Téléconsultation : Comment garantir la sécurité des échanges ?

asipsanté L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

Modalités d'échange de la téléconsultation

- **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 échanges de données peuvent être bidirectionnels

- **Toute téléconsultation, qu'elle soit facturée ou non, doit prendre en compte les aspects sécurité des données personnelles de santé**

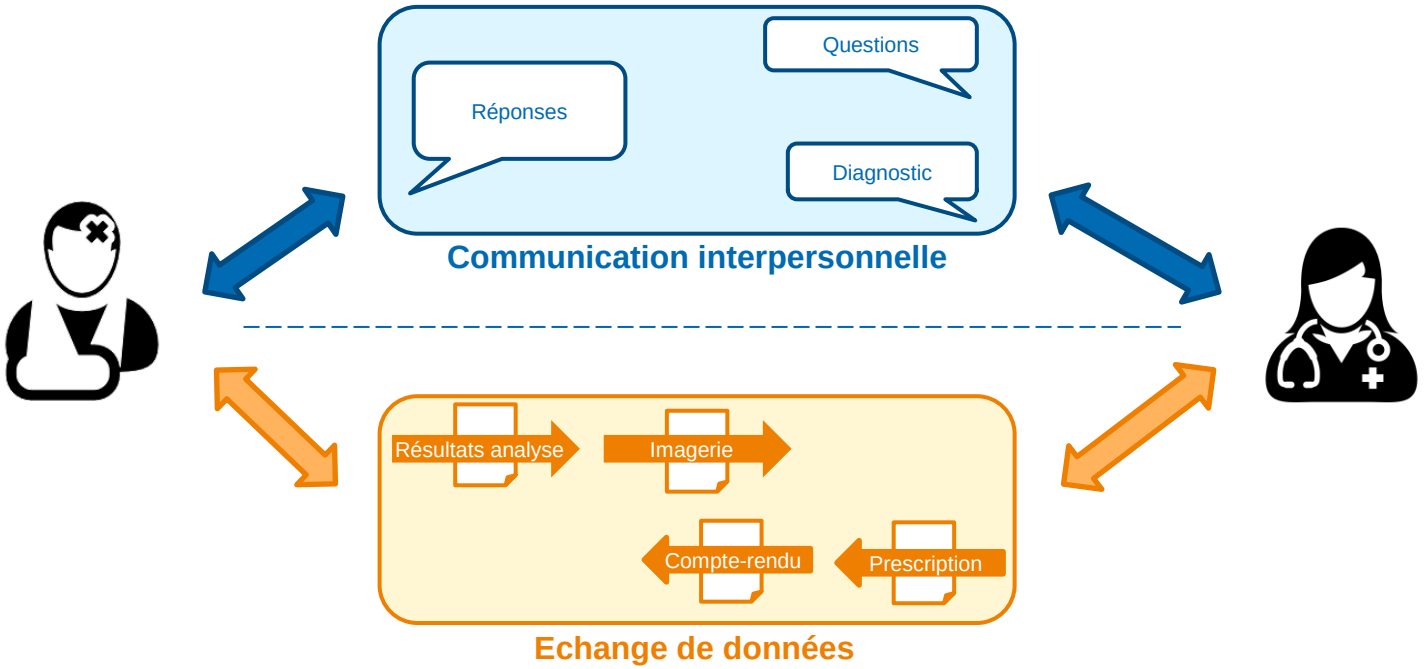
- **Par ailleurs, de nombreux actes sont déjà pratiqués quotidiennement « à distance » par les PS (professionnels de santé) en mode voix ou plus marginalement vidéo, entre des PS ou entre PS et patients**

Conformément à l'Arrêté du 1er août 2018 portant approbation de l'avenant n° 6 à la convention nationale organisant les rapports entre les médecins libéraux et l'assurance maladie signée le 25 août 2016 :

Seuls les actes de téléconsultation associés à une vidéotransmission ouvrent le droit au remboursement de l'acte de téléconsultation par l'assurance maladie.

