E-ID: Risiken auf Gesundheitsfachkräfte und Patienten abgewälzt

Daniel Muster

lic. phil. nat., Physiker Universität Bern, NDS Informationstechnologie ETHZ, selbständiger Sicherheitsfachmann einer GmbH für IT-Risk-Management

Mit der Einführung der gesetzlichen elektronischen Identität (E-ID) beim elektronischen Patientendossier sind nicht weniger Risiken, sondern mehr verbunden. Dies im Widerspruch zur Beteuerung in der Botschaft zum E-ID-Gesetz ans Parlament.

In der Herbstsession 2019 hat das Parlament das Bundesgesetz über die elektronische Identifizierungsdienste (BGEID oder E-ID-Gesetz) verabschiedet. Damit soll die Handhabung elektronischer Identitäten (E-ID) geregelt werden.

Behörden oder andere Stellen, die öffentliche Aufgaben erfüllen, haben nun eine E-ID zu akzeptieren. Dies sofern sie eine elektronische Identifizierung beim Vollzug von Bundesrecht vornehmen und die E-ID die geforderte Sicherheit bietet [1].

Naheliegend ist nun, dass die E-ID ins elektronische Patientendossier, kurz e-Patientendossier, integriert wird. Spitäler inklusive Rehakliniken und Psychiatrien sind dazu verpflichtet, bis April 2020 e-Patientendossiers anzubieten; Geburtshäuser und Pflegeheime bis 2022.

Dabei begann die Sache für die elektronische Identität (E-ID) so «verheissungsvoll». «Einfach», «sicher», «bequem», so die Wortwahl in der Botschaft zum E-ID-Gesetz [2]. Trotz Nachbesserungen durchs Parlament hat das E-ID-Gesetz noch viel Potential zur Verbesserung. Einige Mängel haben negative Auswirkungen auf die Inhaber einer E-ID.

Aufgrund dieser Mängel entstehen neue Risiken für Gesundheitsfachkräfte und Patienten bei der Einbindung der E-ID ins e-Patientendossier. Im Folgenden werden dargelegt:

- Gefahren für den Patienten, dessen Daten im e-Patientendossier mit E-ID-Anbindung abgelegt sind;
- Risiken für Gesundheitsfachkräfte, welche sich mit einer E-ID beim e-Patientendossier anmelden.

Gefahren für den Patienten

Geplant ist, dass jede IT-Verbindung mit einer elektronischen Identität (E-ID) über das IT-System des E-ID-Herausgebers aufgebaut werden muss. Da folglich das IT-System des Herausgebers Dreh- und Angelpunkt für eine Verbindung mit einer von ihm ausgestellten E-ID ist, hat dies Folgen. Und zwar:

1. Funktioniert das IT-System des E-ID-Herausgebers nicht, dann kann sein Kunde keine Verbindung mit seiner E-ID mehr aufbauen. Das heisst z.B., die Gesundheitsfachkraft kann nicht mehr mittels E-ID aufs e-Patientendossier zugreifen. Das IT-System eines E-ID-Herausgebers stellt somit ein Klumpenrisiko dar. Damit verringert sich die Verfügbarkeit des e-Patientendossiers zwangsläufig. Die hohe Verfügbarkeit, im Notfall auf Patientendaten zugreifen zu können, ist eine der Verheissungen des e-Patientendossiers [3]. Zur Verfügbarkeit des E-ID-Systems des Herausgebers äussert sich das Gesetz jedoch nicht.
2. Der E-ID-Herausgeber kann feststellen, welche E-ID-Dienstleistungen sein E-ID-Kunde bezieht. Somit kann er Verhaltensmuster seines Kunden erstellen. Zwar dürfen diese Informationen nicht weitergegeben werden. Was nützt aber ein Verbot, wenn nicht kontrollierbar ist, ob es eingehalten wird?
3. Mit keinem grossen Aufwand kann sich der Herausgeber der E-ID als sein E-ID-Kunde ausgeben. Somit kann er sich z.B. als eine Gesundheitsfachkraft beim e-Patientendossier anmelden und folglich dort Daten einsehen oder sogar verändern. Richtigkeit und Vollständigkeit der Patientendaten sind zentral für die Behandlung.
4. Es bestünden sicherere Lösungen als mit der angedachten E-ID-Implementierung.

