Kleine Anfrage zur schriftlichen Beantwortung
gemäß § 46 Abs. 1 GO LT

Abgeordneter MUDr. PhDr. / Univ.Prag Jozef Rakicky (fraktionslos)

Massive Sicherheitslücken bei der elektronischen Patientenakte?

Anfrage des Abgeordneten MUDr. PhDr. / Univ.Prag Jozef Rakicky (fraktionslos) an die Landesregierung, eingegangen am 07.02.2026

In ihrer Antwort in der Drucksache 19/9499 auf meine Kleine Anfrage zur schriftlichen Beantwortung zum Stand der Einführung der elektronischen Patientenakte in Niedersachsen erklärt die Landesregierung auf meine Frage nach technischen Hürden und Problemen:

„Die wesentlichen technischen Hürden für die Nutzung der elektronischen Patientenakte (ePA) liegen in der erforderlichen Anbindung an die Telematikinfrastruktur (TI) sowie in der Integration eines funktionierenden ePA-Moduls in das Praxisverwaltungssystem (PVS) bzw. das Krankenhausinformationssystem (KIS). Vor allem Krankenhäuser stehen aufgrund der Komplexität der Systeme vor Herausforderungen. Verzögerungen bei der Auslieferung und Integration der ePA-Module durch Hersteller sowie TI-Störungen können als weitere Hindernisse benannt werden. Trotz der Störungen entwickelt sich die Zahl der nutzbaren Funktionen und der abgerufenen ePA-Dokumente positiv."

In dieser Antwort wird keinerlei Bezug genommen auf mögliche Schwachstellen der elektronischen Dateninfrastruktur, insbesondere was die Sicherheit der Patientendaten betrifft. In einem Beitrag des Portals Netzpolitik.org[1] von Ende Dezember 2025 warnt die Sicherheitsforscherin und Vorsitzende des Innovationsverbunds Öffentliche Gesundheit e. V. vor Hackerangriffen und Datendiebstahl: „Ein Großteil der Probleme der Gesundheitsdigitalisierung der vergangenen Jahrzehnte sind Identifikations- und Authentifizierungsprobleme". Zahlreiche Schwachstellen der ePa haben sie und ihre Kollegen offengelegt: „[Eine] Schwachstelle ermöglichte es Angreifenden, falsche Nachweise vom VSDM-Server zu beziehen, die vermeintlich belegen, dass eine bestimmte elektronische Gesundheitskarte vor Ort vorliegt. Auf diese Weise ließen sich dann theoretisch unbefugt sensible Gesundheitsdaten aus elektronischen Patientenakten abrufen."

Weiter schreibt das Medium: „Nach den Enthüllungen versprach der damalige Bundesgesundheitsminister Karl Lauterbach (SPD) einen ePA-Start ‚ohne Restrisiko'. Doch unmittelbar nach dem Starttermin konnten die erwähnte Sicherheitsforscherin und weitere IT-Sicherheitsforscher erneut unbefugt Zugriff auf die ePA erlangen. Auch dieses Mal benötigten sie dafür keine Gesundheitskarte, sondern nutzten Schwachstellen im Identifikations- und Authentifizierungsprozess aus." Neue Sicherheitsprobleme werden laut einer der beteiligten Sicherheitsforschern schon im kommenden Jahr bei der geplanten staatlichen „EUDI-Wallet" erwartet; sie äußerte: „Die Genese der deutschen staatlichen EUDI-Wallet befindet sich auf einem ähnlich unguten Weg wie die ePA".

1. Wie bewertet die Landesregierung grundsätzlich die im Beitrag von Netzpolitik.org als „strukturelle Schwachstellen" geschilderten Identifikations- und Authentifizierungsprobleme in der Digitalisierung der Gesundheitsversorgung?

2. Inwiefern sind der Landesregierung die von Sicherheitsforschern offengelegten konkreten „Schwachstellen" bekannt, die einen unbefugten Zugriff auf ePA-Daten theoretisch ermöglichen sollen?

3. Wie wird sichergestellt, dass sensible Gesundheitsdaten wirksam geschützt sind, wenn laut Expertenangaben selbst wiederholte unbefugte Zugriffe ohne Gesundheitskarte möglich waren?

[1] https://netzpolitik.org/2025/digitale-brieftasche-auf-einem-aehnlich-unguten-weg-wie-die-elektronische-patientenakte/

4. Welche Konsequenzen zieht die Landesregierung gegebenenfalls daraus, dass Sicherheitsforscher auch nach dem angekündigten ePA-Start „ohne Restrisiko“ erneut „Schwachstellen“ nachweisen konnten?

5. Welche Rolle spielt aus Sicht der Landesregierung unabhängige Sicherheitsforschung bei der Weiterentwicklung der ePA, und wie werden gegebenenfalls entsprechende Warnungen unabhängiger Forscher systematisch berücksichtigt?

6. Wie wird das Risiko eingeschätzt, dass bereits bekannte Probleme im Identifikations- und Authentifizierungsprozess künftig auch auf andere digitale Gesundheitsprojekte wie die geplante EUDI-Wallet übertragen werden könnten?

7. Sieht sich die Landesregierung in der Verantwortung, Bürger transparent über gegebenenfalls bestehende Restrisiken bei der Nutzung der elektronischen Patientenakte zu informieren?

8. Wie lässt sich angesichts der beschriebenen Sicherheitsprobleme gewährleisten, dass das Vertrauen der Bevölkerung in die digitale Gesundheitsinfrastruktur nicht nachhaltig beschädigt wird?