G&P
Goetz & Patak
Rechtsanwälte

Sascha Daniel Patak
Dr.iur. Rechtsanwalt
Oberwachtstrasse 13
8700 Küsnacht ZH
Direkt +41 44 991 1211
Office +41 44 991 1212
Fax +41 44 991 12 65
sp@gplegal.ch /www.gplegal.ch

Évaluation des e-Ordonnances

Avec la nouvelle loi sur les médicaments et les dispositions d'exécution correspondantes de l'ordonnance sur les médicaments, il est désormais possible d'établir des ordonnances sous forme numérique (e-Ordonnance). De nouvelles prescriptions ont été adoptées à cet effet à l'art. 51 de l'ordonnance. Il s'agit ci-après d'évaluer ces prescriptions à la lumière de la solution choisie par HIN.

Une e-Ordonnance peut être établie de deux manières. D'une part, selon l'al. 2 de ladite prescription, elles peuvent être établies par voie électronique au moyen d'une signature électronique qualifiée conformément à la loi sur la signature électronique ou «être transmises de manière à ce qu'elles remplissent des exigences de sécurité comparables en termes d'authenticité, d'intégrité des données et de confidentialité».

Le législateur s'écarte ainsi des directives très strictes de la loi sur la signature électronique sans toutefois renoncer à la protection et à la sécurité. Il en va de même dans le rapport explicatif, où l'on peut lire:

«Pour les ordonnances électroniques, il est possible de choisir – au lieu d'une signature électronique qualifiée – une signature ou une forme de transmission qui remplit les différentes fonctions de sécurité telles que la garantie de l'authenticité (autorisation du prescripteur d'établir l'ordonnance), de l'intégrité des données (protection contre les falsifications) et de la confidentialité (protection contre une utilisation multiple) de manière équivalente à la signature électronique qualifiée selon l'art. 14, al. 2bis CO. La signature des prescriptions électroniques est suffisante lorsque la procédure utilisée remplit les fonctions de sécurité susmentionnées. Les exigences de sécurité associées à la procédure utilisée (p. ex. directives de la LDEP et de ses

systèmes communautaires) fournissent alors un environnement suffisamment protégé pour assurer la bonne transmission de l'ordonnance électronique.»[1]

Par conséquent, si une autre forme de transmission que la forme purement numérique[2] est utilisée, il convient d'évaluer si elle remplit les aspects d'authenticité du créateur, de protection contre la falsification et de protection contre l'utilisation multiple de manière comparable à la signature électronique qualifiée.

Pour que tous les utilisateurs (en particulier les plus âgés) puissent participer, une e-Ordonnance doit pouvoir être délivrée sous forme numérique et physique/analogique par le médecin au patient et par le patient à la pharmacie. L'impression rend impossible toute signature numérique qualifiée, car celle-ci ne peut alors plus être vérifiée.

HIN a opté pour un code QR (voir annexe), qui porte les informations de l'e-Ordonnance et peut les transporter de manière numérique ou analogique. La signature HIN Sign est alors utilisée pour la création de l'ordonnance, ce qui garantit la sécurité et le caractère univoque de l'ordonnance. Les conditions requises à cet égard sont ainsi remplies de manière équivalente, pour autant que cela soit manifeste.

L'authentification du médecin, dernier critère, doit permettre d'attribuer l'e-Ordonnance au médecin qui l'a délivrée. Une identité électronique fortement authentifiée est utilisée à cet effet, pour laquelle le médecin doit s'enregistrer personnellement auprès de HIN (identification vidéo conforme à la LDEP et envoi physique des données d'accès). Cette identité électronique renforcée

---

[1] Quatrième train d'ordonnances sur les produits thérapeutiques, Rapport sur les résultats de la consultation, OFSP, septembre 2018, https://www.bag.admin.ch/dam/bag/en/dokumente/biomed/heilmittel/revision-hmg/VL_Bericht_2018.pdf.download.pdf/Vernehmlassungsbericht_fr.pdf

[2] Nota bene: une signature électronique qualifiée doit rester numérique pour que sa validité puisse être vérifiée.

est impérative pour le déclenchement de la signature électronique. Cela se fait conformément à la norme technique contenue dans la prescription CSN EN 419241-1 (Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements; European Standards, https://www.bakom.admin.ch/bakom/fr/page-daccueil/suisse-numerique-et-internet/communication-numerique/signature-electronique/references-normatives.html). Pour la signature électronique qualifiée, il est fait référence à SCAL2 (SRA_SAP1.1). Dans l'annexe A, sous-clause A2.2, p. 41 de l'annexe, la base de l'authentification est décrite comme suit:

«The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.»

Dans la même annexe, il est également précisé que l'authentification doit faire l'objet de deux vérifications (Substantial, ch. 1 «authentication factors») par différents accès (ibid. «different categories»).

Il existe trois options d'inscription dans le présent projet:

Comme première méthode, le médecin s'authentifie en s'inscrivant à HIN via deux facteurs: 1) mot de passe fort pour la connexion à HIN 2) via un SMS avec code. Un mot de passe fort permet déjà d'exclure de facto la recherche aléatoire du mot de passe par des tiers (selon la consigne «higly unlikely»). Si le mot de passe devait être intercepté ou capté, le téléphone devrait également être disponible pour le deuxième facteur. La sécurité de l'authentification est ainsi respectée conformément à la directive.

La deuxième méthode consiste à utiliser le client HIN en plus du mot de passe du médecin. Ce client sert déjà d'accès sécurisé à la plate-forme HIN pour les médecins et est déjà utilisé depuis longtemps comme deuxième facteur. Il vérifie (par une connexion séparée et une technologie hautement sécurisée spécialement développée à cet effet) l'intégrité du mot de passe et assure le deuxième facteur avec un niveau de sécurité comparable.

Une autre procédure a été mise à disposition pour les médecins dans les hôpitaux, où un SMS ne peut pas toujours y être garanti (absence de téléphone portable ou de connexion), et le client HIN ne peut pas être intégré sur tous les sites (directives internes à l'hôpital). Les médecins se connectent alors en interne via un mot de passe fort selon les directives de la direction de la santé et de l'hôpital. Le deuxième facteur est la gestion de la sécurité du site, qui vérifie le site de chaque médecin dans le système HIN et le compare au site autorisé pour lui. L'intégrité de l'accès est ainsi vérifiée par le biais des contrôles et des autorisations d'accès sur chaque site. Ce contrôle d'intégrité permet d'exclure qu'un mot de passe capté, p. ex., puisse être utilisé de l'extérieur (donc en dehors de l'hôpital). Un mot de passe hautement sécurisé (qui est la base dans les hôpitaux) est déjà très sûr, comme indiqué ci-dessus. La gestion de la sécurité du site permet en outre de mettre en place une deuxième sécurité. Celle-ci rend pratiquement impossible (highly unlikely) d'établir une e-Ordonnance via un mot de passe capté, car il faudrait en outre se trouver à l'intérieur de l'hôpital (qui reconnaît et enregistre tous les accès par des fichiers journaux). Cette méthode remplit donc également les conditions de la directive technique et est comparable aux exigences d'autres réglementations à deux facteurs.

Selon le point de vue compris ici, les trois voies décrites permettent de répondre à l'exigence du législateur en matière d'e-Ordonnance.

Küsnacht, le 27 mars 2023

Sascha D. Patak, docteur en droit