Anlage zur Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. November 2014

Anforderungen an den Schutz der Datenübermittlungen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern

Katalog von Anforderungen:

Im Zuge der Umsetzung des Krebsregister- und -früherkennungsgesetzes in den Ländern werden neue Übermittlungswege zwischen verschiedenen medizinischen Leistungserbringern und den klinischen Krebsregistern (KKR) erforderlich. Auf diesen Wegen werden Daten unterschiedlichen Schutzbedarfs transportiert. Der überwiegende Teil von ihnen kann jedoch als hoch sensibel eingeschätzt werden.

Mit dem folgenden Anforderungskatalog sollen Maßnahmen skizziert werden, die einzusetzen sind, um Vertraulichkeit, Authentizität und Integrität der Daten, aber auch die Integrität der eingesetzten Systeme zu gewährleisten. Insgesamt muss ein Schutzniveau erreicht werden, dass dem der Gesundheits-Telematikinfrastruktur gemäß §§ 291a, 291b SGB V entspricht.

Folgende Szenarien können nach den Risiken, die ihnen innewohnen, differenziert werden:

Szenario 1: Die **Meldung** von Daten, die von den klinischen Krebsregistern gemäß § 65 c Abs. 1 Satz 1 Nr. 1 SGB V zu erfassen sind.

Szenario 2: Die **patientenbezogene Rückmeldung** von Auswertungsergebnissen im Sinne von Nr. 3.01 des GKV-Förderkatalog in Hinblick auf die Aufgabe der KKR gemäß § 65c Abs. 1 Satz 1 Nr. 2 SGB V.

Szenario 3: Die **aggregierten Rückmeldungen** an die Leistungserbringer, soweit die übertragenen Daten einen Bezug zu einzelnen behandelnden Personen aufweisen.

Szenario 4: Die **Bereitstellung** von patientenbezogenen Dokumentationsdaten für Zwecke der einrichtungsübergreifenden Behandlung, insbesondere für Tumorkonferenzen im Hinblick auf die Aufgabe der KKR gemäß § 65c Abs. 1 Satz 1 Nr. 4 SGB V.

Im Weiteren wird bei jeder Anforderung auf die Szenarien, auf die sie anwendbar sind, mit ihrer Nummer hingewiesen. Wo erforderlich wird eine zusätzliche Unterscheidung zwischen nachrichtenbasierten Übermittlungsverfahren und webbasierten Dialogverfahren getroffen, worauf durch Zusatz der Buchstaben N bzw. W hingewiesen wird.

