Spitzenverband

Richtlinie des GKV-Spitzenverbands zum Schutz von Sozialdaten der Versicherten vor unbefugter Kenntnisnahme bei Kontakt der Krankenkassen mit ihren Versicherten nach § 217f Absatz 4b SGB V (GKV-SV Richtlinie „Kontakt mit Versicherten“) Stand 12.06.2023

Der GKV-Spitzenverband hat in Abstimmung mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und dem Bundesamt für Sicherheit in der Informationstechnik

aufgrund des § 217f Absatz 4b SGB V

am 12.06.2023 in der nachstehenden Richtlinie Maßnahmen zum Schutz von Sozialdaten der Versicherten vor unbefugter Kenntnisnahme bei Kontakt der Krankenkassen mit ihren Versicherten festgelegt, die von den Krankenkassen bei Kontakten mit ihren Versicherten anzuwenden sind.

Das Bundesministerium für Gesundheit hat die Richtlinie mit Schreiben vom 04.09.2023 genehmigt.

Präambel

Die GKV-SV Richtlinie „Kontakt mit Versicherten“ definiert Anforderungen an die von Krankenkassen zu treffenden Maßnahmen zum Schutz von Sozialdaten der Versicherten vor unbefugter Kenntnisnahme bei Kontakt der Krankenkassen mit ihren Versicherten. Sie adressiert nur die Anforderungen, die von Seiten der Krankenkassen bei einem Kontakt mit ihren Versicherten zu berücksichtigen sind, soweit die jeweiligen Kommunikationswege verwendet werden.

1. Geltungsbereich

1.1. Mit der Richtlinie werden Mindestanforderungen ausschließlich an zu treffende Maßnahmen der Krankenkassen zum Schutz von Sozialdaten der Versicherten vor unbefugter Kenntnisnahme bei Kontakt mit ihren Versicherten festgelegt.

1.2. Vom Regelungsbereich der Richtlinie nicht umfasst sind jene Inhalte und Services, die frei verfügbar und ohne die Notwendigkeit eines Autorisierungsverfahrens zugänglich sind.

1.3. Die Vorgaben dieser Richtlinie sind für alle Krankenkassen der gesetzlichen Krankenversicherung verbindlich.

1.4. Der im Anhang zu der Richtlinie bereitgestellte Leitfaden enthält Konzepte, die bei der Umsetzung der Anforderungen der Richtlinie herangezogen werden können. Im Leitfaden wird zudem die Möglichkeit zur Zertifizierung als Nachweis der Umsetzung der Maßnahmen aufgeführt.

2. Begriffsbestimmungen und Definitionen

2.1. Unter „Kontakt der Krankenkassen mit ihren Versicherten“ ist ein Informationsaustausch zwischen Krankenkasse und Berechtigten zu verstehen, bei denen Vertreter der Krankenkassen mit Berechtigten kommunizieren. Dies umfasst den persönlichen, telefonischen, postalischen oder elektronischen Kontakt.

2.2. Vertreter der Krankenkasse im Sinne dieser Richtlinie sind Personen, die bei der Krankenkasse beschäftigt sind oder ausdrücklich von der Krankenkasse beauftragt wurden mit den Berechtigten zu kommunizieren.

2.3. Berechtigte im Sinne dieser Richtlinie sind Versicherte oder durch sie bzw. wirksam für sie bestimmte Vertreter.

2.4. Unter elektronischem Kontakt wird die Kommunikation unter Verwendung von technischen Einrichtungen und Systemen verstanden. Hierzu zählen unter anderem die Kommunikation unter Nutzung von Kontaktformularen, Chats oder E-Mail mit den Krankenkassen.

2.5. Eine Übermittlung im Sinne dieser Richtlinie kann sowohl mittels elektronischer Übertragungstechniken als auch nicht elektronisch erfolgen. Soweit explizit eine nicht elektronische Übermittlung genutzt wird, wird diese als Bereitstellung bezeichnet. Elektronische Übermittlungen werden als Übertragung bezeichnet.

