Guide concernant les conventions de confidentialité et de traitement des données en sous-traitance

Version du 03/2023

FMH · Verbindung der Schweizer Ärztinnen und Ärzte · Fédération des médecins suisses
Postfach · CH-3000 Bern 16 · Telefon +41 31 359 11 11 · info@fmh.ch · www.fmh.ch

Table des matières

1 Contenu du guide

Le présent guide fournit des explications sur les modèles servant à la conclusion d'une convention de confidentialité et d'une convention de traitement de données en sous-traitance.

2 Qui est soumis au secret professionnel ?

Les médecins et leurs auxiliaires sont soumis au secret professionnel conformément à l'art. 321 CP. La notion d'auxiliaire est large et comprend toutes les personnes qui assistent directement ou indirectement les médecins dans leur activité professionnelle.

3 Quand faut-il conclure une convention de traitement de données en sous-traitance ou une convention de confidentialité ?

Dès qu'un tiers est chargé de traiter des données, il convient de conclure la convention de traitement des données sous-traitance et la convention de confidentialité.

4 Que couvre une convention de confidentialité ?

La convention de confidentialité engage le partenaire contractuel à ne pas divulguer certaines informations qui lui ont été transmises ou dont il a eu connaissance. Cette convention peut préciser à volonté quelles informations doivent rester confidentielles. L'obligation de confidentialité peut donc s'appliquer à toutes les informations transmises ou reçues ou seulement à une partie d'entre elles qualifiées comme telles (p. ex. secrets professionnels, données personnelles). Elle permet donc de sceller par contrat la confidentialité qui s'applique aux secrets professionnels et aux données personnelles mais également de déterminer les informations dont la transmission et le traitement ne sont pas limités ou réglementés par le secret professionnel ou la loi sur la protection des données mais qui doivent rester confidentielles.

Si le destinataire des informations traite des données personnelles sur mandat d'un médecin (p. ex. fournisseur de cloud, service de réponse téléphonique, etc.), il est alors tenu de respecter des dispositions légales encore plus étendues qui ne sont pas couvertes par la convention de confidentialité. Dans ce cas, il convient de conclure une convention de traitement des données en sous-traitance. La convention de confidentialité permet donc de se prémunir uniquement des situations dans lesquelles le destinataire entre en contact avec des informations confidentielles ou des données personnelles de manière fortuite et lorsqu'il n'est pas chargé de traiter

5 Qu'est-ce qu'un traitement de données en sous-traitance ?

Dans le cadre d'un traitement de données en sous-traitance, le mandataire traite des données personnelles conformément aux instructions qui lui ont été données. Il y a typiquement traitement de données en sous-traitance dans les situations suivantes :

- **Prestations de cloud :** prestataires de cloud computing/externalisation de systèmes informatiques et/ou de données dans un centre de calcul externe (outsourcing) ;
- Services informatiques : collecte de données/conversion de données/externalisation et archivage de sauvegardes/prestations d'analyse et de suivi (p. ex. Google Analytics) ;
- **Destruction et conservation des données :** destruction de documents et de dossiers/destruction de supports de données / prestations d'archivage ;
- **Marketing/communication commerciale :** centres d'appels externes/hébergeurs web et d'e-mails/prestataires de services de newsletters/traitement d'adresses publicitaires/agence de marketing traitant les données des clients/prestataires d'analyses marketing ;
- **Comptabilité :** comptabilité dans le cloud/externalisation de la gestion des décomptes de salaires.

6 À quoi dois-je veiller lors de la conclusion d'une convention de traitement de données ?

La prestation à fournir est régie dans un contrat séparé (le « contrat principal »). La convention de traitement de données en sous-traitance ne contient que les dispositions relatives à la protection des données à respecter lors de l'exécution du contrat principal. Celui-ci doit donc être précisément mentionné dans cette convention. De plus, le contrat principal ne doit prévoir aucune primauté sur les dispositions de la convention de traitement de données en sous-traitance. De telles clauses seraient à supprimer du contrat principal. En outre, la convention de traitement de données en sous-traitance doit définir les données personnelles concernées et le type de traitement des données (voir modèle). Enfin, il y a lieu de déterminer les mesures techniques et organisationnelles que le mandataire doit mettre en oeuvre pour assurer la sécurité des données. Ces mesures dépendent de la nature et de l'étendue des données traitées ainsi que du risque en matière de protection des données qui en découle. Il est possible de ne définir, de manière abstraite, que des domaines dans lesquels des mesures concrètes doivent être mises en oeuvre (voir modèle).

7 Quand le sous-traitant doit-il disposer d'un règlement de traitement ?

Un règlement de traitement n'est nécessaire qu'en cas de risque accru, à savoir en cas (a) de traitement de données sensibles à grande échelle ou (b) de profilage à risque élevé. Sont ainsi exclus les cas de traitement sporadique de données sensibles. De nombreuses entreprises, en particulier les PME « traditionnelles », n'effectuent pas de tels traitements. Elles ne sont donc pas concernées par cette obligation.

8 Quand le sous-traitant doit-il tenir un registre de traitement ?

Les personnes en charge du traitement de données comptant plus de 250 membres du personnel doivent tenir un registre de traitement indiquant clairement tous les traitements de données effectués. Lorsque le personnel compte moins de 250 membres au 1er janvier d'une année, la tenue d'un registre de traitement n'est obligatoire qu'en cas (a) de traitement de données sensibles à grande échelle ou (b) de profilage à risque élevé.

9 Quand le sous-traitant est-il soumis à l'obligation de journalisation ?

Lors de traitements de données sensibles à grande échelle ou de profilage à risque élevé, la journalisation est nécessaire lorsque, sans cette mesure, il n'est pas possible de vérifier a posteriori que les données ont été traitées conformément aux finalités prévues. La journalisation porte au moins sur les opérations d'enregistrement, de modification, de lecture, de communication, d'effacement et de destruction de données.

10 Dois-je informer la patientèle du traitement de données en sous-traitance ?

La loi ne prévoit pas d'informer les personnes concernées lors du traitement de données en sous-traitance.

Impressum
Edition: FMH – Fédération des médecins suisses, Berne
Publication: mars 2023
www.fmh.ch