Bundesministerium
für Gesundheit

Bundesministerium für Gesundheit, 53107 Bonn

Ministerium für Soziales, Arbeit,
Gesundheit und Demografie
des Landes Rheinland-Pfalz
Herrn Tom Rutert-Klein
Bauhofstraße 9
55116 Mainz

Dr. Stefan Bales
MinR
Referatsleiter

HAUSANSCHRIFT Rochusstraße 1, 53123 Bonn
POSTANSCHRIFT 53107 Bonn
TEL +49 (0)228 99 441-3181
FAX +49 (0)228 99 441-4997
E-MAIL jana.holland@bmg.bund.de
INTERNET www.bundesgesundheitsministerium.de

nachrichtlich:

Bonn, 9. März 2012
AZ Z24-08400

An die
Obersten Landesgesundheitsbehörden

gematik
Gesellschaft für Telematikanwendungen
der Gesundheitskarte mbH
Friedrichstraße 136
10117 Berlin

Bundesversicherungsamt
Friedrich-Ebert-Allee 38
53113 Bonn

Betreff: Einführung der elektronischen Gesundheitskarte;
hier: Identitätsprüfung bei der Lichtbildbeschaffung für die Ausgabe der elektronischen Gesundheitskarte nach §§ 291, 291a SGB V
Bezug: Ihr Schreiben vom 17.02.2012

Sehr geehrter Herr Rutert-Klein,

vielen Dank für Ihr o. g. Schreiben, in dem Sie das Bundesministerium für Gesundheit um Überprüfung seiner Rechtsauffassung zur Erforderlichkeit einer Identitätsfeststellung des Versicherten bei der Lichtbildbeschaffung für die Ausgabe der elektronischen Gesundheitskarte bitten, weil Ihnen von dritter Seite Bedenken gegen die Verfahren der Krankenkassen bei der Lichtbildbeschaffung vorgetragen wurden.

Die Ihnen vorgetragenen Bedenken sind auch dem Bundesministerium für Gesundheit bekannt; sie werden gerne von Firmen wiederholt, die entsprechende Verfahren zur Identitätsfeststellung vermarkten.

Auch wenn ich angesichts der unverändert gültigen Rechtsgrundlagen für die Einführung der Gesundheitskarte, insbesondere der Regelungen zur Aufbringung des Lichtbildes, und der dazu eindeutigen gemeinsamen Positionierung von Bund und Ländern keinen neuen Sachverhalt erkenne, möchte ich im Hinblick auf die Komplexität der organisatorischen und technischen Sicherheitsmaßnahmen, die häufig in ihrer Gesamtbreite nicht bekannt sind, die Gelegenheit gerne nutzen, zur Thematik noch einmal ausführlich Stellung zu nehmen:

Ich sehe nach wie vor keine gesetzliche Verpflichtung für die Krankenkassen, die Identität des Versicherten bei der Lichtbildübermittlung in der vorgetragenen Weise zu überprüfen.

Wie bekannt ist, wurde die Verpflichtung zur Aufbringung eines Lichtbildes bereits für die Krankenversichertenkarte eingeführt. Aus wirtschaftlichen Gründen wurde den Krankenkassen zugebilligt, das Lichtbild erst mit der elektronischen Gesundheitskarte einzuführen. Ziel war und ist es, mit Hilfe des Lichtbildes die missbräuchliche Inanspruchnahme von Leistungen in der gesetzlichen Krankenversicherung zu reduzieren.
Es war demgegenüber nie angedacht, dass das Lichtbild das entscheidende Identifizierungsmerkmal der Gesundheitskarte bei der Nutzung der medizinischen Anwendungen ist. Dies ergibt sich bereits daraus, dass es Versicherte gibt, die nach dem Willen des Gesetzgebers überhaupt kein Lichtbild auf der Gesundheitskarte haben. So sehen die gesetzlichen Regelungen u.a. vor, dass Kinder und Jugendliche bis zur Vollendung des 15. Lebensjahres sowie Personen, deren Mitwirkung an der Erstellung eines Lichtbildes nicht möglich ist, kein Lichtbild benötigen. Gleichwohl können diese Personengruppen medizinische Anwendungen in Anspruch nehmen und sind auch beim Online-Abgleich der Versichertenstammdaten nicht ausgenommen.

