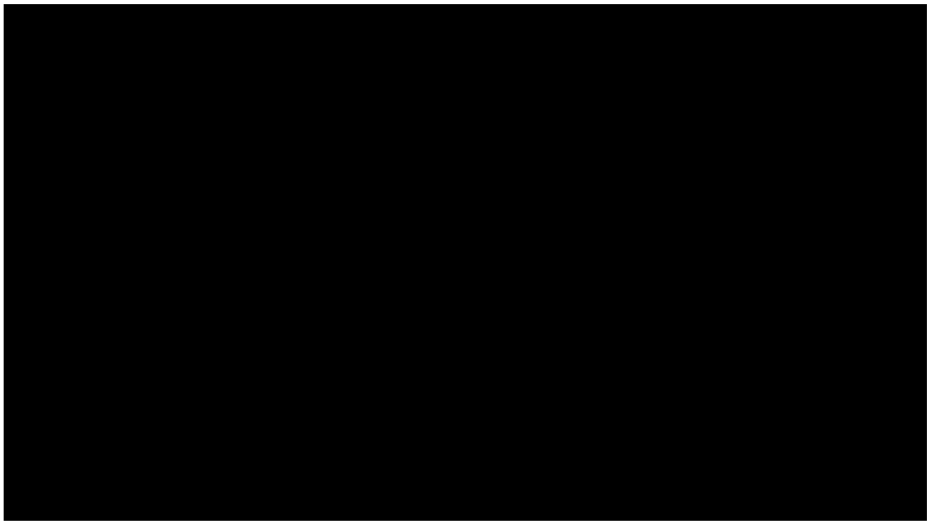
Spitzenverband
Digitale
Gesundheitsversorgung



via Email

02. April 2025

Dringender Handlungsbedarf: Umsetzung der BSI TR-03161 für Digitale Gesundheitsanwendungen (DiGA)

Sehr geehrte Damen und Herren,

als Spitzenverband Digitale Gesundheitsversorgung (SVDGV) wenden wir uns mit großer Sorge an Sie. Die Einführung der Technischen Richtlinie TR-03161 in ihrer aktuellen Form führt zu massiven Unsicherheiten, finanziellen Belastungen und praktischen Hürden für die Hersteller digitaler Gesundheitsanwendungen und schon heute zu Reibungen in der Patientenversorgung von DiGA. Wir teilen das Ziel einer höchstmöglichen Datensicherheit vollumfänglich. Jedoch sind sowohl die Ausgestaltung der Richtlinie, als auch deren Umsetzung durch BSI, BfArM und die beteiligten Prüfstellen bislang nicht ausreichend praxistauglich.

Die derzeitige Situation ist für einige Hersteller sogar existenzbedrohend. Ohne kurzfristige Korrekturen in Prozessen und Anforderungen können neue DiGA kaum noch wirtschaftlich entwickelt oder bestehende Anwendungen weiter gepflegt werden. Wir sehen zudem die große Gefahr, dass keine DiGA-Neuzulassungen in diesem Jahr möglich sein werden. Neben der

Vorsitzender: Dr. Paul Hadrossek
Geschäftsführerin: Dr. Anne Sophie Geier

Spitzenverband Digitale
Gesundheitsversorgung e.V.
Pappelallee 78/79, 10437 Berlin

Telefon: +49 30 62 93 84 94
Fax: +49 30 62 93 84 96
E-mail: impressum@digitalversorgt.de

www.digitalversorgt.de

Vereinsregisternummer: VR 37693 B
Vereinsregister Berlin, Amtsgericht Charlottenburg

Bankverbindung apoBank
IBAN: DE88 3006 0601 0007 3667 91
BIC: DAAEDEDDXXX

Patientenversorgung ist damit auch die vom Gesetzgeber geforderte kontinuierliche Weiterentwicklung gemäß EU-MDR 2017/745 sowie die Nutzerfreundlichkeit gemäß § 5 Abs. 5 DiGAV praktisch nicht umsetzbar.

