



UNIVERSITÉ CLAUDE BERNARD LYON 1

UE RB25 – INFORMATIQUE MÉDICALE

Protection et circulation des données de santé numériques :

enjeux juridiques, techniques et perspectives
pour les professionnels de santé à l'ère du numérique

Jacques DADIE

Étudiant en deuxième année de médecine

Encadrement

Maître Aude BONNARD

Année universitaire 2025-2026

RÉSUMÉ

La numérisation du système de santé entraîne une production et une *circulation croissantes* de données médicales. Si ces données permettent d'améliorer la prise en charge des patients, la coordination des soins et la recherche, elles posent également des enjeux majeurs en matière de protection de la vie privée et de confidentialité. Cette revue de littérature analyse les cadres juridiques, les dispositifs techniques et les responsabilités des professionnels de santé face à ces défis, afin de proposer une synthèse des connaissances actuelles et des perspectives d'évolution.

SOMMAIRE

INTRODUCTION	3
1. Les données de santé : une ressource indispensable mais particulièrement sensible	4
1.1. Définition et spécificités des données de santé.....	4
1.2. Une ressource indispensable au fonctionnement du système de santé	4
1.3. Une sensibilité qui justifie une protection renforcée.....	5
2. Encadrer la circulation des données de santé : un cadre juridique au service de la protection des patients	6
2.1. Les principes fondamentaux du traitement des données de santé	6
2.2. Les acteurs de la protection des données de santé.....	7
2.3. Les droits reconnus aux patients	7
2.4. Le contrôle du respect des règles : responsabilités et sanctions	8
3. De la théorie à la pratique : protéger les données au quotidien.....	9
3.1. L'intégration de la protection des données dans l'exercice médical.....	9
3.2. Les bonnes pratiques au sein d'un cabinet médical	10
3.3. Les violations de données : prévenir et réagir	10
4. L'anonymisation : entre protection et exploitation des données	11
4.1. L'anonymisation : un outil essentiel de protection des données	11
4.2. Les limites de l'anonymisation : le risque de réidentification	12
5. Quels défis pour les professionnels de santé à l'ère du numérique ?	13
CONCLUSION.....	14

INTRODUCTION

Le système de santé connaît actuellement une transformation numérique sans précédent. La numérisation progressive des pratiques médicales a profondément changé les informations médicales produites, stockées, échangées et utilisées. Aujourd'hui, les dossiers médicaux électroniques, les logiciels professionnels, les plateformes de téléconsultation, les systèmes de messagerie sécurisée et les systèmes de recherche médicale et de santé publique sont tous utilisés.

Ce développement est très positif pour le système de santé, mais ce flux croissant d'informations soulève également de sérieuses préoccupations concernant la confidentialité et la sécurité et la vie privée des patients.

Ainsi, les données de santé sont les données personnelles les plus sensibles. Par conséquent, les protéger n'est pas seulement une exigence réglementaire, mais aussi une condition essentielle pour maintenir un équilibre. En d'autres termes, l'objectif n'est pas d'empêcher la circulation de ces données, devenues indispensables au fonctionnement du système de santé, mais plutôt d'assurer leur utilisation sécurisée et proportionnée conformément au cadre juridique en vigueur.

Dans ce contexte, la question est de savoir **comment concilier la circulation des données de santé, indispensable au domaine médical avec les exigences juridiques et techniques destinées à garantir leur protection ainsi que le respect des droits des patients ?**

Pour répondre à cette question, cette revue présentera dans un premier temps la spécificité des données de santé et les raisons qui justifient leur protection renforcée. Elle évaluera ensuite la base légale de leur traitement et discutera des implications de cela pour les professionnels de santé. Enfin, elle abordera certains mécanismes de protection avec l'anonymisation parmi eux avant de se tourner vers les compétences que les travailleurs de la santé doivent acquérir à l'ère numérique.