Dem steht nicht entgegen, dass das Lichtbild den Arzt bei seiner Verpflichtung nach § 19 i. V. m. der Anlage 4a, Anhang 1.2 des BMV-Ä, die Identität des Versicherten zu prüfen, unterstützt.

Es ist unbestritten, dass die richtige Zuordnung der Daten der Gesundheitskarte zum Karteninhaber gewährleistet sein muss. Dafür ist eine Identifizierung des Versicherten erforderlich, die jedoch nicht zum Zeitpunkt der Lichtbildübermittlung durchzuführen ist. Für den überwiegenden Anteil der gesetzlich Versicherten (die Pflichtversicherten) gelten bei Eintritt in die gesetzliche Krankenversicherung gesetzliche Meldebestimmungen. Dafür sieht § 5 Absatz 6 der Verordnung über die Erfassung und Übermittlung von Daten für die Träger der Sozial-

versicherung (DEÜV) vor, dass alle persönlichen Angaben, die an die Träger der Sozialversicherung gemeldet werden, aus amtlichen Unterlagen zu entnehmen sind. Damit wird eine ausreichende Identifizierung der Pflichtversicherten sichergestellt. Auch eine freiwillige Mitgliedschaft kann nur begründet werden, wenn die gesetzlichen Voraussetzungen vorliegen, die vom Betroffenen nachzuweisen und von der Krankenkasse zu prüfen sind.

Über die Identifizierung des Versicherten bei Eintritt in die gesetzliche Krankenversicherung hinaus erfolgt die richtige Zuordnung der Daten der Gesundheitskarte zum Karteninhaber sowie der Schutz vor unberechtigtem Zugriff auch durch folgende Maßnahmen:

- Prüfung der Identität des Versicherten durch den Arzt, künftig unterstützt durch den Online-Abgleich der Versichertenstammdaten
  Nach § 19 i. V. m. der Anlage 4a, Anhang 1.2 BMV-Ä sind Ärzte verpflichtet, die Identität des Versicherten anhand der auf der Gesundheitskarte aufgebrachten Identitätsdaten und in Zweifelsfällen durch Heranziehung eines Ausweisdokuments zu prüfen. Im Lastenheft VSDM wird auf diese Verpflichtung des Arztes Bezug genommen. Zusammen mit dem Online-Abgleich der Versichertenstammdaten, dessen Testung im nächsten Jahr stattfinden soll, kann so regelmäßig die richtige Zuordnung der Daten der Gesundheitskarte zum Karteninhaber geprüft werden. Der gesetzlich Versicherte hat der Aufforderung des Arztes zur Vorlage seiner Gesundheitskarte bzw. seines Personaldokuments Folge zu leisten, um seinen Leistungsanspruch nachzuweisen.

- Einverständniserklärung des Versicherten bei Speicherung freiwilliger Daten (insbesondere Gesundheitsdaten) mittels der Gesundheitskarte
  Auf den von den Krankenkassen ausgegebenen Gesundheitskarten befinden sich zunächst keine medizinischen Daten des Versicherten. Diese werden erst auf Wunsch des Versicherten auf die Gesundheitskarte gespeichert. Vor einer Speicherung von medizinischen Daten durch die Leistungserbringer ist eine schriftliche Einwilligungserklärung vom Versicherten einzuholen, mit der sichergestellt wird, dass der Versicherte der Speicherung von medizinischen Daten auf der ihm zugeordneten Gesundheitskarte zustimmt. Die Einwilligung wird gemäß § 291a Absatz 3 SGB V durch den Leistungserbringer selbst oder unter seiner Aufsicht auf der Gesundheitskarte dokumentiert. Da die ordnungsgemäße Dokumentation voraussetzt, dass die Einwilligung einer bestimmten Person und einer bestimmten Gesundheitskarte zugeordnet werden kann, ist dies ohne Identifizierung der betreffenden Person nicht möglich.

