Fiche d’information : la télémédecine pendant la pandémie de COVID-19

Version du : 12 juillet 2021

FMH · Verbindung der Schweizer Ärztinnen und Ärzte · Fédération des médecins suisses
Elfenstrasse 18 · Case postale 300 · CH-3000 Berne 15 · Téléphone +41 31 359 11 11 · Fax +41 31 359 11 12 · info@fmh.ch · www.fmh.ch

Version abrégée : la télémédecine pendant la pandémie de COVID-19

Cette fiche a pour but d'informer les médecins des possibilités de la télémédecine pendant la pandémie de COVID-19. Elle passe en revue les bases légales régissant les consultations de télémédecine et leur tarification, et récapitule dans un tableau les risques liés aux outils informatiques et de communication les plus courants.

Bases légales	Une consultation de télémédecine n'exempte pas le médecin de tenir le dossier médical du patient de façon à permettre de reconstituer l'historique du traitement. Les résultats d'analyse et les étapes du traitement doivent être documentés. Il convient par ailleurs d'indiquer quand les données ont été obtenues, par qui et de quelle manière.	Dossier médical
	Les dispositions relatives à la protection des données et celles de l'art. 321 CP concernant le secret médical s'appliquent de la même manière que pour les consultations ordinaires.	Protection des données et secret médical
	Si les données sont stockées à un endroit non régi par la loi suisse sur la protection des données (p. ex. données stockées dans un système de cloud basé à l'étranger) et que le prestataire informatique n'est pas disposé à s'engager à respecter la législation suisse en matière de protection des données, le médecin en informera le patient par écrit. Les données de celui-ci ne seront recueillies que s'il donne son accord exprès à ce mode de stockage. Les mêmes règles s'appliquent si le prestataire informatique n'est pas en mesure de garantir un niveau de sécurité adéquat.	Obligation d'obtenir l'accord du patient
	Dès le moment où le médecin n'est plus certain de pouvoir traiter son patient en télémédecine avec le niveau de fiabilité requis, il doit soit adapter le traitement en conséquence et examiner lui-même le patient, soit le référer à un confrère.	Devoir de diligence
Possibilités en matière de facturation	La seule position tarifaire actuellement disponible pour facturer les prestations de télémédecine est la position « Consultation téléphonique par le spécialiste » (positions tarifaires 00.0110 et ss). Dans le domaine de la psychiatrie, le médecin pourra recourir aux positions tarifaires spécifiques « Consultation téléphonique par le spécialiste en psychiatrie » 02.0060, 02.0065 et 02.0066. Les limitations applicables sont à respecter pour toutes les prestations.	TARMED
Applications recommandées par la FMH	La FMH et Health Info Net AG (HIN) proposent aux médecins un système gratuit, simple et fiable de vidéoconférence. Le système est hébergé dans le centre de calcul de HIN et répond aux exigences de sécurité les plus strictes. Le service et les instructions requises sont disponibles sur le site https://hintalkvideo.hin.ch (pour l'heure, uniquement avec Chrome).	Offre de la FMH et de HIN
	Le recours aux services de messagerie ou de vidéo relève de la responsabilité propre du médecin. La FMH a réuni dans un tableau les produits les plus courants permettant de tenir des consultations à distance (vidéoconférence), avec une évaluation des risques spécifiques à chacun d'eux.	Autres offres

Objectifs

Dans le cadre du diagnostic ambulatoire des cas suspectés d'infection au COVID-19, il est important d'encadrer précisément, et si possible de limiter les contacts directs avec les patients. Dans ce contexte, il est important que les médecins et le personnel de soins puissent disposer d'outils de communication adéquats pour mener à bien une consultation de télémédecine (diagnostic et traitement) mais aussi pour communiquer entre eux.

Cette fiche a pour but d'informer les médecins des possibilités techniques leur permettant de privilégier les consultations de télémédecine au cours de la pandémie actuelle. Elle passe en revue les bases légales régissant les consultations de télémédecine et leur tarification, et récapitule les risques liés aux outils informatiques et de communication les plus courants.

Quelles sont les dispositions légales encadrant les consultations de télémédecine ?

Lors de consultations de télémédecine, le médecin est tenu de respecter les principes usuels relatifs au dossier médical du patient, ainsi que les dispositions régissant la protection de données, le secret médical et le devoir de diligence.

Dossier médical

Les mêmes principes en matière de tenue du dossier médical que lors d'un traitement en contact direct avec le patient doivent être appliqués. Le dossier médical sera tenu de manière à permettre de reconstituer l'historique du traitement. Cela n'est possible que si chaque étape du traitement est rigoureusement et adéquatement consignée, de façon à ce que l'on puisse notamment reconstituer qui a exécuté quelle étape du traitement et à quel moment. Cela concerne bien sûr aussi les résultats d'analyse, raison pour laquelle les données transmises et stockées au moyen des outils de communication mis en œuvre doivent être enregistrées dans le dossier médical. Il doit également être possible d'établir qui a relevé ces données, de quelle manière et à quel moment.