2.6. Im Sinne dieser Richtlinie gilt ein Übermittlungsweg als sicher, wenn die Anforderungen nach Punkt 7 dieser Richtlinie erfüllt sind.

2.7. Unter Identifizierung versteht man einen Vorgang, der dem eindeutigen Feststellen der Identität einer Person dient.

2.8. Mit der Authentifizierung wird die Echtheit der angegebenen Identität einer Person bestätigt.

2.9. Mit der Autorisierung werden Berechtigungen (Einräumen von Rechten) einer Identität zugeordnet.

2.10. Ein Portal im Sinne dieser Richtlinie ist ein über einen Webbrowser abrufbarer Service, auf dessen jeweilige Funktionalitäten nach einer Autorisierung mittels Authentifizierungsverfahren zugegriffen werden kann. Anwendungen im Sinne dieser Richtlinie sind über Betriebssystemsoftware hinausgehende Softwareteile, die auf einem Endgerät ausgeführt werden.

2.11. Als Anforderungen im Sinne dieser Richtlinie werden Vorgaben bezeichnet, die durch festzulegende Maßnahmen erfüllt werden müssen.

2.12. In dieser Richtlinie erfolgt die Unterscheidung der Schutzanforderungsniveaus auf Basis der Vertrauensniveaus der eIDAS-Verordnung analog der Technischen Richtlinie TR-03107-1 zwischen den Kategorien „normal“, „substantiell“ und „hoch“. Hierbei ist die Kategorie „normal“ im Sinne der TR-03107-1 dem Vertrauensniveau „niedrig“ im Sinne der eIDAS-Verordnung zuzuordnen.

3. Ermittlung der Schutzanforderungen und erforderlicher Gegenmaßnahmen

3.1. Für alle beim Kontakt mit Berechtigten betroffenen persönlichen Daten, sind die erforderlichen Schutzanforderungen entsprechend dem Stand der Technik individuell von der jeweiligen Krankenkasse festzulegen. Zudem sind die gesetzlichen Regelungen zur Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO zu beachten. Bei den Festlegungen sind dabei insbesondere die aus einem Verlust der Vertraulichkeit resultierenden Risiken für die informationelle Selbstbestimmung des Berechtigten zu berücksichtigen.

3.2. Die Festlegungen der Schutzanforderungen für die Daten sind auf Grundlage einer gesamtheitlichen Würdigung aller Prozesse zu treffen, in denen die Daten verwendet werden.

3.3. Sofern für dieselben Daten in unterschiedlichen Zusammenhängen unterschiedliche Schutzanforderungen ermittelt werden, ist mindestens das höchste ermittelte Schutzanforderungsniveau anzusetzen.

3.4. Bei besonderen Kategorien von personenbezogenen Daten im Sinne der Datenschutz-Grundverordnung, die insbesondere Gesundheitsdaten umfassen, ist grundsätzlich vom Schutzanforderungsniveau „hoch“ auszugehen.

3.5. In einem Sicherheitskonzept, das aus mehreren Dokumenten für verschiedene Geltungsbereiche bestehen kann, sind von der Krankenkasse Maßnahmen zu beschreiben, die den Anforderungen des ermittelten Schutzanforderungsniveaus der verwendeten Daten genügen. Hierzu hat die Einbindung des betrieblichen Datenschutzbeauftragten und des Informationssicherheitsbeauftragten, soweit vorhanden, zu erfolgen.

3.6. Das Sicherheitskonzept umfasst die Ermittlung der Schutzanforderungen, die erforderlichen Maßnahmen sowie eine Begründung der Festlegungen, für die beim Kontakt mit den Berechtigten betroffenen Daten und ist nachweisbar zu dokumentieren.

4. Festlegungen von Authentifizierungsverfahren

Die Festlegungen für die jeweils zu verwendenden Authentifizierungsverfahren sind an den Daten mit den höchsten Schutzanforderungen auszurichten, auf die nach der entsprechenden Authentifizierung zugegriffen werden kann.