- Zugriffskontrolle auf Basis persönlicher Schlüssel und PIN
  Für den Zugriff auf die auf der Gesundheitskarte gespeicherten medizinischen Daten – d.h. auch für das erstmalige Anlegen/Schreiben solcher Daten auf die Karte –

authentifiziert sich der Versicherte gegenüber der Karte als berechtigter Karteninhaber durch die Eingabe einer persönlichen, geheimen Zugangsnummer (PIN) und kann damit den Zugriff durch einen Leistungserbringer autorisieren. Eine Ausnahme hiervon bilden die Notfalldaten, die aufgrund ihrer Anwendungsfälle (Notfallversorgung) auch ohne explizite Autorisierung durch die PIN Eingabe des Versicherten gelesen werden können.

Auch die Zustellung der PIN an den Versicherten wird durch geeignete Verfahren abgesichert. Dazu wird entweder die PIN dem Versicherten in gesonderter Post in einem sogenannten PIN-Brief von seiner Kasse zugesandt oder die Karte wird mit einer vorläufigen, nicht für den Datenzugriff nutzbaren PIN, der sogenannten Transport-PIN ausgeliefert, die der Versicherte vor der erstmaligen Nutzung in eine Echt-PIN umwandeln muss (PIN-Initialisierung). Durch organisatorische und technische Maßnahmen ist sichergestellt, dass diese PIN-Initialisierung nur in einer kontrollierten Umgebung unter Aufsicht eines Leistungserbringers erfolgen kann bzw. darf. Der verantwortliche Leistungserbringer hat sich dabei wiederum von der behaupteten Identität des Karteninhabers zu überzeugen (s.o.).
Durch die Eingabe der PIN können außerdem persönliche Schlüssel auf der Gesundheitskarte freigeschaltet werden, mit denen der Versicherten sich gegenüber Diensten der Telematikinfrastruktur authentisieren und den Zugriff auf außerhalb der eGK gespeicherten medizinischen Daten kontrollieren kann. Die Kassen stellen diese Schlüssel auf der Karte bereit. Die Zuordnung des Schlüsselmaterials zur Person des Versicherten und damit die Zuordnung des Zugriffs zur Person erfolgt über Identitätsattribute des Versicherten über das dem Schlüsselmaterial zugeordnete X.509-Zertifikat, das von einem Zertifizierungsdienste-Anbieter signiert wird und regelmäßig auf Gültigkeit überprüft werden kann (OCSP-Anfrage). Hierzu haben die Kassen und die Gematik eine Public-Key-Infrastruktur (PKI) aufgebaut, die technisch und aus Sicht der Datensicherheit der PKI für qualifizierte elektronische Signatur-Zertifikate in Deutschland entspricht – d.h. die PKI der Zertifizierungsdienste-Anbieter bildet letztlich die oberste Vertrauensinstanz, die bei der Überprüfung der Identität (Authentifizierung) des Versicherten durch elektronische Dienste der Telematikinfrastruktur zu Grunde gelegt wird.

Auf diesen Rahmenbedingungen wurde auch das von Ihnen zitierte Sicherheitskonzept der Gematik konzipiert, das derzeit allerdings nur in Teilen für den Basis-Rollout gültig ist. Sofern das Sicherheitskonzept eine Identifizierung des Karteninhabers fordert, so wird diese – wie oben dargestellt – bereits bei Eintritt in die gesetzliche Krankenversicherung erfüllt.

Vor diesem Hintergrund sind für mich keine Anhaltspunkte ersichtlich, die dafür sprechen, dass die von den Krankenkassen praktizierten Verfahren nicht rechtmäßig sind oder dazu führen, dass die Gesundheitskarten nicht für die beabsichtigten Zwecke genutzt werden dürfen.

Mit freundlichen Grüßen
Im Auftrag

Dr. Stefan Bales