INFORMATIONS ET DISPOSITIONS-CADRES POUR LA COMMUNICATION ÉLECTRONIQUE DE DONNÉES

(valables à partir du 1er novembre 2020)

A Champ d'application et objet

Les présentes dispositions-cadres pour la communication électronique de données font partie intégrante de la relation contractuelle entre le contractant et Health Info Net AG (HIN).

Utilisation de l'identité HIN (eID HIN)

Le contractant et les utilisateurs autorisés par ce dernier utilisent leur identité HIN (eID HIN) pour des transactions électroniques et la communication de données (e-mail, connexion à diverses applications de cybersanté). L'expéditeur et le destinataire sont vérifiés en ligne. Le contractant ou l'utilisateur autorisé est conscient des faits suivants:

- les parties partent du principe que la communication émane d'une personne ou d'une institution désignée et autorisée et que la communication est confidentielle;
- lui-même est engagé et peut être lié par la communication et les transactions qui passent par sa propre eID HIN;
- lui-même est responsable en cas d'utilisation abusive des identités attribuées dans le cadre de son raccordement HIN.

Par conséquent, il est dans l'intérêt du contractant de s'assurer que

- toute ID HIN personnelle de son contrat n'est utilisée que par l'utilisateur correspondant;
- que seuls les utilisateurs qu'il a autorisés à utiliser les eID HIN impersonnelles de son contrat les utilisent;
- les utilisateurs autorisés sont informés des risques d'utilisation correspondants;
- les mesures de sécurité décrites ci-après sont prises.

L'adresse e-mail associée à une eID HIN est destinée uniquement au détenteur de l'ID (dans le cas d'une eID personnelle) ou du contractant (dans le cas d'une identité d'équipe) pour une durée illimitée et n'est pas transmissible. Ce droit reste également en vigueur dans le cas d'une résiliation ou d'une désactivation. Les paramètres de l'eID HIN restent enregistrés chez HIN pour une durée de six mois.

B Accès aux services

Conditions techniques

La communication est assurée par le contractant lui-même, via les moyens suivants:

1. un accès Internet,
2. le logiciel de sécurité de HIN,
3. des programmes Internet à jour de tiers (navigateur, programme de messagerie) et
4. l'équipement informatique adapté à la connexion Internet.

Autorisation d'accès

L'accès aux services de HIN est réglementé par un système d'identification et de cryptage HIN. Les conditions suivantes doivent être remplies à cette fin:

1. Pour accéder à la plate-forme HIN, le contractant a besoin d'un raccordement HIN. C'est la seule façon pour lui, pour son institution et pour tout utilisateur personnalisé de s'identifier et de se légitimer auprès de HIN.
2. L'accès aux différents services et données n'est accordé qu'à ceux qui ont passé avec succès les contrôles d'identification et qui ont été reconnus comme utilisateurs enregistrés et autorisés par HIN.

C Vérification de la légitimité lors de l'utilisation des services

Si le contractant ou l'utilisateur autorisé utilise les services de HIN par voie électronique, la personne ne doit pas être identifiée au moyen d'une vérification de signature ou d'identité. L'identification des utilisateurs légitimes s'effectue sur la base de l'identification personnelle. Ainsi, toute personne correctement légitimée a accès aux données de la personne identifiée. Toutes les transactions qui ont passé avec succès un contrôle de légitimation sont attribuées à l'ID HIN correspondant et ont un caractère obligatoire pour le contractant de cet eID HIN.

Invalidation d'une identité HIN

Une eID HIN ne peut être invalidée que par HIN. Une eID HIN est invalidée dès qu'un abus ou un soupçon justifié d'abus de l'eID HIN existe ou que le contrat a expiré. D'autres motifs d'invalidation restent réservés.

Cette déclaration d'invalidité peut être initiée par HIN, le contractant/l'utilisateur d'identités ou l'émetteur du certificat.

Après la vérification, l'eID HIN est suspendue pendant six mois et le certificat HIN correspondant est révoqué. Pendant la période de suspension, une demande de rétablissement de l'eID HIN peut être présentée à HIN.