1. Unklare Anforderungen und fehlende Einheitlichkeit in der Prüfpraxis

Viele Anforderungen der TR-03161 sind unklar formuliert und bieten Spielraum für unterschiedliche Auslegungen. Beispielsweise bestehen unterschiedliche Ansichten zur zulässigen "Active Time" (in der gematik-Sprechstunde wurde z. B. vom BSI kommuniziert, dass 24 Stunden nicht akzeptabel seien, obwohl dies von Prüfstellen akzeptiert wurde) oder zur Definition und Handhabung interner Tools und Softwarebibliotheken. Obwohl in Gesprächen mit dem BSI eindeutige Vorstellungen formuliert wurden, fehlen hierzu verbindliche und praxistaugliche schriftliche Festlegungen. Das führt dazu, dass Prüfstellen voneinander abweichende Prüfmaßstäbe anlegen und selbst positive Prüfergebnisse der Prüfstellen nicht zur Zertifizierung durch das BSI führen. Wiederholte Nachprüfungen, lange Wartezeiten und Unklarheiten in der Kommunikation binden erhebliche Ressourcen auf Seiten der Hersteller und der Prüfer.

2. Widersprüchliche Anforderungen und technische Zielkonflikte

Einige Anforderungen der TR-03161 stehen in einem direkten technischen Widerspruch zueinander oder mit anderen bestehenden gesetzlichen Anforderungen. Solche Zielkonflikte führen dazu, dass Hersteller in der praktischen Umsetzung nicht gleichzeitig allen Anforderungen gerecht werden können. Hier besteht dringender Klarstellungsbedarf, um praxistaugliche, widerspruchsfreie Vorgaben zu etablieren.

Beispiele für solche Zielkonflikte sind z.B., dass die TR-03161 die ungesicherte Herausgabe personenbezogener Daten untersagt, die DiGAV fordert jedoch einen menschenlesbaren Export von Gesundheitsdaten im PDF- oder XML-Format. Ein weiterer Konflikt besteht z.B. darin, dass Anwendungen laut der technischen Richtlinie keine übermäßige Protokollierung durchführen sollen, gleichzeitig wird jedoch verlangt, auch abgebrochene Verbindungen und bestimmte Kommunikationsdetails umfassend zu loggen.

Weitere Anmerkungen auf inhaltlicher Ebene haben wir in der ausführlichen Kommentierung vom 19.01.2024 sowie 19.12.2024 (siehe Anhang) zusammengetragen.

3. Fehlende Berücksichtigung ungewollter Folgeeffekte

Der aktuelle Fokus auf reine Datensicherheit blendet medizinische Risiken und Auswirkungen auf die Nutzerfreundlichkeit weitgehend aus. Beschwerden über Inaktivitäts-Logout und komplexe Authentifizierungspflichten häufen sich. Patienten mit Panikstörungen könnten im Notfall keinen Zugang zur verordneten DiGA erhalten. Das Ziel einer sicheren, aber auch nutzbaren Versorgungslösung wird damit verfehlt. Zudem wird ein nicht unwesentlicher Teil der Patientinnen und Patienten von der Nutzung von DiGA ausgeschlossen - aufgrund der Anforderungen an die unterstützten Endgeräte, denen ältere Smartphones nicht vollends genügen.

4. Umgang mit Produktupdates nach erfolgter Zertifizierung

Derzeit sollen alle Produktupdates dem BSI zur Beurteilung vorgelegt werden. Für jede Version fällt eine Prüfgebühr von 425 Euro an. Die Bewertung, ob es sich um ein sicherheitsrelevantes Update handelt, erfolgt ausschließlich durch das BSI anhand eines nicht öffentlich zugänglichen Kriterienkatalogs. Wird ein Update als sicherheitsrelevant eingestuft, ist eine kostenpflichtige Nachprüfung erforderlich. Da die Erstzertifizierung einer DiGA je nach Komplexität zwischen 20.000 und 80.000 Euro kosten kann, sind auch Nachprüfungen mit erheblichen finanziellen Belastungen verbunden. Da die meisten Hersteller alle 3 Monate größere Funktionsupdates herausbringen, ist aktuell davon auszugehen, dass hier finanzielle Aufwände im 5-stelligen Bereich auf die Hersteller zukommen.

Um eine hohe Qualität digitaler Gesundheitsanwendungen zu gewährleisten, veröffentlicht rund die Hälfte der DiGA-Hersteller wöchentlich oder im 14-tägigen Rhythmus Updates ihrer Anwendungen. Bei einer Prüfgebühr von 425 Euro pro Meldung bedeutet dies für einen einzelnen Hersteller Kosten von bis zu 22.100 Euro pro Jahr für jedes Produkt – allein für die Mitteilung, ob ein Update als sicherheitsrelevant einzustufen ist oder nicht!

