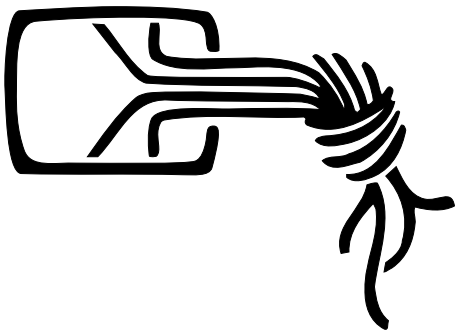

Stellungnahme zum Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz – PDSG)

Stellungnahme des Chaos Computer Club (CCC) zum Gesetzentwurf der Bundesregierung (Drucksache 19/18793)

Martin Tschirsich

Chaos Computer Club

19. Mai 2020

Inhalt

VORBEMERKUNGEN

Im Dezember 2019 hat der Chaos Computer Club (CCC) grobe Mängel in der Vergabe von Zugangsberechtigungen zur Telematikinfrastruktur festgestellt[1].

Neben einer sofortigen Schadensbegrenzung forderte der CCC mit Blick auf die Einführung der elektronischen Patientenakte zum 1. Januar 2021:

1. Zuverlässige Kartenbeantragungs- und herausgabeprozesse: Beantragung, Identifikation und Ausgabe müssen entsprechend dem Schutzbedarf von Gesundheits- und Sozialdaten durchgeführt werden.
2. Volle Umsetzung der eGK als Identitätsnachweis.
3. Neuplanung und saubere Implementierung der Prozesse, die zur Ausstellung von eGK, HBA und SMC-B führen, sowie Kontrolle der Umsetzung.
4. Organisierte Verantwortung statt organisierter Verantwortungslosigkeit: Eine unabhängige zentrale Stelle sollte für die Informationssicherheit der Telematikinfrastruktur verantwortlich sein. Diese Stelle sollte Prozesse nicht nur vorgeben, sondern auch ihre ordnungsgemäße Umsetzung unabhängig prüfen.

Wir stellen fest, dass der vorliegende Gesetzentwurf nicht geeignet ist, die diagnostizierten Mängel sowie die ursächlichen Fehlanreize abzustellen:

- Die eGK wird weiterhin unsicher und ohne zuverlässige Identitätsprüfung der Antragsteller ausgegeben. Statt die Mängel – unter deren Ausnutzung der Zugriff auf Gesundheitsdaten Dritter gelingt – abzustellen, werden diese nunmehr sogar gesetzlich festgeschrieben.
- Die bislang nicht erfolgte Umsetzung der bestehenden gesetzlichen Vorgaben wird weiterhin nicht ausreichend sanktioniert. Krankenkassen als Herausgeber der eGK bleiben im Gegensatz zu Arztpraxen von den Sanktionen der DSGVO ausgenommen. Trotzdem sollen Krankenkassen zukünftig mit Erlaubnis des Versicherten die Gesundheitsdaten der Patientenakte verarbeiten dürfen.

Daraus ergeben sich wesentliche Änderungsvorschläge am Gesetzentwurf zu den Punkten

1. Sichere Identitätsprüfung bei Beantragung der Gesundheitskarte und sichere Ausgabe,
2. DSGVO-Bußgeldvorschriften auch für Krankenkassen sowie
3. Kein Zugriff der Krankenkassen auf Gesundheitsdaten,

die im Folgenden detailliert ausgeführt sind.

[1] CCC diagnostiziert Schwachstellen im deutschen Gesundheitsnetzwerk, https://www.ccc.de/de/updates/2019/neue-schwachstellen-gesundheitsnetzwerk

1. Sichere Identitätsprüfung bei Beantragung der Gesundheitskarte und sichere Ausgabe

§ 336 SGB V Zugriffsrechte der Versicherten

Änderungsvorschlag:

§ 336 SGB V Abs. 5 ist zu streichen. Regelungen auf dieser Detailtiefe sind zudem Bestandteil des regelmäßig an den Stand der Technik anzupassenden Sicherheitskonzepts der Gematik nach § 311 Abs. 1 Nr. 1 Buchstabe a.