Je suis un patient

- **La communication avec mon médecin et mes échanges de données (ordonnance, résultats, images, etc…) sont-ils sécurisés lors d'une téléconsultation?**
  - **La communication interpersonnelle avec votre médecin en téléconsultation, qu'elle soit par vidéo ou uniquement par voix, utilise des services de communication sur Internet ou des services d'opérateurs de télécommunication qui sont encadrés, en termes de confidentialité.**
  - **Les échanges de documents de santé contenant des données à caractère personnel réalisés avant, pendant ou après la téléconsultation sont également encadrés par diverses réglementations.**



Je suis un professionnel de santé

- **La communication interpersonnelle avec votre patient qu'elle soit vidéo ou uniquement voix utilise des services de communication sur Internet qui sont encadrés, en termes de confidentialité, par des réglementations : RGPD, la directive européenne 2018/1972**
  - Lors de la communication interpersonnelle avec le patient, une attention particulière devra être portée sur l'identitovigilance (pour couvrir le risque lié à une mauvaise identification du patient)

- **Les échanges de documents de santé contenant des données à caractère personnel réalisés avant, pendant ou après la téléconsultation sont encadrés par diverses réglementations : PSSI MCAS, PGSSI-S, HDS, etc. Cela concerne :**
  - Les échanges avec le patient-lui-même. Ceux-ci ne peuvent être réalisés avec la messagerie sécurisée de santé (pour l'instant non encore ouverte au patient), ni avec les outils de communication interpersonnelle de type « grand public » non conformes à la réglementation en vigueur pour ce type d'échange. Ils doivent être réalisés via des solutions de téléconsultation intégrant la fonctionnalité d'échange sécurisé de données personnelles avec le patient. L'analyse de risque et la sécurité sont de la responsabilité du responsable de traitement de la solution
  - Les échanges avec d'autres PS qui peuvent être réalisés via la messagerie sécurisée de santé ou tout autre dispositif conforme à la réglementation (notamment pour l'envoi de compte rendu)
  - La mise en partage avec d'autres acteurs de santé via le DMP

RGPD :	Règlement général sur la protection des données	**HDS :**	Hébergement des données de santé
PSSI MCAS :	Politique de sécurité des systèmes d'information du Ministère chargé des affaires sociales	**PGSSI-S :**	Politique générale de sécurité des systèmes d'information en santé
DMP :	Dossier médical partagé		

Réglementation sécurité applicable à la téléconsultation

Protection des communications électroniques interpersonnelles

- **Les actes de téléconsultation dans leur dimension relative à la communication interpersonnelle sont réalisés à l'appui de solutions techniques délivrés par :**
  - **les opérateurs de communication électronique traditionnels** : fournisseurs d'accès à internet et opérateurs de téléphonie
  - **les acteurs dits « over the top »(OTT)** : ils déploient des systèmes qui permettent de communiquer (voix, vidéo, messagerie instantanée, etc.), d'échanger des fichiers, 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.
- **Les opérateurs de communication électronique traditionnels et les acteurs OTT sont tenus d'assurer :**
  - **la sécurité de leurs réseaux et services**
  - **la confidentialité des échanges** : interdiction pour toute autre personne que les utilisateurs concernés d'écouter, d'intercepter, de stocker les communications (sauf dérogations pour sauvegarder la sécurité nationale, la défense et la sécurité publique, poursuite d'infractions pénales ou d'utilisations non autorisées du système électronique).
  - **la protection des données personnelles** : suivant la directive « vie privée et communications électroniques » qui devrait être prochainement remplacée par le règlement ePrivacy. Exemples d'obligations : conservation de traces pour les besoins de recherche, constatation et poursuite d'infractions pénales, utilisation de ces données soumise au consentement préalable des personnes concernées

