. 95, transposée en France par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[8] Article 3 du RGPD: champ d'application territorial.

dans la mesure, où elles offrent des biens ou des services au sein de l'Union, devront aussi se conformer à ces nouvelles dispositions[9]. L'exercice des professionnels de santé établis dans un État membre, sera impacté dans la mesure où il peut s'appuyersur des éléments cliniques ou biologiques des malades. Les données de santé se définissent désormais comme un ensemble de données qui révèlent des informations sur l'état de santé physique ou mentale, passé, présent ou futur d'un patient. Elles renvoient notamment à des renseignements résultant d'un test ou de« l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques » ou bien à une information relative à« une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro »[10].

Par principe interdit, le traitement de ces données sensibles ou particulières, peut néanmoins être entrepris sur la base du consentement explicite, libre et éclairé de la personne concernée, ou encore se justifier par l'exercice de droits propres en matière de droit du travail et de protection sociale[11]. Ces finalités déterminées, spécifiques et légitimes, devront alors être exposées de manière claire, appropriée et loyale[12]. A l'égard des mineurs, le RGPD précise que le traitement sera licite s'il concerne un enfant d'au moins seize ans. Pour les plus jeunes, le consentement devra être recueilli auprès du titulaire de l'autorité parentale[13]. S'appuyant sur la marge de manœuvre laissée aux États membres, les parlementaires français ont choisi abaissé à quinze ans « la majorité numérique »[14]. L'information devra alors être adaptée aux facultés de compréhension des adolescents. Au-delà, dans le cadre du traitement de données personnelles réalisé lors de recherches non interventionnelles ou présentant des risques minimes, un mineur âgé de quinze ans ou plus pourra s'opposer à l'information du ou des titulaires de l'autorité parentale lorsqu'elle est relative à « une action de prévention, un dépistage, un diagnostic, un traitement ou une intervention pour laquelle le mineur s'est expressément opposé à la consultation des titulaires de l'autorité parentale, en application des

[9] J. Schwartz, "Le point sur le RGPD: nouvelles obligations, nouveaux enjeux", Les Cahiers Sociaux, avril 2018, n°306, p.228.

[10] Considérant 35 du RGPD.

[11] Article 9 du RGPD: Traitement portant sur des catégoriesparticulières de données à caractère personnel.

[12] F. Gaulier, « Le principe de finalité dans le RGPD: beaucoup d'ancien et un peu de nouveau », Lexisnexis communication, commerce électronique, n°4, avril 2018.

[13] Article 8 du RGPD: Conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information.

[14] Article 20 de la loi du n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, JORF 21 juin 2018.

articles L. 1111-5 et L. 1111-5-1 du Code de la santé publique[15], ou si les liens de famille sont rompus »[16].

Le respect du principe de transparence s'impose à tout responsable de traitement. En effet la collecte des données devra rester adéquate, pertinente et limitée au regard de la finalité du traitement[17]. La durée de conservation sera réduite de façon strictement proportionnée. Dans ce sens, les articles 13 et 14 du RGPD listent de manière détaillée l'ensemble des informations à fournir lors de l'exploitation de données personnelles, dont notamment l'identité et les coordonnées du responsable, les finalités et la base juridique afférente, l'existence d'une prise de décision automatisée, y compris le profilage ou encore l'intention de réaliser un transfert dans un pays tiers. Plus encore, de larges dispositions visent à garantir l'effectivité des droits des personnes : Droits d'accès[18], de rectification[19] et de suppression, d'opposition pour motif légitime[20]. Plusieurs innovations permettent d'atteindre un haut niveau de protection face au développement de l'économie du numérique. Ainsi apparaissent un droit à l'effacement, au retrait de son consentement[21], à la limitation du traitement[22] ou encore à la portabilité[23].

