

**DU BON USAGE DES DONNÉES MÉDICALES
AUDIOVISUELLES
LORS DES PRATIQUES OPÉRATOIRES
CONFORME À L'ÉTHIQUE MÉDICALE
ET À LA PROTECTION DES DONNÉES DES PATIENTS**

**GUIDE D'ORIENTATION
DES CHIRURGIENS ET DES MÉDECINS INTERVENTIONNELS**

30 mars 2023

PRÉAMBULE

Pourquoi un guide pratique sur l'utilisation des images et vidéos médicales pour les chirurgiens et médecins interventionnels ?

L'Académie Nationale de Chirurgie (ANC) et l'IRCAD ont élaboré conjointement ce guide dont l'objectif est de sensibiliser et d'accompagner les professionnels de santé et les organismes de formation continue dans le respect des principes d'utilisation et de protection des données audiovisuelles médicales (en conformité avec le règlement général de protection des données ou RGPD) réalisées à des fins :

- de formation chirurgicale initiale ou continue des professionnels de santé
- d'information du public
- et de promotion de la recherche chirurgicale.

Depuis une quarantaine d'années, les technologies numériques ont pris une part de plus en plus déterminante dans l'apprentissage et le partage du savoir-faire chirurgical. Elles permettent de suivre en toutes circonstances, en présentiel et à distance, des opérations chirurgicales réalisées et diffusées dans le monde entier. Le recours à ce type de techniques audiovisuelles numériques pour la formation, la transmission et le partage des savoirs s'avère d'un intérêt incontestable. La majorité des jeunes chirurgiens en formation initiale utilise actuellement des ressources vidéo en complément ou à la place des ressources pédagogiques classiques.

L'ANC et l'IRCAD constatent que ces vidéos sont souvent trouvées librement en ligne sans régulation sur la qualité scientifique du contenu, ni sur l'effort pédagogique qui devrait leur être consacré.

Alors que les instances chirurgicales nationales chirurgicales et universitaires se dotent progressivement d'outils pour produire des vidéos chirurgicales pédagogiques de qualité, elles soulignent qu'elles sont confrontées à un manque de clarté de la réglementation et de la loi en la matière.

Il leur paraît cependant qu'une clarification de cette réglementation est nécessaire tant pour protéger et accompagner leurs auteurs que pour protéger les patients d'une divulgation à leur insu de leurs données personnelles de santé, voire du secret médical les concernant.

En effet, les images et vidéos peuvent être considérées, même après application de mesures de précaution, d'anonymisation, de masquage d'éléments identifiants, de floutage et de sécurité, comme des données personnelles de santé, hautement sensibles et couvertes par le secret médical, dont la réutilisation est strictement encadrée afin de protéger les personnes concernées (patients, personnels soignants, etc.).

L'ANC et l'IRCAD considèrent que la protection des données personnelles et de la vie privée des patients constituent un impératif et une préoccupation dont il convient de tenir compte en conciliant le droit des personnes, l'éthique des bonnes pratiques cliniques avec l'intérêt de la formation, la recherche et les avancées thérapeutiques.

L'objectif de ce guide est de répondre à la question suivante : comment réaliser et diffuser des vidéos et images à visée exclusivement pédagogique pour l'information du public d'une part et d'autre part pour le partage des connaissances à destination des professionnels de santé tout en respectant la réglementation en vigueur en matière de protection de données personnelles, sachant que la doctrine dans la jurisprudence nationale et européenne n'apporte pas suffisamment d'éclairage sur ce sujet.

L'un des rares documents proposant des préconisations concrètes est celui publié par l'ANC en 2019, intitulé « Préconisations pour une session de Chirurgie en direct ou Live Surgery » (cf. www.academie-chirurgie.fr). [Les Rapports | Académie Nationale de Chirurgie \(academie-chirurgie.fr\)](#)

C'est la raison pour laquelle l'ANC et l'IRCAD ont décidé d'élaborer un guide juridique et éthique concernant notamment la transmission en direct ou en différé audiovisuelle et digitalisée via le web de séances de pratiques opératoires chirurgicales et interventionnelles.

L'usage légitime de ces informations à des fins pédagogiques, de recherche et de formation doit être encadré par des règles protectrices des droits du patient qu'il s'agisse du respect de son consentement, du secret médical et de la confidentialité. Ce guide a pour but de favoriser le développement nécessaire de ces approches dans un contexte d'éthique et de rigueur des pratiques, de respect de la déontologie, de responsabilisation des professionnels de santé, de transparence et de confiance.

Les patients qui acceptent une intervention chirurgicale relayée par des moyens audiovisuels digitalisés et mis en ligne, doivent être considérés comme des partenaires de la recherche : les engagements des professionnels de santé à leur égard relèvent de valeurs et d'engagement inconditionnels.

Ce Guide d'orientation des pratiques a été rédigé en février 2023 en tenant compte de l'état de l'art des pratiques innovantes en chirurgie et des encadrements juridiques qui s'imposent. Il pourra subir des adaptations en fonction de l'évolution des dispositifs et des réglementations.

En effet, qu'il s'agisse du code de déontologie du Conseil National de l'Ordre des Médecins (CNOM), et ses commentaires en particulier l'article 19-1, du guide pratique sur la protection des données personnelles CNOM-CNIL de juin 2018, du décret 2020-1662 du 24 décembre 2020 sur l'information du public par les médecins, nulle part les vidéos pseudonymisées ne sont mentionnées. Ces points nécessiteront d'être précisés par la Commission nationale de l'informatique et des libertés (CNIL). Il faudra probablement considérer différemment, sur certains points, les vidéos pseudonymisées des données personnelles de santé.

Dans la mesure où ce guide n'a pas été validé par la CNIL, et même si les textes de référence ont été examinés par plusieurs juristes, il n'a pas de valeur juridique.

I/ MISE AU POINT SUR L'ÉTAT DE LA RÉGLEMENTATION APPLICABLE

- Le 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 (ci-après le « RGPD »).
- En France, c'est la CNIL qui est responsable de son application.
- La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, telle que modifiée (ci-après la « loi Informatique et Libertés »).
- Le code de santé publique, dont sa modification par décret 2020-1662 du 22 décembre 2020.

La réglementation de protection des données à caractère personnel (RGPD)

Il s'agit de protéger les données personnelles :

- des patients,
- de l'équipe médico-chirurgicale,
- de l'établissement de santé

afin de permettre une anonymisation des données (voir Annexe 1).