Nachrichtenbasierte versus dialogbasierte Übermittlung

1. Vorzugswürdige Form der Übermittlung ist die Lieferung verschlüsselter strukturierter Dateien, wie sie derzeit bei der Meldung der Klinikregister an eine Reihe von epidemiologischen Registern praktiziert wird. Die verschlüsselten Dateien können dabei auch per Web-Upload bzw. -Download übertragen werden.
   Leistungserbringer benötigen für diese Übermittlungsvariante ein Krankenhaus-Informationssystem (KIS) bzw. Praxisverwaltungssystem (PVS), das einen Datenexport in dem vom KKR vorgegebenen Format ermöglicht, oder eine Software zur dezentralen Datenerfassung, die von dem KKR bereitgestellt werden könnte. Die Verschlüsselung bzw. Entschlüsselung und die Signatur der Daten bzw. die Signaturprüfung kann durch separate Software realisiert werden, die kostenfrei erhältlich ist. Investitionen für eine Anpassung von Netzen und Systemen der Leistungserbringer werden in dieser Variante voraussichtlich nur in geringem Maße erforderlich.
   Die Anforderungen an die Transportsicherheit und die Sicherheit der Systeme und Netze, die ausschließlich mit verschlüsselten Daten in Berührung kommen, liegen auf normalem, nicht erhöhtem Niveau. (Szenarien 1N-4N)
2. Eine Übermittlung von Daten zwischen meldenden Leistungserbringern und klinischen Krebsregistern in einem webbasierten Dialogverfahren steht erheblich größeren Schwierigkeiten gegenüber. Für Szenario 1 liegen praktische Erfahrungen aus der epidemioloigschen Krebsregistrierung vor, die sich allerdings nur auf eine Erhebung pseudonymisierter Daten beziehen. *Von einer Umsetzung für das mit besonders hohen Risiken verbundene Szenario 4 wird dagegen dringend abgeraten.*
   Leistungserbringer können bei dieser Variante zwar KIS bzw. PVS verwenden, die nicht für Zwecke der Kommunikation mit den KKR angepasst wurden. Jedes für den Zugriff auf die Webanwendung des KKR verwendete System des Leistungserbringers muss jedoch besonders gesichert und in einem Netzabschnitt betrieben werden, der gleichzeitig den Sicherheitsansprüchen für die Verarbeitung von klaren Patientendaten und für eine Anbindung an dedizierte medizinische Netze genügt, vgl. hierzu den Beschluss des Düsseldorfer Kreises vom 04./05. Mai 2011 zu Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze. Soweit nicht bereits ein hierfür geeigneter Netzaufbau vorliegt, sind nennenswerte Aufwendungen bei den Leistungserbringern zu tätigen.
   Ferner sind hohe (Szenarien 1-2) bis sehr hohe (Szenario 4) Anforderungen an die Sicherheit der auf Seiten des KKR beteiligten Systeme zu ergreifen, die bei der Ausgestaltung des Dialogsystems und bei dessen Anbindung an das Backend zu berücksichtigen sind. Eine nachträgliche Anpassung eines bestehenden Systems, dessen Design nicht von vornherein auf die besonderen Sicherheitsanforderungen dieses Einsatzumfeldes ausgerichtet wurde, erscheint wenig erfolgversprechend. (Szenarien 1W, 2W, 4W)
3. Die Anwendung weiterer Übermittlungsverfahren, deren Anwendung bisher noch nicht in Betracht gezogen wurde, ist möglich. Sie bedürfen jedoch einer eigenen Risikoanalyse. Als Beispiel sei eine direkte Übermittlung von Meldedaten aus dem KIS bzw. PVS eines Leistungserbringers an das Register über eine von diesem Register angebotene Webschnittstelle und einen gesicherten Kanal genannt. Auch hier wäre Verschlüsselung und Signatur der Inhaltsdaten geboten. Würde dieses Verfahren auch für den Abruf verwendet, entsprächen die Risiken weitgehend denen des webbasierten

Dialogverfahrens. Darüber hinaus wäre der Gewährleistung der Integrität des abrufenden Systems besondere Aufmerksamkeit zu widmen.

Vertrauensdienste, kryptografische Algorithmen und Verfahren

4. Die verwendeten kryptografischen Algorithmen und Verfahren müssen eine langfristige Sicherheit gewähren und dem Katalog BSI -TR 03116-1 entnommen sein. (Szenarien 1-4)
5. Für die Identifizierung der Teilnehmer des Verfahren, die zu verwendenden Authentisierungsmittel, deren Ausgabe, Anwendung und Rückruf, sowie die Schlüsselspeicherung sind mindestens die Anforderungen des Schutzniveaus hoch+ gemäß Abschnitten 3 und 4 der BSI-TR 03107-1 zu erfüllen. (Szenarien 1-4)
6. *(optional)* Für Übermittlung, Authentisierung und Verschlüsselung sollen Verfahren der Telematikinfrastruktur nach § 291b SGB V verwendet werden, sobald diese verfügbar sind. (Szenarien 1-4)
7. Die Wurzel der zur Zertifizierung von Teilnehmer- und KKR-Schlüsseln verwendeten PKI ist allen Beteiligten integritätsgeschützt zur Verfügung zu stellen. Die Revokation von öffentlichen Schlüsseln bei Kompromittierung der zugeordneten privaten Schlüssel muss unverzüglich in einem im Vorhinein festgelegten Zeitrahmen erfolgen. (Szenarien 1-4)