Le RGPD innove aussi par la volonté de responsabiliser les acteurs, de la conception d'un traitement de données personnelles à l'analyse de l'impact sur la vie privée. L'esprit est de passer d'un régime d'autorisation à un système de déclaration de conformité sur la base de codes de conduite ou de recommandations diffusés par les autorités compétentes. Ces mécanismes de co-régulation peuvent se résumer par l'apparition au sein de la règlementation européenne, des principes d'« *accountability* », de « *privacy by design* » et de « *privacy by default* »[24].

[15]Article L.1111-5 du Code de la santé publique : « Par dérogation à l'article 371-1 du code civil, le médecin ou la sage-femme peut se dispenser d'obtenir le consentement du ou des titulaires de l'autorité parentale sur les décisions médicales à prendre lorsque l'action de prévention, le dépistage, le diagnostic, le traitement ou l'intervention s'impose pour sauvegarder la santé d'une personne mineure, dans le cas où cette dernière s'oppose expressément à la consultation du ou des titulaires de l'autorité parentale afin de garder le secret sur son état de santé. »

[16]Article 16 de la loi du n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, JORF 21 juin 2018.

[17] Article 5 du RGPD: Principes relatifs au traitement des données à caractère personnel.

[18] Article 15 du RGPD: Droit d'accès de la personne concernée.

[19] Article 16 du RGPD: Droit de rectification.

[20] Article 21 du RGPD: Droit d'opposition.

[21] Article 17 du RGPD : Droit à l'effacement.

[22]Article 18 du RGPD: Droit à la limitation du traitement.

[23]Article 20 du RGPD :Droit à la portabilité des données.

[24] F. Chaltiel, « La protection des données personnelles. A propos de l'entrée en vigueur du règlement général de protection des données », LPA 4 juin 2018, n°111, p.6.

En pratique, les responsables de traitement, et le cas échéant les sous-traitants, devront tenir à jour un registre répertoriant notamment les finalités de la collecte, les catégories de personnes concernées et des destinataires, y compris dans les pays tiers[25]. Les professionnels de santé libéraux devront veiller à mettre en œuvre ces nouvelles obligations tant à l'égard de leurs patients ou clients que de leurs salariés. Les contrats de sous-traitance devront en particulier contenir des clauses propres à garantir la sécurité des enregistrements ; les hébergeurs de données de santé devront être agréés ou certifiés. En outre toute violation des fichiers, tout piratage ou perte de données sensibles devront être notifiés par le responsable du traitement, à l'autorité de contrôle dans les 72 heures[26]. Les personnes concernées devront en être informées, notamment en cas de risque élevé pour les droits et libertés fondamentales. Les professionnels qui traitent des données de santé, comme les médecins ou les pharmaciens, devront se montrer vigilants et mettre en place des procédures en vue de prévenir toute intrusion ou atteinte des systèmes informatiques. De simples règles de bon sens peuvent participer à la sécurisation des accès telles que le choix et le renouvellement de mots de passe complexes, le verrouillage des accès après trois tentatives infructueuses, l'authentification des utilisateurs, la réalisation de fichiers de sauvegarde conservés dans des lieux sécurisés, le verrouillage del'ordinateur en cas d'éloignement du poste de travail…

En cas d'atteinte aux droits à la protection des données reconnus par les traités, les patients disposeront d'un recours auprès des autorités de contrôle, comme la CNIL. Celles-ci pourront prononcer des sanctions administratives, pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires. En parallèle les personnes concernées pourront exercer un recours juridictionnel afin d'obtenir une réparation. La loi du 20 juin 2018 organise en particulier les actions de groupe ;en effet toute personne pourra mandater une association aux fins d'exercer en son nom, les droits explicités par le RGPD devant les tribunaux ou encore pour agir devant la Commission nationale de l'informatique et des libertés.

1-2 Les échanges ou transferts de données personnelles hors E-U

Face à l'internationalisation des échanges, une norme qui vise à protéger les droits des personnes physiques, doit imposer un haut niveau de sauvegarde de la vie privée lors de transfert des données en dehors de l'Union européenne. Tel est l'objet des articles 44 et suivants du RGPD, qui doivent être appréhendés en cohérence avec la jurisprudence

[25]Article 30 du RGPD : Registre des activités de traitement.