Le droit à l'image (voir annexe 2)

Le secret médical (voir annexe 3)

La protection par le droit de la propriété intellectuelle (voir annexe 4)

Afin de permettre la conformité des enregistrements à ces différentes réglementations, il est nécessaire de disposer d'une connaissance claire des caractéristiques du projet, des modalités d'enregistrement et de réutilisation, de façon à identifier et appliquer les obligations entre les parties prenantes et à assurer leur respect.

A - Détermination des principales caractéristiques du projet

Nature des données collectées et traitées

- Lister précisément les données collectées et générées grâce aux dispositifs d'enregistrement installés : images opératoires « externes », par exemple segment cutané, organes, etc. ; images peropératoires, issues des caméras endoscopiques ; sons par exemple la voix des chirurgiens et du personnel médical, la voix d'autres praticiens apportant leur expertise.
- Si ces enregistrements font l'objet de mesures de pseudonymisation ou d'anonymisation.
- Lister les personnes concernées : patient, professionnel de santé, autre personnel, administration, établissement, etc.

Nature des flux et des opérations de traitement sur les données

La description de la nature des flux et des opérations de traitements sur les données doit permettre de suivre l'enregistrement depuis sa création jusqu'à son archivage ou sa destruction. Elle permet d'identifier les destinataires des enregistrements, d'identifier les finalités pour lesquelles les enregistrements sont effectivement utilisés et de suivre les mesures de sécurité (y compris de pseudonymisation ou d'anonymisation) dont ils font l'objet.

Au demeurant, cette description permet de démontrer aux autorités de protection des données la maîtrise du traitement, la conformité des procédures, et notamment que le promoteur et l'investigateur respectent les règles en vigueur, en particulier les droits des patients qui pourraient s'opposer à l'utilisation ou à la diffusion des enregistrements, si ceux-ci ne sont pas anonymisés.

Identification des objectifs et des finalités d'utilisation des enregistrements

Il est impératif d'identifier les raisons pour lesquelles les enregistrements seront utilisés.

Du point de vue de la propriété intellectuelle, cela permet de vérifier que les destinataires des enregistrements disposent des licences d'utilisation adéquates pour réutiliser les enregistrements.

Du point de vue de la protection des données, cela est nécessaire pour assurer la maîtrise du traitement et sa conformité. La finalité doit être précisée, légitime et explicite, compatible avec les missions de l'organisme traitant les données personnelles. Les finalités doivent être indiquées aux personnes concernées (les patients et les professionnels de santé intervenant pendant l'opération).

De façon générale, les opérations chirurgicales font l'objet d'enregistrements audiovisuels pour les finalités suivantes :

- Dans un premier temps, les enregistrements audiovisuels sont réalisés dans le cadre et pour les finalités du soin (chirurgie), au bénéfice direct des patients.
- Dans un second temps, ces enregistrements audiovisuels sont réutilisés :
 - o À des fins pédagogiques (de formation initiale ou continue, des professionnels de santé, ou des patients) et
 - o À des fins de recherche.

B - Rôles et qualifications des parties prenantes

Il est également essentiel d'identifier les parties prenantes afin de déterminer leur statut ou qualification, ce qui permettra ensuite de répartir de façon adéquate les obligations de chacune, notamment par voie contractuelle.

Du point de vue de la propriété intellectuelle, il est nécessaire d'identifier le titulaire des droits sur les enregistrements de façon à établir les conditions de cession ou la concession des droits sur les enregistrements aux destinataires identifiés.

Du point de vue de la réglementation de protection des données personnelles, il est nécessaire de qualifier les parties, qu'il s'agisse :

- Du responsable de traitement, qui détermine, seul ou conjointement, les finalités et les moyens du traitement ;
- Du sous-traitant, qui agit pour le compte et sur instructions du responsable de traitement.

Les qualifications de chacune des parties vont varier selon les étapes de la diffusion des enregistrements et des finalités initiales et ultérieures.

- *Par exemple*, un hôpital qui enregistre une opération dans le cadre d'un acte de soin que son personnel effectue sur un patient est responsable de ce traitement dont la finalité est le soin. Toutefois, si cet hôpital transmet ensuite les enregistrements à un institut de recherche ou de formation, ce dernier devient responsable du traitement de ces enregistrements aux fins de recherche ou de formation.

Du point de vue du droit de la santé, il est nécessaire d'identifier la personne réglementairement responsable de la recherche ou le promoteur, ainsi que les investigateurs, afin de répartir adéquatement les obligations corollaires.

II/ RAPPEL SUR LES PRINCIPALES OBLIGATIONS À RESPECTER

Nous proposons dans ce Guide d'orientation des pratiques, les repères indispensables sous forme d'une liste de contrôle ou « checklist » qui n'a pas vocation à se substituer à l'impératif d'une approche juridique et éthique spécifiques à tout recours aux données médicales audiovisuelles en chirurgie.

- 1- Consentement du patient, garanties sur l'anonymisation et sur le respect du secret médical
- 2- Droit du patient de se rétracter à tout moment sur le consentement donné
- 3- Respect des obligations de documentation d'information sur les traitements réalisés
- 4- Engagements conformes aux règles éthiques, des sous-traitants pour la production, les traitements et l'hébergement des données
- 5- Transferts internationaux
- 6- Respect du code de santé publique
- 7- Analyse d'impact éventuel
- 8- Durée de conservation consentie et précisée

1 - Rappel du régime applicable : consentement ou intérêt public accompagné d'une autorisation de la CNIL

Le RGPD impose que tous les traitements de données de santé à caractère personnel soient fondés à la fois sur une base légale (telle qu'une mission d'intérêt public, l'intérêt légitime du responsable de traitement, le consentement)¹ et sur une exception au principe d'interdiction de traitement des données sensibles.

Ce sont ces exigences qui entraînent la nécessité d'obtenir soit le consentement du patient, soit une autorisation de la CNIL en s'appuyant sur la démonstration d'un intérêt public (*autorisation ad hoc ou déclaration de conformité*) pour réutiliser les enregistrements à des fins d'information, de formation ou de recherche.

¹ RGPD, art. 6

Les exceptions au principe d'interdiction sont multiples ; elles proviennent à la fois du RGPD et de la loi Informatique et Libertés (Annexe 5).

Ainsi, afin de réutiliser les enregistrements à des fins d'information, de formation et de recherche, il est donc nécessaire de se baser sur :

- Le recueil du consentement exprès du patient, qui constitue une exception à l'interdiction de traitement des données de santé et une exception à l'obligation d'autorisation CNIL et de démonstration d'un intérêt public ;
- La démonstration d'un intérêt public qui va de pair avec une autorisation de la CNIL.
- Dans le cadre de ce régime, *la CNIL a développé des méthodologies de référence, qui permettent d'effectuer une simple déclaration de conformité à l'une de ces méthodologies, sans avoir à effectuer une demande d'autorisation ad hoc.*

Ces méthodologies de référence ont notamment vocation à s'appliquer à des traitements ayant pour finalités les recherches, évaluations et études dans le domaine de la santé.