Die genannten Gefahren machen das E-ID-System des Herausgebers für Hacker überaus attraktiv.

Risikoabwälzung

Risiken sind bei der Digitalisierung nicht wegzudenken. Es stellt sich die Frage, wer für die Risiken eines Schadens einzustehen hat. Für einen Schaden ist nur einzustehen, wenn die Verantwortlichkeiten/Pflichten im Gesetz umschrieben sind und eine Haftung dazu besteht.

Systemwechsel

Bei vielen IT-Anwendungen im Geschäftsbereich haben die Kleinkunden die Risiken zu tragen. Viele Online-Anbieter bedingen die Haftung soweit zulässig oder gar darüber hinaus weg. Selbst, wenn ein Kunde Anspruch auf Schadenersatz hat, so gilt «Recht haben und Recht bekommen sind 2 Paar Schuhe». Ein Zivilprozess (bis zu einem Bundesgerichtsentscheid) kann den Kunden teuer zu stehen kommen. Das Prozessrisiko steht meist in keinem Verhältnis zum Schaden.

Anders sieht es bis anhin im Amtsverkehr zwischen Staat und Bürger aus. Die Haftung ist meist umfassender, darf nicht wegbedungen werden, und die Prozesskosten übers Verwaltungsgericht sind meist überschaubar. Dies kann sich nun bei E-ID-Anwendungen ändern. Die Haftung einer E-ID-Anwendung, z.B. des e-Patientendossiers, richtet sich nach dem Obligationenrecht (OR), dies auch dann, wenn die Anwendung Aufgaben des öffentlichen Rechts abwickelt [4]. Die Haftung für öffentlich-rechtliche Dienste wäre jedoch umfassender, was für den Geschädigten vorteilhaft ist.

Haftung des E-ID-Kunden

Für die Gesundheitsfachkraft gilt: «Der E-ID-Inhaber hat die nach den Umständen notwendigen und zumutbaren Massnahmen zu treffen, damit seine E-ID nicht missbräuchlich verwendet werden kann [5].» Problematisch an dieser Pflicht ist, dass im Gesetz nicht definiert ist, was eine E-ID ist. Schwierigkeiten bei der Rechtsprechung sind voraussehbar. (In der entsprechenden EU-Verordnung [6] werden 41 Begriffe definiert, im E-ID-Gesetz nur 2.)

Gemäss Gesetz umfasst die E-ID Komponenten, welche ausserhalb des Einflusses ihres Inhabers sind, z.B. Daten zur physischen Identifizierung zwecks Ausstellung einer E-ID. Doch diese Komponenten sind für die Sicherheit einer E-ID-Anwendung wie des e-Patientendossiers von grosser Wichtigkeit.

Welche Massnahmen für den E-ID-Inhaber nach den Umständen notwendig und zumutbar sind, wird in keiner Verordnung näher beschrieben werden [7]. Somit bleiben die Anforderungen an den E-ID-Inhaber nebulös. Dies ist der Rechtssicherheit abträglich, folglich risikobehaftet.

Entsteht ein Streit zwischen E-ID-Herausgeber und seinem E-ID-Kleinkunden, so hat dieser schlechte Karten. Der Rechtsweg ist privatrechtlich, d.h. übers Zivilgericht, und somit finanziell schwer kalkulierbar.

Fehlende Umschreibung der Verantwortlichkeiten

Wie erwähnt ist das IT-System Dreh- und Angelpunkt für den Verbindungsaufbau mit einer E-ID. Doch sind die Pflichten und die Rechte zwischen dem e-Patientendossier und dem E-ID-Herausgeber per Gesetz nicht definiert. Rechte und Pflichten müssten aber im Gesetz festgehalten werden [8].

Damit die Ursache eines Schadens bestimmt werden kann, bedarf es der Nachvollziehbarkeit der Prozesse. Die Nachvollziehbarkeit wird aber im Gesetz nicht ge-

fordert. Kann der Verursacher des Schadens nicht festgestellt werden, hat grundsätzlich der Geschädigte den Schaden zu tragen. Dies sofern eine Versicherung den Schaden nicht übernimmt.