[26] Article 33 du RGPD : Notification à l'autorité de contrôle d'une violation de données à caractère personnel.

communautaire. En effet le 6 octobre 2015, la Cour de justice de l'Union européenne a invalidé l'accord « *Safe Harbor* », qui autorisait le transfert de données personnelles entre l'Europe et les États-Unis, en raison notamment d'un manque de transparence et de l'insuffisance des contrôles[27]. Depuis lors, un nouvel accord pour la protection des données personnelles a été négocié.

Le « *Privacyshield* » est entré en vigueur le 1er août 2016. En conséquence, lors d'un transfert de données personnelles, relatives notamment à la santé, vers une société américaine, les principes considérés comme fondamentaux par les instances européennes doivent être respectés : consentement, droit d'information, d'accès ou de rectification…Cette protection doit perdurer en cas de transferts successifs ou ultérieurs[28]. Les résidents européens doivent, en outre, pouvoir bénéficier de recours administratifs ou judiciaires effectifs. Les accords prévoient qu'une réclamation puisse être introduite auprès de la commission fédérale du commerce ou encore auprès d'un comité d'arbitrage constitué à cet effet. Malgré tout, les procédures à disposition des Européens en vue d'imposer une action correctrice ou d'obtenir une réparation peuvent s'avérer relativement complexes. Au surplus, la CNIL a exprimé des préoccupations concernant l'accès aux données personnelles, par les autorités publiques américaines.Tout comme les États-Unis, le Canada est reconnu comme un pays qui adhère partiellement aux droits européens de protection des données personnelles. Le commissariat à la protection de la vie privée du Canada a notamment élaboré des lignes directrices sur le fondement de la loi fédérale pour la protection des renseignements personnels et les documents électroniques.

Dans ce contexte, le chapitre V du RGPD organise les « transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales ». La Commission européenne et les autorités de contrôle des États membres doivent favoriser des coopérations internationales, afin de garantir l'effectivité des droits des personnes[29]. Trois modalités de protection sont successivement prévues par la norme communautaire. Sur le fondement d'une décision d'adéquation aux droits et libertés fondamentaux reconnus par les traités, les instances européennes autoriseront le transfert vers un pays tiers[30]. En cas

[27]CJUE, 6 octobre 2015, aff. C-362/14 MaximillianSchrems / Data Protection Commissioner, ECLI:EU:C:2015:650.
[28]R. Perray, « Quelle stratégie pour les transferts de données personnelles hors de l'Union européenne à l'aune du RGPD? », Lexisnexis communication, commerce électronique, n°4, avril 2018.
[29] Article 50 du RGPD : Coopération internationale dans le domaine de la protection des données à caractère personnel.
[30] Article 45 du RGPD : Transferts fondéssur une décision d'adéquation.

d'impossibilité, des garanties peuvent aussi être établies par des moyens alternatifs.Les responsables des traitements et leurs sous-traitants peuvent alors avoir recours à des règles d'entreprise contraignantes, à des clauses types reconnues par la Commission ou une autorité de contrôle, à des codes de conduite ou encore à un mécanisme de certification, afin d'apporter la preuve du respect des droits des personnes[31]. Le cas échéant, des dérogations peuvent être admises, pour des situations particulières, à condition notamment d'obtenir le consentement de la personne concernée ou en cas de nécessité pour la sauvegarde d'intérêts vitaux.

Si les précautions imposées pour le transfert de données personnelles entre les entreprises européennes et américaines, ne concernent pas directement l'exercice quotidien des professionnels de santé, ces derniers doivent néanmoins veiller à protéger méticuleusement la vie privée de l'ensemble de leurs patients, au sein d'un système de santé, où les échanges de données sont devenus essentiels pour la coordination et la qualité des soins ou traitements.

