Gutachterliche Stellungnahme:

Versichertenstammdatendienst (VSD) in der Arztpraxis und Strafbarkeitsrisiken für Ärzte nach § 203 StGB
(Fassung vom 11.9.14)

Dr. phil.nat. André Zilch
(Managing Partner LSc LifeScience Consult GmbH; Sachverständiger und Fachexperte Identitätsmanagement im Gesundheitswesen CertEuropA)

Rechtsanwältin Dr. iur. Franziska Meyer-Hesselbarth

I. Sachstand

Im Rahmen der Einführung der eGK ist beabsichtigt, den Ärzten eine zentrale Rolle bei der Nutzung der Telematikinfrastruktur (TI) zuzuweisen. Ärzte sollen verpflichtet werden, einerseits z. B. VSD zu nutzen und andererseits die hierbei notwendige Identitätsüberprüfung der Versicherten in den Praxen durchzuführen, um einen unberechtigten Zugriff auf Sozialdaten zu verhindern. Denn nur mittels Identitätsüberprüfung ist ein Zugriff auf Sozialdaten durch Unberechtigte zu verhindern.

Entgegen der Namenskonvention „Versichertenstammdaten (VSD)“ enthält der Versichertenstammdatensatz weit mehr Informationen als die auf der eGK aufgebrachten sichtbaren Informationen wie Name, Vorname und Versichertennummer. So sind im VSD-Datensatz u. a. auch die Teilnahme an Disease-Management-Programmen und der Zuzahlungsstaus und damit dem Sozialdatenschutz unterliegende Daten enthalten (s. Lastenheft VSD).

Gemäß gültigem und durch die Krankenkassen verbindlich einzuhaltendem Sicherheitskonzept der Gematik sind die Krankenkassen verpflichtet, bei **Beantragung** der eGK die Identität des Versicherten durch eine vom Benutzer unabhängige Instanz zweifelsfrei bestätigen zu lassen, da sonst kein datenschutzgerechter Zugriff auf Sozialdaten gewährt werden kann.

Es heißt im Sicherheitskonzept zu den private Keys (Verschl. und Auth.) der eGK: „Die **Beantragung**, die Ausstellung und das Zertifikatsmanagement entsprechen dem Niveau einer qualifizierten Signatur nach SigG/SigV“ (Tabelle C3.1 Schutzbedarfsklasse für das Schutzziel „Vertraulichkeit“ „sehr hoch“).

Und weiter heißt es zu den Prozessen zur Behandlung der Authentisierungsdaten zur Verteilung der eGKs (kartenindividuelle Schlüssel), dass sowohl eine Bestätigung der Identität als auch eine Bestätigung der Adresse durch eine vom Benutzer unabhängige Instanz erfolgen muss.

Der Grund für diese Vorschriften ist, dass nur dann die datenschutzrechtlichen Bestimmungen eingehalten werden können, wenn durchgängig über alle Prozessschritte hinweg dasselbe Sicherheitsniveau „hoch“ gewährleistet wird. Das schwächste Glied in der datenschutzrechtlichen Sicherheitskette bestimmt die Gesamtstärke.

Anforderungen an die Stärke der Authentisierungsverfahren

Verfahren	Anforderungen	Zugriff Rente wie QES	eID-Funktion Meldestelle	eGK DEÜV	eGK Papier	eGK VSD	eMail/ Telefon	de-mail wie QES
Qualität der Registrierung								
Nachweis der Identität	hoch	hoch	hoch	mittel	niedrig		niedrig	hoch
Vertrauenswürdigkeit der Registrierungsinstanz	hoch	hoch	hoch	niedrig	niedrig	niedrig	niedrig	hoch
Übergabe der Authentisierungs-Daten	hoch	hoch	hoch	mittel	mittel		niedrig	hoch
Qualität der Implementierung								
Authentisierungs-Prinzip	hoch	hoch	hoch			hoch	niedrig	hoch
Auflösbarkeit der Zuordnung der Authentisierungs-Daten	hoch	hoch	hoch			hoch	niedrig	hoch
Aufbewahrung der Authentisierungs-Daten	hoch	hoch	hoch			hoch	niedrig	hoch
Übertragungssicherheit der Authentisierungs-Daten	hoch	hoch	hoch			hoch	niedrig	hoch
Nachvollziehbarkeit								
Rückführbarkeit	hoch	hoch	hoch			hoch	niedrig	hoch
Protokollierbarkeit der Authentifizierung	hoch	hoch	hoch			hoch	niedrig	hoch
Gesamtbewertung	**hoch**	**hoch**	**hoch**	**niedrig**	**niedrig**	**niedrig**	**niedrig**	**hoch**

Das schwächste Glied bestimmt die Stärke der Sicherheitskette. Da die Qualität der Registrierung „niedrig“ ist, ist auch die Gesamtbewertung nur „niedrig“.

