Repères juridiques pour mettre en œuvre la téléconsultation et le télésoin dans le contexte de la crise du COVID 19

RESUME 1

1. Pas de nécessité de mesures juridiques supplémentaires pour les échanges interpersonnels : application des règles relatives aux communications électroniques 4

a. Protection juridique des communications électroniques interpersonnelles 5

b. Obligations caractéristiques pesant sur les opérateurs de communications électroniques .. 6

2. Mais nécessité de respecter les règles propres aux données de santé pour les fonctionnalités d'échange ou de partage de documents 7

3. Nécessité d'une vigilance accrue en temps de crise à l'égard du cyber risque 8

Conclusion 9

RESUME

Depuis le communiqué de presse du ministère chargé de la santé du 4 avril 2020 établi dans le cadre de la gestion de la crise du COVID 19, la téléconsultation par téléphone est autorisée pour les patients dépourvus de moyens de connexion en vidéo.

Les actes de téléconsultation ou télésoin dans leur dimension relative à la communication interpersonnelle sont souvent réalisés à l'appui de solutions techniques délivrées par les opérateurs de communications électroniques traditionnels mais également par les acteurs dits « Over The Top » (OTT) offrant, pour certains, la possibilité d'envoyer des fichiers et de la vidéo.

Le présent article met en avant quelques repères juridiques relatifs à la confidentialité des données de santé générées par ces actes, à l'appui d'une distinction entre deux cas d'usage : d'une part, le recours à des outils qui permettent la réalisation des actes par le biais d'échanges interpersonnels (appel téléphonique, messagerie instantanée) et, d'autre part, des outils qui organisent l'échange et le partage de documents.

Le cas d'usage consistant uniquement dans l'échange interpersonnel est soumis aux règles habituelles des communications électroniques mais celles-ci ont été étendues aux nouveaux acteurs de ce secteur. En revanche, l'échange et le partage de documents est soumis à des exigences spécifiques.

Crédits photo : Créateur :AndreyPopov / Crédits :Getty Images/iStockphoto / Informations extraites des métadonnées photo IPTC

Les outils numériques destinés à tracer le parcours des personnes prises en charge de télésanté, en particulier de téléconsultation mais aussi de télésuvi, se développent dans le contexte exceptionnel du COVID-19 (applications de suivi des patients suspects ou confirmés COVID-19 ne nécessitant pas d'hospitalisation, de téléconsultation, etc.). Depuis le communiqué de presse du 4 avril 2020, le ministère chargé de la santé autorise la téléconsultation par téléphone, pour les patients dépourvus de moyens de connexion en vidéo. Cette décision vise à améliorer le suivi médical dans un contexte de confinement, et à permettre la détection de cas suspects ou le suivi de personnes particulièrement fragiles, lorsque les patients n'ont pas accès aux technologies numériques (smartphone ou matériel de vidéotransmission, connexion internet ou mobile permettant l'échange vidéo). On rappellera que le Conseil National de l'Ordre des Médecins a appelé depuis plusieurs années le ministère chargé de la santé à se prononcer sur le statut de l'activité de téléconseil, afin de déterminer les conditions dans lesquelles cette activité s'inscrit ou pas dans le cadre des règles de la télémédecine.

Le cadre juridique qui encadre la réalisation d'actes médicaux à distance à l'aide de technologies de communications électroniques a évolué depuis sa consécration par la loi de 2009 dite HPST[1]. On parle désormais de « télésanté », terme qui recouvre plusieurs catégories d'actes dont la téléconsultation et le télésoin.