1. Les données de santé : une ressource indispensable mais particulièrement sensible

1.1. Définition et spécificités des données de santé

Les données de santé sont désormais utilisées comme fondement pour les soins aux patients, la coordination des soins de santé, la recherche et les avancées numériques. Cela peut sembler intuitif, mais c'est en réalité bien plus large que cela. Les données de santé ne sont pas seulement des informations issues d'un acte médical lui-même, par exemple, un diagnostic ou une analyse biologique. Elles incluent toutes les informations sur la santé physique ou mentale d'un individu, qu'elles soient recueillies lors d'une consultation, d'un examen médical ou déduites d'autres données. Le *Dictionnaire Permanent Santé, Bioéthique, Biotechnologies* rappelle ainsi que cette catégorie comprend notamment les comptes rendus médicaux, les prescriptions, les traitements, les examens d'imagerie, les données génétiques, mais également toute information susceptible de révéler, directement ou indirectement, l'état de santé d'une personne.

Cette définition particulièrement large est un bon exemple de la santé numérique. Mais les informations médicales ne sont plus seulement générées par les médecins et les infirmières, elles peuvent être générées à partir d'objets connectés, d'applications mobiles et d'autres systèmes d'information. Des données qui semblent triviales en surface deviendront des données de santé dès que nous pourrons donner un sens à la santé de quelqu'un. Cette extension de l'idée est conforme au souhait du législateur d'assurer la plus grande protection possible pour la personne concernée. Elle reflète également l'importance croissante des données dans le fonctionnement quotidien du système de santé.

Les données de santé ont donc une double dimension qui sera au cœur de notre travail. D'une part, elles sont devenues indispensables pour les soins aux patients et le développement du domaine médical. D'autre part, elles constituent également des données personnelles qui touchent à l'intimité, à la vie privée et au secret médical du bénéficiaire des soins. Leur divulgation ou utilisation inappropriée peut avoir un impact très grave, y compris la perte de confidentialité, la perte de confiance envers les professionnels de santé et même la discrimination. C'est pourquoi les données de santé sont désormais protégées par davantage de moyens juridiques où repose la base de ce travail.

1.2. Une ressource indispensable au fonctionnement du système de santé

Les données de santé constituent un outil indispensable à la prise en charge des patients en permettant aux différents professionnels de santé d'accéder à des informations fiables, actualisées et pertinentes. Dans un contexte où les parcours de soins sont de plus en plus complexes et impliquent

de nombreux intervenants, ces données favorisent la continuité des soins, limitent les risques d'erreurs médicales et améliorent la coordination entre les différents acteurs du système de santé. Elles contribuent ainsi directement à la qualité et à la sécurité des soins dispensés aux patients.

Les données de santé jouent également un rôle central dans le développement de la recherche médicale et des politiques de santé publique. L'accès à des informations utiles pour comprendre les pathologies et les traitements, ainsi que pour les stratégies de diagnostic, de traitement et de prévention, voire pour améliorer les nouvelles technologies médicales, est très important. La médecine numérique, la télémédecine et la technologie de l'intelligence artificielle ne font qu'ajouter à ce besoin d'une grande quantité d'informations de bonne qualité, fiables et accessibles. Le *Dictionnaire Permanent Santé, Bioéthique, Biotechnologies* souligne ainsi que les traitements de données de santé poursuivent aujourd'hui des finalités variées, allant de la prise en charge individuelle des patients à la recherche scientifique, en passant par la gestion du système de santé et les missions d'intérêt public.

Cette place croissante des données de santé dans le fonctionnement de la médecine moderne met toutefois en évidence un équilibre délicat. Si leur circulation est devenue indispensable pour garantir une prise en charge efficace des patients et accompagner les innovations médicales, elle accroît également les risques liés à leur confidentialité et à leur sécurité. Dès lors, l'enjeu n'est plus de limiter leur utilisation, mais de mettre en place des mécanismes permettant d'assurer une circulation sécurisée, conforme aux exigences juridiques et respectueuse des droits des patients. Cette nécessité justifie l'existence d'un cadre juridique spécifique.

