

Sehr geehrte Herren,

Im Rahmen des Gespräches zum geplanten RefE AbEM haben wir das Thema der BSI-Zertifizierung angesprochen. Die aktuelle Umsetzung der TR-03161 stellt aus Sicht von Pharma Deutschland erhebliche organisatorische und gesetzliche Friktionen im Rahmen des Inverkehrbringens und Betreibens von DiGA dar. Sie ist zudem aus standortpolitischen Gründen schwer nachzuvollziehen. Pharma Deutschland schlägt im Sinne einer gesetzlich intendierten und an der Versorgung angepassten Umsetzung verhältnismäßiger IT-Sicherheitsvorgaben nachfolgende Änderungen vor:

Anpassung des § 139e Abs. 10 SGB V

Der gesetzlichen Intention des § 139e Absatz 10 Satz 4 SGB V nach, hat der DiGA-Nutzende das Recht auf Wahl eines Authentisierungsverfahrens mit einem geringeren Sicherheitsniveau. Dies deckt sich mit dem Beschluss der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder „Zur Möglichkeit der Nichtanwendung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO auf ausdrücklichen Wunsch betroffener Personen“ vom 24. November 2021. Sie ist zudem kongruent mit dem Recht auf Gesundheitsdatenverarbeitung welches mit Art. 2. Abs. 2 Satz 1 GG, dem Recht auf körperliche Unversehrtheit, einhergeht. In der aktuellen Fassung der TR 03161 wird den Nutzenden die Wahlfreiheit des Sicherheitsniveaus zur Authentifizierung jedoch nahezu vollständig entzogen.

Um den Grundsatz des Art. 32 DSGVO iVm § 139e SG V rechtlich klarzustellen, schlägt Pharma Deutschland vor, nach § 139e Absatz 10 Satz 4 SGB V folgenden Satz 5 anzufügen:

„Dies kann auch die Einwilligung in ein normales oder niedrigeres Sicherheitsniveau sein, wenn Versicherte dies freiwillig fordern.“

Zertifikatsverfügbarkeit – Anpassung § 7 Abs. 3 DiGAV

Die aktuelle Anforderung, dass Hersteller mit einem Antrag auf vorläufige Listung bereits in der formalen Prüfphase das TR-03161 Zertifikat erbringen müssen, steht aus Sicht von Pharma Deutschland der Intention des Fast-Track-Verfahrens, DiGA schnell der Versorgung verfügbar zu machen, entgegen. Die Vorgabe ist eine weitere große Hürde im Prozess zur Aufnahme in das DiGA. Entsprechend sollte die Anforderung um die Möglichkeit ergänzt werden, dass ein Prüfnachweis einer Prüfstelle ausreichend ist.

Pharma Deutschland schlägt daher folgende Änderung des § 7 Abs. 3 DiGAV vor:

„Die Verpflichtung nach Satz 2 und 3 gilt sowohl für Hersteller digitaler Gesundheitsanwendungen, deren digitale Gesundheitsanwendung bereits in das Verzeichnis für digitale Gesundheitsanwendungen aufgenommen wurde, als auch für Hersteller, die die Aufnahme einer digitalen Gesundheitsanwendung in das Verzeichnis für digitale Gesundheitsanwendungen erstmalig beantragen; im erstgenannten Fall ist der Nachweis im Verfahren nach § 139e Absatz 6 Satz 1 des Fünften Buches Sozialgesetzbuch zu erbringen. Im zweitgenannten Fall muss das Zertifikat bei der Beantragung einer dauerhaften Aufnahme zum Abschluss der inhaltlichen Prüfung spätestens vorliegen; *wird eine vorläufige Aufnahme in das Verzeichnis für digitale Gesundheitsanwendungen beantragt, ist das Zertifikat spätestens zum Ende des Erprobungszeitraumes, nicht aber später als 12 Monate nach erstmaliger Listung im Verzeichnis, vorzulegen. Für die formale Prüfung des Antrags auf vorläufige Aufnahme in das Verzeichnis für digitale Gesundheitsanwendungen ist mindestens eine Erklärung einer Prüfstelle vorzulegen, die ein laufendes Prüfverfahren zu der eingereichten Version der digitalen Gesundheitsanwendung für das Zertifikat nachweist. Wenn das BSI oder die Prüfstelle zu dem Ergebnis kommt, dass eine Zertifizierung auch mit Auflagen nicht*

möglich ist und nicht in Aussicht gestellt werden kann erfolgt die Einstellung des Antragsverfahrens oder die Streichung der Anwendung aus dem Verzeichnis für digitale Gesundheitsanwendungen.“

Zertifikatsgültigkeit – Anpassung § 7 Abs. 3 DiGAV

Das BSI Zertifikat zur TR-03161 wird auf eine spezifische Softwareversion, also eine Momentaufnahme, der Software ausgestellt. Die Gültigkeit für Softwareversionen mit einer Wildcard (bspw. 1.0.*) ist nicht gegeben. Folglich muss jede Änderung mindestens ein Maintenance-Verfahren des BSI durchlaufen. Hinsichtlich der Schnelllebigkeit von Software und darüber hinaus auch der Verpflichtungen für Hersteller gemäß MDR, ist Software stets aktuell und sicher zu halten. Diese regulatorische und vom Markt geforderte Anforderung wird für DiGA-Hersteller zu einem Problem, wenn die Rahmenbedingungen ein zeitnahe Update der Software nicht zulassen. Die Umsetzung der Zertifikatspflicht nach § 139e Abs. 10 SGBV i.V.m. § 7 Abs. 3 DiGAV blockiert in der aktuellen Fassung notwendige ad-hoc App-Updates und führt zu weniger Patientensicherheit und medizinischem Nutzen für die Versicherten. Hinzu kommt, dass derzeit jegliche Aktualisierung des BSI TR-03161 Zertifikats als wesentliche Änderung dem BfArM gemeldet werden muss, da es sich um ein Update zur Aufrechterhaltung bei einer Zertifikaterneuerung immer um eine Widerherstellung der DiGA-Fähigkeit handelt. Das bedeutet, dass jegliche Änderung an einer DiGA automatisch eine immer wesentliche Veränderung sein muss.

Pharma Deutschland schlägt daher eine entsprechende Regelung zu Zertifikatsanpassungen in einem neuen § 7 Abs. 3b DiGAV vor:

„Wird durch eine im Sinne von § 18 Abs. 1 im Umfang geringfügige Änderung vorgenommen, ist das aktualisierte Nachweis der im Rahmen einer redaktionellen Änderung an den Angaben im Verzeichnis für digitale Gesundheitsanwendungen dem Bundesinstitut für Arzneimittel und Medizinprodukte mitzuteilen. Die Mitteilung ist unverzüglich nach Ausstellung des Zertifikats erforderlich und muss spätestens 8 Kalenderwochen nach Veröffentlichung der Änderung dem Bundesinstitut für Arzneimittel und Medizinprodukte vorliegen.“

Wie auch bereits im Workshop zur BSI-Zertifizierung verdeutlicht, stehen DiGA-Hersteller und Pharma Deutschland einem konstruktiven Austausch offen gegenüber.

Für Rückfragen stehen wir gern zur Verfügung.

Pharma Deutschland