Protection des données et secret professionnel

Les dispositions en matière de protection des données et celles de l'art. 321 CP concernant le secret médical s'appliquent de la même manière à toutes les consultations, qu'elles aient lieu à distance ou de façon usuelle en cabinet ou en centre de soins.

Toutes les données recueillies par le biais des outils informatiques ou de communication mis en œuvre dans le cadre d'une consultation de télémédecine doivent être consignées dans le dossier médical, au même titre que celles qui y sont habituellement consignées. Le principe général est que les données personnelles doivent être traitées conformément aux dispositions légales, et par conséquent que leur traitement remplisse un objectif précis et qu'il soit proportionné. La durée de conservation recommandée est de vingt ans, ce qui correspond au délai de prescription en droit privé.

Il faut s'assurer que les données ne puissent être ni endommagées ni détruites, ni traitées par un tiers non autorisé. Cela implique également que la confidentialité, la disponibilité, l'authenticité et l'intégrité de ces données soient garanties. Si des données sont stockées sur le cloud ou ailleurs qu'au cabinet médical, on s'assurera que le système d'authentification des utilisateurs soit suffisamment fiable et que la sécurité soit garantie.

Si les données sont stockées dans un endroit non soumis au droit suisse en matière de protection des données (p. ex. parce qu'elles sont stockées dans un système de cloud basé à l'étranger) et que le prestataire n'est pas disposé à s'engager à appliquer la législation suisse, le médecin est tenu d'en informer le patient par écrit. Il ne pourra collecter des données le concernant qu'à partir du moment où il aura donné son accord exprès. La même chose s'applique si le prestataire n'est pas en mesure d'offrir des garanties suffisantes en matière de sécurité des données. Dans ce cas aussi, le patient doit être informé par écrit de la situation et donner son accord exprès. Si le médecin transmet des données médicales à des tiers sans en avoir informé son patient et recueilli son accord préalable, le patient pourra l'attaquer en justice pour violation du secret médical.

Devoir de diligence
Dès lors que le médecin n'est plus certain de pouvoir traiter son patient en télémédecine avec le niveau de fiabilité requis, il doit adapter le traitement en effectuant lui-même un examen en présence du patient, soit le référer à un confrère. Si un médecin se trouve lui-même en quarantaine après avoir contracté le virus, il lui est possible de délivrer des instructions à l'intention du personnel non médical de son cabinet via les outils utilisés pour la télémédecine. Dans ce cas aussi, il va de soi que cela ne vaut que tant que le traitement peut être dispensé dans les règles de l'art. Il n'est bien évidemment pas admissible que les assistantes médicales outrepassent leurs compétences en effectuant des tâches habituellement du ressort exclusif du médecin.

Comment facturer les consultations de télémédecine ?

La seule position tarifaire actuellement disponible pour facturer les prestations de télémédecine est la position « Consultation téléphonique par le spécialiste » (positions tarifaires 00.0110 et ss). Dans le domaine de la psychiatrie, le médecin peut recourir aux positions tarifaires spécifiques « Consultation téléphonique par le spécialiste en psychiatrie » 02.0060, 02.0065 et 02.0066.

La FMH a établi une **fiche d'information** concernant la facturation des prestations médicales en lien avec le COVID-19. Vous trouverez la version actualisée sur son site internet.

Quelles applications la FMH recommande-t-elle pour les consultations de télémédecine ?

Le recours aux services de messagerie ou de vidéo relève de la responsabilité propre du médecin. **De manière générale, la FMH recommande de toujours s'assurer que la conférence n'est activée qu'entre les participants souhaités (utiliser un mot de passe, bloquer la réunion pour d'autres participants, ne pas partager publiquement les liens vers les réunions).** Dans le tableau 1 ci-dessous, la FMH a recensé les produits les plus courants de vidéoconférence permettant de tenir des consultations à distance, avec une évaluation des risques spécifiques à chacun d'eux (sans prétention à l'exhaustivité). Les produits de prestataires commerciaux offrant des services de télémédecine ne sont pas pris en compte. Les recommandations de la FMH se basent exclusivement sur les indications fournies par les concepteurs de logiciels.

La FMH et Health Info Net AG (HIN) proposent aux médecins un système gratuit, simple et fiable de vidéoconférence. Le système est hébergé dans le centre de calcul de HIN et répond à ce titre aux exigences de sécurité les plus strictes. Le service est accessible[1] via le lien https://hintalkvideo.hin.ch et les instructions à l'adresse https://www.hin.ch/fr/services/hin-talk-video/.

[1] Pour l'heure, il est techniquement nécessaire d'avoir un navigateur Chrome. La FMH et HIN travaillent à ce que cela fonctionne aussi avec d'autres navigateurs.