À cela s'ajoutent dans certains cas des formalités ou demandes d'avis complémentaires à effectuer, par exemple auprès des Comités de protection des personnes (CPP), du Comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé (Health Data Hub, CESREES), des autorités sanitaires (ANSM).

- Il peut être dérogé à l'obligation d'obtenir l'autorisation de la CNIL et de démonstration d'un intérêt public si le traitement entre dans le champ de *certaines exceptions limitativement énumérées* par l'article 65 de la Loi Informatique et Libertés (Annexe 6).

2 - Consentement du patient

1- Consentement explicite

Le consentement explicite des patients présente certains avantages. Il permet d'assurer un haut niveau de transparence et de loyauté du traitement, en donnant au patient un moyen de contrôle sur le traitement. Ceci implique de fortes exigences à respecter en termes d'information ainsi que de conditions de validité du consentement (univoque, libre, spécifique, informé, et dans le cadre des données de santé, explicite).

Toutefois, cet avantage est fortement contrebalancé par les risques liés à l'impossibilité de donner suite à un retrait de consentement, dans le cadre des traitements aux fins d'information, de formation et de recherche. A la différence du droit d'opposition, le consentement peut être retiré de façon discrétionnaire et sans motif par les patients.

Le responsable du traitement doit veiller à ce qu'il soit aussi simple pour la personne concernée de retirer que de donner son consentement, et à ce que cela puisse être fait à tout moment².

Comme rappelé par le CEPD, si le consentement est retiré, « *toutes les opérations de traitement des données basées sur le consentement ayant eu lieu avant le retrait du consentement – et conformes au RGPD – restent licites, mais le responsable du traitement doit cesser les activités de traitement en question. Si aucune autre base juridique ne justifie le traitement des données (par exemple, période de conservation), celles-ci devraient être supprimées par le responsable du traitement* »³.

Or, compte tenu des mesures visant à protéger la confidentialité de l'identité des patients, il apparaît en pratique difficile de retrouver l'enregistrement correspondant au patient et donc de lui permettre d'exercer effectivement ce droit de retrait. *Il est possible d'envisager de maintenir une table de correspondance confidentielle, tenue par le promoteur, permettant de donner suite à une demande, y compris sur les réseaux* – toutefois, une telle mesure réduirait le niveau de protection de la confidentialité de l'identité des personnes. Si ce fondement ne pouvait être mis en œuvre en respectant pleinement les garanties pour les droits et libertés des personnes, il existerait un risque que ce fondement ne soit donc pas considéré comme adapté par les autorités de protection des données.

Il peut exister d'autres limites à la demande de retrait du consentement :

Par ailleurs, il n'est pas certain que le seul consentement des patients, au sens du RGPD, soit suffisant pour lever le secret professionnel applicable à tout élément du dossier médical du patient.

Le secret professionnel est un secret absolu, qui s'impose directement au professionnel de santé et pour lequel il n'appartient pas nécessairement au patient de décider s'il peut être levé.

² RGPD, art. 7, §3

³ CEPD, Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679, v 1.1, 4 mai 2020, §117

Les dérogations à la règle du secret médical doivent être prévues par un texte de nature législative ou en être, selon la jurisprudence du Conseil d'État, la conséquence nécessaire.

Or, les exceptions prévues par la Loi Informatique et Libertés renvoient plutôt au régime d'autorisation et d'intérêt public, prévoyant que « *nonobstant les règles relatives au secret professionnel, les membres des professions de santé peuvent transmettre au responsable d'un traitement de données autorisé en application de l'article 66 les données à caractère personnel qu'ils détiennent* »⁴. Il existe ainsi un risque que le secret professionnel ne puisse être levé par le seul consentement du patient.

Enfin, le consentement pose des limites rigides aux traitements ultérieurs pouvant être réalisés, dès lors qu'en vertu de la condition de spécificité du traitement, le patient devrait pouvoir être informé avec précision de l'ensemble des finalités, y compris pour chaque recherche : le RGPD, dans ses considérants, apporte une certaine flexibilité sur ce point : « *il n'est pas possible de cerner entièrement la finalité du traitement des données à caractère personnel à des fins de recherche scientifique au moment de la collecte des données. Par conséquent, les personnes concernées devraient pouvoir donner leur consentement en ce qui concerne certains domaines de la recherche scientifique, dans le respect des normes éthiques reconnues en matière de recherche scientifique* »⁵.

Toutefois, au-delà du fait que cette ouverture ne peut concerner que des traitements aux fins de recherche et non d'enseignement, les autorités de protection des données ont adopté une vision plus restrictive de cette possibilité de « consentement large », surtout lorsque des données de santé sont traitées : « *en principe, les projets de recherche scientifique ne peuvent inclure des données à caractère personnel sur la base du consentement de la personne concernée que si leur finalité est décrite avec précision (...) lorsque des catégories particulières de données sont traitées sur la base d'un consentement explicite, l'application de l'approche flexible décrite au considérant 33 devra être soumise à une interprétation plus stricte et nécessitera un contrôle minutieux* »⁶.

⁴ L. n° 78-17, 6 janv. 1978 mod., art. 68.

⁵ RGPD, csd. 33

⁶ CEPD, Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679, v1.1, 4 mai 2020, §155 et s.

Les autorités recommandent, lorsque les finalités de recherche ne peuvent pas être spécifiées dans leur intégralité, que le responsable trouve « *d'autres méthodes* », notamment avec un premier consentement « *pour une finalité de recherche exprimée en termes plus généraux* », puis des consentements spécifiques par étape, au fur et à mesure de l'avancement du projet de recherche. Ce type d'approche peut être particulièrement difficile à mettre en œuvre en pratique.

Conformément aux articles 12, 13 et 14 du RGPD et L. 1111-7 du code de la santé publique, le responsable de traitement doit fournir aux personnes concernées par ses traitements de données un certain nombre d'informations, notamment l'identité du responsable de traitement, les finalités pour lesquelles les données sont traitées, les personnes à qui ces données peuvent être transmises, la durée pendant laquelle ces données sont conservées ainsi que les droits des personnes concernées sur leurs données (droit d'accès, droit d'opposition, etc.).

En ce qui concerne les patients :

En ce qui concerne les patients, il convient d'identifier le meilleur support et moment d'information afin que le patient comprenne bien la différence entre l'enregistrement effectué à des fins de soins et la potentielle transmission pour les finalités ultérieures d'information, de formation et de recherche. Cette transparence est d'autant plus importante si le fondement pour traiter les données est le consentement, afin d'en garantir la validité.