Stärke des Verfahrens der eGK liegt auf dem Niveau von eMail/Telefon

Daher darf die aktuell verwendete eGK nicht für den Zugriff auf Sozialdaten eingesetzt werden.

Es ist anzumerken, dass Verantwortliche nach § 203 StGB entsprechend sanktioniert werden können, wenn relevante Sicherheitsrichtlinien entweder durch aktives Handeln oder auch durch Unterlassen nicht eingehalten werden.

II. Zusammenfassendes Ergebnis

Die Nicht-Einhaltung der datenschutzrechtlichen Bestimmungen durch Krankenkassen bei Beantragung und Ausgabe der eGKs hat erhebliche Auswirkungen für die Durchführung von VSD in Arztpraxen. Der fehlende Identitätsnachweis kompromittiert die gesamte Telematikinfrastruktur, die somit als „datenschutzrechtlich unsicher zum Zugriff auf Sozialdaten“ einzustufen ist.

Die eGK ist zwar gesetzeskonform gemäß §291 Abs. 2a Satz 4 technisch geeignet, eine Authentisierung zu ermöglichen, jedoch fehlen die zwingend notwendigen organisatorischen datenschutzkonformen Maßnahmen bei Beantragung und Ausgabe der eGK, so dass die eGK weder als elektronischer noch als physischer Identitätsnachweis eingesetzt werden kann.

Unter Authentisierung versteht man den Nachweis einer behaupteten Eigenschaft. Die behauptete Eigenschaft im Falle der eGK ist dabei die Identität des Versicherten, da jeder Versicherte auf seiner eGK zur Authentisierung personenbezogene Zertifikate (AUT/AUTN-

Zertifikate) mit zugehörigem privatem Schlüssel hat. Personenbezogene Zertifikate beinhalten u.a. Namen, Vornamen, Geburtsdatum, Anschrift des Versicherten.

Mittels der Zertifikate AUT und AUTN weist sich also der Versicherte gegenüber der Telematikinfrastruktur aus. Die eGK ist somit ein elektronischer Identitätsnachweis. Dieser ist innerhalb des Gültigkeitsbereichs des Sozialgesetzbuchs rechtlich gleichzusetzen mit der eID-Funktion nach §18 PersAuswG (s. auch §36a Abs. 2 Satz 5 SGB I).

Neben der Eigenschaft elektronischer Identitätsnachweis zu sein, hat die eGK auch die Eigenschaft physischer Identitätsnachweis zu sein.

Diese Eigenschaft ist zwingend notwendig, um ohne die Nutzung von PINs eine datenschutzrechtlich zwingend notwendige Zwei-Faktor Authentisierung (hier Besitz der eGK und biometrisches Merkmal) beim Zugriff auf VSD realisieren zu können.

Dazu sind im Gegensatz zu rein elektronischen Nachweisen und Instrumenten zur Willensbekundung (z.B. Signaturkarten) auf der eGK biometrische Merkmale (Unterschrift, Lichtbild) aufgebracht. Diese Merkmale sollen in Kombination mit den personenbezogenen Zertifikaten (AUT/AUTN) zur Authentisierung gegenüber der Telematikinfrastruktur genutzt werden (VSD).

Rechtlich ist die eGK somit sowohl physisch als auch elektronisch als Identitätsnachweis nach §291 SGB V konzipiert.

