Spitzenverband

Anlage A

zur 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

Umsetzungsleitfaden
für
Verfahren zur Authentifizierung von Berechtigten und Übermittlung von Daten bei Kontakt der Krankenkassen mit ihren Versicherten (Stand: 12.06.2023)

A 1. Allgemeines

A 1.1. Dieser Leitfaden zeigt Möglichkeiten zur Umsetzung der Festlegungen in der Richtlinie des GKV-Spitzenverbands zum Schutz von Sozialdaten der Versicherten vor unbefugter Kenntnisnahme bei Kontakt der Krankenkassen mit ihren Versichertennach § 217f Absatz 4b SGB V auf. Die in dieser Anlage enthaltenen Umsetzungsmöglichkeiten sind nicht abschließend und beleuchten ausschließlich herausragende Aspekte einzelner Themen.

A 1.2. Der Umsetzungsleitfaden setzt auf dem zum Zeitpunkt der Erstellung aktuellen Stand der Technik auf. Künftige technische Entwicklungen können dabei die Notwendigkeit einer Anpassung der aufgezeigten Maßnahmen erfordern, die ggf. bereits vor der Bereitstellung einer überarbeiteten Fassung umzusetzen sind.

A 2. Ermittlung der Schutzanforderungen und erforderlicher Maßnahmen

A 2.1. Die Ermittlung der Schutzanforderungen und erforderlicher Maßnahmen soll entsprechend der Vorgehensweise Standard-Absicherung des BSI-Standards 200-2 IT-Grundschutz-Methodik sowie 200-3 Risikoanalyse auf der Basis von IT-Grundschutz – jeweils unter Berücksichtigung des BSI-Standards 200-1 – oder vergleichbaren europäischen oder internationalen Standards (z. B. ISO/IEC 27000-Reihe) erfolgen.

A 2.2. Bei der Festlegung der Schutzanforderungen ist insbesondere zu beachten, dass für die Festlegung bzw. Änderung von Daten, die für die Authentifizierung bzw. Bereitstellung von Authentifizierungsdaten genutzt werden, das Schutzniveau der zu übermittelnden Daten maßgeblich ist.

A 2.3. Bei einer Änderung der Adresse des Berechtigten ist vom Schutzniveau „hoch“ hinsichtlich Integrität auszugehen, da diese auch für eine Bereitstellung von Daten mit Schutzniveau „hoch“ genutzt wird.

A 2.4. Die im Rahmen von Datenaustauschverfahren, welche auf Informationen nach dem Bundesmeldegesetz (BMG) bzw. den entsprechenden Regelungen auf Landesebene basieren, erlangte Adresse gilt als sicher, wenn in dem zugrundeliegenden Verfahren eine Identifizierung des Versicherten unter Wahrung eines hohen Schutzanforderungsniveaus erfolgt ist und die Meldung eindeutig dem Versicherten zugeordnet werden kann. Dies gilt insbesondere für an die Krankenkasse nach § 196 Absatz 2 SGB VI weitergeleitete Daten.

A 3. Festlegungen von Authentifizierungsverfahren

A 3.1. Authentifizierungsverfahren können auch abgestuft ausgestaltet werden. Dabei sind vor einem Zugriff auf Daten, die einer höheren Schutzanforderung zugeordnet sind als mit der grundsätzlich vorgesehenen Authentifizierung gewährleistet wird, zusätzliche Maßnahmen für ein höheres Schutzniveau vorzusehen.

A 3.2. Es kann eine Anforderung zur Übermittlung von Daten vorgesehen werden, für die eine höhere Schutzanforderung festgelegt wurde als durch das verwendete Authentifizierungsverfahren gewährleistet wird, sofern die Bereitstellung der Daten auf gesichertem Übermittlungsweg und nur an einen berechtigten Empfänger erfolgt. Dies kann bspw. die postalische Bereitstellung einer Patientenquittung an eine gesicherte Adresse sein, wenn diese über ein Portal nach Authentifizierung mit einem normalen Schutzniveau angefordert wurde.

A 4. Mögliche Authentifizierungsverfahren bei persönlichem, postalischem, telefonischem oder elektronischem Kontakt (außerhalb von Portalen und Anwendungen) mit Vertretern der Krankenkassen

A 4.1. Bei telefonischem oder persönlichem Kontakt (bspw. via Chat, postalisch oder vor Ort) kann ein substantielles Schutzniveau, bspw. durch ein im Voraus vereinbartes Kundenkennwort, sichergestellt werden. Das Kundenkennwort ist mit einem sicheren Verfahren gemäß Punkt 7 der Richtlinie zu übermitteln.

A 4.2. Für ein hohes Schutzniveau ist die Abfrage bzw. der Abgleich von Daten erforderlich, bei denen davon ausgegangen werden kann, dass sie nur dem Berechtigten bekannt sind.