L'information peut être indiquée dans un document d'information à communiquer en amont aux patients, avec une possibilité pour le patient d'en discuter avec le professionnel de santé avec lequel il ou elle est en contact.

Par ailleurs, les supports d'information disponibles sur une source publiquement accessible, telle que le site Internet de l'hôpital, de l'institut de formation ou de recherche, ou tout autre réseau, sont des modalités utiles d'information ultérieure plus précises sur les réutilisations effectivement réalisées.

Le document d'information initiale doit y faire référence, préciser les aspects de la pseudonymisation de la vidéo pédagogique et le patient pourra ainsi trouver des informations mises à jour sur les projets de formation ou de recherche réalisées ou en cours et les projets de diffusion. Ce type de support permet également de faciliter l'exercice des droits des patients ultérieurement.

On rappelle que la qualité de la disponibilité et d'une communication bienveillante conditionne le rapport de confiance indispensable dans la relation entre la personne, ses proches et l'équipe médicale.

Enfin, il existe des cas particuliers, non résolus par ce guide qui devront être examinés avec la CNIL :

- Cas pédiatriques : qu'en est-il de l'avis de l'enfant devenu adulte (même si les parents étaient d'accord), il faut être très vigilant surtout concernant le droit à l'image éventuel
- Cas de la chirurgie de la face (neurochirurgie, chirurgie plastique et esthétique, orale, ophtalmologique, maxillofaciale, ORL)

Un document type est fourni dans l'annexe 9.

En ce qui concerne les professionnels de santé

En ce qui concerne les professionnels de santé, cette information peut être tracée dans le contrat conclu entre le responsable de traitement et les professionnels de santé, s'il en existe un, ou bien dans des documents d'information mis à des dispositions des professionnels.

- Par exemple, si le responsable de traitement des enregistrements utilisés à des fins de formation, d'information et de recherche est l'employeur des professionnels de santé, l'information peut être indiquée dans leur contrat de travail, dans des politiques internes ainsi que par des affichages à l'entrée des blocs.
- Par exemple, si le responsable de traitement n'est pas l'employeur, il conviendrait de prévoir dans le contrat permettant la transmission des enregistrements des obligations d'information précises des professionnels de santé, auquel l'employeur est tenu de s'engager.

2 - Intérêt public et autorisation CNIL

Les traitements de transmissions audiovisuelles médicales à des fins d'enseignement et de recherche pourraient être justifiés par une autorisation CNIL (y compris sous la forme d'un engagement de conformité à une méthodologie de référence), basée sur l'existence d'un intérêt public.

Les finalités de l'intérêt public, telles qu'explicitées par l'ancien Institut National des Données de Santé (INDS), désormais le Health Data Hub sont précisées dans l'annexe 7.

Pour caractériser un intérêt public, il n'est pas nécessaire de cumuler ces finalités, chacune d'entre elles peut permettre de justifier de cette exception. Par ailleurs, en France, la poursuite de l'intérêt public n'est pas réservée aux seules personnes publiques (CNIL, délib. n° 2017-285, 26 oct. 2017 ; CNIL, délib. n° 2017-347, 21 déc. 2017 ; CNIL, délib. n° 2018-289, 12 juill. 2018).

3 - Respecter les obligations de documentation des traitements

L'organisme en charge de la réutilisation des enregistrements doit **tenir un registre** des traitements de données à caractère personnel, mentionnant de façon précise :

- les finalités pour lesquelles ces enregistrements sont traités ;
- la base légale et l'exception sur le fondement desquels les enregistrements sont traités ;
- la durée de conservation des enregistrements ;
- les destinataires de ces enregistrements ;
- les sous-traitants impliqués dans le traitement ;
- les éventuels transferts de données vers des pays situés en dehors de l'Union européenne ;
- les mesures de sécurité appliquées au traitement.

4 - Engagement des sous-traitants pour la production, le transfert et l'hébergement des données

Il est essentiel de distinguer la vidéo **brute** non encore anonymisée ou pseudonymisée de la vidéo **traitée** anonymisée ou pseudonymisée.

Tant les responsables de traitement que les sous-traitants doivent assurer la sécurité des enregistrements, au regard de leur nature sensible, non seulement au regard de l'obligation générale de sécurité prévue par le RGPD, mais également au titre des dispositions relatives aux référentiels de sécurité et d'interopérabilité des données de santé (art. L. 1110-4-1 du CSP).

Cette obligation de sécurité passe par des mesures de sécurité telles que :

- **Authentification forte** : Les accès aux données de santé doivent s'effectuer après authentification forte (de type authentification triangulaire)⁷. Les mots de passe doivent présenter une complexité suffisante et ne doivent en aucun cas être transmis en clair⁸.
- **Mesures de contrôle des enregistrements** : dans l'idéal, les enregistrements bruts devraient demeurer sous le contrôle de l'équipe de chirurgie. Les enregistrements, voire leur transmission, depuis le bloc opératoire ne devraient pas être automatiques. Par exemple, les enregistrements pourraient être activés et désactivés manuellement et au cas par cas, sur instruction du chirurgien responsable de l'opération. En cas d'oubli, l'enregistrement, voire la transmission, doivent s'arrêter automatiquement en l'absence de flux de données. Au redémarrage des équipements, l'enregistrement, voire la transmission, devraient être désactivés par défaut.
- **Gestion des habilitations** et traçabilité des accès aux données personnelles, incluant une politique de gestion des incidents.
- **Sensibilisation des utilisateurs** : il convient d'assurer la sensibilisation des professionnels de santé ainsi que du personnel médical intervenant sur les enregistrements.
- **Chiffrement des données** : les enregistrements devraient, dans l'idéal, être transmis et stockés de façon chiffrée.
- **Hébergement certifié** : les données « *recueillies à l'occasion des activités de prévention, de diagnostic, de soin ou de suivi médico-social* » doivent être hébergés sur les serveurs d'un hébergeur certifié, lorsque cet hébergement est externalisé⁹.

Conformément aux dispositions du RGPD, il est nécessaire de prévoir :

- **Un contrat avec tout sous-traitant** intervenant dans le traitement des données à caractère personnel, contenant les clauses listées par l'article 28 du RGPD. Il s'agit de rappeler au sous-traitant ses obligations vis-à-vis du responsable de traitement (respect des instructions, limitation des finalités de traitement, modalités des audits, obligation de notification de violation des données personnelles, description précise des mesures de sécurité, etc.). La CNIL a émis

⁷ Cette recommandation de la CNIL s'inspire des principes de la PGSSI-S (Politique générale de sécurité des systèmes d'information de santé, et notamment le référentiel d'authentification des acteurs de santé, v2.0 et la grille d'applicabilité des référentiels de la PGSSI-S v1.0), qui ne sont pas à date directement applicables compte tenu de l'absence des arrêtés d'application, mais qui sont fréquemment appliqués par la CNIL.