[1] LOI n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires (1) – article L6316-1 du code de la santé publique

La téléconsultation[2] est une consultation réalisée à distance entre un professionnel médical, le téléconsultant, et un patient, qui peut ou non être accompagné par un professionnel de santé, par l'intermédiaire des technologies de l'information et de la communication. En principe, un médecin ne peut réaliser de consultations vidéo pour ses patients qu'après les avoir reçus à son cabinet dans les 12 derniers mois. Dans le contexte exceptionnel créé par le COVID-19, le décret du 9 mars[3] a levé cette condition pour tous les patients exposés au COVID-19. Concrètement, le texte autorise les patients atteints ou potentiellement affectés par le coronavirus de bénéficier de la téléconsultation même s'ils n'ont pas de médecin traitant, s'ils n'ont pas été orientés par celui-ci et même s'ils ne connaissent pas le médecin téléconsultant. Ces actes pourront être réalisées *« en utilisant n'importe lequel des moyens technologiques actuellement disponibles pour réaliser une vidéotransmission (lieu dédié équipé mais aussi site ou application sécurisée via un ordinateur, une tablette ou un smartphone, équipé d'une webcam et relié à internet)* ».

Qu'en est-il pour cette nouvelle catégorie d'actes pouvant également être réalisés à distance appelés télésoins ? Le télésoin[4] permet la pratique de soins à distance utilisant les technologies de l'information et de la communication. Il met en rapport un patient avec un ou plusieurs pharmaciens et auxiliaires médicaux. Pendant la durée de l'épidémie, de manière dérogatoire et transitoire et afin d'assurer la surveillance à domicile des patients atteint ou suspect d'infection, le suivi à distance en télésoin pour IDE, **ou télésuivi infirmier**, a été défini par l'arrêté ministériel du 23 mars 2020[5]. Le suivi des patients dont le diagnostic d'infection au COVID-19 a été posé cliniquement ou biologiquement peut être assuré par les infirmiers diplômés d'Etat libéral ou salarié d'une structure mentionnée au 1er alinéa de l'article L. 162-1-7 par télésoin sous la forme d'un télésuivi. Le télésuivi infirmier participe, sur prescription médicale, à la surveillance clinique des patients suspectés d'infection ou reconnus atteints du COVID-19. Le télésuivi infirmier est réalisé préférentiellement par vidéotransmission avec le patient, ou par téléphone si les équipements du patient et de l'infirmier ne le permettent pas.

Les actes de téléconsultation ou télésoin dans leur dimension relative à la communication interpersonnelle sont souvent réalisés à l'appui de solutions techniques délivrés par **les opérateurs de communications électroniques traditionnels** (« fournisseurs d'accès à internet » et « opérateurs de téléphonie ») mais également par **les acteurs dits « Over The Top » (OTT)** offrant, pour certains, la possibilité d'envoyer des fichiers et de la vidéo.

D'une façon générale, les outils qui permettent la réalisation des actes de téléconsultation comme les actes de télésoin doivent veiller à protéger la confidentialité, d'une part, des documents échangés et, d'autre part, les échanges interpersonnels. Le cas d'usage consistant uniquement dans l'échange interpersonnel est soumis aux règles habituelles des communications électroniques mais celles-ci ont été étendues aux nouveaux acteurs de ce secteur (**1**). En revanche, l'échange ou le partage de documents comportant des données de santé est soumis à des exigences spécifiques (**2**).

[2] Article R. 6316-1 du code de la santé publique

[3] Décret n° 2020-227 du 9 mars 2020 adaptant les conditions du bénéfice des prestations en espèces d'assurance maladie et de prise en charge des actes de télémédecine pour les personnes exposées au COVID-19

[4] Article L6316-2 du code de la santé publique

[5] Arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de COVID-19 dans le cadre de l'état d'urgence sanitaire

1. Pas de nécessité de mesures juridiques supplémentaires pour les échanges interpersonnels : application des règles relatives aux communications électroniques

L'agence du numérique en santé (ANS, ex-ASIP Santé), dans un document publié sur son site internet, décrit de façon synthétique des mesures et références permettant de garantir la sécurité des échanges entre professionnels de santé et patients dans le cadre d'un acte de téléconsultation[6].

