Kleine Anfrage zur schriftlichen Beantwortung
gemäß § 46 Abs. 1 GO LT
mit Antwort der Landesregierung

Anfrage des Abgeordneten MUDr. PhDr. / Univ.Prag Jozef Rakicky (fraktionslos)

Antwort des Niedersächsischen Ministeriums für Soziales, Arbeit, Gesundheit und Gleichstellung namens der Landesregierung

Massive Sicherheitslücken bei der elektronischen Patientenakte?

Anfrage des Abgeordneten MUDr. PhDr. / Univ.Prag Jozef Rakicky (fraktionslos), eingegangen am 07.02.2026 - Drs. 19/9928,
an die Staatskanzlei übersandt am 26.02.2026

Antwort des Niedersächsischen Ministeriums für Soziales, Arbeit, Gesundheit und Gleichstellung namens der Landesregierung vom 26.03.2026

Vorbemerkung des Abgeordneten

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

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

Die bestehenden Sicherheitsstandards im Gesundheitswesen gehören zu den anspruchsvollsten in Deutschland. Grundsätzlich ist jedoch festzuhalten, dass eine absolute, hundertprozentige Sicherheit in komplexen digitalen Infrastrukturen realistisch schwer zu erreichen ist.

Identifikations- und Authentifizierungsverfahren innerhalb der TI werden auf Bundesebene durch die gematik GmbH und das Bundesamt für Sicherheit in der Informationstechnik (BSI) festgelegt und unterliegen einem permanenten sicherheitstechnischen Prüf- und Weiterentwicklungsprozess. Hinweise aus Sicherheitsforschung und Fachöffentlichkeit werden kontinuierlich einbezogen, bewertet und fließen in Anpassungen der Infrastruktur ein. Dadurch soll gewährleistet werden, dass neue sicherheitsrelevante Erkenntnisse zeitnah berücksichtigt werden und das Schutzniveau der TI den aktuellen technischen Standards entspricht. Mitarbeitende und Nutzende der TI werden stetig im Umgang mit IT-Sicherheitsaspekten und Patientendaten sensibilisiert.

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

Die in den Medien beschriebenen Schwachstellen sind der Landesregierung und den zuständigen Institutionen bekannt. Es handelt sich nach aktuellem Kenntnisstand jedoch nicht um erfolgreich ausgenutzte Angriffe auf reale ePA, sondern um theoretische Zugriffsszenarien, die stark spezialisierte technische Voraussetzungen in einer Praxis erfordern und damit in der realen Versorgungssituation als äußerst unwahrscheinlich gelten.

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

Der Schutz sensibler Gesundheitsdaten basiert auf einer vielschichtigen Sicherheitsarchitektur der TI, welche die technischen, organisatorischen und kryptografischen Schutzmaßnahmen miteinander verzahnt. Diese Systeme werden kontinuierlich überwacht, in enger Abstimmung mit der gematik, dem BSI, der Bundesbeauftragten für den Datenschutz und die Informationssicherheit (BfDI) und von externen Sicherheitsfachleuten technisch weiterentwickelt und an neue Bedrohungslagen angepasst. Jeder Zugriff auf eine ePA ist nachvollziehbar protokolliert.

Außerdem werden sensible Gesundheitsdaten durch Maßnahmen zur Vermeidung des Missbrauchs von TI-Ausweisen wie SMC-B und eHBA, der Schließung erkannter Schwachstellen sowie dem Ausbau von Monitoring-, Protokollierungs- und Anomalie-Erkennungsverfahren geschützt. Leistungserbringende werden im Umgang mit Komponenten der TI, IT-Sicherheitsaspekten sowie einem ausgeprägten Sicherheitsbewusstsein im Umgang mit Patientendaten kontinuierlich sensibilisiert.

Im Rahmen von Praxisübergaben oder -aufgaben wird zudem sichergestellt, dass Komponenten der TI ordnungsgemäß und sicher außer Betrieb genommen werden. Ergänzend wurden der Freigabe- und Sperrprozess für SMC-B-Karten weiter optimiert, um unbefugte Nutzung der TI zu verhindern und veraltete Karten konsequent zu deaktivieren.