⁸ CNIL, délib. n° 2017-012 du 19 janvier 2017 et n° 2017-190 du 22 juin 2017 portant adoption et modification d'une recommandation relative aux mots de passe

⁹ Code de la santé publique, Art. L. 1111-8

des recommandations précises sur ce point : <https://www.cnil.fr/fr/sous-traitant>.

➤ *par exemple, si les enregistrements des interventions chirurgicales sont hébergés par un prestataire ou font l'objet de retraitement ou d'analyse par un prestataire, un contrat conforme à l'article 28 doit être conclu.*

Les clauses prévues par l'article 28 sont un minimum, mais il est recommandé au responsable de traitement d'en adapter le contenu afin d'imposer au sous-traitant des obligations renforcées compte tenu de la sensibilité des données. Par ailleurs, des obligations complémentaires peuvent s'appliquer (cf. infra).

- **Un contrat avec tout responsable conjoint du traitement**, répartissant les responsabilités de chacun conformément à l'article 26 du RGPD. Le contenu des clauses n'est pas expressément prévu par la réglementation. Les responsables de traitement doivent cependant s'assurer que l'intégralité des obligations prévues par le RGPD est bien traitée et répartie de façon claire entre les responsables.

➤ *Par exemple, dans le cadre d'une recherche menée en commun par plusieurs instituts de recherche sur différents enregistrements fournis par les partenaires. Le contrat doit permettre de répartir les responsabilités de chacun, par exemple en assurant respectivement le respect des droits des personnes pour les enregistrements que chacun a fourni.*

Bien que le RGPD ne le mentionne pas expressément, il est recommandé d'encadrer contractuellement la relation avec tout autre responsable indépendant.

➤ *Par exemple, si les enregistrements sont transmis à un tiers responsable de traitement indépendant (un hôpital fournissant à un institut de recherche ou à un organisme de formation de chirurgiens les enregistrements d'interventions chirurgicales réalisés dans le cadre du soin), il est essentiel que l'hôpital impose au destinataire des obligations strictes eu égard à la sensibilité des données traitées. Des obligations telles que l'interdiction de chercher à réidentifier les patients ou encore des mesures de sécurité adaptées doivent être prévues.*

5 - Transferts internationaux de données

Le responsable de traitement doit encadrer les transferts de données personnelles vers des pays situés hors de l'Union Européenne ou de l'Espace économique européen. Un transfert peut être constitué par une transmission active de données vers l'étranger (par exemple, stockage des données sur un cloud dont certains serveurs sont en dehors

de l'UE/EEA) ou par le simple fait de donner accès à des organismes situés dans ces zones (par exemple, stockage sur un cloud dont les serveurs sont en UE mais dont la maintenance est effectuée depuis l'Inde ou les Etats-Unis).

Un tel transfert doit avoir fait l'objet d'une décision d'adéquation de la Commission européenne (certains pays bénéficient de telles décisions, comme l'Argentine, la Corée du Sud, le Japon, Israël...) voire, à défaut, de garanties appropriées en particulier, des clauses contractuelles types ou des règles contraignantes d'entreprise. Depuis la décision de la Cour de Justice de l'Union Européenne (CJUE) dite « Schrems II », une analyse de l'impact et de la capacité de la législation du pays tiers à garantir l'effectivité des droits accordés aux personnes concernées au titre de ces garanties appropriées doit être menée.

Aussi, comme pour tous ses transferts, le responsable de traitement doit cartographier les transferts de données et mettre en place les garanties appropriées (contrat de transfert utilisant les clauses contractuelles type et analyse de l'impact du transfert). Le RGPD a élargi la gamme d'outils juridiques (16 juin 2021) permettant d'encadrer les transferts hors de l'Union européenne (UE) et de l'Espace économique européen (EEE) à condition d'assurer un niveau de protection des données suffisant et approprié. Ils doivent encadrer ces transferts en utilisant les différents outils juridiques définis au chapitre V du RGPD. La question du Cloud reste en suspens.

Les modèles de clauses contractuelles types sont toujours d'actualité et ont été mis à jour par la Commission européenne le 4 juin 2021. Ils peuvent être utilisés tant par les responsables de traitement que par les sous-traitants.

Afin d'assurer un haut niveau de protection des données transférées du territoire européen à des Etats tiers, les organismes souhaitant transférer des données peuvent recourir aux outils suivants :

- La décision d'adéquation (art. 45 du RGPD), qui constitue le premier outil juridique d'encadrement, dans la mesure où elle est prise sur la base d'un examen global de la législation en vigueur dans un Etat, sur un territoire ou applicable à un ou plusieurs secteurs déterminés au sein de cet Etat ;
- En l'absence d'une telle décision, des « garanties appropriées » (art. 46 du RGPD), constituées pour la majorité de décisions des autorités de contrôle et qui sont prises à la lumière des engagements des organismes concernés ;

6 - Respect du Code de Santé Publique

- Interdiction de procéder à une cession ou à une exploitation commerciale des données de santé (art. L. 1111-8 du CSP, art. L 4113-7 du CSP)

- Violation du secret médical (art R. 4127-4)

Conseil d'État, 26 septembre 2018, n° 407856 (Secret médical, Vie privée, Procédé publicitaire, Chirurgie esthétique, Conseil de l'ordre des médecins)

26/09/2018

En l'espèce, un chirurgien esthétique avait participé à de nombreuses émissions dans lesquels il faisait filmer ses consultations et opérations sur des vedettes de télé-réalité, qui avaient consenti à la réalisation et à la diffusion de ces reportages et articles de presse. Le conseil départemental de la Ville de Paris de l'ordre des médecins saisit la chambre nationale de l'ordre des médecins qui interdit au chirurgien l'exercice de sa profession pendant une durée de 2 ans dont 1 an de sursis. Le chirurgien forme alors un pourvoi en cassation devant le Conseil d'État qui confirme et maintient la sanction disciplinaire.