1.3. Une sensibilité qui justifie une protection renforcée

La double nature des données de santé explique pourquoi nous avons besoin d'une meilleure protection. En effet, si ces informations sont devenues indispensables, elles demeurent également parmi les données personnelles les plus sensibles ce qui impose une vigilance particulière quant à leur collecte, leur conservation et leur utilisation.

La santé numérique a considérablement augmenté la capacité de partager et d'exploiter ces données. Cette évolution est essentielle mais présente également des risques pour les patients. Les violations de données, les accès non autorisés, les cyberattaques ou les risques de réidentification sont désormais les plus grandes préoccupations pour les prestataires de soins de santé et les professionnels travaillant dans la communauté. La protection des données de santé ne consiste pas seulement à respecter les règles de conduite mais aussi à protéger le patient et la confiance qui est au cœur de la relation thérapeutique.

Face à ces enjeux, il est apparu nécessaire de mettre en place un cadre juridique spécifique permettant d'encadrer le traitement des données de santé tout en garantissant leur utilisation au service des soins, de la recherche et de l'intérêt général. Ce cadre vise à concilier deux objectifs complémentaires : assurer la circulation des informations nécessaires au fonctionnement du système

de santé et préserver les droits fondamentaux des personnes concernées. Les principaux mécanismes juridiques qui organisent cette protection seront présentés dans la partie suivante.

2. Encadrer la circulation des données de santé : un cadre juridique au service de la protection des patients

2.1. Les principes fondamentaux du traitement des données de santé

La technologie numérique en santé a modifié la manière dont nous collectons, partageons et utilisons les données médicales. Et autant il est bénéfique pour la qualité des soins d'être améliorée et pour la recherche médicale de se développer, autant cela augmente le risque pour la vie privée des patients. Le processus de traitement des données de santé est désormais régi par un cadre juridique très strict, notamment en raison du **Règlement général sur la protection des données (RGPD)**. Cela ne limitera cependant pas l'utilisation des données de santé, mais garantira plutôt qu'elles soient utilisées de manière sécurisée et respectueuse des droits des personnes. Il repose sur plusieurs principes fondamentaux qui régissent tout traitement de données.

Le premier de ces principes réside dans la licéité du traitement. Les données de santé sont un sujet plutôt sensible et ne peuvent être collectées et utilisées arbitrairement. Tout traitement doit être basé sur une base légale claire et avoir un objectif précis. En plus de cela, la loyauté et la transparence sont également des exigences, c'est-à-dire informer les personnes concernées sur les méthodes et les objectifs de la collecte de données, et qui aurait accès aux données. Le cadre juridique doit garantir une information claire et compréhensible, il promeut l'utilisation responsable des données et la confiance dans les outils de santé numériques.

Le cadre juridique repose également sur le principe de finalité : les données ne doivent être collectées que pour quelque chose de concret et légitime. Cette logique est complétée par le principe de minimisation des données, ce qui signifie que seules les données pertinentes pour atteindre ces objectifs sont collectées. En d'autres termes, chaque donnée ne peut pas être systématiquement exploitée : seules celles qui ont réellement de la valeur pour les soins aux patients, la recherche ou une mission d'intérêt public peuvent être utilisées. De plus, les données ne peuvent pas être conservées indéfiniment. Elles doivent être conservées pendant la période nécessaire à la finalité poursuivie, puis supprimées ou sauvegardées selon les exigences légales. Tous ces principes visent à minimiser les risques de surutilisation et d'utilisation inappropriée des connaissances médicales et à permettre leur exploitation lorsque cela est justifié.