Im Zuge der Weiterentwicklung zur TI 2.0 sind zusätzliche Sicherheitsmechanismen wie Zero-Trust-Architekturen und neue Identifikationsverfahren (z. B. Proof of Patient Presence [PoPP]) vorgesehen, um das bestehende Sicherheitsniveau weiter zu erhöhen und bekannten Risiken strukturell entgegenzuwirken.

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

Digitale sicherheitskritische Infrastrukturen wie die TI werden fortlaufend weiterentwickelt, da absolute Sicherheit in komplexen Systemen technisch nicht erreichbar ist. Daher ist es ein zentrales Ziel, Sicherheitsprobleme frühzeitig zu erkennen und konsequent zu beheben. Hinweise aus Sicherheitsforschung und Praxis werden daher systematisch ausgewertet und in die Weiterentwicklung einbezogen. Sie tragen dazu bei, technische Prozesse, Zertifizierungen, organisatorische Abläufe und Sicherheitsstandards dauerhaft zu optimieren und so das Gesamtsystem resilienter gegen Angriffe zu machen.

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?

Unabhängige Sicherheitsforschung spielt eine wesentliche Rolle bei der Weiterentwicklung sicherheitskritischer digitaler Infrastrukturen wie der ePA. Erkenntnisse aus der Forschung, Fachöffentlichkeit und Praxis werden systematisch geprüft und in die Bewertung des Sicherheitsniveaus einbezogen. Bei Bedarf fließen sie in technische Verbesserungen, Anpassungen der Prozesse oder organisatorische Maßnahmen ein. Dieser kontinuierliche Austausch ermöglicht es, Schwachstellen frühzeitig aufzudecken und das System nachhaltig zu stärken.

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?

Bekannte Schwachstellen aus bestehenden Systemen lassen sich nicht automatisch auf andere Digitalisierungsprojekte übertragen. Die Bewertung möglicher Risiken erfolgt stets im spezifischen technischen und rechtlichen Kontext der jeweiligen Anwendung.

Die europäische digitale Identitäts-Wallet (EUDI-Wallet) stellt ein eigenständiges, noch im Aufbau befindliches EU-Projekt dar, dessen konkrete Ausgestaltung national weiterentwickelt wird. Erfahrungen aus der ePA und anderen Infrastrukturen werden dabei grundsätzlich berücksichtigt, sodass erkannte Probleme nicht unreflektiert in neue Systeme übernommen werden.

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

Transparenz ist ein entscheidender Faktor, um das Vertrauen der Bevölkerung in digitale Gesundheitsanwendungen zu stärken. Versicherte werden durch ihre Krankenkassen umfassend über Funktion, Zugriffsrechte, Steuerungs- und Widerspruchsmöglichkeiten der ePA informiert. Der gesetzliche Rahmen stellt sicher, dass sensible Gesundheitsdaten besonders geschützt sind und dass die Versicherten weitreichende Rechte zur Kontrolle ihrer Daten behalten. Damit besteht ein klar strukturierter Informationsrahmen, der es Bürgerinnen und Bürgern ermöglicht, informierte Entscheidungen über ihre Daten zu treffen.

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

Das Vertrauen der Bevölkerung in die digitale Gesundheitsinfrastruktur stützt sich auf mehrere tragende Säulen: Verlässliche gesetzliche Rahmenbedingungen, hohe technische Sicherheitsstan-

dards, eine fortlaufende Weiterentwicklung der Systeme und eine transparente, sachliche Kommunikation mit den Nutzenden. Durch kontinuierliche Begleitung, Evaluation und Verbesserung digitaler Gesundheitsanwendungen wird dieses Vertrauen dauerhaft gestärkt. Die konsequente Weiterentwicklung der Sicherheitsarchitektur sowie die transparente Kommunikation über Chancen und Risiken tragen dazu bei, auch bei auftretenden Sicherheitsfragen das Vertrauen langfristig zu erhalten.