Fazit

Der Digitalisierung bedarf es, jedoch nicht zu Lasten der IT-fachunkundigen Anwender. Die Haftung sollte zukünftig anders ausgestaltet sein. Nämlich so, dass die Haftung grundsätzlich auf denjenigen fällt, der durch die Digitalisierung Risiken schafft.

Wenn weiterhin zu Lasten von Otto Normalverbraucher Abläufe staatlich kontrolliert digitalisiert werden, dann schwindet das Vertrauen in die digitalen Prozesse und in den Staat. Erste Symptome sind z.B. an der ablehnenden Haltung vieler Bürger zu E-Voting erkennbar und berechtigterweise zur E-ID.

Aus meiner Optik haben sich Verbände bisher kaum gegen die Einführung oder für die Verbesserung des E-ID-Gesetzes zum Schutz ihrer davon betroffenen Mitglieder eingesetzt. Ob das Vertrauen der Mitglieder in ihre Verbände künftig auch schwinden wird?

Bildnachweis
© Pop Nukoonrat | Dreamstime.com

Literatur

1 Art. 22 BGEID.
2 Bundesblatt S. 3915ff, 2018.
3 Unterschied elektronische Krankengeschichte und elektronisches Patientendossier, eHealth Suisse, Koordinationsorgan Bund Kantone, 8. Dezember 2015.
4 Art. 32 BGEID, siehe Kommentar zu Art. 3 VG, N54, Thierry Luterbacher, Willi Fischer (Hrsg.), Haftpflichtkommentar, Dike Verlag, 2016.
5 Art. 12 Abs. 1 BGEID.
6 EU-Verordnung vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt.
7 Eine Legitimation fehlt im Gesetz.
8 Art. 164 Bundesverfassung.

Das Wichtigste in Kürze

- Das im Herbst verabschiedete Bundesgesetz über die elektronischen Identifizierungsdienste (BGEID oder E-ID-Gesetz) soll die Handhabung elektronischer Identitäten (E-ID) re-geln. Behörden oder andere Stellen, die öffentliche Aufgaben erfüllen, haben nun eine E-ID zu akzeptieren. Dies sofern sie eine elektronische Identifizierung beim Vollzug von Bundesrecht vornehmen und die E-ID die geforderte Sicherheit bietet.
- Es ist naheliegend, dass die E-ID ins elektronische Patientendossier integriert wird. Spitäler inkl. Rehakliniken und Psychiatrien sind dazu verpflichtet, bis April 2020 e-Patientendossiers anzubieten; Geburtshäuser und Pflegeheime bis 2022.
- Aufgrund diverser Mängel im E-ID-Gesetz entstehen jedoch neue Risiken für Gesundheitsfachkräfte und Patienten bei der Einbindung der E-ID ins e-Patientendossier. Auch sind die Pflichten und die Rechte zwischen dem e-Patientendossier und dem E-ID-Herausgeber per Gesetz nicht definiert.

L'essentiel en bref

- La loi fédérale sur les services d'identification électronique (LSIE) adoptée à l'automne est censée réglementer la gestion des identités électroniques (e-ID). Les autorités ou d'autres services assumant des tâches publiques doivent maintenant accepter une e-ID. Et ce, dans la mesure où ils procèdent à une identification électronique lors de l'exécution du droit fédéral et que l'e-ID offre la sécurité requise.
- Il est vraisemblable que l'e-ID sera intégrée dans le dossier électronique du patient. Les hôpitaux – cliniques de réadaptation et unités de psychiatrie comprises - seront contraints de proposer un dossier électronique du patient d'ici avril 2020, et les maisons de naissance et les établissements médico-sociaux d'ici 2022.
- Diverses lacunes dans la LSIE entraînent cependant de nouveaux risques pour les professionnels de santé et les patients au niveau de l'intégration de l'e-ID dans le dossier électronique du patient. Les obligations et les droits entre le dossier électronique du patient et l'éditeur de l'e-ID ne sont pas non plus définis par la loi.