En effet, la Haute juridiction administrative rappelle que le secret médical est défini comme « Le secret professionnel institué dans l'intérêt des patients s'impose à tout médecin dans les conditions établies par la loi. Le secret couvre tout ce qui est venu à la connaissance du médecin dans l'exercice de sa profession, c'est-à-dire non seulement ce qui lui a été confié, mais aussi ce qu'il a vu, entendu ou compris ». Elle affirme que même dans les cas où le patient avait sciemment consenti à la réalisation et à la diffusion de reportages concernant des opérations chirurgicales, « le concours apporté par le médecin à la divulgation de leur identité à l'occasion d'émissions ou d'articles est constitutif d'une méconnaissance de l'article R. 4127-4 du code de la santé publique, qui prohibe la violation du secret médical ».

7 - Analyse d'impact éventuel

Le responsable de traitement doit également conduire une analyse d'impact sur la protection des données (AIPD), dès lors que les traitements de ces enregistrements aux fins de formation, d'information et de recherche peuvent présenter un « risque élevé » pour les personnes concernées (art. 35 du RGPD).

Le risque élevé est caractérisé lorsqu'un certain nombre de critères sont remplis, et notamment la présence de données à caractère personnel de santé, concernant des personnes vulnérables (les patients), le tout dans le cadre d'un traitement à grande échelle. Ce dernier critère implique qu'un certain volume de données soit traité, ou concerne un nombre important de personnes.

Les volumes de données traitées doivent être analysés au cas par cas pour confirmer si une AIPD est effectivement nécessaire. Les exemples fournis par la réglementation pour caractériser la grande échelle (traitement des données de patients par un hôpital dans le cadre du déroulement normal de ses activités, utilisation par un magazine en ligne d'une liste de diffusion pour communiquer à ses abonnés son digest générique quotidien...) amènent à penser que les critères seront déterminants.

Par ailleurs, les méthodologies de référence telles que la MR-004 imposent de conduire une AIPD. Dans l'hypothèse où un traitement de données des enregistrements serait basé sur cette MR, la conduite d'une AIPD est systématiquement requise.

8 - Fixation et respect des durées de conservation

Le responsable de traitement doit déterminer les durées limitées pendant lesquelles elle conserve les données personnelles et mettre en place des mécanismes pour assurer des purges automatisées ou régulières.

Ces durées peuvent s'articuler entre les durées de conservation en base active, pour les besoins quotidiens de l'activité, et les durées de conservation en base archive, qui peuvent être plus longues si l'archivage respecte bien certains principes (stockage logique ou physique séparé, restriction des accès, etc.).

Une fiche pratique figure dans l'annexe.

Nous remercions les Professeurs Albert-Claude Benhamou, Hubert Johanet (ANC), Jacques Marescaux, Didier Mutter (IRCAD), le Dr. François Simon (APHP), le Pr. Emmanuel Hirsch (Paris Saclay), Maîtres Lorraine Mesnier-Boché (Cabinet McDermott Will & Emery AARPI) et Vanina Bachvarova (avocats) pour la relecture de ce travail.

ANNEXES

Annexe 1 : RGPD

Les termes de réglementation de protection des données (RGPD) à caractère personnel couvrent notamment :

Données personnelles. Les enregistrements traitent des images et des sons issus des opérations chirurgicales, qui se rattachent à des éléments du dossier médical du patient. Ces enregistrements risquent fréquemment de permettre d'identifier de façon unique un patient, même indirectement. En effet, ces enregistrements sont uniques et révélateurs, en raison de la spécificité d'une pathologie, du recoupement de symptômes ou d'éléments biologiques uniques visibles sur l'enregistrement. Le croisement avec d'autres informations (date et lieu de l'opération, pathologie précise, stade, malformations, spécificités de l'intervention, etc.) concourt à ces facteurs d'identification.

Pseudonymisation versus anonymisation. Dans le cadre de leur réutilisation à des fins d'information, de formation ou de recherches, ces enregistrements sont (et doivent, cf. *infra*) être « pseudonymisés », c'est-à-dire ne contenir aucun élément directement identifiant (l'absence d'indication du nom, de l'IPP ou de visualisation du visage d'un patient, etc.). Toutefois, à ce jour, la pseudonymisation n'équivaut pas, pour la réglementation de protection des données à caractère personnel dans l'Union européenne, à une « anonymisation », c'est-à-dire l'impossibilité totale, pour quelque acteur que ce soit, de réidentifier une personne. Seule l'anonymisation exclut l'application de la réglementation de protection des données à caractère personnel.

- *Exemple : un enregistrement parfaitement pseudonymisé d'une opération pourrait théoriquement être comparé aux dossiers médicaux afin de retrouver à quel patient cet enregistrement correspond.*

Ces risques de réidentification apparaissent cependant relativement théoriques, compte tenu de la zone filmée et des multiples mesures qui peuvent être mises en place pour éviter toute réidentification. Il pourrait ainsi être possible de considérer que la majorité des enregistrements ne permettent pas d'identifier directement ou indirectement un patient.

Compte tenu de la position exigeante des autorités de protection des données personnelles dans l'Union européenne, il convient ainsi d'effectuer une analyse au cas par cas, selon les méthodes utilisées pour protéger l'identité des patients, afin de déterminer si les enregistrements peuvent être considérés comme effectivement anonymisés ou s'ils ne sont que pseudonymisés.

Il est important de préciser jusqu'où on peut apporter du contexte à la vidéo, dans l'état actuel, nous proposons :

- nom de l'équipe chirurgicale
- âge du patient en pédiatrie : mettre une tranche d'âge
- identification de la pathologie par l'imagerie préopératoire ou autres examens paracliniques anonymisés
- histoire de la maladie, succincte, à limiter à ce qui est indispensable pour la bonne compréhension du geste chirurgical.

Tous ces points seront à valider par la CNIL.

NB : la notion d'anonymisation ou de « dé-identification » peut varier selon les pays et notamment en dehors de l'Union européenne.

Données de santé. Compte tenu de leur source médicale et de leur contenu, révélateur d'une pathologie, ces enregistrements sont considérés comme contenant des données de santé, à savoir des données sensibles au sens du RGPD¹⁰. Quand bien même l'opération ne révélerait aucune pathologie (par exemple lors d'une chirurgie exploratoire), la sphère médicale dans laquelle a lieu l'enregistrement et la nature même de l'acte rattachable au soin, qualifie les enregistrements de données de santé. Le RGPD adopte en effet une interprétation large de la notion de donnée de santé, qui peut couvrir tout état de santé, bon ou mauvais. L'utilisation des enregistrements doit ainsi s'effectuer en assurant un haut niveau de protection de ces données sensibles.