Maßnahmen zum Vertraulichkeitsschutz während des Transports der Daten

8. Bei jeder Übermittlung ist eine Ende-zu-Ende-Verschlüsslung einzusetzen. (Szenarien 1-4)
9. Bei Übermittlungen an KKR sind Schlüssel einzusetzen, deren Authentizität die sendende Stelle zweifelsfrei feststellen kann. (Szenario 1)
10. Bei Übermittlungen an Leistungserbringer sind zertifizierte personen- oder leistungserbringerspezifische Schlüssel einzusetzen. (Szenarien 2-4)
11. Übermittlungen zu und von den klinischen Krebsregistern sollen über besonders geschützte medizinische Netze abgewickelt werden, bei webbasierten Verfahren ist dies zwingend erforderlich. (Szenarien 1-4)
12. Die erfolgreiche Authentisierung des KKR muss für die meldenden bzw. abrufenden Personen klar erkennbar sein. (Szenarien 1W-4W)
13. Es dürfen ausschließlich behandelnde Ärztinnen und Ärzte sowie Personen, die bei ihnen oder in einem behandelnden Krankenhaus als berufsmäßige Gehilfen tätig sind, personenbezogene Abrufe tätigen. (Szenarien 2+4)
14. Im Zuge eines Datenabrufs müssen sich die abrufenden Personen in analoger Anwendung der Regelungen des § 291a Abs. 3 Satz 1 Nr. 4 SGB V zum Zugriff auf Daten mit einer Zwei-Faktor-Lösung authentifizieren. Der elektronische Heilberufeausweis ist hierfür geeignet. (Szenarien 2W+4W)
15. Die Registrierung der Leistungserbringer muss durch die KKR selbst oder durch Stellen vorgenommen werden, die von den Ländern in analoger Anwendung von § 291a Abs. 5c SGB V bestimmt wurden. (Szenarien 2-4)
16. Das System, das zur Bereitstellung der Daten für die Rückmeldung von Auswertungsergebnissen an die Leistungserbringer verwendet wird, muss sicherstellen, dass Rückmeldungen mit Daten eines Patienten oder einer Patientin nur für solche Leistungserbringer bereitgestellt werden, die bezüglich dieses Patienten bzw. dieser Patientin eine Meldung abgegeben haben, und nur dann, wenn kein Widerspruch der Betroffenen vorliegt. (Szenario 2)

17. Aggregierte Auswertungsergebnisse, die sich auf einzelne behandelnde Personen beziehen, dürfen nur an diese selbst bzw. an die Stellen übermittelt werden, bei denen sie tätig sind. (Szenario 3)
18. Abrufe von Daten müssen auf der Grundlage eines Berechtigungskonzeptes autorisiert werden, mit dem sichergestellt wird, dass nur an der Behandlung der jeweiligen betroffenen Person beteiligte Leistungserbringer Zugang zu den Daten über diese Person erhalten. Das Bestehen des Abrufrechts ist auf die Dauer der Behandlung zu beschränken. Soweit landesrechtlich vorgesehen muss das Berechtigungskonzept vorsehen, dass Willenserklärungen der Betroffenen, die auf die Einschränkung der Offenbarung ihrer Daten gerichtet sind, effektiv berücksichtigt werden können. (Szenario 4)

Maßnahmen zum Vertraulichkeitsschutz gespeicherter Daten und zur Gewährleistung der Integrität der beteiligten IT-Systeme