Laut einer aktuellen Umfrage unter DiGA-Herstellern rechnen wir mit über 1.100 Produkt-Releases pro Jahr, die dem BSI gemeldet werden müssten. Diese Masse an Einzelmeldungen würde das BSI

Vorsitzender: Dr. Paul Hadrossek
Geschäftsführerin: Dr. Anne Sophie Geier

Spitzenverband Digitale
Gesundheitsversorgung e.V.
Pappelallee 78/79, 10437 Berlin

Telefon: +49 30 62 93 84 94
Fax: +49 30 62 93 84 96
E-mail: impressum@digitalversorgt.de

www.digitalversorgt.de

Vereinsregisternummer: VR 37693 B
Vereinsregister Berlin, Amtsgericht Charlottenburg

Bankverbindung apoBank
IBAN: DE88 3006 0601 0007 3667 91
BIC: DAAEDEDDXXX

personell stark fordern und wir haben Sorge, dass es hier zu einem absehbaren Bearbeitungsstau kommt. Bereits jetzt berichten Hersteller von erheblichen Wartezeiten auf Rückmeldungen. Dies konterkariert insbesondere die Notwendigkeit, Sicherheits-Updates schnell auszurollen. Aus unserer Sicht kann daher der Prozess nur als Meldung nach erfolgtem Release sinnvoll in der Praxis umgesetzt werden. Dies wäre auch im Einklang mit der MDR, die eine umgehende Behebung erkannter Sicherheitsmängel fordert.

Die geschilderten Umstände bringen eine hohe Unsicherheit bei der Planung und hohe finanzielle Belastungen mit sich. Um diesen Zustand zu verbessern, fordern wir, dass der Kriterienkatalog veröffentlicht wird. Zudem schlagen wir vor, dass nur sicherheitsrelevante Updates melde- und prüfpflichtig sind. Die Einschätzung der Relevanz soll auf Grundlage veröffentlichter, klar definierter Kriterien durch die Hersteller erfolgen. Alternativ könnte eine Meldepflicht für alle Updates in festen Intervallen (z. B. halbjährlich) erfolgen, sofern keine sicherheitskritischen Änderungen betroffen sind. Damit würde der Aufwand für Hersteller und BSI reduziert, ohne die Sicherheit der Anwendungen zu beeinträchtigen.

5. Unsere Vorschläge im Überblick

- Ein **Moratorium für die Zertifizierungspflicht bis zum 01.01.2026** basierend auf einer bis dahin **weiterentwickelten Richtlinie** für alle DiGA, die bereits gelistet sind und für alle neuen DiGA.
- Die **Einbindung der Hersteller und Prüfstellen in die zeitnahe Weiterentwicklung der Richtlinie**, um eine einheitliche Prüfpraxis sicherzustellen.
- Eine **kurzfristige Veröffentlichung eines Leitfadens**, der offene Interpretationsfragen verbindlich klärt.
- Ein **klar definiertes Verfahren für Produktupdates**, das auf Herstellerverantwortung, standardisierten und transparenten Bewertungskriterien und definierten Antwortzeiten durch das BSI basiert und die Prozesskosten senkt.

Wir unterstützen das Ziel, Datensicherheit im Gesundheitswesen auf höchstem Niveau zu gewährleisten. Dazu braucht es jedoch ein Verfahren, das mit den regulatorischen Anforderungen, der Produktrealität und den medizinischen Notwendigkeiten kompatibel ist. Wir bitten um einen

gemeinsamen Termin zum weiteren Dialog und stehen für eine konstruktive Zusammenarbeit jederzeit zur Verfügung.

Vorsitzender: Dr. Paul Hadrossek
Geschäftsführerin: Dr. Anne Sophie Geier

Spitzenverband Digitale
Gesundheitsversorgung e.V.
Pappelallee 78/79, 10437 Berlin

Telefon: +49 30 62 93 84 94
Fax: +49 30 62 93 84 96
E-mail: impressum@digitalversorgt.de

www.digitalversorgt.de

Vereinsregisternummer: VR 37693 B
Vereinsregister Berlin, Amtsgericht Charlottenburg

Bankverbindung apoBank
IBAN: DE88 3006 0601 0007 3667 91
BIC: DAAEDEDDXXX