Données des chirurgiens et du personnel médical. Les enregistrements peuvent également impliquer le traitement de données de professionnels intervenant dans le système de santé, soit parce qu'ils sont directement filmés, soit parce que leurs interventions (verbales ou chirurgicales) sont enregistrées. Il ne s'agit pas de données

¹⁰ CEPD, Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo, v.2.0, 29 janvier 2020, §65

de santé, mais bien de données à caractère personnel. Leur utilisation doit également être encadrée.

Annexe 2 : Droit à l'image

Tant les patients que les professionnels disposent d'un droit sur leur image (art. 9 du code civil). Selon la nature des enregistrements, c'est-à-dire si la personne est directement reconnaissable, ce droit peut impliquer la nécessité d'obtenir son accord écrit pour toute prise d'images et réutilisation (notamment diffusion) de celle-ci.

En l'occurrence, compte tenu des nécessités de la protection des données à caractère personnel et du secret médical, qui doivent entraîner de façon systématique des mesures de pseudonymisation poussées, ce droit ne devrait pas trouver à s'appliquer.

Annexe 3 : Secret médical

Le secret médical couvre toutes les informations concernant le patient, qui sont venues à la connaissance de tout professionnel intervenant dans le système de santé, et notamment dans le cadre d'une prise en charge par un professionnel de santé ou un établissement de santé¹¹. A cet égard, les enregistrements des opérations chirurgicales sont couverts par le secret médical. Seules des mesures d'anonymisation, voire de pseudonymisation poussée pourraient en exclure l'application.

Le secret médical est une obligation générale et absolue pour les professionnels de santé et un droit fondamental du patient. Cette nature absolue du secret professionnel, en droit français, limite les possibilités de lever ce secret par le seul consentement du patient. En tant qu'obligation imposée aux professionnels de santé, elle est « *établie pour assurer la confiance nécessaire à l'exercice de certaines professions ou de certaines fonctions, [qui] s'impose aux médecins, comme un devoir de leur état ; qu'elle est générale et qu'il n'appartient à personne de les en affranchir* »¹². Ainsi, « *L'obligation au secret professionnel, établie par l'article 226-13 du code pénal, pour assurer la confiance nécessaire à l'exercice de certaines professions ou de certaines fonctions, s'impose aux médecins, hormis les cas où la loi en impose autrement, comme un devoir de leur état ; que sous cette seule réserve, elle est générale et absolue* »¹³. Des praticiens ont ainsi été sanctionnés pour avoir apporté leur concours à la divulgation d'images chirurgicales, avec le consentement du

¹¹ Code de la santé publique, art. L. 1110-4.

¹² Cass.Crim. 8 mai 1947 ; Cass. Crim. 22 décembre 1966 ; Cass. Crim. 27 juin 1967 ; Cass. Crim. 5 juin 1985, Cass. Crim. 8 avril 1998

¹³ Cass. Crim, 8 avril 1998.

patient¹⁴. Ce devoir absolu ne peut ainsi être levé par le seul consentement du patient, sauf à ce que la loi le permette.

Par exemple, les professionnels de santé sont relevés du secret médical lorsqu'ils transmettent des données à caractère personnel de santé à des responsables de traitement qui disposent d'une autorisation de la CNIL octroyée au regard de l'intérêt public de ce traitement (par exemple, un projet de recherche en santé)¹⁵. Une autre illustration est donnée par le régime du secret médical partagé, qui permet le partage de données de santé couvertes par le secret médical, entre différents professionnels, sous réserve du consentement du patient¹⁶.

Annexe 4 : Propriété intellectuelle

S'il n'existe pas, en droit de l'Union européenne, de droit de propriété sur des données à caractère personnel, les enregistrements réalisés par un hôpital peuvent cependant faire l'objet d'une protection par certains droits de propriété intellectuelle (par exemple, le droit d'auteur, si le critère d'originalité est rempli, ou encore le droit sui generis des producteurs de base de données, en ce qui concerne l'ensemble d'enregistrements organisés).

Les titulaires de ces droits de propriété intellectuelle (qui peuvent être distincts du responsable de traitement au sens du RGPD) peuvent imposer des conditions pour la réutilisation de ces enregistrements.

La situation diffère entre le secteur public et le secteur libéral. Des contractualisations peuvent être envisagées.

Annexe 5 : Autorisations incluses dans le RGPD

Il s'agit, notamment des exceptions suivantes :

- le consentement explicite de la personne (*RGPD, art. 9 (2) a*) ;
- le traitement est nécessaire pour des motifs d'intérêt public important (*RGPD, art. 9 (2) g*) ;

¹⁴ Conseil d'État, 26 septembre 2018, n° 407856

¹⁵ Loi Informatique et Libertés, art. 68

¹⁶ Code de la santé publique, art. L. 1110-4.

- les traitements nécessaires aux fins de la médecine préventive ou de la médecine du travail, 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 (*RGPD, art. 9 (2) h*) ;
- les traitements nécessaires pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux (*RGPD, art. 9 (2) i*) ; les traitements nécessaires à des fins de recherche scientifique ou à des fins statistiques, conformément à l'article 89, paragraphe 1 (*RGPD, art. 9 (2)*) les traitements nécessaires à la recherche publique au sens de l'article L. 112-1 du code de la recherche, sous réserve que des motifs d'intérêt public important les rendent nécessaires (au sens du 9 (2) g) du RGPD), après avis motivé et publié de la CNIL¹⁷ ;
- les traitements comportant des données concernant la santé justifiés **par l'intérêt public** et disposant d'une **autorisation préalable de la CNIL** (sauf exceptions)¹⁸.

Annexe 6 : Autorisations incluses dans la loi Informatique et Libertés

à savoir, notamment¹⁹ :

- les traitements réalisés aux fins de **médecine préventive, diagnostics médicaux, administration de soins ou de traitements, ou gestion de services de santé** (*art. 44 1° LIL*) et études réalisées à partir du 44 1° (recherche interne), et mis en œuvre par un membre d'une profession de santé, ou par une autre personne soumise au secret professionnel ;
- le **consentement explicite** des patients (*RGPD, art. 9 (2) a*).

Annexe 7 : Finalités d'intérêt public du Health Data Hub

¹⁷ L. n° 78-17, 6 janv. 1978 mod., art. 44, 6°

¹⁸ L. n° 78-17, 6 janv. 1978 mod., art. 44, 3°

¹⁹ Les autres exceptions comprennent notamment l'exercice des missions de l'assurance maladie obligatoire (AMO) et de la prise en charge par l'assurance maladie complémentaire (AMC), les traitements relatifs à l'information médicale, dans le cadre du suivi local de l'activité des établissements de santé (PMSI), les traitements relatifs aux informations sur les activités des établissements de santé, par les ARS, l'Etat, etc. et la gestion des alertes sanitaires par certains organismes publics en cas de situation d'urgence. De plus, il est également possible de passer par un cadre de référence (référentiels ou règlements types de la CNIL) tel que le référentiel vigilances sanitaires, le référentiel sur la gestion des traitements courants des cabinets médicaux et paramédicaux ou encore le référentiel relatif aux entrepôts de données de santé, si la finalité du traitement s'y prête.