Enfin, la sécurité est un principe transversal de la protection des données de santé. Les responsables du traitement doivent prendre des mesures techniques et organisationnelles appropriées pour protéger la confidentialité, l'intégrité et la disponibilité des informations qu'ils détiennent. Il ne s'agit pas seulement de mettre en place un bon système informatique, mais aussi d'adopter une approche appropriée de gestion des risques pour la sécurité de l'information, la sécurité des systèmes d'information, la sensibilisation des utilisateurs et la prévention des violations de données. Les divers principes régissant le traitement des données de santé ont un objectif commun : permettre l'exploitation des informations cruciales pour le fonctionnement du système de santé tout en protégeant les droits des patients. Ils sont à la base de toutes les obligations légales qui sont discutées dans les paragraphes suivants.

2.2. Les acteurs de la protection des données de santé

La mise en œuvre des principes dérivés du RGPD dépend également de la participation d'acteurs complémentaires dans le domaine de la protection des données de santé. La protection des données de santé ne repose pas seulement sur les outils techniques utilisés, mais aussi sur l'organisation dans laquelle chacun se voit attribuer des responsabilités spécifiques. Cette répartition des rôles garantit que les données sont protégées et sécurisées tout au long du processus.

Le responsable du traitement est l'épine dorsale de tout le système. Il décide des finalités du traitement et de la manière dont cela sera fait. Il est de sa responsabilité de se conformer au RGPD et de prendre des mesures pour protéger les données. À ses côtés intervient le sous-traitant, qui traite les données pour le compte du responsable de traitement selon les instructions qui lui sont données. Si leurs missions diffèrent, leur collaboration est indispensable pour assurer une gestion conforme et sécurisée des données de santé.

Afin d'accompagner ces acteurs dans leurs obligations, certaines structures disposent également d'un délégué à la protection des données (Data Protection Officer – DPO). Véritable référent en matière de protection des données, il conseille les organismes, veille au respect de la réglementation et participe à la diffusion d'une véritable culture de la protection des données au sein des établissements. Son intervention illustre l'importance croissante accordée à la gouvernance des données de santé dans un contexte de transformation numérique.

Enfin, la protection des données de santé passe également par un hébergement répondant à des exigences de sécurité renforcées. Les hébergeurs certifiés « Hébergeur de Données de Santé » (HDS) garantissent que les informations médicales sont conservées dans un environnement répondant aux exigences réglementaires en matière de confidentialité, de disponibilité et d'intégrité. L'intervention conjointe de ces différents acteurs traduit une idée essentielle : la protection des données de santé ne repose pas sur une obligation individuelle, mais sur une responsabilité partagée mobilisant des compétences juridiques, techniques et organisationnelles.

2.3. Les droits reconnus aux patients

La protection des données de santé ne consiste pas seulement à imposer des obligations aux professionnels de santé ou aux organisations manipulant ces informations. Il s'agit également de reconnaître les droits des patients à garder le contrôle de leurs données et à conserver une capacité à les utiliser. Cela place l'individu concerné au centre du système de protection et crée la confiance dans le système de santé numérique.

À cet égard, chaque individu doit être correctement informé sur la collecte et l'utilisation des données. Des informations telles que la finalité du traitement, les personnes recevant les données, la période de conservation et les droits du patient. En plus de cette exigence de transparence, la réglementation reconnaît des droits garantis aux individus : y accéder, demander que les informations soient corrigées si les données sont inexactes, ou s'opposer à certains traitements dans les cas prévus par la loi. Le *Dictionnaire Permanent Santé, Bioéthique, Biotechnologies* rappelle que ces droits constituent des garanties essentielles destinées à assurer le respect de la vie privée et des libertés individuelles.

La réglementation prévoit également, dans certaines situations, le droit à l'effacement, la limitation du traitement ou encore la portabilité des données. Toutefois, l'exercice de ces droits n'est pas absolu. En matière de santé, certaines limitations peuvent être justifiées afin d'assurer la continuité des soins, de répondre à des obligations légales ou de préserver des missions d'intérêt public, notamment dans le domaine de la recherche médicale. Cette recherche permanente d'un équilibre entre les droits des patients et les besoins du système de santé illustre toute la complexité de la protection des données de santé.