Begründung:

Die eGK ist nach in § 291 Abs. 2 Nr. 1 enthaltenem geltenden Recht sowie den daraus abgeleiteten Vorgaben im Sicherheitskonzept der Gematik nach § 311 Abs. 1 Nr. 1 Buchstabe a als Schlüssel bzw. Authentisierungsinstrument für den Zugriff auf besonders schützenswerte Gesundheitsdaten auszugeben.

Gemäß den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) und dem in zugrundeliegenden internationalen Normen dokumentierten Stand der Technik setzt dies eine Identitätsprüfung des Versicherten auf hohem Vertrauensniveau und eine Ausgabe aller Authentisierungsmittel ebenfalls auf hohem Vertrauensniveau voraus.

Mit den neuen Regelungen aus § 336 Abs. 5 Satz 1 Nr. 1 bis 3 jedoch wird dieses bisher gesetzlich geforderte hohe Sicherheitsniveau deutlich abgeschwächt: Die Verpflichtung zur sicheren Identifikation des Versicherten entfällt; die Ausgabe der Authentisierungsmittel wird nicht mehr auf hohem Vertrauensniveau vorgeschrieben.

Damit sind aber die vom CCC beschriebenen Mängel nicht behoben, unter deren Ausnutzung bereits erfolgreiche Angriffe auf die Telematikinfrastruktur demonstriert wurden[2]. Derart nach bisher geltendem Recht nicht gesetzeskonform ausgegebene Gesundheitskarten (eGK) dürfen weder für den Zugriff auf Gesundheitsdaten noch zur Abgabe von Einwilligungen oder Vergabe von Zugriffsberechtigungen eingesetzt werden.

Hintergrund:

In § 336 Abs. 5 Satz 1 Nr. 1 bis 3 werden im Ergebnis völlig unterschiedliche Verfahren vorgegeben. Während Nr. 1 und Nr. 2 lediglich eine Übergabe eines Authentisierungsmittels entweder auf einem persönlichen Weg oder durch Versand an eine Meldeadresse beschreiben, wird in Nr. 3 eine nachträgliche, sichere „Identitätsprüfung“ des Versicherten und Abgleich mit seiner bereits ausgegebenen eGK dargestellt. Durch die „oder“-Verknüpfung von Nr. 1 bis Nr. 3 werden Verfahren zur „Übergabe“ mit Verfahren zur „Identitätsprüfung“ alternativ ermöglicht und

[2] CCC diagnostiziert Schwachstellen im deutschen Gesundheitsnetzwerk, https://www.ccc.de/de/updates/2019/neue-schwachstellen-gesundheitsnetzwerk

somit als gleichwertig ersetzend formuliert. Diese Verfahren zur „Übergabe“ und „Identitätsprüfung“ sind aber gemäß BSI TR-03107-1 und internationalen Standards nicht alternativ, sondern ergänzend durchzuführen. Es muss eine „Identitätsprüfung“ auf „hohem“ Vertrauensniveau und eine „Übermittlung“ aller Authentisierungsmittel auf „hohem“ Vertrauensniveau erfolgen. Darüber hinaus weisen die in Nr. 1 und Nr. 2 beschriebenen Verfahren jeweils in sich mehrere Ungenügendheiten auf. Für § 336 Abs. 5 Nr. 1. erfolgt lediglich die Übergabe eines Authentisierungsfaktors in einem sicheren Verfahren. § 336 Abs. 5 Nr. 2 stellt kein Verfahren auf „hohem“ Vertrauensniveau dar.