2- Confidentialité et partage des données de santé

Le respect du secret professionnel reste à travers les temps, un des fondements de la pratique de la médecine ou la pharmacie ; admis dans l'intimité des personnes, les professionnels de santé doivent se taire sur ce qu'ils ont pu entendre, voir ou comprendre lors de leur exercice quotidien[32]. Néanmoins tant le développement de la protection sociale et des technologies numériques que la prise en charge des patients par une équipe multidisciplinaire de soin imposent la recherche d'un équilibre entre protection et partage des données personnelles.

2-1- Partage des données de santé au sein de l'équipe multidisciplinaire de soins

Le code pénal définit le secret professionnel à travers la sanction en cas de non-respect et les dérogations strictement prévues par la loi[33]. Le concept de secret partagé n'est intervenu qu'à partir de l'adoption de la loi du 4 mars 2002, selon laquelle : « 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

[31] Article 46 du RGPD : Transferts moyennant des garanties appropriées.

[32] ArticleR.4127-4 du Code de la santé publique (médecin); article R4235-5 du Code de la santé publique (pharmacien).

[33] Article 226-13 du Code pénal.

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 »[34]. Par la suite, face au développement de la médecine de groupe, un nouvel alinéa est venu préciser les modalités de la mise en commun des informations, par des professionnels exerçant au sein d'une maison ou d'un centre de santé, sous réserve de l'obtention du consentement du patient, y compris sous forme dématérialisée[35].

Avec un objectif de simplification, la loi de modernisation de notre système de santé a élargi aux professionnels du secteur médico-social ou social et aux établissements ou services sociaux et médico-sociaux, les personnes et structures soumises au secret[36]. La notion d'« *équipe de soin* » devient centrale pour le partage des données de santé d'un patient en vue de la continuité des soins ou du suivi médico-social. A défaut d'appartenance à l'« *équipe* », un professionnel devra recueillir en préalable le consentement de la personne concernée pour pouvoir accéder aux informations nécessaires à la coordination. L'article L.1110-12 du Code de la santé publique permet d'apporter des précisions pour une meilleure compréhension des mécanismes d'échange de données au sein du système de santé. Ainsi le dispensateur d'un traitement pourra contacter le prescripteur, pour obtenir des renseignements relatifs à une ordonnance au travers de la reconnaissance par le patient de la qualité de membre de l'équipe, responsable de la prise en charge. Dans l'éventualité d'un échange par voie électronique, les professionnels de santé devront prioriser l'utilisation d'une messagerie sécurisée[37].

Plusieurs outils ont en outre été prévus par la loi ou les règlements afin d'optimiser la qualité des échanges et des soins au sein d'une équipe multidisciplinaire. Il est possible de citer la lettre de liaison dans le cadre d'une demande d'hospitalisation[38] ou encore le dossier pharmaceutique, qui permet aux pharmaciens d'officine, hospitaliers et aux médecins des établissements de santé d'avoir accès aux traitements dispensés à un patient durant les quatre derniers mois[39]. Au-delà « dans le respect des règles déontologiques qui lui sont applicables (…), chaque professionnel de santé, quels que soient son mode et son lieu d'exercice, reporte

[34] Article L.1110-4 du Code de la santé publique, issu de la loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé.

[35] Article L.1110-4 du Code de la santé publique,modifié parla loi n° 2011-940 du 10 août 2011 modifiant certaines dispositions de la loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires.

[36] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, JO 27 janvier 2016.

[37] Article 96, loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, JO 27 janvier 2016.

[38] Article 95, loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, JO 27 janvier 2016.

[39] Article L.1111-23 du Code de la santé publique.

dans le dossier médical partagé, à l'occasion de chaque acte ou consultation, les éléments diagnostiques et thérapeutiques nécessaires à la coordination des soins de la personne prise en charge »[40]. Selon une instructionministérielle diffusée auprès des agences régionales de santé et des directeurs-coordinateurs de la gestion du risque de l'assurance maladie,l'ensemble des établissements de santé, supports de Groupement Hospitalier de Territoire, devraient être en mesure d'alimenter les dossiers médicaux partagés à la fin du premier semestre 2019[41].

