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

Beurteilung E-Rezepte

Mit der Gesetzesnovelle des Arzneimittelgesetzes sowie den entsprechenden ausführenden Bestimmungen der Arztneimittelverordnung, besteht neu die Möglichkeit, Rezepte auch digital zu erstellen (E-Rezept). Dazu wurden in Art. 51 der Verordnung neue Vorschriften erlassen. Nachfolgend gilt es, diese Vorschriften im Hinblick auf die von HIN gewählte Lösung zu beurteilen.

Ein E-Rezept kann auf zwei Arten erstellt werden. Einerseits kann gemäss Abs. 2 der besagten Vorschrift elektronisch mit einer qualifizierten elektronischen Signatur gemäss Signaturgesetz erfolgen oder aber „so übermittelt werden, dass sie in Bezug auf Authentizität, Datenintegrität und Vertraulichkeit die Anforderungen an die Sicherheit in vergleichbarer Weise erfüllen, wie wenn sie mit einer qualifizierten elektronischen Signatur versehen wären".

Damit weicht der Gesetzgeber von den sehr eng gefassten Richtlinien des Signaturgesetzes ab, ohne aber den Schutz und die Sicherheit aufzugeben. Gleiches geht auch aus dem erläuternden Bericht hervor, in welchem steht:

„Bei elektronischen Rezepten kann – anstelle einer qualifizierten elektronischen Signatur – eine Signatur beziehungsweise eine Übermittlungsform gewählt werden, welche die verschiedenen Sicherheitsfunktionen wie Sicherung der Authentizität (Berechtigung der verschreibenden Person für das Ausstellen des Rezeptes), der Datenintegrität (Schutz vor Verfälschungen) sowie der Vertraulichkeit (Schutz vor mehrfacher Verwendung) gleich gut gewährleistet wie die qualifizierte elektronische Signatur nach Artikel 14 Absatz 2 bis OR. Die Unterschrift bei elektronischen Verschreibungen ist damit hinreichend, wenn das für sie verwendete Verfahren die vorgenannten Sicherheitsfunktionen erfüllt. Die mit dem verwendeten Verfahren verbundenen Sicherheitsvorgaben (z.B. Vorgaben des EPDG und seiner Gemeinschaftssysteme) bilden dann eine

genügend geschützte Umgebung für die einwandfreie Übermittlung des elektronischen Rezeptes."[1]

Wird also eine andere Form der Übermittlung, als die rein digitale[2] verwendet, ist zu beurteilen, ob diese die Aspekte Authentizität des Erstellers, Verfälschungsschutz und Schutz vor Mehrfachverwendung in vergleichbarer Weise erfüllt, wie bei der qualifizierten elektronischen Signatur.

Um alle Nutzer (besonders auch die älteren) partizipieren lassen zu können, muss ein E-Rezept sowohl digital wie auch physisch/analog vom Arzt an den Patienten und vom Patienten an die Apotheke ausgegeben werden können. Mit dem Ausdruck wird die Möglichkeit einer qualifizierten digitalen Signatur verunmöglicht, da diese dann nicht mehr überprüft werden kann.

HIN hat sich für einen QR-Code (siehe Beilage) entschieden, welche die Informationen des E-Rezeptes darstellen und digital wie analog transportieren können. Dabei wird die HIN-Sign-Signatur für die Erstellung des Rezeptes verwendet, welche die Sicherheit und die Eineindeutigkeit des Rezeptes garantiert. Damit werden die diesbezüglichen Voraussetzungen soweit ersichtlich gleichwertig erfüllt.

Die Authentifizierung des Arztes als letztes Kriterium, soll das E-Rezept dem ausstellenden Arzt zuordnen. Diesbezüglich wird eine stark authentisierte elektronische Identität eingesetzt, für welche sich der Arzt bei der HIN persönlich registrieren lass muss (EPDG-konformen Videoidentifizierung und physische Zustellung der Zugangsdaten). Diese gehärtete elektronische Identität ist zwingend für die Auslösung der elektronischen Signatur notwendig.

---

[1] Heilmittelverordnungspaket IV, Erläuterungen zur, Verordnung über die Arzneimittel (Arzneimittelverordnung, VAM), BAG, September 2018, https://www.bag.admin.ch/dam/bag/de/dokumente/biomed/heilmittel/revision-hmg/erlaeuterungen-vam.pdf.download.pdf/VAM_Erläuterungen_de.pdf

[2] Nota bene: eine qualifizierte elektronische Signatur muss digital bleiben, um deren Gültigkeit überprüfen zu können.