Der Gesetzentwurf macht zudem die gültige Einwilligung des Versicherten zur Grundlage der Verarbeitung seiner medizinischen Daten. An eine datenschutzrechtlich gültige Einwilligung zum Zugriff auf Gesundheitsdaten mit „hohem“ Schutzbedarf sind die Regelungen der BSI TR-03107-1 verbindlich anzuwenden. Diese basiert auf internationalen Normen und dient zur Festlegung des „Stands der Technik“ zur Einhaltung der Datenschutzgrundverordnung. Um eine gültige Einwilligung abgeben zu können, ist eine rein technische Zugriffsfreigabe z. B. in § 339 Abs. 1 Satz 2 ohne Einhaltung zentraler Anforderungen an Beantragung und Ausgabe der Authentisierungsmittel ungenügend. Zunächst muss die eGK auch als Identitätsnachweis im Bereich des SGB V umgesetzt sein – ohne elektronischen Identitätsnachweis in Form der eGK kann keine gültige elektronische Einwilligung mittels eGK erfolgen. Darüber hinaus müssen sowohl die Identitätsprüfung bei Beantragung der eGK als auch die Ausgabe der Authentisierungsmittel auf „hohem“ Vertrauensniveau erfolgen und setzen nach auch vom BSI referenzierten internationalen Standards ein persönliches Erscheinen mit Identitätsprüfung durch eine vertrauenswürdige Stelle voraus. Diese Anforderungen sind sowohl für die als technische Zugriffsfreigabe vorgesehenen Authentisierungsmittel eGK und PIN als auch für die geplante alternative Versichertenidentität mit zweitem Faktor nicht erfüllt. Daher entspricht die Formulierung im Gesetzentwurf zu elektronischen Einwilligungen nicht den datenschutzrechtlichen Anforderungen.

2. DSGVO-Bussgeldvorschriften auch für Krankenkassen

§ 395 SGB XIII Bußgeldvorschriften

Änderungsvorschlag:

Gemäß Vorschlag des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)[3] wird dem § 395 folgender Absatz 5 angefügt: „(5) Abweichend von § 85a Absatz 3 des Zehnten Buches Sozialgesetzbuch kann gegen eine Krankenkasse wegen eines Verstoßes nach Artikel 83 Absatz 4, 5 oder 6 der Verordnung (EU) 2016/679, der sich auf Sozialdaten bezieht, eine Geldbuße nach Artikel 58 Absatz 2 Buchstabe i) der Verordnung (EU) 2016/679 verhängt werden. § 17 Absatz 4 des Gesetzes über Ordnungswidrigkeiten ist anzuwenden."

Begründung:

Krankenkassen kommen ihren datenschutzrechtlichen Verpflichtungen als Herausgeber der eGK regelmäßig nicht nach. Der CCC hat zuletzt demonstriert, wie seit vielen Jahren und spätestens seit 2014 regelmäßig ausgenutzte Mängel bei der Beantragung und Ausgabe der eGK die Gesundheitsdaten der Versicherten gegenüber Dritten offenbaren[4]. Die im Gesetzentwurf vorgesehenen und im Verhältnis zum Ausgabevolumen der gesetzlichen Krankenkassen von mehr als 25 Mrd. Euro völlig unzureichenden Bußgeldvorschriften setzen keinen dringend notwendigen Anreiz zur Schließung dieser datenschutzrechtlichen Lücken. Der Vorschlag der damaligen BfDI berücksichtigt dagegen die wirtschaftliche Tätigkeit und das wirtschaftliche Auftreten der gesetzlichen Krankenkassen und ermöglicht „in diesem Rahmen bestimmte Verstöße gegen die Datenschutz-Grundverordnung nach Art. 58 Absatz 2 Buchst. i) i. V. m. Art. 83 DSGVO mit einem Bußgeld zu sanktionieren".

