

# INFORMATIONS ET DISPOSITIONS-CADRES POUR LA COMMUNICATION ÉLECTRONIQUE DE DONNÉES

## A Champ d'application et objet

Les présentes dispositions-cadres pour la communication électronique de données ~~s'appliquent à l'inscription en ligne de HIN par identification vidéo et~~ font partie intégrante de la relation contractuelle entre le contractant et Health Info Net SA (HIN).

~~HIN attache une grande importance à la protection des données (voir aussi <https://www.hin.ch/fr/ueber-hin/plattform/hin-und-der-datenschutz/>). La collecte et le traitement de vos données personnelles s'effectuent conformément aux réglementations et lois en vigueur en matière de protection des données.~~

### Utilisation de l'identité HIN (ID HIN)

Le contractant et les utilisateurs autorisés par ce dernier utilisent leur identité HIN (ID HIN) pour les transactions électroniques et la communication de données (e-mail, connexion à diverses applications eHealth). L'expéditeur et le destinataire sont vérifiés en ligne. Le contractant et les utilisateurs autorisés sont conscients que

- ~~le destinataire peut (et doit) supposer qu'une personne ou une institution désignée et autorisée communique avec lui et que la communication est confidentielle;~~
- ~~ils sont engagés et liés par la communication et les transactions via leur propre ID HIN;~~
- ~~le contractant d'un raccordement HIN est engagé et lié par la communication et les transactions via l'un des ID HIN qu'il a achetés;~~
- ~~le contractant est responsable de l'utilisation abusive des identités attribuées dans le cadre de son raccordement HIN.~~
- 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 ID 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 ID HIN est destinée uniquement au détenteur de l'ID (dans le cas d'une ID personnelle) ou du contractant (dans le cas d'une ID impersonnelle) 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'ID HIN restent enregistrés chez HIN pour une durée de six mois.

## B Accès aux services

### Conditions techniques

La communication s'effectue via des moyens assurés par le contractant lui-même, à savoir

- ~~1. un fournisseur Internet choisi par le contractant lui-même, un accès Internet,~~
2. le logiciel de sécurité de HIN,
3. les 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 ID HIN.

## ~~D Obligation de diligence~~

~~Le contractant prend les mesures nécessaires et appropriées pour empêcher tout accès non autorisé (systèmes propriétaires et systèmes de tiers), pour empêcher la propagation de virus et de spams et pour se conformer aux dispositions applicables du droit des télécommunications, du droit de protection des données et du droit d'auteur.~~

~~Le contractant est responsable de la protection de ses équipements, logiciels et données utilisés pour l'utilisation des services HIN ainsi que de toutes les données accessibles ou transmises via HIN contre tout accès non autorisé, manipulation, dommage et perte. HIN n'est pas responsable des dommages subis par le contractant à cet égard.~~

~~Le contractant est tenu de conserver avec le plus grand soin les aides mises à disposition à des fins de légitimation. Les codes et mots de passe spéciaux ne doivent pas être des combinaisons facilement identifiables ou permettre de tirer des conclusions (p. ex. date de naissance, numéro de téléphone) et doivent être tenus secrets. Ils ne peuvent en aucun cas être transmis à des tiers non autorisés. Le contractant est tenu de protéger les mots de passe ou les clés d'identification.~~

~~Le contractant supporte toutes les conséquences résultant de l'utilisation incorrecte de ses éléments et indicateurs de légitimation. Il incombe également au contractant de veiller à ce que les utilisateurs autorisés auxquels les aides électroniques sont mises à disposition respectent également les obligations susmentionnées.~~

~~Dans le cas de processus automatisés par le client et qui ne permettent pas l'utilisation d'une identification personnelle, le client doit prendre des mesures de sécurité adéquates pour protéger l'équipement de communication et pour empêcher l'utilisation abusive des ID HIN utilisées (salle fermée avec accès réservé aux personnes autorisées, etc.).~~

## **Invalidation d'une identité HIN**

Une identité HIN ne peut être invalidée que par HIN. Une identité HIN est invalidée dès qu'un abus ou un soupçon justifié d'abus de l'identité 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/utilisateur d'identités HIN ou l'émetteur du certificat.

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

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

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

## **E Services de tiers**

~~Si le contractant ou les utilisateurs qui lui appartiennent utilisent les offres et les services de tiers via les services HIN, le contractant est lui-même responsable du respect des conditions d'utilisation applicables et de la facturation avec les tiers. HIN n'assume aucune responsabilité quant à la disponibilité, aux contenus, à la qualité ou à l'utilité des services de tiers.~~

~~Si le contractant utilise et facture directement les services de tiers, il est responsable du respect des conditions d'utilisation de ces services de tiers et doit régler toutes les dispositions correspondantes avec ces tiers.~~

## 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.

## ~~G Exclusion de responsabilité~~

~~HIN décline toute responsabilité pour les dommages subis par le contractant en raison d'erreurs de transmission, de défauts techniques, d'interruptions, de dysfonctionnements ou d'interventions illégales dans les liaisons de télécommunications, de surcharge du réseau ou d'autres insuffisances de la part des fournisseurs de réseau lors de l'utilisation d'Internet. HIN décline expressément toute responsabilité pour les logiciels qu'elle fournit et pour les conséquences découlant de la transmission des logiciels via Internet. HIN se réserve le droit d'interrompre les services à tout moment pour protéger le contractant dans le cas où des risques de sécurité sont identifiés, et ce jusqu'à leur élimination.~~

## 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 postal, les informations concernant tant l'expéditeur que le destinataire peuvent être lus 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 en utilisant 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.

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

L'inscription en ligne permet une identification sécurisée via une caméra ~~ou la vidéo de votre de~~ l'appareil. ~~Le son, une photo de votre pièce d'identité et de vous sera prise par ce biais, vérifiée numériquement et comparée.~~ 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 AG SA. Les données d'inscription sont collectées par HIN et transmises à Intrum AG SA. En utilisant ce service, ~~vous consentez le détenteur de l'ID consent~~ expressément à la transmission de ces données à Intrum AG 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 obtenues précédemment avec les données figurant sur la pièce d'identité. Toutes les données collectées par Intrum AG SA sont exclusivement utilisées pour identifier l'utilisateur final. La validation est transmise à HIN et sera supprimée des serveurs Intrum au plus tard 90 jours après, 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 ~~période déterminée et jusqu'à dix ans après la fin de la relation commerciale entre HIN et vous.~~ 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

Toutes les dispositions légales régissant l'échange électronique de données sont réservées et s'appliquent également aux présentes dispositions-cadres pour la communication électronique de données au moment de leur entrée en vigueur.

## ~~K Modifications des présentes dispositions-cadres~~

~~Ces dispositions-cadres peuvent être modifiées sans préavis.~~