A 4.3. Bei einem elektronischen Kontakt mit Vertretern der Krankenkassen kann eine zweifelsfreie Authentifizierung gegeben sein, sofern die Anfrage mit einer elektronischen Signatur i.S.d. Artikel 3 Nummer 12 eIDAS-Verordnung versehen ist.

A 4.4. Bei postalischem Kontakt kann eine Authentifizierung des Berechtigten mittels eines vom Berechtigten persönlich unterzeichneten Schreibens erfolgen, indem eine Angabe von Daten erfolgt, die eine eindeutige Zuordnung des Berechtigten sicherstellt (bspw. Krankenversichertennummer, Aktenzeichen).

A 4.5. Beim persönlichen Kontakt vor Ort kann eine zweifelsfreie Authentifizierung auch gegeben sein, sofern der Berechtigte dem jeweiligen Vertreter der Krankenkasse persönlich bekannt ist oder der Berechtigte mit einem Lichtbildausweis authentifiziert wird.

A 5. Mögliche Authentifizierungsverfahren bei Kontakten über Portale oder Anwendungen

A 5.1. Mit einer Authentifizierung mittels Benutzername und Passwort kann nur ein normales Schutzniveau erreicht werden.

A 5.2. Sofern die Verwendung eines Einmalkennwortes an eine bestimmte Transaktion bzw. Sitzung gekoppelt wird, kann ein substantielles Schutzniveau realisiert werden. Gleiches gilt für die Kombination von einem Verfahren mit normalem Schutzniveau und der Verwendung von anderen transaktionsgebundenen Verfahren. Die Bereitstellung bzw. Übertragung von Authentifizierungsmerkmalen soll entsprechend den Vorgaben unter Punkt 7 der Richtlinie erfolgen.

A 5.3. Eine Authentifizierung mit hohem Schutzniveau, die auf zwei unterschiedlichen Faktoren basiert, kann bspw.:

A 5.3.1. mittels eGK (elektronischer Gesundheitskarte), mit dem elektronischen Identitätsnachweis des elektronischen Personalausweises, der eID-Karte für Unionsbürgerinnen und -bürger oder dem elektronischen Aufenthaltstitel (eID-Funktion) erfolgen.

A 5.3.2. unter Verwendung eines registrierten Endgerätes des Berechtigten als Besitz-Faktor in Verbindung mit einem Passwort oder einer PIN als Wissens-Faktor. Bei der Registrierung des Gerätes ist eine sichere Authentifizierung des Berechtigten zu gewährleisten. Dies kann bspw. durch die Verwendung eines postalisch bereitgestellten Registrierungscodes realisiert werden.

A 5.3.3. mit einer Authentifizierung mittels Benutzername/Passwort in Verbindung mit einem transaktionsgebundenen Verfahren gewährleistet werden. Transaktionsgebundene Authentifizierungsmerkmale sind dem Berechtigten mit einem sicheren Verfahren bereitzustellen.

A 5.3.4. unter Verwendung einer digitalen Identität nach § 291 Absatz 8 SGB V erfolgen.

A 6. Anforderungen an Authentifizierungsverfahren bei Kontakten über Portale oder Anwendungen

A 6.1. Die Umsetzung von Authentifizierungsverfahren kann sich am IT-Grundschutz-Kompendium des BSI und den in den Grundschutzkatalogen des BSI bzw. vergleichbaren internationalen Standards (z.B. ISO/IEC-Reihe) festgelegten Maßnahmen für das jeweilige Verfahren orientieren. Die Bewertung des Schutzniveaus von Verfahren soll sich an der TR-03107-1 des BSI orientieren.

A 6.2. Bei der Umsetzung der Authentifizierungsverfahren sollen Maßnahmen berücksichtigt werden, die in der TR-03107-1 des BSI für das definierte Schutzniveau empfohlen werden.

A 6.3. Bei der Verwendung von Passwörtern sollte eine geeignete Passwortrichtlinie, bspw. entsprechend dem Grundschutz Kompendium des BSI-ORP.4.A8 oder eines vergleichbaren europäischen oder internationalen Standards, erstellt und durchgesetzt werden.

A 6.4. Einmalkennwörter und andere transaktionsgebundene Authentifizierungsmerkmale müssen individuell für jede zugriffsberechtigte Person erzeugt, auf gesichertem Weg übertragen oder an eine gesicherte Adresse bereitgestellt werden.

A 6.5. Einmalkennwörter dürfen während ihrer Gültigkeitsdauer nur für einen Berechtigten gültig sein.

A 6.6. Für transaktionsgebundene Einmalkennwörter ist ein Verfallsdatum festzulegen. Zudem sollen sie verfallen, sobald der entsprechende Geschäftsprozess vollständig durchgeführt wurde. Im Falle eines Abbruches des Verwendungsprozesses kann das Kennwort für eine Wiederaufnahme weiterverwendet werden.