Elle indique que les actes de téléconsultation sont caractérisés par deux modalités d'échange distinctes:

- Une communication interpersonnelle directe (voix ou vidéo) entre le médecin téléconsultant et le patient ;
- Des documents de santé contenant des données à caractère personnel échangés en amont (prise de RDV, envoi de documents, etc.), pendant (échanges d'images de document, etc.) et après l'acte de téléconsultation (compte-rendu par exemple). Ces supports ne sont pas nécessairement produits au cours de l'acte de téléconsultation.

Les principaux risques identifiés, à ce stade, par l'ANS concernant ces échanges interpersonnels (voix ou vidéo) qui n'ont pas, à ce jour, fait l'objet d'une réglementation spécifique, sont :

- *la confidentialité au sens écoute ou enregistrement de l'échange, l'intégrité de l'échange*

  A priori couvert par la réglementation sur les opérateurs de télécommunication et ceci pour toutes les communications interpersonnelles qu'il s'agisse de télémédecine ou pas

- *la confidentialité au sens identification/authentification du tiers de l'échange*

  L'identito vigilance due par le PS couvre une partie de ce risque.

  Le risque peut être particulièrement diminué si le patient et le PS utilisent une plateforme qui requiert une authentification avant les échanges de données préalables (prise de RDV par exemple) et surtout avant la mise en œuvre de la communication interpersonnelle.

  Le risque peut être annulé si le PS et le patient se connaissent préalablement

- *l'auditabilité*

  - *Le risque peut être particulièrement diminué si le patient et le PS utilisent une plateforme qui requiert une authentification avant la mise en œuvre de la communication interpersonnelle et les éléments de preuve sont conservés dans des conditions compatibles avec leur opposabilité.*

- *la disponibilité des communications interpersonnelles (voix ou vidéo) dépend de technologies ou d'opérateurs grand public qui n'ont pas plusieurs niveaux de SLA en terme de disponibilité qu'il s'agisse de voix ou de vidéo. »*

L'examen de la réglementation relative aux communications électroniques interpersonnelles permet effectivement de constater l'existence d'obligations importantes portant sur la confidentialité des communications électroniques, qui pèsent désormais également sur les acteurs OTT.

[6] https://esante.gouv.fr/sites/default/files/media_entity/documents/20191202_Réflexions%20sécurité%20et%20téléconsultation_VF2.pdf

a. Protection juridique des communications électroniques interpersonnelles

Les acteurs dit « OTT » déploient des systèmes qui permettent de communiquer, d'envoyer des fichiers, parfois de faire de la vidéo, sans procéder par eux-mêmes à l'acheminement des signaux. Il en résultait un doute sur leur qualification d'opérateurs de communications électroniques, jusqu'à la directive (UE) 2018/1972 du parlement européen et du conseil du 11 décembre 2018 établissant le code des communications électroniques européen.

La Directive du 11 décembre 2018[7] qui établit le code des communications électroniques européen constate que les utilisateurs finaux remplacent la téléphonie vocale traditionnelle, les messages textuels (SMS) et les services de transmission de courrier électronique par des services en ligne équivalents sur le plan fonctionnel, tels que la voix sur IP, des services de messagerie et des services de courrier électronique en ligne.

Si l'acheminement de signaux reste un paramètre important pour déterminer les services qui relèvent du champ d'application de la présente directive, la définition couvre désormais ces autres services qui rendent possible la communication.

La définition de services de communications électroniques englobe trois types de services qui peuvent se chevaucher en partie :

- les services d'accès à l'internet,
- les services de communications interpersonnelles,
- les services consistant totalement ou principalement en l'acheminement de signaux.

Les considérants précisent la notion de rémunération et ajoute que le service est par nature bidirectionnel, permettant ainsi aux deux parties de communiquer.