2-2 Partage des données de santé au sein du réseau numérique

Avec l'avènement de l'économie des algorithmes et la commercialisation de dispositifs médicaux connectés, les professionnels de santé devront communiqués avec les patients, les membres de l'équipe soignante, mais aussi éventuellement avec des objets intelligents, qui risquent alors de s'immiscer dans la relation de soin. Dans un tel environnement numérique, la mise en conformité avec le RGPD représente un enjeu majeur de la sécurité des soins, pour l'ensemble des professionnels de santé, responsables de traitements de données personnelles. A cet égard, la désignation d'un délégué à la protection des données (DPO: Data protection officer) devient obligatoire pour les organismes publics ou assurant une mission d'intérêt public mais aussi pour les structures privées qui peuvent gérer des données personnelles à grande échelle. En conséquence, pourront être soumis à un tel impératif d'une part les établissements de santé et d'autre part les laboratoires de biologie médicale, les pharmaciens d'officine ou les médecins, ayant intégré un groupement, une maison de santé ou d'une manière générale un réseau de soins. Dans tous les cas, les professionnels de santé libéraux devront réaliser une cartographie précisedes traitements de données personnelles dont ils sont responsables, sans oublier les messageries électroniques ou les plateformes de rendez-vous[42].

En outre, le développement d'actes de télémédecine ou de téléconsultation oblige à la vigilance à l'égard de la vie privée des patients, tout comme l'utilisation d'objets connectés pour la surveillance ou le suivi à distance des malades. Des clauses de confidentialité devront notamment être présentées aux prestataires ou sous-traitants. En parallèle, les patients devront être informésde la finalité du traitement de leurs données personnelles. Les professionnels de santé auront aussi une mission de conseil et d'éducation à l'égard de l'emploi des

[40]Article L.1111-15 du Code de la santé publique.

[41]Instruction n° SG/DSSIS/DGOS/DGCS/CNAM/2018/72 du 13 mars 2018 relative à l'accompagnement en région de la généralisation du dossier médical partagé (DMP).

[42]CNOM, CNIL, Guide pratique sur la protection des données, juin 2018, p.40.

technologies numériques. Un message de prudence pourra en particulier être délivré en préalable au téléchargement d'une application santé sur un téléphone portable. Dans le même sens, les échanges professionnels au moyen de smartphone, tablette ou courriel non sécurisés devront autant que possible être réduits, en absence de chiffrement de données ou de moyen d'authentification par mot de passe. Les produits de santé connectés comme les logiciels autonomes ou encore les plateformes de partage d'information qui bénéficient du statut de dispositif médical avec une certification européenne, présentent aussi une meilleure sécurisation, à l'inverse d'autres objets de santé ou applications utilisés d'avantage avec une finalité de bien-être.

Le RGPD fournit à l'ensemble des professionnels qui manipulent des données sensibles comme celles issues d'un dossier médical ou pharmaceutique, des éléments essentiels à la protection de la vie privée des personnes physiques. D'application immédiate, cette norme européenne n'exige pas de transposition, la loi relative à l'informatique, aux fichiers et aux libertés a néanmoins été adaptée en vue d'élargir les missions confiées à la commission nationale de l'informatique et des libertés, comme celles liées à la préparation de lignes directrices ou référentiels[43]. Au demeurant un règlement concernant « le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vieprivée et communications électroniques») » devrait aussi être adopté par les instances européennes[44]. En complément du RGPD, il aura pour objectifs de garantir un droit à l'information des usagers optimisé,à l'égard de la politique de confidentialité des échanges électroniques et de l'utilisation de traceurs ou « *cookies* ». Ce corpus réglementaire et législatif apparaît donc indispensable pour la sauvegarde de la confiance des patients envers les soignants, sa mise en œuvre par les professionnels de santé pourrait en revanche s'avérait complexe, au vu de la multiplicité des sources.

[43]Article 1de la loi du n° 2018-493 du 20 juin 2018.

[44] Commission européenne, proposition de règlement du parlement européen et du conseil concernant « le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques») », COM(2017) 10 final 2017/0003 (COD).