Hintergrund:

Gesetzliche Krankenkassen nehmen laut der damaligen BfDI „als öffentliche Unternehmen am Wettbewerb teil (§ 2 Absatz 5 BDSG). […] Auch in der Öffentlichkeit gerieren sich die gesetzlichen Krankenkassen als öffentliche Wettbewerbsunternehmen, die mit verschiedenen Angeboten – ähnlich wie privatrechtliche Krankenversicherungsunternehmen – um ihre Kundschaft werben. So bieten etwa einige Krankenkassen in Zusammenarbeit mit privaten Anbietern ihren Kunden die Nutzung von elektronischen Gesundheitsakten an, die über eine App auf dem Smartphone oder Tablet genutzt werden sollen. Die Angebote und das Datenschutzniveau unterscheiden sich dabei deutlich und dies wird von den gesetzlichen Krankenkassen auch als Wettbewerbsvorteil gegenüber anderen Krankenkassen gesehen. […] Im Verhältnis zu ihren

[3] Beschlussempfehlung und Bericht zu einem Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU, BT-Drs 19/11181

[4] CCC diagnostiziert Schwachstellen im deutschen Gesundheitsnetzwerk, https://www.ccc.de/de/updates/2019/neue-schwachstellen-gesundheitsnetzwerk

Versicherten ist das Verhalten der Krankenkassen unmittelbar am UWG zu messen, soweit dieses die Richtlinie 2005/29/EG (UGP-RL) über unlautere Geschäftspraktiken umsetzt (vgl. hierzu statt vieler BGH, Urteil vom 30. April 2014 – I ZR 170/10 –; Urteil vom 18. September 2013 – I ZR 183/12 –; EuGH, Urteil vom 03. Oktober 2013 – C-59/12 –). Schließlich ist es einem Versicherten (bei den gesetzlichen Krankenkassen intern „Kunde“ genannt) möglich, frei von einer gesetzlichen Krankenkasse zu einer anderen zu wechseln. Dies ist bei anderen Sozialversicherungsträgern (Deutsche Rentenversicherungen, gesetzliche Unfallversicherer) nicht möglich. Die gesetzlichen Renten- und Unfallversicherungsträger stehen im Gegensatz zu den gesetzlichen Krankenkassen untereinander nicht im Wettbewerb. Es gibt daher tatsächliche Gründe, die Krankenkassen im Unterschied zu anderen Sozialversicherungsträger Wirtschaftsunternehmen gleich zu stellen.“

3. Kein Zugriff der Krankenkassen auf Gesundheitsdaten

§ 284 SGB V Sozialdaten bei Krankenkassen

Änderungsvorschlag:

Gemäß Vorschlag des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)[5] wird in § 284 SGB V folgender Absatz 5 eingefügt: „(5) Krankenkassen dürfen Sozialdaten, sofern sie besondere Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 sind, auf Grundlage einer Einwilligung nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe a der Verordnung (EU) 2016/679 in Verbindung mit Artikel 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 nur verarbeiten, sofern in diesem Buch eine Verarbeitung dieser Daten mit Einwilligung ausdrücklich vorgesehen ist. Dies gilt nicht für die Übermittlung für Zwecke der wissenschaftlichen Forschung und Planung Dritter."

Begründung:

Über die sehr unspezifisch formulierten Öffnungsklauseln des § 284 „das Angebot zusätzlicher Inhalte und Anwendungen" können Krankenkassen leicht über entsprechende Einwilligungen der Versicherten an solche Informationen gelangen, die zurecht der ärztlichen Schweigepflicht unterliegen. Dies ist als großes Risiko aus Sicht der Versicherten einzustufen.

Die in einer Patientenakte zu speichernden Daten unterliegen einem besonderen Schutz und nicht ohne Grund wird im vorliegenden Gesetzentwurf formuliert, dass Krankenkassen die Daten der elektronischen Patientenakte (ePA) nicht verarbeiten dürfen (§ 344 Abs. 2). Mittels der o. g. generellen Öffnungsklausel kann aber genau dieser Schutz durch Krankenkassen ausgehebelt werden. Hierbei ist zu berücksichtigen, dass Versicherte gegenüber Krankenkassen als nicht gleichberechtigt anzusehen sind. Der neu einzufügende Absatz 5 beseitigt dieses Risiko aus Sicht des Versicherten sowohl für das Angebot zusätzlicher Inhalte und Anwendungen als auch für die in der Vergangenheit aufgetretenen Fälle, dass Krankenkassen Versicherte veranlasst haben, Schweigepflichtentbindungserklärungen abzugeben, um hiermit von Ärzten medizinische Daten über die Versicherten zu erheben, die ihnen gesetzlich nicht zustehen.