Dans un arrêt du 5 juin 2019, la Cour de justice de l'UE avait estimé que le service de Skype, SkypeOut, est bien un service de communications électroniques. La Cour a en effet estimé que « *l'article 2, sous c), de la directive 2002/21/CE du Parlement européen et du Conseil, du 7 mars 2002, relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive « cadre »), telle que modifiée par la directive 2009/140/CE du Parlement européen et du Conseil, du 25 novembre 2009, doit être interprété en ce sens que la fourniture, par l'éditeur d'un logiciel, d'une fonctionnalité offrant un service « Voice over Internet Protocol (VoIP) [voix sur le protocole Internet], qui permet à l'utilisateur d'appeler un numéro fixe ou mobile d'un plan national de numérotation via le réseau téléphonique public commuté (RTPC) d'un État membre à partir d'un terminal, constitue un « service de communications électroniques », au sens de cette disposition, dès lors que la fourniture dudit service, d'une part, donne lieu à rémunération de l'éditeur et, d'autre part, implique la conclusion par ce dernier d'accords avec les fournisseurs de services de télécommunications dûment autorisés à transmettre et à terminer des appels vers le RTPC.* »

Cet arrêt se rapporte au service SkypeOut, qui constitue une fonctionnalité ajoutée au logiciel de l'éditeur permettant à son utilisateur de passer des appels téléphoniques depuis un terminal vers une ligne de téléphone fixe ou mobile, en utilisant le protocole IP, à savoir la voix sur IP (VoIP). Ce service payant est disponible sans la participation d'un opérateur de communications traditionnel. Il ne

[7] Cette directive a été publiée au Journal officiel le 17 décembre 2018. Elle entre en vigueur le 20 décembre 2020. Elle doit être transposée en droit interne par les États membres au plus tard le 20 décembre 2020. Elle n'a pas encore eu lieu à ce jour.

permet pas, en revanche, de recevoir des appels provenant d'utilisateurs de numéros de téléphone belges.

b. Obligations caractéristiques pesant sur les opérateurs de communications électroniques

→ Sécurité des réseaux et des services

Tout fournisseur de service de communications électroniques accessible au public doit garantir la sécurité de ses services, le cas échéant avec l'aide du fournisseur de réseau. Ce dernier informe également les personnes concernées ainsi que toute autorité compétente en cas de risque de violation de la sécurité du réseau et d'atteinte aux données.

→ Secret des correspondances (article L. 32-3 du CPCE)

Cette règle garantit la confidentialité des communications interdisant à toute autre personne que les utilisateurs concernés d'écouter, d'intercepter, de stocker les communications. Des dérogations, dont la mise en œuvre est encadrée, sont autorisées pour sauvegarder la sécurité nationale, la défense et la sécurité publique ; et assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système électronique. Sa violation est en outre sanctionnée par les articles 226-15 et 432-9 du Code pénal.

→ Protection des données personnelles

La protection des données personnelles dans le domaine des télécommunications relève de la directive « vie privée et communications électroniques » qui devrait être prochainement remplacée par le Règlement e-privacy, en complément du RGPD. Il s'agit d'un nouveau texte proposé par la Commission Européenne le 10 janvier 2017 (non adopté à ce jour).

La directive actuelle reprend les grands principes de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des données en général (et notamment CPCE, art. L. 34). Des règles spécifiques sont à respecter concernant par exemple les données de trafic et de connexion.

Parmi les nouvelles mesures proposées, le projet de règlement prévoit des règles pour veiller au respect des droits des utilisateurs sur les données personnelles et pour certaines en essayant de les simplifier (par exemple en matière de cookies ou encore de traitement des métadonnées).

L'évolution du cadre juridique des communications électroniques impacte le secteur de la santé qui est concerné par le développement appliqué à la santé des outils d'échanges fournis par les OTT. Cette évolution va dans le sens d'un plus grand contrôle.