Dies erfolgt gemäss der technischen Norm in der CSN EN 419241-1 (Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements; European Standards, https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/digitale-kommunikation/elektronische-signatur/normierungsreferenzen.html). Für die qualifizierte elektronische Signatur wird hierfür auf SCAL2 (SRA_SAP1.1) verwiesen. In Annex A, subclause A2.2, S. 41 des Annexes wird die Grundlage der Authentifizierung wie folgt umschrieben:

„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."

Im Gleichen Annex wird ebenfalls festgehalten, dass für die Authentifizierung zwei Überprüfungen (Substanital, Ziff. 1 «authentication factors») durch verschiedene Zugänge (ebenda «different categories») erfolgen soll.

Im vorliegenden Projekt gibt es drei Anmeldeoptionen:

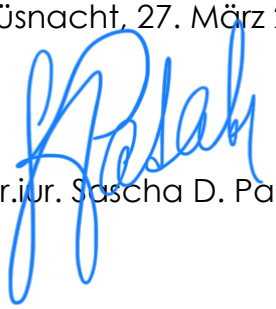
Der Arzt authentifiziert sich als erste Methode durch seine Anmeldung bei HIN über zwei Faktoren: 1) starkes Passwort für die HIN-Anmeldung 2) über ein SMS mit Code. Mit einem starken Passwort kann die zufällige Suche nach dem Passwort durch Dritte bereits faktisch ausgeschlossen werden (gemäss Vorgabe «higly unlikely»). Sollte das Passwort abgefangen oder erhascht werden, so müsste auch noch das Telefon für den zweiten Faktor zur Verfügung stehen. Damit wird der Sicherheit der Authentifizierung nach der Richtlinie entsprechend Folge geleistet.

Als zweite Methode wird zusätzlich zum Passwort des Arztes der HIN-Client verwendet. Dieser Client dient bereits für die HIN-Plattform als sicherer Zugang für Ärzte und ist bereits seit langem als zweiter Faktor im Einsatz. Er prüft (durch separate Anmeldung und eigens speziell entwickelter hochsicherer Technologie) die Integrität des Passwortes und stellt mit vergleichbar hoher Sicherheit den zweiten Faktor sicher.

Besonders für Ärzte in Spitälern wurde ein weiteres Verfahren zur Verfügung gestellt, da dort ein SMS nicht immer gewährleistet werden kann (fehlendes Mobiltelefon oder fehlende Verbindung) und der HIN-Client nicht an allen Standorten integriert werden kann (spitalinterne Richtlinien). Sie melden sich über ein starkes Passwort nach Richtlinien der Gesundheitsdirektion und des Spitales intern an. Als zweiter Faktor besteht dort ein Standort-Security-Management, welches bei jedem Arzt im System der HIN dessen Standort überprüft und mit dem für ihn zulässigen Standort vergleicht. So wird die Integrität des Zugangs über die Zutrittskontrollen und -Berechtigungen am jeweiligen Ort verifiziert. Mit dieser Integritätsprüfung kann ausgeschlossen werden, dass ein z.B. erhaschtes Passwort von extern (also ausserhalb des Spitales) verwendet werden kann. Ein hochsicheres Passwort (welches Grundlage in den Spitälern ist) ist bereits wie oben dargestellt sehr sicher. Mit dem Location-Security-Management wird zudem von zweiter Seite eine Sicherheit errichtet. Entsprechend ist es praktisch unmöglich (highly unlikely), ein E-Rezept durch Erhaschen eines Passwortes zu erstellen, da man zudem noch innerhalb des Spitales (welches sämtliche Zugriffe durch Log-files erkennt und speichert) sein müsste. Dieses erfüllt damit auch die Voraussetzungen der technischen Richtlinie und ist vergleichbar mit den Anforderungen anderer Zwei-Faktoren-Regelungen.

Nach hier verstandener Auffassung kann mit den drei beschriebenen Wegen die Anforderung des Gesetzgebers an ein E-Rezept erfüllt werden.

Küsnacht, 27. März 2023



Dr.iur. Sascha D. Patak