Ainsi, les droits du patient ne doivent pas être perçus comme une contrainte supplémentaire pour les praticiens de santé, mais comme une garantie essentielle d'une utilisation éthique, transparente et responsable des données médicales. Ils résultent de la volonté du législateur de placer le patient au centre des décisions concernant ses informations personnelles et constituent l'un des piliers de la confiance nécessaire au développement de la santé numérique.

2.4. Le contrôle du respect des règles : responsabilités et sanctions

L'efficacité du cadre juridique des données de santé dépend non seulement des règles de protection mais aussi de leur capacité à être surveillées. De nombreuses nations et agences sont chargées de l'application et de l'exécution des normes du RGPD et en France, **la Commission Nationale de l'Informatique et des Libertés (CNIL)** est au cœur de ce système. Elle peut assister les organisations dans la conformité et la surveillance du traitement des données et peut intervenir si une violation des règles est reconnue. Le *Dictionnaire Permanent Santé, Bioéthique et Biotechnologies* rappelle également que les responsables de traitement sont tenus de signaler certaines violations de données à la CNIL ou aux personnes concernées lorsque ces violations représentent une grande menace pour leurs droits et libertés.

Le respect de ces obligations peut également faire l'objet d'un contrôle judiciaire. À ce titre, la décision récente du Conseil d'État d'anonymiser les données de santé montre comment les juridictions jouent un rôle dans la construction et l'interprétation du droit lié à la santé numérique. La protection des données n'est pas un domaine statique, nous devons évoluer constamment et être sensibles aux nouvelles technologies et aux façons dont les données médicales sont utilisées.

Les responsables de traitement sont responsables en cas de non-conformité, qu'elle soit administrative, civile ou pénale. En plus des sanctions, ces mécanismes visent principalement à aider les participants du système de santé à être plus sûrs et durables dans leur pratique. Ainsi, le contrôle par les autorités compétentes contribue à garantir la confiance des patients dans les outils numériques et contribue pleinement à la sécurité du système de santé.

3. De la théorie à la pratique : protéger les données au quotidien

3.1. L'intégration de la protection des données dans l'exercice médical

Intégrer la protection des données dans le travail médical. La transformation numérique du système de santé a complètement changé la pratique professionnelle. Désormais, les professionnels de santé ne se contentent pas de poser un diagnostic ou de prescrire un traitement. La quantité de données médicales qu'ils doivent traiter au quotidien est très élevée et est traitée par le personnel médical à partir de dossiers patients informatisés, de formulaires de prescription électronique, de messageries sécurisées, de dispositifs de téléconsultation, etc. Dans ce contexte, la protection des informations de santé n'est plus seulement un devoir légal, c'est un composant fondamental de la pratique médicale.

Cette transformation nécessite un véritable changement d'attitude des professionnels de santé. Le médecin n'est pas seulement responsable de la qualité des soins prodigués, il est également responsable de la sécurité des informations qu'il collecte, consulte et partage. Toute décision concernant l'utilisation d'un outil numérique, d'un logiciel ou d'une méthode pour transmettre des informations médicales peut avoir un impact sur la confidentialité des données des patients. Ainsi, la protection des données n'est plus le travail des avocats ou des experts en informatique, mais fait partie du travail quotidien du médecin.

L'article publié par *Le Quotidien du Médecin* illustre cette évolution en soulignant que les exigences relatives à la protection des données doivent être intégrées dès l'installation d'un cabinet médical. Le choix des outils numériques, l'organisation des échanges d'informations ou encore la sécurisation des

données ne constituent pas des démarches secondaires réalisées après l'ouverture du cabinet. Elles participent pleinement à la construction d'un exercice professionnel conforme aux exigences actuelles du numérique en santé. Cette approche montre que la protection des données doit être pensée en amont et intégrée à l'organisation même de la pratique médicale.