Hintergrund:

In Ihrer Stellungnahme zum 2. DSAnpUG[6] hat die damalige BfDI ausgeführt, dass, um auszuschließen, dass Krankenkassen allein auf der Grundlage einer Einwilligung nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe a in Verbindung mit Artikel 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 Daten für Zwecke verarbeiten, die nicht zu ihrem gesetzlich zugewiesenen Auf-

[5] Beschlussempfehlung und Bericht zu einem Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU, BT-Drs 19/11181

[6] Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines 2. Datenschutzanpassungs- und Umsetzungsgesetzes EU (2. DSAnpUG-EU), Ausschussdrucksache 19(4)151

gabenbereich gehören, § 284 Absatz 5 SGB V auf der Grundlage der Öffnungsklausel des Artikels 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 vorsieht, dass Krankenkassen besondere Kategorien personenbezogener Sozialdaten auf der Grundlage einer Einwilligung nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe a in Verbindung mit Artikel 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 trotz Einwilligung der betroffenen Person nur dann verarbeiten dürfen, wenn im SGB V eine Verarbeitung dieser Daten mit Einwilligung ausdrücklich vorgesehen ist. Um dies zu erreichen, schlug sie die Einführung des angeführten Absatzes 5 in § 284 SGB V vor: „Eine derartige Klarstellung ist nicht zuletzt deshalb erforderlich, da eine erhebliche Anzahl von Beschwerden von Versicherten, aber auch von Ärzten vorliegen, wonach in der Praxis diese Rechtsauffassung der Aufsichtsbehörden von Krankenkassen umgangen wird, indem Versicherte veranlasst werden, Schweigepflichtentbindungserklärungen abzugeben, um hiermit von Ärzten medizinische Daten über die Versicherten zu erheben, die ihnen gesetzlich nicht zustehen. Eine derartige Klarstellung würde zudem Erwägungsgrund 43 der DSGVO präzisieren, wonach eine Einwilligung dann keine gültige Rechtsgrundlage ist, wenn zwischen der betroffenen Person (Versichertem) und dem Verantwortlichen (gesetzliche Krankenkasse) ein klares Ungleichgewicht besteht, und deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde. Tatsächlich erfolgt die Forderung an den Versicherten, eine Schweigepflichtentbindungserklärung abzugeben, häufig in Fällen, in denen der Versicherte auf die Zahlung von Krankengeld angewiesen ist. Über die Probleme habe ich mehrfach berichtet (u. a. in meinem 26. [Nr. 9.2.5], 25. [Nr. 13.7.1] und 22. [Nr. 11.1.8] Tätigkeitsbericht).“

§ 345 SGB V Angebot und Nutzung zusätzlicher Inhalte und Anwendungen

Änderungsvorschlag:

Nach § 345 SGB V Abs. 1 Satz 1 wird der Satz „§ 344 Abs. 2 Satz 2 SGB V bleibt unberührt.“ eingefügt.

Begründung:

Nach § 284 SGB V Abs. 1 Satz 1 Nr. 20 dürfen Krankenkassen für das Angebot zusätzlicher Anwendungen im Sinne des § 345 SGB V Abs. 1 Satz 1 Sozialdaten erheben und speichern. Dazu zählen insbesondere die Gesundheitsdaten in der ePA. Der Änderungsvorschlag dient zur einheitlichen Gestaltung der gesetzlichen Grundlage zur Verarbeitung von Sozialdaten wie im Änderungsvorschlag zu § 284 ausgeführt.