Kleine Anfrage zur kurzfristigen schriftlichen Beantwortung
gemäß § 46 Abs. 2 GO LT
mit Antwort der Landesregierung

Anfrage des Abgeordneten Eike Holsten (CDU)

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

Cyberangriff auf unimed® Abrechnungsservice für Kliniken und Chefärzte GmbH: Welches Ausmaß hat der Vorfall für niedersächsische Krankenhäuser sowie für Patientinnen und Patienten?

Anfrage des Abgeordneten Eike Holsten (CDU), eingegangen am 15.07.2026 - Drs. 19/11189,
an die Staatskanzlei übersandt am 16.07.2026

Antwort des Niedersächsischen Ministeriums für Soziales, Arbeit, Gesundheit und Gleichstellung namens der Landesregierung vom 29.07.2026

Vorbemerkung des Abgeordneten

Medienberichten zufolge kam es Mitte April 2026 zu einem Cyberangriff auf den Krankenhaus-Abrechnungsdienstleister unimed® Abrechnungsservice für Kliniken und Chefärzte GmbH. Infolge des Vorfalls sollen personenbezogene Daten von Patientinnen und Patienten mehrerer Krankenhäuser abgeflossen sein. Nach bisherigen öffentlichen Angaben sind hiervon u. a. die Medizinische Hochschule Hannover, die Universitätsmedizin Göttingen sowie das Klinikum Oldenburg betroffen.[1]

Vorbemerkung der Landesregierung

Nach den öffentlich zugänglichen Informationen und Mitteilungen betroffener Einrichtungen betraf der Vorfall die IT-Infrastruktur des externen Dienstleisters und nicht die klinischen Systeme der betroffenen Krankenhäuser. Die Patientenversorgung war nach den vorliegenden Informationen nicht beeinträchtigt. Angaben zu Umfang und Art der betroffenen Daten beruhen auf Mitteilungen des Dienstleisters beziehungsweise der jeweils betroffenen Einrichtung.

1. Wie viele Datensätze wurden nach Kenntnis der Landesregierung abgegriffen?

Eine zentrale, landesseitige Statistik über die Zahl der bei dem Cyberangriff auf den externen Abrechnungsdienstleister unimed® Abrechnungsservice für Kliniken und Chefärzte GmbH abgeflossenen Datensätze wird nicht geführt. Der Landesregierung liegen daher keine eigenen, abschließend geprüften Zahlen zum Gesamtumfang des Datenabflusses vor.

[1] https://www.haz.de/der-norden/schon-wieder-hacker-stehlen-tausende-patientendaten-diese-krankenhaeuser-sind-betroffen-ZSGRMLOP4VGDJH36777TCHCAFI.html?utm_medium=social&utm_source=app_ios&utm_campaign=share_button

2. Welche Arten personenbezogener Daten der betroffenen Patientinnen und Patienten wurden nach bisherigem Kenntnisstand entwendet, und in wie vielen Fällen handelt es sich gegebenenfalls dabei um besondere Kategorien personenbezogener Daten im Sinne von Artikel 9 Datenschutz-Grundverordnung?

Nach den öffentlich zugänglichen Informationen betraf der Vorfall insbesondere abrechnungsbezogene personenbezogene Daten von Privatpatientinnen und Privatpatienten, Selbstzahlerinnen und Selbstzahlern sowie gesetzlich Versicherten mit privater Zusatzversicherung. Öffentlich genannt wurden insbesondere Stammdaten wie Name, Anschrift und Geburtsdatum sowie abrechnungsbezogene Informationen. In einzelnen Fällen können auch Gesundheitsdaten beziehungsweise Daten, aus denen Rückschlüsse auf Diagnosen oder Behandlungsarten möglich sind, betroffen sein. Gesundheitsdaten sind besondere Kategorien personenbezogener Daten im Sinne von Artikel 9 Datenschutz-Grundverordnung (DSGVO).

3. Welche Anforderungen an die IT-Sicherheit und den Datenschutz gelten nach Kenntnis der Landesregierung für externe Dienstleister, die im Auftrag niedersächsischer Krankenhäuser Patientendaten verarbeiten, und inwieweit wurden diese im vorliegenden Fall nach bisherigem Kenntnisstand erfüllt?

Die Prüfung der Einhaltung datenschutzrechtlicher Vorgaben und der Anforderungen an die IT-Sicherheit externer Dienstleister ist nicht Aufgabe der Krankenhausaufsicht nach dem Niedersächsischen Krankenhausgesetz. Die Krankenhausaufsicht überwacht nach § 30 des Niedersächsischen Krankenhausgesetz (NKHG), ob Krankenhäuser und ihre Träger ihre Tätigkeit im Einklang mit den Vorschriften des NKHG sowie den aufgrund dieses Gesetzes erlassenen Vorschriften ausüben. Ein allgemeiner Prüfauftrag der Krankenhausaufsicht für Datenschutzverstöße oder IT-Sicherheitsvorfälle bei externen Dienstleistern ergibt sich daraus nicht.

Externe Dienstleister, die im Auftrag von Krankenhäusern personenbezogene Daten verarbeiten, unterliegen den allgemeinen datenschutzrechtlichen Anforderungen der DSGVO, insbesondere den Vorgaben zur Auftragsverarbeitung nach Artikel 28 DSGVO sowie zur Sicherheit der Verarbeitung nach Artikel 32 DSGVO. Danach darf ein Verantwortlicher nur solche Auftragsverarbeiter einsetzen, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen umgesetzt werden und der Schutz der Rechte der betroffenen Personen gewährleistet ist. Die konkrete Auswahl, vertragliche Absicherung, Überprüfung und laufende Steuerung solcher Dienstleister obliegen grundsätzlich der jeweils verantwortlichen Einrichtung.

Soweit Krankenhäuser zusätzlich in den Anwendungsbereich der Regelungen zur IT-Sicherheit für Kritische Infrastrukturen fallen, gelten ergänzende bundesrechtliche Anforderungen, insbesondere zu technisch-organisatorischen Maßnahmen, Meldepflichten und Nachweisen gegenüber dem Bundesamt für Sicherheit in der Informationstechnik. Für den Krankenhausbereich besteht hierfür u. a. der branchenspezifische Sicherheitsstandard „Medizinische Versorgung“.

Der Landesregierung liegen keine eigenen, abschließend geprüften Erkenntnisse dazu vor, ob und in welchem Umfang die im konkreten Vertragsverhältnis zwischen den jeweils betroffenen Krankenhäusern und dem Dienstleister vereinbarten oder gesetzlich bestehenden Anforderungen im vorliegenden Fall eingehalten wurden. Die Prüfung datenschutzrechtlicher Verantwortlichkeiten und etwaiger Verstöße obliegt den zuständigen Datenschutzaufsichtsbehörden. Eine zusätzliche zentrale und anlassunabhängige Erhebung einzelvertraglicher Datenschutz- und IT-Sicherheitsmaßnahmen externer Krankenhausdienstleister durch die Landesregierung erfolgt im Rahmen der Krankenhausaufsicht nicht. Sie würde erhebliche zusätzliche Berichts-, Dokumentations- und Nachweispflichten für die Krankenhäuser begründen, ohne die gesetzlich bestehende Verantwortlichkeit der jeweiligen Einrichtungen und Dienstleister sowie die Zuständigkeiten der Datenschutzaufsicht und der IT-Sicherheitsbehörden zu ersetzen.