19. Ambulante Leistungserbringer müssen die "Empfehlungen zu Datenschutz und Datensicherheit in der Arztpraxis" der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung beachten. Hierauf ist bei der Registrierung hinzuweisen. (Szenarien 1-4)
20. Die Verschlüsselung der zu meldenden und die Entschlüsselung der von einem klinischen Krebsregister abgerufenen Daten darf nur auf Geräten erfolgen, die zur allgemeinen Verarbeitung von Patientendaten der Leistungserbringer vorgesehen sind. (Szenarien 1-4)
21. Hierzu gehört, dass von den zu Meldung oder Abruf genutzten Geräte dann kein allgemeiner Zugang zu Diensten des Internets möglich sein darf, wenn unverschlüsselte Patientendaten auf ihnen zur Anzeige gebracht oder gespeichert werden. (Szenarien 1-4)
22. Bei den KKR sind für die Server, welche zur Abwicklung der Übermittlungen eingesetzt werden, Informationssicherheitsmaßnahmen zu treffen, die bei ausschließlicher Verarbeitung verschlüsselter Daten dem normalen, sonst dem besonders hohen Schutzbedarf der zu übermittelnden Daten gerecht werden. Dies schließt die Maßnahmen nach den Grundschutzbausteinen des Bundesamtes für Sicherheit in der Informationstechnik, insbesondere nach Baustein B 5.21 der Grundschutzkataloge, und die in der ISi-Reihe empfohlenen Maßnahmen ein. (Szenarien 1-4)
23. Bei Dialogverfahren sind die dort aufgeführten Maßnahmen jedoch nicht notwendig ausreichend. Es wird eine besonders eingehende Risikoanalyse erforderlich, die sich auf alle beteiligten Systeme erstrecken und alle bekannten Angriffsvektoren, die gegenwärtig hohe Angriffsintensität auf Webanwendungen sowie darüber hinaus aufgrund einschlägiger Erfahrung der Vergangenheit die Kompromittierung einzelner Sicherheitsvorkehrungen berücksichtigen muss (*defense in depth).* (Szenarien 1W-4W)
24. Die Sicherung hat alle OSI-Netzebenen einschließlich der Anwendungsebene zu berücksichtigen. Nur im Vorhinein autorisierten Systemen ist der Aufbau einer Verbindung zu ermöglichen. Diese Beschränkung muss kryptografisch durchgesetzt werden; eine Beschränkung auf Basis von IP-Adressen reicht nicht aus. Die Absicherung mittels TLS allein bietet aufgrund der Häufigkeit und Schwere der in der vergangenen Zeit aufgetretenen Schwachstellen keine ausreichenden Garantien für die Sicherheit des Zugriffs. (Szenarien 1W-4W)
25. Die Integrität der Komponenten für die Bereitstellung eines Webdienstes (Webserver, Anwendungsserver, Datenbank) bedürfen besonderen Integritätsschutzes. Eine direkte

Anbindung an das Datenhaltungssystem des Registers in der inneren Sicherheitszone ist nicht zulässig. Die Datenhaltung des Backends der Webanwendung ist nur verschlüsselt zulässig. (Szenarien 1W-4W)

26. Kryptografische Schlüssel, deren Kenntnis für den Zugriff auf den Datenbestand erforderlich ist, sind in dedizierten Systemen hardwareseitig zu kapseln und ihre Nutzung durch ein Intrusion Prevention System zu überwachen. Ungewöhnliche Nutzungsmuster müssen zu einer Unterbrechung der Nutzungsmöglichkeiten und einer Untersuchung des Sicherheitsstatus des Verfahrens führen. Kryptografische Schlüssel, die in der inneren Sicherheitszone des Registers verwendet werden, dürfen innerhalb der Webanwendung nicht genutzt werden. (Szenario 4W)

Maßnahmen zur Gewährleistung der Authentizität der Daten

27. Da die übermittelten Daten einer folgenden Behandlung zugrundegelegt werden können, ist es erforderlich, die Integrität der Daten während ihrer Übermittlung zu schützen und sicherzustellen, dass die Daten stets ihrem Ursprung zuzuordnen sind. (Szenarien 1+4)
28. Nachrichten der Leistungserbringer mit Krebsregisterdaten sind entweder mit einer personenbezogenen mindestens fortgeschrittenen elektronischen Signatur oder leistungserbringerbezogen mit einem mindestens fortgeschrittenen elektronischen Siegel i. S. v. Artikel 3 Nr. 26 der EU-Verordnung 910/14 zu authentisieren. (Szenarien 1+4)

Maßnahmen zur Transparenz und Datenschutzkontrolle

29. Abrufe sind leistungserbringer- und personenbezogen zu protokollieren. Die Protokolle sind mindestens ein Jahr zu speichern. Sie müssen gegen Veränderung geschützt werden. (Szenarien 2-4)
30. Für die Protokolle ist ein Verfahren zur anlassbezogenen Auswertung vorzuhalten. (Szenarien 2-4)
31. Der Inhalt der Protokolldaten ist bezogen auf Abrufe von Daten einer Patientin oder eines Patienten auf deren Antrag zu beauskunften. (Szenario 4)

Um einen datenschutzgerechten Betrieb der Verfahren der klinischen Krebsregister für die Kommunikation mit den Leistungserbringern zu gewährleisten, wird den verantwortlichen Stellen der Länder empfohlen, die vorgenannten Anforderungen bereits bei der Ausschreibung von Leistungen zur Bereitstellung der von den KKR benötigten Informationstechnik zu berücksichtigen.