A 7. Umsetzung der Identifizierung für dauerhaften Zugang

A 7.1. Die Identifikation für einen dauerhaften Zugang kann mit Verfahren realisiert werden, die ein vollständiges Identifizierungsverfahren (A7.2) oder eine Überprüfung und Zuordnung der für den dauerhaften Zugang behaupteten Identität zu einer bereits im Bestandssystem vorhandenen Versichertenidentität (A7.3) vorsehen.

A 7.2. Die sichere Identifizierung des Berechtigten kann bspw. mit den nachfolgenden Verfahren realisiert werden:

A 7.2.1. mit dem elektronischen Identitätsnachweis des elektronischen Personalausweises, der eID-Karte für Unionsbürgerinnen und -bürger oder dem elektronischen Aufenthaltstitel (eID-Funktion) oder der elektronischen Gesundheitskarte als Zwei-Faktor-Verfahren

A 7.2.2. mit einem Identitätsnachweis auf dem Sicherheitsniveau „hoch“ im Sinne der Durchführungsverordnung (EU) 2015/1502

A 7.2.3. mit Post-Ident-Verfahren durch Postfiliale oder Postbote

A 7.2.4. mit sonstigen Identifizierungsmethoden im Sinne des § 11 Absatz 1 Vertrauensdienstegesetz, die durch Verfügung im Amtsblatt der Bundesnetzagentur anerkannt wurden und das für den dauerhaften Zugang erforderliche Schutzniveau erreichen

A 7.2.5. mit innovativen Identifizierungsmethoden, die noch nicht durch Verfügung im Amtsblatt der Bundesnetzagentur anerkannt sind, aber entsprechend § 11 Absatz 3 Vertrauensdienstegesetz vorläufig anerkannt, auf der Internetseite der Bundesnetzagentur veröffentlicht wurden und das für den dauerhaften Zugang erforderliche Schutzniveau erreichen.

A 7.3. Eine sichere Identifizierung des Berechtigten kann auch mit einem Verfahren realisiert werden, bei dem die Punkte A 7.3.1 und A 7.3.2 umgesetzt werden.

A 7.3.1. Im Zuge der Identifikation für einen dauerhaften Zugang sind Merkmale zur eindeutigen Identifizierung des Versicherten heranzuziehen. Dies können bspw. Name, Vorname, Geburtsdatum sowie ein eindeutiges Identifikationsmerkmal wie die Krankenversichertennummer (KVNR) oder ein Teil der aktuellen Kennnummer der Gesundheitskarte (ICCSN) sein.

A 7.3.2. Im Anschluss ist zur Prüfung der behaupteten Identität dem Berechtigten ein Freischaltcode auf sicherem Weg zu übermitteln. Der Freischaltcode kann bspw. postalisch an eine im Bestandssystem hinterlegte sichere Adresse entsprechend Punkt 7.2.1 der Richtlinie übertragen oder im persönlichen Kontakt nach einer zweifelsfreien Authentifizierung gemäß Punkt A 4.5 dieses Leitfadens bereitgestellt werden. Die Gültigkeit des Codes für die Freischaltung sollte dabei zeitlich beschränkt werden. Der festgelegte Zeitraum der Gültigkeit soll 60 Tage nicht überschreiten.

A 8. Datenübermittlung

A 8.1. Bei der elektronischen Übertragung von Daten im Fall von Zugriffen über Portale oder Anwendungen sollten die Empfehlungen des BSI beachtet werden. Insbesondere sollten die Vorgaben der Technischen Richtlinie TR-03116-4 eingehalten werden.

A 8.2. Eine Übermittlung von Daten mit dem Schutzbedarf „substantiell“ per E-Mail ist nur zulässig, sofern die Versendung verschlüsselt und an eine authentifizierte Adresse des Berechtigten erfolgt (bspw. via De-Mail). Soll ein „hoher“ Schutzbedarf erreicht werden, muss die an die authentifizierte Adresse des Berechtigten versandte Nachricht zudem Ende-zu-Ende-verschlüsselt übermittelt werden. Die Vorgaben der Technischen Richtlinie TR-03108 sollten beachtet werden.

A 9. Nachweis der Umsetzung der Maßnahmen

A 9.1. Die Krankenkasse kann den Nachweis der Umsetzung der in der GKV-SV Richtlinie „Kontakt mit Versicherten“ festgelegten Maßnahmen durch eine Zertifizierung erbringen. Dazu eignen sich die einschlägigen Verfahren zum Nachweis der Einhaltung der Anforderungen an die Informationssicherheit (z. B. Zertifizierung nach ISO/IEC 27001).