Ainsi, l'évolution du système de santé change progressivement les compétences que les professionnels sont censés posséder. Les médecins doivent, en plus d'être des experts médicaux et scientifiques, être capables de prendre en compte la confidentialité, l'intégrité et la sécurité des données de santé et devront agir pour les protéger. La connaissance de ces éléments est désormais aussi essentielle pour des soins médicaux responsables et la confiance des patients.

3.2. Les bonnes pratiques au sein d'un cabinet médical

Le respect des règles relatives à la protection des données de santé repose avant tout sur l'adoption de bonnes pratiques au quotidien. Si le cadre juridique fixe les obligations des professionnels de santé, leur mise en œuvre dépend de nombreux choix organisationnels et techniques réalisés dès l'installation du cabinet. Comme le souligne *Le Quotidien du Médecin*, la sécurité des données ne s'improvise pas : elle doit être anticipée et intégrée à l'organisation de l'exercice médical.

Parmi les recommandations importantes figurent l'équipement à usage professionnel uniquement. L'ordinateur, les logiciels professionnels et les outils de communication de la pratique doivent être mis à jour régulièrement pour éviter les vulnérabilités de sécurité qui pourraient être exploitées lors de cyberattaques. De même, l'utilisation des données médicales doit être sécurisée de manière à ce que seules les personnes autorisées puissent accéder aux informations des patients avec une authentification forte d'un ou plusieurs mots de passe personnels et sécurisés du patient.

L'article souligne également la nécessité de solutions numériques pour les soins de santé. Les échanges d'informations médicales doivent privilégier des outils sécurisés, tels que la messagerie sécurisée de santé (MSSanté), tandis que les données doivent être confiées à des hébergeurs certifiés « Hébergeur de Données de Santé » (HDS), répondant à des exigences spécifiques en matière de confidentialité et de sécurité. Enfin, la réalisation régulière de sauvegardes constitue une mesure essentielle afin de garantir la continuité de l'activité en cas de panne, de perte de données ou d'attaque informatique.

Outre ces mesures techniques, ces recommandations traduisent une évolution plus profonde de la pratique médicale. La protection des données de santé n'est plus une question de conformité à la loi mais fait désormais partie de l'ensemble de la gestion de la qualité et des risques. Et adopter ces meilleures pratiques signifie protéger non seulement les informations médicales des patients mais aussi la continuité des soins ainsi que la confiance qui est fondamentale dans la relation thérapeutique.

3.3. Les violations de données : prévenir et réagir

Malgré la mise en place de nombreuses mesures de sécurité, le risque de violation des données de santé ne peut être totalement éliminé. La violation de sécurité peut être causée par une cyberattaque, un ordinateur portable perdu, un accès non autorisé aux dossiers médicaux ou une mauvaise transmission. C'est un gros problème pour la sécurité des patients dans les établissements de santé et les pratiques médicales qui sont désormais davantage exposés aux risques informatiques.

Le professionnel de santé doit être prêt à intervenir dans cette situation. La réglementation impose d'évaluer rapidement la gravité de l'incident et, lorsque celui-ci est susceptible d'engendrer un risque pour les droits et libertés des personnes concernées, d'en informer la CNIL. Dans les situations les plus graves, les patients concernés doivent également être informés afin qu'ils puissent prendre les mesures nécessaires pour protéger leurs intérêts. L'objectif de ces démarches n'est pas uniquement de satisfaire une obligation réglementaire, mais de limiter les conséquences de la violation et de préserver la confiance des patients.

Toutefois, la meilleure réponse demeure la prévention. La sensibilisation des professionnels de santé, la mise à jour régulière des outils numériques, la sauvegarde des données et l'élaboration de procédures internes permettent de réduire considérablement le risque d'incident. Comme le souligne *Le Quotidien du Médecin*, la protection des données ne doit pas être envisagée uniquement comme une réaction face aux cyberattaques, mais comme une démarche continue intégrée à l'exercice professionnel. Cette approche préventive apparaît aujourd'hui comme l'un des principaux défis de la médecine numérique.