Entsprechend den Bestimmungen sowohl des durch die Krankenkassen verbindlich einzuhaltenden Sicherheitskonzepts der Gematik als auch der europäischen Datenschutzrichtlinie (95/46/EG) und des e-Government-Handbuchs „Authentisierung im eGovernment“ **muss bei Beantragung/Ausgabe der eGK eine Bestätigung der Identität durch eine vom Benutzer unabhängige Instanz erfolgen.** Die Mitarbeiter der Registrierungsinstanz müssen selbst entsprechend den Anforderungen nach der vorgeschriebenen Schutzbedarfsklasse identifiziert worden sein und nach festgelegter Policy arbeiten.

Es ist davon auszugehen, dass die Ärzteschaft umfassend über den fehlenden Identitätsnachweis bei Beantragung/Ausgabe der eGK Kenntnis hat.

Um als Arzt nicht Gefahr zu laufen, selbst gegen die Regelungen des §203 StGB zu verstoßen, kann der Arzt nur durch die Nichtbeteiligung am VSD wegen der immanenten rechtlichen Mängel seine eigene Strafbarkeit – sei es als Täter oder Teilnehmer – sicher vermeiden.

Schon die Bereitstellung einer unsicheren IT-Infrastruktur kann einen Verstoß i. S. v. § 203 StGB darstellen.[1] Es ist nicht notwendig, dass tatsächlich ein unberechtigter Zugriff auf Sozialdaten (VSD) erfolgt. Es reicht die aus, wenn ein Zugriff ohne weiteres möglich wäre.

[1] Denn i. S. v. § 203 offenbart der Schweigepflichtige nicht erst dann tatbestandsmäßig, wenn die Daten von Dritten tatsächlich abgerufen werden, sondern schon dann, wenn der unberechtigte Abruf ohne weiteres möglich wäre, wie schon entsprechend beim Herumliegenlassen von Akten allgemein bekannt ist.

III. Rechtliche Herleitung

Das interne Rechtsgutachten der KBV (http://docs.dpaq.de/6324-20130731_rechtlicher_vermerk_zur_egk_als_identit_tsnachweis_kbv.pdf) hat bereits dargestellt, dass wesentliche Grundsätze des Datenschutzes bei der Ausgabe der eGK nicht beachtet werden.

Gestützt wird diese Herleitung auch vom verbindlich durch die Krankenkassen einzuhaltenden und gültigen Sicherheitskonzept der Gematik, welches die Krankenkassen verpflichtet die Identität des Versicherten bei Beantragung zweifelsfrei durch eine vom Benutzer unabhängige Instanz bestätigen zu lassen (s. Sachstand) sowie dem e-Government Handbuch des BSI (Authentisierung im eGovernment) und internationalen Standards wie ISO/IEC 10181-2.

Der BGH hat entschieden, dass Ärzte keine Erfüllungsgehilfen von Krankenkassen sind (GSSt 2/11).[2]

Gemäß BMV-Ä Anlage 4a (Stand 1.10.2013) sind Ärzte verpflichtet, die Identität des Versicherten anhand der auf der eGK aufgebrachten Identitätsdaten zu prüfen. Auch bei einer positiven Übereinstimmung von Lichtbild mit der zu behandelnden Person kann aufgrund des fehlenden Identitätsnachweises bei der Beantragung der eGK nicht mit der notwendigen Sicherheit davon ausgegangen werden, dass die zu behandelnde Person auch die versicherte Person ist. Es können ohne jegliche Kontrolle bei Beantragung eGKs mit Lichtbildern von verschiedenen Personen zu einem Namen erstellt werden.

<u>Finanzielle Regelungen des BMV-Ä zur Identitätsprüfung:</u>

In den Regelungen des BMV-Ä (Gültigkeit 1.10.2013) in § 48 Abs. 4 ist festgelegt, dass bei einer unzulässigen Verwendung einer Versichertenkarte ein Schadensersatzanspruch gegen den Vertragsarzt grundsätzlich ausgeschlossen ist, es sei denn, die Entstehung des Schadens lag im Verantwortungsbereich des Vertragsarztes. Der fehlende Identitätsnachweis bei Beantragung der eGK ist in jedem Fall ursächlich für jeglichen Missbrauch einer Versichertenkarte und außerhalb des Verantwortungsbereichs des Vertragsarztes, so dass in keinem Fall ein Schadensersatzanspruch der Kasse gegenüber dem Vertragsarzt abgeleitet werden kann.