- amélioration des soins et de la santé publique
 - *par exemple, étude de pathologies présentant un degré particulier de gravité, de rareté, etc.*
- amélioration du système de santé ;
 - *par exemple, études évaluatives, sur l'efficacité, les bons usages, la qualité, l'efficience, etc.*
- recherche et augmentation des connaissances ;
 - *par exemple, connaissances médicales, soins, méthodes, etc.*
- contribution à l'intérêt général, d'une étude aux finalités d'intérêt privé ;
 - *par exemple, innovation pouvant profiter à d'autres, rayonnement international, etc.*

Annexe 8 : Information et consentement

Madame, Monsieur,

Vous allez bénéficier d'une intervention chirurgicale/endoscopique dans le Pôle Hépato-Digestif X... Nous souhaitons pouvoir utiliser les informations médicales, iconographiques ou vidéo de votre prise en charge à des fins d'information, de recherche, d'enseignement et de publication. Cette utilisation nécessite votre consentement. En effet, ceci implique d'utiliser des données à caractère personnel, y compris des données personnelles de santé, vous concernant.

Votre identification sera rendue impossible par anonymisation/pseudonymisation et/ou « floutage » de l'ensemble des données utilisées.

Le traitement de ces données est soumis au respect du règlement européen n° 2016/679 du 27 avril 2016 sur la protection des données, dit « RGPD », et à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi relative à la protection des données personnelles du 20 juin 2018. La base légale du traitement des données personnelles est votre consentement, conformément aux articles 6 et 9 du RGPD. En application de l'article 32 du RGPD, tous les moyens logistiques, humains, techniques et organisationnels à leur disposition pour assurer la sécurité de vos données personnelles sont mis en œuvre. Les personnes accédant aux données personnelles directement ou indirectement identifiantes, sont soumises à une obligation de confidentialité et au secret professionnel. Par ailleurs, vos données personnelles, après anonymisation, peuvent être partagées avec des chercheurs ne participant pas à cette intervention et ce, à des fins de recherche ou pour faire avancer la science et la santé publique. Dans le cadre de ce consentement, l'éventuel transfert des données hors Union Européenne s'appuie sur les articles 45 et 46 de la CNIL.

Vos droits : Votre consentement est facultatif. Vos données sont celles de votre dossier médical.

Vous disposez du droit d'introduire une réclamation auprès de la Commission National de l'Informatique et des Libertés (CNIL), par courrier à l'adresse suivante : 3 Place de Fontenoy, 75334 PARIS ou sur son site Internet <https://www.cnil.fr/fr/plaintes>.

Par ailleurs, le médecin qui vous suit est à votre disposition pour vous fournir toutes les explications nécessaires concernant l'utilisation éventuelle de vos données pour des recherches portant sur votre maladie. Si vous souhaitez retirer à quelque moment que ce soit votre accord, et quel que soit le motif, vous continuerez à bénéficier du suivi médical approprié et cela n'affectera en rien votre surveillance future (loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par le règlement général sur la protection des données (RGPD) du 20 juin 2018). Vous pouvez également demander des informations complémentaires à tout moment (article L 1111 – 7 du code de santé publique).

Si vous avez des questions à poser à propos de ce consentement, vous pouvez contacter Dr X... au n° de téléphone suivant : .

OUI, j'autorise l'utilisation des informations issues de mon dossier médical, des résultats biologiques, iconographiques et vidéo à des fins d'information, de recherche, d'enseignement et de publication scientifique.

NON, je n'autorise pas l'utilisation des informations issues de mon dossier médical, des résultats biologiques, iconographiques et vidéo à des fins d'information, de recherche, d'enseignement et de publication scientifique.

Nom :	Date :	Signature du patient :	Signature
du médecin :			
Prénom :			
Date de naissance :			

Annexe 9 : Fiche pratique



Information et consentement

- **Inform**er le patient de façon claire et appropriée
- Obtenir le **consentement éclairé signé** du patient
- Déclarer le droit à l'image / voix du chirurgien et soignants
- Clarifier les **droits d'utilisation** des vidéos
 - > patient / établissement de santé / opérateur

Le consentement doit autoriser:

- La **création** d'une vidéo pédagogique
- La **finalité précise** de cette vidéo

Doit contenir les éléments suivants:

- Non-obligation de signer le consentement
- Possibilité de retirer le consentement à tout moment
- Préciser l'identité du responsable du traitement
- Préciser la durée de conservation des données
- Déclarer les accès et qui utilise les données
- Éventuels transferts de données hors UE
- Interdiction de commercialisation de la vidéo



Acquisition de la vidéo brute

L'acquisition de la vidéo brute se fait au bloc opératoire dans un contexte de soin du patient. Toutes les règles du **secret médical** s'appliquent à cette vidéo, qui est nominative et fait partie du **dossier médical** du patient.



Edition d'une vidéo pédagogique non-identifiante

- **Désidentification de la vidéo** : suppression des meta-data et floutage de parties identifiantes du corps du patient : le visage, signes distinctifs (tatouages, piercings, etc.), voix...
- Edition de la **vidéo à visée pédagogique**:
 - découpage en séquences utiles
 - narration, ajouts de schémas, etc.
- **Ajout de contexte à visée pédagogique**
 - données démographiques : tranche d'âge (éviter l'âge exact)
 - histoire de la maladie, antécédents, imagerie désidentifiée
 - identification de la pathologie / procédure chirurgicale
 - identification de l'opérateur ou équipe chirurgicale



La protection du secret médical est essentielle pour ces cas particuliers :

- Chirurgie de la face (identification possible)
- Chirurgie de l'enfant (enfant devenu adulte)
- Live surgery (données liées au direct)



Attention au risque de ré-identification

Ajouter le minimum de contexte nécessaire pour comprendre la vidéo et rester vague



Diffusion de la vidéo

- **Un contrat entre la plateforme vidéo et l'établissement de santé** peut être signé permettant le meilleur contrôle des droits d'utilisation, stockage de la vidéo et diffusion hors UE
- Le choix du moyen de diffusion doit être détaillé dans le consentement et le **patient informé des risques spécifiques**



Diffusion sur les réseaux sociaux / YouTube

Ne permet pas de contrôler la conservation, le transfert hors-UE, ni l'accès à la vidéo