Protection des documents de santé à caractère personnel échangés

- **La création de contenu tel que le compte-rendu d'un acte médical entre dans la définition d'un traitement de données à caractère personnel au sens du RGPD et de la loi informatique et libertés modifiée :**
  - obligation d'identifier un responsable de traitement
  - nécessité de conduire une analyse d'impacts sur la vie privée et de respecter les droits des personnes concernées
- **En outre, il existe une réglementation propre aux données de santé à caractère personnel codifiée dans le code de la santé publique. Le responsable de la sécurité du système d'information doit veiller au titre de cette réglementation sectorielle au respect :**
  - de la PSSI-MCAS et de la PGSSI-S (identification et authentification des acteurs de santé, force probante des documents en particulier)
  - des règles relatives à la certification des hébergeurs de données de santé, à l'échange et au partage des données de santé (notion d'équipe de soins, identifiant national de santé, etc.)

Macro-évaluation des risques concernant la téléconsultation

- **Les principaux risques liés aux échanges de données personnelles de santé sont identiques, que ces échanges soient réalisés avant, pendant ou après un acte de téléconsultation**
  - **La réglementation existante doit s'appliquer indépendamment du moment de ces échanges**

- **Les actes de téléconsultation ont recours à des communications interpersonnelles (voix ou vidéo) qui n'ont pas, à ce jour, fait l'objet d'une réglementation spécifique. Les principaux risques identifiés, à ce stade, concernant ces échanges 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 téléconsultations ou pas
  - **la confidentialité au sens identification / authentification du tiers de l'échange**
    - L'identitovigilance 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 (prérequis à la prise en charge de l'acte sauf exceptions)
  - **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 si les éléments de preuve tels que le compte-rendu et les traces des échanges (il n'est pas recommandé de sauvegarder l'échange vidéo) 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 termes de disponibilité qu'il s'agisse de voix ou de vidéo**

- **« Il faut 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 facturées »**

SLA : « Service Level Agreement » = Contrat de niveau de service

Solutions permettant de mettre en œuvre la téléconsultation

- **A ce stade il apparait qu'il y a deux grandes familles de solutions permettant de mettre en œuvre un acte de téléconsultation :**
  - **Des solutions professionnelles intégrant les modalités d'échanges de données personnelles amont (prise de RDV) , connexe (échanges d'images, etc.) et aval (envoi des CR au DMP par exemple) en plus de la communication interpersonnelle entre le médecin téléconsultant et le patient**
    - L'analyse de risque et plus largement la sécurité en général est alors de la responsabilité du responsable de traitement de la solution
  - **Des solutions « grand public » de communication interpersonnelle mises en œuvre à l'initiative du médecin téléconsultant**
    - L'analyse de risque et plus largement la sécurité en général est alors de la responsabilité du médecin téléconsultant
    - Seule la communication interpersonnelle est possible, l'échange de données ne peut se faire par ces solutions à moins qu'elles respectent les réglementations encadrant les échanges de données de santé (PSSI MCAS, PGSSI-S, HDS, etc.). Ce dernier point n'étant pas vérifié dans la majorité des cas, l'usage de ces solutions pour la téléconsultation, s'il est possible, n'est pas recommandé

- **Les deux familles de solutions présentées ci-dessus pourront probablement être complétées à terme par les solutions suivantes :**
  - **L'ENS (Espace Numérique Santé de l'usager) qui semble devoir comporter des outils de télémédecine. A ce titre cet ENS serait une plateforme orientée patient ; plateforme pour laquelle l'aspect PS n'est pas encore documenté**
  - **Les Logiciels de Gestion de Cabinet[1] (LGC) nouvelle génération, en particulier en mode Software as a Service[2] (SaaS), pourraient intégrer une plateforme de télémédecine orientée PS**
  - **Les offres technologiques de sociétés prestataires**

asipsanté L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

1: Logiciel intégrant tout ou partie des outils nécessaires à l'exercice du PS tels que l'agenda, l'édition de prescriptions, etc.
2: Offre technologique dans laquelle le logiciel est hébergé sur un serveur distant accessible par internet plutôt que sur la machine de l'utilisateur. Le paiement du service correspondant s'effectue généralement par abonnement.