À compter du 21 décembre 2020, les services OTT, c'est-à-dire les applications de messagerie instantanée, de courriels, d'appels téléphoniques sur Internet et de messages personnels émis par le biais de réseaux sociaux devront, à l'instar des fournisseurs de télécommunications traditionnels, se conformer aux obligations figurant dans le CPCE (et le code de la consommation) et notamment aux obligations de confidentialité des données électroniques établies par la Directive « Vie privée et Communications électroniques ».

c. Quelques interrogations soulevées par l'évolution du cadre juridique des communications électroniques

Des interrogations méritent d'être soulevées en premier lieu concernant **le rôle de l'ARCEP lorsque les communications électroniques interpersonnelles portent sur des données personnelles**.

Comment les deux autorités compétentes, l'ARCEP et le CNIL, travailleront ensemble lorsque les sujets se recouvriront au moins partiellement ?

Le rappel des obligations pesant sur les opérateurs de communications électroniques devra être mis à jour au vu de la transposition qui sera faite en droit interne de la directive 2018/1972 de 2018. Par ailleurs, cette législation européenne impacte les secteurs de la santé et du médico-social. Il y aurait lieu que l**e ministère chargé de la santé** soit associé aux travaux relatifs à cette loi qui peut avoir des impacts sur les activités de télésanté et de l'activité de médecine d'urgence. Existe-t-il une coordination interministérielle sur ce sujet ?

Quelques soient les réponses à ces interrogations, il ressort de l'analyse qu'un médecin peut continuer d'échanger des propos avec un confrère par téléphone via un opérateur classique ou un OTT, y compris dans un contexte de télésanté, sans s'interroger sur l'existence de règles supplémentaires par rapport aux règles existantes et dont le respect pèse sur les opérateurs de communications électroniques. Qu'en est-il s'ils veulent s'envoyer et le cas échéant partager des clichés d'imagerie ? ou un compte-rendu d'acte de télémédecine ?

2. Mais nécessité de respecter les règles propres aux données de santé pour les fonctionnalités d'échange ou de partage de documents

Dans le document précité, l'ANS légitime le recours aux solutions d'échange instantanés sans envoi de pièces jointes. En revanche, dans le cas de fonctionnalités d'échange ou de partage de documents comportant des données de santé, elle rappelle qu'il est nécessaire de respecter les règles propres aux données de santé à caractère personnel rappelées ci-après. La recommandation de l'agence consiste à veiller « *à ne pas étendre en l'état le champ d'applicabilité de la réglementation sur la gestion des données personnelles de santé (PGSSI-S, HDS, etc.) aux communications interpersonnelles (voix ou vidéo), car on se heurterait aux limites techniques et économiques, et on délégitimerait toutes les pratiques existantes de communications interpersonnelles non facturés.* »

La réalisation d'un acte de téléconsultation, ou de télésoin, génère la création d'un traitement de données à caractère personnel au sens du RGPD[8] ou l'alimentation d'un traitement déjà existant (par exemple pour ajouter au dossier du patient le compte-rendu de l'acte). **Au titre du RGPD et de la loi Informatique et libertés modifiées**, un pré-requis est à remplir : il y a lieu d'identifier le (ou les) responsable(s) de traitement et une fois ce pré-requis rempli la détermination des mesures à mettre en œuvre pour veiller à la confidentialité et à la sécurité des données de santé (base légale, principes clés tels que la minimisation des données collectées, analyse d'impacts sur la vie privée, procédure de respect des droits des personnes concernées, etc.).

En outre, il existe une **réglementation propre aux données de santé à caractère personnel principalement codifiée dans le code de la santé publique**. Au titre de cette réglementation sectorielle, le responsable de la sécurité du système d'information doit veiller au respect de la PSSI-MCAS et de la PGSSI-S (identification et authentification des acteurs, force probante en particulier)

[8] Règlement 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, désigné dans les termes suivants : « règlement général sur la protection des données » ou « RGPD ».

ainsi que, le cas échéant, des règles relatives à la certification des hébergeurs de données de santé. Doivent également être respectées, sans que cette liste ne soit exhaustive, les règles relatives à l'échange et au partage des données de santé mais également à l'utilisation de l'identifiant national de santé dit INS pour veiller à ce que les données de santé soient rattachées à la bonne personne, ou encore, à la force probante des documents de santé dématérialisés, condition nécessaire pour aller vers le zéro papier.