5. Anforderungen an Verfahren zur Authentifizierung bei persönlichem, postalischem, telefonischem oder elektronischem Kontakt (außerhalb von Portalen und Anwendungen) mit Vertretern der Krankenkassen

5.1. In Abhängigkeit von den festgelegten Schutzanforderungen der betroffenen Daten, sind im Sicherheitskonzept für den persönlichen, postalischen, telefonischen oder elektronischen Kontakt mit Vertretern der Krankenkassen technische und organisatorische Maßnahmen festzulegen, mit denen das für die im jeweiligen Prozess betroffenen Daten erforderliche Schutzniveau sichergestellt wird.

5.2. Bei der Abfrage von Dritten leicht zugänglichen Versichertendaten (bspw. Name, Adresse, Geburtsdatum, Krankenversichertennummer) kann grundsätzlich nur ein normales Schutzniveau erreicht werden.

5.3. Ein substantielles bzw. hohes Schutzniveau kann nur durch eine zweifelsfreie Authentifizierung des Berechtigten erreicht werden.

5.4. Die betroffenen Vertreter der Krankenkasse sind verbindlich zur Einhaltung der nach den Vorgaben in dieser Richtlinie von den Krankenkassen festgelegten Verfahrensweisen zu verpflichten. Hierfür sind die Verfahrensweisen in die entsprechenden Dienstanweisungen oder anderen verbindlichen Regelungen einzubinden.

5.5. Bei direktem Kontakt des Berechtigten zu Vertretern der Krankenkassen über elektronische Kommunikationswege (bspw. E-Mail), muss eine Beachtung der nach den Vorgaben in dieser Richtlinie von den Krankenkassen festgelegten Verfahrensweisen durch organisatorische Maßnahmen sichergestellt werden.

6. Anforderungen an Verfahren zur Authentifizierung bei Kontakten über Portale oder Anwendungen

6.1. Bei Kontakten über Portale oder Anwendungen sind technische Verfahren zur Authentifizierung und Übertragung von Daten vorzusehen, mit denen ein Schutzniveau sichergestellt wird, das mindestens den für die jeweils betroffenen Daten festgelegten Schutzanforderungen entspricht. Die Bewertung des Schutzniveaus von Verfahren soll sich an der TR-03107-1 des BSI bzw. vergleichbaren internationalen Standards (z.B. ISO/IEC-Reihe) orientieren.

6.2. Die verwendeten Verfahren sollen Sicherheitsmaßnahmen nach dem Stand der Technik berücksichtigen. Die in der TR-03107-1 des BSI bzw. vergleichbaren internationalen Standards (z.B. ISO/IEC-Reihe) definierten Maßnahmen sollen berücksichtigt werden.

6.3. Vor der Übertragung der Authentifizierungsdaten ist eine entsprechend dem Stand der Technik gesicherte Verbindung aufzubauen.

6.3.1. Den Stand der Technik stellen bei Einsatz des Protokolls von Transport Layer Security (TLS) die Vorgaben der technischen Richtlinie TR-02102-2 des Bundesamts für Sicherheit in der Informationstechnik dar.

6.4. Durch unterschiedliche Authentifizierungsverfahren erreichbare Schutzniveaus:

6.4.1. Mit einem Authentifizierungsverfahren, das nur auf einem Faktor basiert und nicht transaktionsgebunden bzw. sitzungsgebunden ist, kann nur ein normales Schutzniveau erreicht werden.

6.4.2. Für ein Schutzniveau, substantiell oder hoch, ist grundsätzlich die Verwendung von Authentifizierungsverfahren erforderlich, die auf mindestens zwei Faktoren basieren.

6.5. Sofern ein dauerhafter Zugang für ein Portal oder eine Anwendung vorgesehen wird, ist eine Identifizierung des Berechtigten vor der Nutzung des Zugangs erforderlich, die das Schutzanforderungsniveau der Daten gewährleistet, auf die mit dem Zugang zugegriffen werden soll. Die in der TR-03147 des BSI definierten Anforderungen sind dabei zu berücksichtigen.

6.6. Sofern eine postalische Übermittlung von Authentifizierungsinformationen und/oder -mitteln erfolgt, muss die Zustellung inhaltlich und zeitlich getrennt voneinander und von anderen Informationen an den Berechtigten erfolgen.