4. L'anonymisation : entre protection et exploitation des données

4.1. L'anonymisation : un outil essentiel de protection des données

L'anonymisation est un outil clé pour la protection des données. Les données de santé sont désormais une source critique pour améliorer la qualité des soins, la recherche médicale et le soutien aux innovations numériques. Mais la confidentialité doit être prise en compte pour que nous puissions les utiliser pour l'exploration de données. L'anonymisation est clairement l'un des mécanismes clés pour concilier l'exploitation des données avec la confidentialité. Elle vise à rendre impossible l'identification d'une personne à partir des données traitées afin que celles-ci puissent être utilisées sans porter atteinte à ses droits.

Le but de l'anonymisation est de conserver la valeur des données tout en rendant le risque de leur utilisation aussi négligeable que possible. Une fois anonymisées, les données peuvent être utilisées

pour des études scientifiques ou des examens de politiques de santé et pour approfondir la connaissance des problèmes de santé, mais sans révéler l'identité de la personne concernée. Cette approche a donc le double objectif de faire progresser la santé et de protéger le patient. Comme l'indique le *Dictionnaire Permanent Santé, Bioéthique, Biotechnologies*, l'anonymisation occupe aujourd'hui une place centrale dans les réflexions relatives au traitement des données de santé.

Pour autant, l'anonymisation n'est pas seulement une opération technique pour supprimer le nom ou le prénom d'un patient. Elle implique des processus plus complexes pour empêcher l'identification directe ou indirecte de la personne concernée. Avec le développement des capacités de traitement des données et le croisement de multiples bases d'informations, cette exigence est particulièrement ambitieuse. Ainsi, bien que l'anonymisation soit un outil puissant de protection, l'efficacité de cet outil est désormais une question que nous aborderons dans la sous-section suivante.

4.2. Les limites de l'anonymisation : le risque de réidentification

Si l'anonymisation constitue un outil essentiel de protection des données de santé, son efficacité soulève néanmoins plusieurs interrogations. Les progrès des technologies numériques et le développement de puissants outils d'analyse rendent aujourd'hui possible le croisement d'un grand nombre de bases de données. Dans certaines situations, ces recoupements permettent de retrouver l'identité d'une personne à partir d'informations qui avaient pourtant été anonymisées. L'anonymisation ne doit donc plus être envisagée comme une garantie absolue, mais comme un processus dont l'efficacité dépend des méthodes employées et du contexte dans lequel les données sont utilisées.

C'est un point soulevé par le Conseil d'État le 13 février 2026 dans le *Dictionnaire Permanent Santé, Bioéthique, Biotechnologies*. La cour indique que l'évaluation du caractère véritablement anonyme d'un ensemble de données ne peut se limiter à la suppression des éléments identifiants de l'ensemble de données. Elle nécessite également de prendre en compte qu'une personne peut être ré-identifiée par le croisement de plusieurs informations. C'est une étape importante dans la protection des données de santé qui prend désormais en compte les capacités de plus en plus avancées de traitement des données et d'exploitation des technologies numérique.

Cette évolution met en lumière une difficulté majeure : plus les données conservent de précision, plus elles sont intéressantes pour la recherche, l'évaluation des pratiques médicales ou le développement de l'intelligence artificielle. En comparaison, une anonymisation excessive peut limiter sévèrement l'utilité scientifique des données de santé. La protection des données de santé ne consiste donc plus simplement à supprimer les éléments identifiants, mais à déterminer le niveau de protection nécessaire pour que les données restent utiles pour la mission pour laquelle elles sont employées. Cette réflexion nous amène donc à plus qu'une simple approche technique de l'anonymisation, c'est une recherche constante d'un équilibre optimal entre innovation et protection de la vie privée.