3. Nécessité d'une vigilance accrue en temps de crise à l'égard du cyber risque

Le ministère de l'intérieur a constaté un accroissement des cyberattaques et des cyberescroqueries liées à la crise du Covid-19. Dans le domaine de la santé, comme le rapporte le site Cyberveille-sante-gouv.fr, le coronavirus est utilisé pour réaliser des cyberattaques au travers différents messages d'information sur le Covid-19. Il s'agit en réalité de virus informatiques. Par le biais de faux e-mails des autorités de santé, de fausses notes internes en entreprise ou encore de fausses alertes de retard de livraison, les cybercriminels tentent dans le monde entier d'exploiter la peur liée à la pandémie pour s'infiltrer sur les réseaux informatiques des entreprises et des particuliers, y compris des établissements de santé. Une partie des serveurs de l'AP-HP ont été rendus inaccessibles des heures durant, lors d'une attaque le 22 mars dernier. En outre, des outils de visioconférence ont récemment fait l'objet de vives critiques alors même que leur usage s'élargit dans le contexte du COVID 19.

En conséquence, il est demandé de surveiller de près tout élément anormal sur les systèmes d'information et, le cas échéant de faire un signalement immédiat. Il est également demandé de vérifier le bon fonctionnement des sauvegardes. Enfin, il est important de sensibiliser l'ensemble des personnels.

Il est important de s'assurer de choisir un outil sécurisé de télésanté, même en temps de crise. En effet, la fuite de données personnelles, dont des données de santé de même que le risque d'atteinte à la confidentialité plus largement des propos échangés à distance peut entraîner de graves préjudices. S'il faut être pragmatique, il est également important de ne pas se créer de nouveaux risques à gérer. **Il y a également lieu de veiller à une description des rôles et donc des responsabilités des différents acteurs par voie contractuelle.**

Conclusion

Les professionnels peuvent continuer de s'appeler sans contrainte juridique supplémentaire pour leurs échanges interpersonnels et ce, de façon traditionnelle ou par le biais des outils proposés par les acteurs OTT. En revanche, il apparaît important de distinguer le cas d'usage de l'échange interpersonnel, du cas d'usage dans lequel des documents comportant des données de santé sont échangés entre les professionnels. L'échange et le partage de documents comportant des données de santé est encadré par le biais d'obligations spécifiques, dont le respect pèse sur les professionnels quel que soit leur mode d'exercice (libéral ou en structure). Il est donc important que les outils de télésanté intègrent « by design », c'est-à-dire dès leur conception, ces contraintes pour faciliter l'exercice de leurs missions en intégrant les exigences de confidentialité et de sécurité des données de santé.

Le contexte actuel de l'épidémie de COVID-19 contribue largement au développement de la télésanté. L'Assurance-maladie dénombre 601 000 téléconsultations entre le 1er et le 28 mars, contre 40 000 en février. Le site internet du ministère chargé de la santé recense les outils de télésanté disponibles dans le contexte de l'épidémie COVID-19. Il a été précisé par arrêté ministériel que les professionnels sont tenus d'utiliser des outils (qu'ils soient référencés ou non), respectant le règlement général sur la protection des données (RGPD), la réglementation relative à l'hébergement des données de santé (HDS) et la politique générale de sécurité des systèmes d'information en santé (PGSSI-S). Toutefois, en cas d'impossibilité et exclusivement dans le cadre de la réponse à l'épidémie de COVID-19 les professionnels peuvent utiliser d'autres outils (arrêté du 23 mars 2020). **A chacun donc de prendre ses responsabilités conformément à l'esprit d'accountability porté par le RGPD !**