7. Übermittlung von Daten

7.1. Der Zugriff auf schutzbedürftige Daten darf nur nach vorheriger Authentifizierung entsprechend dem Schutzanforderungsniveau der Daten erfolgen.

7.2. Für die Übermittlung von Daten mit der Schutzanforderung „substantiell“ oder „hoch“ ist ein sicherer Übermittlungsweg zu verwenden.

7.2.1. Eine postalische Bereitstellung gilt als sicher, sofern die Zustellung an eine Anschrift erfolgt, die zweifelsfrei dem Berechtigten persönlich zugeordnet und bei der von einer persönlichen Zustellung auszugehen ist. Im Fall einer Änderung der Anschrift durch den Berechtigten gilt dies nur, wenn eine Änderung der Anschrift unter Wahrung eines hohen Schutzniveaus erfolgt ist.

7.2.2. Bei der direkten Kommunikation mit dem Versicherten gilt eine elektronische Übermittlung als sicher, wenn die Übertragung entsprechend dem Stand der Technik verschlüsselt und an einen Empfänger erfolgt, der entsprechend dem Schutzanforderungsniveau der übermittelten Daten authentifiziert wurde.

8. Postalische Bereitstellung der elektronischen Gesundheitskarte oder deren PIN/PUK

Ergänzend zu den gesetzlichen Vorgaben des § 336 Absatz 5 SGB V werden gemäß § 217f Absatz 4b Satz 3 SGB V folgende Regelungen getroffen:

8.1. Die postalische Bereitstellung sowohl der elektronischen Gesundheitskarte als auch deren PIN/PUK darf nur an eine Anschrift erfolgen, für die vor dem Versand durch einen Abgleich mit dem Melderegister überprüft wurde, dass die Anschrift dem Berechtigten zugeordnet ist.

8.2. Ein Abgleich mit dem Melderegister vor der postalischen Bereitstellung ist nicht erforderlich, wenn:

8.2.1. eine persönliche Zustellung entsprechend den Vorgaben gemäß § 336 Absatz 5 Satz 1 Nummer 1 oder 4 SGB V erfolgt oder

8.2.2. eine Bereitstellung an eine Anschrift erfolgt, für die in einem Zeitraum von höchstens 12 Monaten vor der jeweiligen Bereitstellung eine erfolgreiche Zustellung mit einem Verfahren nach § 336 Absatz 5 Satz 1 Nummer 1 oder 4 SGB V erfolgt ist, oder

8.2.3. für die Anschrift, an die die Bereitstellung erfolgen soll, im Zeitraum von höchstens 12 Monaten vor der jeweiligen Bereitstellung bereits ein Abgleich mit dem Melderegister durchgeführt wurde, oder

8.2.4. in einem Zeitraum von höchstens 12 Monaten vor der konkreten Bereitstellung die Mitteilung der Anschrift bzw. des Empfängers und seiner Anschrift mit einem Verfahren erfolgt ist, bei dem die Identifizierung des Berechtigten sowie die Zurechnung der Mitteilung zum Berechtigten überprüfbar unter Gewährleistung eines hohen Schutzniveaus erfolgt, oder

8.2.5. die Bereitstellung an die Institution, den Dienstsitz oder die Arbeitsstätte eines Vertreters erfolgen soll, die oder der in einer der Krankenkasse vorliegenden Vorsorgevollmacht, Betreuungsurkunde oder vergleichbaren Urkunde benannt ist

und die Krankenkasse keine konkreten Anhaltspunkte dafür hat, dass die Anschrift unrichtig ist.

9. Inkrafttreten und Bekanntgabe

9.1. Die Richtlinie wurde den Krankenkassen in der vorliegenden Fassung mit Rundschreiben vom 14.09.2023 bekanntgegeben.

9.2. Die Richtlinie tritt mit dem Tag der Bekanntgabe in Kraft.

9.3. Die Anforderungen der Nummer 8 dieser Richtlinie sind zum 01.10.2023 umzusetzen.