5. Quels défis pour les professionnels de santé à l'ère du numérique ?

Les développements précédents montrent que la protection des données de santé ne constitue plus une simple obligation réglementaire venant s'ajouter à l'exercice médical. Elle s'impose désormais comme une composante essentielle de la pratique professionnelle. La transformation numérique du système de santé a profondément modifié les modalités de prise en charge des patients, les échanges entre professionnels et les usages des données médicales. Cette évolution, porteuse de nombreux bénéfices pour la qualité des soins et le développement de la recherche, impose également de nouvelles responsabilités aux professionnels de santé. Ceux-ci doivent aujourd'hui être capables d'intégrer les exigences juridiques, techniques et éthiques relatives à la protection des données dans leur pratique quotidienne, tout en garantissant une prise en charge efficace des patients. Les documents analysés montrent ainsi que la protection des données ne peut plus être considérée comme une contrainte extérieure à l'exercice médical, mais comme une condition indispensable à son bon fonctionnement.

Cette évolution devrait se poursuivre dans les années à venir avec le développement de nouveaux outils numériques. L'intelligence artificielle, les dispositifs médicaux connectés, la télésurveillance ou encore la médecine personnalisée reposent sur l'exploitation d'un volume toujours plus important de données de santé. Ces innovations ouvrent des perspectives considérables pour améliorer le diagnostic, personnaliser les traitements ou renforcer la prévention. Toutefois, elles soulèvent également de nouvelles interrogations concernant la confidentialité des informations, la sécurité des systèmes numériques et le risque de réidentification des patients. Les débats récents autour de l'anonymisation montrent que les mécanismes de protection devront continuer à évoluer afin de s'adapter aux progrès technologiques sans freiner l'innovation médicale.

Dans ce contexte, les compétences attendues des professionnels de santé sont appelées à évoluer. Au-delà des connaissances scientifiques et cliniques, l'exercice médical nécessite désormais une compréhension minimale des outils numériques, des principes juridiques encadrant le traitement des données ainsi que des bonnes pratiques en matière de cybersécurité. Cette évolution ne signifie pas que le médecin devient un spécialiste du droit ou de l'informatique. En revanche, elle implique qu'il soit en mesure d'identifier les principaux enjeux liés à la protection des données, de collaborer avec les différents acteurs concernés et d'adopter des pratiques conformes aux exigences actuelles du numérique en santé. Cette approche rejoint les recommandations formulées pour l'installation des professionnels de santé, qui insistent sur l'intégration de ces questions dès le début de l'exercice professionnel.

CONCLUSION

En définitive, la protection des données de santé apparaît aujourd'hui comme un enjeu transversal, à la croisée du droit, de la médecine, de l'informatique et de l'éthique. Les évolutions technologiques continueront sans doute à transformer les pratiques médicales et à faire émerger de nouveaux défis. Dans ce contexte, l'objectif ne sera pas d'opposer innovation et protection des données, mais de construire un cadre permettant de concilier ces deux exigences. La confiance des patients, indispensable au développement du numérique en santé, dépendra largement de cette capacité à garantir une utilisation responsable, sécurisée et transparente de leurs données. C'est à cette condition que les innovations numériques pourront pleinement contribuer à l'amélioration des soins tout en respectant les droits fondamentaux des personnes.

BIBLIOGRAPHIE

Ouvrage / Documentation juridique

Dictionnaire Permanent Santé, Bioéthique, Biotechnologies. *Traitement de données de santé.* Éditions Législatives, version 2025.

Dictionnaire Permanent Santé, Bioéthique, Biotechnologies. *E-santé : L'anonymisation des données de santé devant le Conseil d'État.* Mars 2026.

Presse professionnelle

Le Quotidien du Médecin. *Comment intégrer la protection des données lors de son installation.* Mars 2024.