<u>Strafrechtliche Würdigung:</u>

Vom Zugang zur Telematikinfrastruktur ist das bisherige Handeln in der Arztpraxis zu unterscheiden. Hierbei ist es von entscheidender Bedeutung, dass immer „derselben Person“ die gespeicherten Daten zugänglich gemacht werden und immer „derselben Person“ weitere medizinische Daten der elektronischen Akte hinzugefügt werden. Ob „dieselbe Person“ mit bürgerlichem Namen „Müller“ oder „Meyer“ heißt, ist dabei unerheblich. Der bürgerliche

[2] http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=60679&pos=0&anz=1

Name und die entsprechenden Versichertendaten dienen lediglich zu Abrechnungszwecken. So hat das BSG entschieden, dass ein Arzt lediglich einen Unterschriftenvergleich mit der auf der Versichertenkarte aufgebrachten Unterschrift durchzuführen hat, um seinen Vergütungsanspruch nicht zu verwirken.

In den bisherigen Praxisabläufen hat der Arzt als Schweigepflichtiger nach § 203 StGB dafür Sorge zu tragen, dass nur dem jeweils *Betroffenen* Auskunft erteilt wird. Die Identitätsprüfung erfolgt über biometrische Merkmale (Aussehen, Größe, Alter) als Wiedererkennung – nicht über den Namen. Für den Namen einer Person gilt: Er ist kein der Person unmittelbar und unlöslich anhaftendes Wesensmerkmal. Vielmehr wird er, nachdem der Zustand der Namensfreiheit aus polizei- und strafrechtlichen Gesichtspunkten aufgehoben wurde, vom Staat durch Gesetz oder Verwaltungsakt verliehen. Der Name ist daher kein geborenes, sondern ein gekorenes Persönlichkeitsgut. Seine Zuordnungsfunktion ist auch von geringerer Zuverlässigkeit, da es das Recht hinnimmt, dass mehrere Personen den gleichen Namen tragen. Ein geläufiger Name ist daher nur beim Hinzutreten weiterer Umstände ein personenbezogenes Datum.[3]

Erst wenn auf Daten zugegriffen oder Daten zusammengeführt werden sollen, die aus unterschiedlichen Quellen stammen, spielen maschinenverarbeitbare Merkmale wie Name und Versichertennummer eine Rolle. Und erst dann wird die zweifelsfreie Identität von entscheidender Bedeutung:

Für den Ablauf in einer Praxis ist es zunächst unerheblich, wie der Patient mit bürgerlichem Namen (wirklich) heißt. Da ein Vertragsarzt *eigene* Daten aufgrund einer *eigenen* personellen Zuordnung verwendet, kann ein Vertragsarzt auch ohne die wahre Identität des Patienten zu kennen, datenschutzrechtlich korrekt einen Zugriff auf die in der Praxis zu dieser Person gespeicherten Daten zulassen.

Für die Nutzung der Telematikinfrastruktur (VSD) ist die Situation grundlegend anders. Die Ermöglichung eines Zugriffs auf Sozialdaten via Telematikinfrastruktur (z. B. VSD) birgt in strafrechtlicher Hinsicht das Problem, dass der Arzt nicht aufgrund einer eigenen Prüfung die Zuordnung der abgerufenen Daten zu der richtigen Person sicherstellen kann und dass die offenbarende Krankenversicherung als Geheimnisträger i. S. v. § 203 StGB gleichfalls keine Sicherheit hat, dass die in der Praxis erscheinende Person tatsächlich die Identität hat, die sie laut der eGK haben sollte. In sämtlichen Fällen, in denen die Identität falsch angegeben wird und diese Angaben im Rahmen des VSD zugrunde gelegt werden, ist § 203 StGB hinsichtlich des objektiven Tatbestands erfüllt. Dabei kann an dieser Stelle offen bleiben, ob der Arzt durch Verwendung des VSD sich direkt als Mittäter oder „lediglich“ wegen Beihilfe zu einer Tat der Krankenversicherung i. S. v. § 203 StGB strafbar macht.