Tableau 1 : évaluation des risques des produits courants de vidéoconférence pour les consultations à distance (par ordre alphabétique, sans prétention à l'exhaustivité)

Solution	Certifications (sans prétention à l'exhaustivité)	App mobile	Compte nécessaire pour le patient	Liens (informations importantes pour la sécurité)	Recommandation de la FMH
HIN Talk Video	ISO 27001 Fournisseur du centre de calcul (Suisse) certifié ISO 27001:2013 et PCI DSS, audit et respect des circulaires FINMA CI 08/7, CI 08/21 et CI 18/3.	oui	Non	Avis de droit sur la protection des données : https://community.hin.ch/wp-content/uploads/160105-Gutachten-final-sig.pdf	**A**
Cisco WebEx	ISO 27001 ISO 9001 ISO 27018 SOC 2 Type 2 SOC 3 FedRAMP C5: Cloud Computing Compliance Controls Catalogue Swiss Privacy Shield Framework certified	oui	non	https://www.webex.com/webexremotehealth.html https://www.cisco.com/c/dam/en/us/products/conferencing/cisco-webex-security-infographic.pdf Security White Paper: https://www.cisco.com/c/dam/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.pdf	**A**
Google Meet	HIPAA EU Model Contract Clauses ISO 27001 ISO 27017 ISO 27018 EY POINT SOC 1 - Type 2 SOC 2 - Type 2 SOC 3 - Type 2 FedRAMP FISC Compliance Esquema Nacional de Seguridad (ENS)	oui	non	https://support.google.com/a/answer/7582940?hl=en https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf https://gsuite.google.com/security/?secure-by-design_activeEl=data-centers https://cloud.google.com/security/compliance?hl=de	**B**
GoToMeeting	SOC 2 Type 2 SOC 3 C5 BSI Cloud Computing ISO 27001 AICPA`s Trust Services Criteria EU-U.S. Privacy Shield Swiss Privacy Shield	oui	non	https://documentation.logmein.com/documentation/EN/pdf/common/LogMeIn_SecurityWhitepaper.pdf https://logmeincdn.azureedge.net/gotomeetingmedia/-/media/pdfs/ucc_security_white_paper.pdf https://www.logmeininc.com/legal/professional-services-terms	**B**
Lifesize	SOC ISO 27001 Swiss-U.S. Privacy Shield Framework	oui	oui	https://www.lifesize.com/en/solutions/industry/healthcare https://www.lifesize.com/~/media/Documents/Related%20Resources/Product%20Papers/Lifesize%20Cloud%20Security.ashx	**B**
Microsoft Teams	ISO 27001 ISO 27018 SOC 1 Type 2 SOC 2 Type 2 HIPAA FINMA HITRUST EU-US Privacy Shield Swiss-US Privacy Shield	oui	non	https://docs.microsoft.com/en-us/microsoftteams/security-compliance-overview https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-eu-us-privacy-shield?view=o365-worldwide https://docs.microsoft.com/en-us/microsoftteams/teams-security-guide	**A**
Prexip	National Institutes of Standards & Technology (NIST) Pexip complies with the GDPR	oui	non	https://www.pexip.com/healthcare https://docs.pexip.com/admin/security_best_practice.htm https://docs.pexip.com/admin/encryption_methodologies.htm	**B**
Signal	Keine Angaben	oui	oui (appli d'installatio)	https://www.signal.org	**B**

Solution	Certifications (sans prétention à l'exhaustivité)	App mobile	Compte nécessaire pour le patient	Liens (informations importantes pour la sécurité)	Recommandation de la FMH
Skype	Swiss-US Privacy Shield	oui	oui	https://support.skype.com/en/skype/all/privacy-security/ https://support.skype.com/en/faq/FA31/does-skype-use-encryption https://download.skype.com/share/security/2005-031%20security%20evaluation.pdf https://privacy.microsoft.com/en-gb/privacystatement	**B**
Vidyo	ISO 9001	oui	non	https://www.vidyo.com/	**A**
WhatsApp	EU-U.S. Privacy Shield Framework Swiss-U.S. Privacy Shield Framework	oui	oui (appli d'installatio)	https://www.whatsapp.com/security/ https://www.whatsapp.com/legal/privacy-shield-addendum/	**B**
Wire (Pro)	GDPR-compliant ISO CCPA SOX-ready	oui	non	https://wire-docs.wire.com/download/Wire+Security+Whitepaper.pdf https://wire-docs.wire.com/download/Wire+Privacy+Whitepaper.pdf https://wire.com/en/security/#audits	**A**
Zoom	SOC 2 Type 2 TRUSTe EU-US Privacy Shield FedRAMP Swiss-US Privacy Shield	oui	non	https://zoom.us/security Security White Paper: https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf	**B**

Informations importantes

- Les indications proviennent des informations publiées par le concepteur, selon le principe du « best effort » (sans garantie).
- Les différents services sont en évolution permanente. De nouvelles publications sur de possibles points faibles ou limitations en matière de protection des données arrivent en permanence : la validité dépend donc de la date indiquée
- Certains prestataires ont atteint des limites suite à la forte demande actuelle de solutions de visioconférence (performance primaire).
- La recommandation se réfère principalement à la protection et à la sécurité des données. D'autres aspects (convivialité, simplicité, etc.) ont été autant que possible pris en compte.

Légende

A : recommandé
B : recommandé mais avec des réserves
C : pas recommandé