Après six mois, l'eID HIN est définitivement déclarée invalide et tous les droits d'accès sont révoqués.

En cas de perte ou de mauvaise utilisation présumées de l'eID HIN (virus, vol de données, perte de l'appareil, lettre du mot de passe initial non parvenue), le client doit en informer HIN. Pendant les heures d'ouverture, HIN suspend l'eID HIN concernée dans un délai de 30 minutes.

D Obligation de déclaration

Le contractant doit informer immédiatement HIN de tout cas (y compris les cas suspects) d'utilisation illégale ou non contractuelle des services HIN par les utilisateurs appartenant au contractant ou par des tiers non autorisés.

E Sécurité et protection des données

Le contractant reconnaît que les données sont transportées sur Internet via un réseau de télécommunications ouvert. Bien que les paquets de données soient transmis sous forme cryptée, l'expéditeur et le destinataire ne sont pas cryptés. Comme pour le courrier normal, leurs coordonnées peuvent être lues par des tiers.

Sécurité

Pour ses services, HIN accorde une importance particulière à la sécurité. Le système de sécurité de HIN est notamment basé sur des méthodes cryptographiques aux normes très strictes. En raison du cryptage, il n'est en principe pas possible, pour des personnes non autorisées, de consulter les données confidentielles des clients. Néanmoins, même avec toutes les mesures de sécurité les plus modernes, la sécurité absolue ne peut être garantie tant du côté de HIN que du côté du contractant.

Risques sur Internet

Le contractant reconnaît donc les risques suivants associés à l'utilisation d'Internet:

1. Une connaissance insuffisante du système et des mesures de sécurité inadéquates peuvent faciliter un accès non autorisé. Il incombe au contractant de s'informer des mesures de sécurité nécessaires.
2. Il existe un danger latent qu'une personne non autorisée ou un tiers externe puisse accéder à l'ordinateur du contractant sans se faire remarquer pendant l'utilisation d'Internet. HIN recommande l'utilisation d'un pare-feu (protection interne).
3. Il existe également un risque permanent que des virus informatiques se propagent dans l'ordinateur du contractant lorsque celui-ci utilise Internet. A cet égard, HIN recommande l'utilisation de logiciels antivirus qui peuvent aider le contractant à se défendre contre de tels risques.

F Utilisation de l'inscription en ligne (identification vidéo HIN)

L'inscription en ligne permet une identification sûre via une caméra de l'appareil du détenteur de l'ID. La caméra enregistre le son, la pièce d'identité et la photo du détenteur de l'ID, les vérifie numériquement et les compare avec une copie d'une pièce d'identité prise initialement. Le service est assuré par la société Intrum SA. Les données d'inscription sont collectées par HIN et transmises à Intrum SA. En utilisant ce service, le détenteur de l'ID consent expressément à la transmission de ces données à Intrum SA aux fins décrites ci-dessus.

Les informations fournies sont les nom et prénom, adresse, date de naissance, lieu de naissance, numéro de téléphone portable et adresse e-mail. Pendant le processus d'identification, des enregistrements photo et/ou vidéo de la pièce d'identité sont effectués pour comparer les données d'utilisateur final reçues précédemment avec les données figurant sur la pièce d'identité.

Toutes les données collectées par Intrum SA sont exclusivement utilisées pour identifier l'utilisateur final. La validation est transmise à HIN et sera supprimée des serveurs Intrum après 90 jours au plus

tard, dans la mesure où HIN n'aura pas déjà émis une demande de suppression. En raison des périodes de conservation légales, les données peuvent être stockées chez HIN pendant la durée de la relation commerciale entre HIN et le contractant et jusqu'à dix ans après qu'elle a pris fin.

G Réserve de dispositions légales

D'éventuelles dispositions légales régissant l'échange électronique de données sont réservées et s'appliquent également, lorsqu'elles entrent en vigueur, aux présentes dispositions-cadres pour la communication électronique de données.