In subjektiver Hinsicht setzt § 203 StGB *Vorsatz* voraus, wobei es ausreicht, dass die Rechtsverletzung mit dem sog. dolus eventualis begangen worden ist. Hierunter ist zu verstehen,

[3] Identitätsdaten als Persönlichkeitsgüter; M. SCHEMITSCH; 2004

dass der Täter es subjektiv billigend in Kauf nimmt, dass der objektive Tatbestand erfüllt wird. In Abgrenzung dazu liegt nur eine nicht strafbare grobe Fahrlässigkeit vor, wenn der Täter auf einen guten Ausgang ernsthaft vertraut. Hinsichtlich des Offenbarens eines Geheimnisses ist der subjektive Tatbestand grundsätzlich durch den Arzt erfüllt. Juristisch stellt sich nur die Frage, wie es zu bewerten ist, dass der Arzt ggf. aufgrund fehlerhafter Identitätsangaben – irrtümlich – glaubt, zur Offenbarung von Geheimnissen befugt zu sein.

Das Merkmal „unbefugt" in § 203 StGB ist nämlich ein sog. ***Rechtfertigungsgrund***. Der Glaube an eine Befugnis i. S. v. § 203 StGB ist rechtlich als Irrtum über das Vorliegen eines Rechtfertigungsgrundes zu bewerten. Einzelheiten sind insofern umstritten. Im Rahmen des § 203 StGB wird dem Arzt die Argumentation „ich habe doch geglaubt, dass eine Befugnis vorliegt" regelmäßig nicht weiterhelfen. Andernfalls liefe § 203 StGB nämlich in der Praxis weitgehend leer! So wäre ohne weiteres möglich, durch telefonische Abfrage unter Nennung falscher Personendaten Behandlungsdaten fremder Personen zu erhalten – ein undenkbares Ergebnis! Die vorherige Identifizierung des Betroffenen i. S. des Datenschutzes gehört zu den zentralen, jedem Arzt bekannten Datenschutzanforderungen, weshalb Verstöße gegen diese eminent bedeutsame Verpflichtung mit nachfolgendem „Irrtum" des Arztes über seine Offenbarungsbefugnis regelmäßig den Vorwurf eines (zumindest bedingt) vorsätzlichen Verstoßes nach sich ziehen.[4]

Die Involvierung der Ärzte im Bereich des VSD führt zu keiner anderen Beurteilung, denn aufgrund diverser Veröffentlichungen in allgemeinen Medien sowie in ärztlichen Fachzeitschriften ist allgemein bekannt, dass die Identifizierung des Betroffenen seitens der Kassen nicht anhand der auf der eGK aufgebrachten Personaldaten (Lichtbild, Unterschrift) erfolgt ist und somit auch im weiteren Procedere seitens der Ärzte anhand der eGK nicht erfolgen kann. Der einzige sichere Weg zur Vermeidung einer Strafbarkeit nach § 203 StGB wäre für die Ärzte, dass sie sich von den Betroffenen ein gültiges Ausweisdokument vorzeigen lassen und die Personaldaten mit der eGK abglichen. Da es aber kein gesetzlich determiniertes Recht des Arztes gibt, die Vorlage eines gültigen Ausweisdokumentes zu verlangen[5], kann der Arzt nur durch die Nichtbeteiligung am VSD wegen der immanenten rechtlichen Mängel seine eigene Strafbarkeit – sei es als Täter oder Teilnehmer – sicher vermeiden.

---

[4] Die Definitionen für Eventualvorsatz sind Gegenstand weiterführender juristischer Diskussion. Unter anderem wird für den Eventualvorsatz auch vertreten, dass er zu bejahen ist, wenn der Täter sich über das erlaubte Risiko hinaus zur Handlung entschließt (Risikotheorie) oder eine unabgeschirmte Gefahr für ein Rechtsgut schafft (Lehre von der unabgeschirmten Gefahr). Insbesondere die Risikotheorie und die Lehre von der unabgeschirmten Gefahr scheinen im Anwendungsbereich des § 203 StGB vom Grundgedanken her sehr passend - wobei davon auszugehen ist, dass bei Zugrundelegung der allgemein von der Rechtsprechung anerkannte Definition des Eventualvorsatzes „billigend in Kauf genommen" das Ergebnis dasselbe ist.

[5] Die Dokumentenvorlage *verlangen* können laut PersAusweisG lediglich „zur Identitätsfeststellung berechtigte Behörden" wie z. B. Polizei, Grenzschutz etc. Siehe auch den Wortlaut des § 20 Abs. 1 PersAuswG.