DEUTSCHE KRANKENHAUS GESELLSCHAFT

Stellungnahme

zum Referentenentwurf
des Bundesministeriums für Gesundheit

für eine

C5-Äquivalenz-Verordnung

FAIR

Diskutieren, entscheiden, handeln.

Zusammenfassung

Die Deutsche Krankenhausgesellschaft begrüßt die Öffnung der Vorgaben des § 393 SGB V, indem der Nachweis der Einhaltung eines zu einem Typ1-Testat gleichwertigen Sicherheitsniveaus über die Testierung oder Zertifizierung alternativer Sicherheitsstandards ermöglicht wird. Die vorgesehene Umsetzung der vergleichbaren Anforderungen ist jedoch überaus komplex, sodass im Ergebnis die Zielsetzung der Verordnung, den Nachweis zu vereinfachen, verfehlt wird. Vor diesem Hintergrund werden im Folgenden Anpassungen vorgeschlagen, um für Anbieter von Cloud-Computing-Diensten sowie für Krankenhäuser handhabbare Vorgaben zu erhalten.

Allgemeine Bewertung

Mittelbar entwickelt sich der § 393 SGB V zu einem Instrument, das bei Verabschiedung des NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes mit erheblichen Strafzahlungen versehen sein wird, wenn die Vorgaben für C5-Testate nicht vollständig eingehalten werden. Klarheit, wie die Anforderungen des § 393 SGB V dauerhaft umgesetzt werden können, sind daher von großer Bedeutung auch für die Krankenhäuser.

Alternative Nachweismöglichkeiten werden begrüßt

Die Krankenhäuser befürworten die Möglichkeit, den Nachweis der Einhaltung eines zu einem C5-Testat gleichwertigen Sicherheitsniveaus durch eine Testierung oder Zertifizierung nach der C5-Äquivalenz-Verordnung erbringen zu können.

Verordnungsermächtigung gemäß § 393 Absatz 4 SGB V ausschöpfen

Der Gesetzgeber hat mit § 393 Absatz 4 SGB V das BMG ermächtigt, durch Rechtsverordnung Anforderungsstandards festzulegen. Der vorliegende Verordnungsentwurf schöpft diesen gesetzlichen Spielraum nicht vollständig aus, da Standards festgelegt werden, die lediglich übergangsweise und lediglich bezogen auf einzelne Maßnahmen ein im Vergleich zum C5-Standard vergleichbares oder höheres Sicherheitsniveau sicherstellen. Die Krankenhäuser sehen in diesen Beschränkungen kein zielführendes Vorgehen im Sinne einer langfristig handhabbaren Umsetzung. Daher sollte der Gesetzgeber der Verordnungsermächtigung folgen und im Verordnungsentwurf § 1 Absatz 2 sowie den Verweis auf Absatz 2 in Absatz 1 streichen.

Vorgaben an Auftraggeber/ Auftragnehmer-Verhältnis anpassen

Der Verordnungsentwurf zählt in § 1 äquivalente Standards auf und definiert dazu ergänzende Maßnahmen, die auf die Erstellung eines Maßnahmenplans abzielen, der u. a. für den Auftraggeber bereitgehalten werden soll. Es bleibt unklar, wie Auftraggeber einen Maßnahmenplan zu vertraglich bereits vereinbarten Maßnahmen handhaben sollen. Daher ist im Verordnungsentwurf § 1 Absatz 3 sowie der Verweis auf Absatz 3 in Absatz 1 zu streichen.

Übergangsfristen für Bestandssysteme

Der Zeitraum seit Einführung des § 393 SGB V war nicht ausreichend, um Bestandssysteme auf Cloud-Anbieter umzustellen, die über C5-Testate verfügen. Den üblichen Vertragslaufzeiten in diesem Bereich folgend sollte ein Übergangszeitraum von zwei Jahren eingeführt werden, um jedem Krankenhaus die Erfüllung der Anforderungen aus § 393 SGB V zu ermöglichen. Anderenfalls führen die Regelungen zu den C5-Testaten zu neuen Haftungsfragen an Stelle einer Verbesserung der Cybersicherheit. Die derzeitigen Übergangsfristen nach § 1 Absatz 2 regeln lediglich Fälle, in denen Cloud-Anbieter die Erstellung eines C5-Testats anstreben und z. B. entsprechende Verhandlungen mit einem C5-Auditor beginnen.

Ergänzung von Äquivalenz-Regeln für C5-Typ2-Testate

Gemäß § 393 Absatz 4 SGB V gelten ab dem 1. Juli 2025 nur noch C5-Typ2-Testate als aktuelles C5-Testat. Der vorliegende Entwurf regelt nicht ausdrücklich, dass äquivalente Nachweise für C5-Typ1-Testate bei einer Testierung der Wirksamkeit von Maßnahmen für C5-Typ2-Testate weiterhin verwendet werden können. Diese Klarstellung sollte in der Verordnung vorgenommen werden. Auch sollte klargestellt werden, dass Zertifizierungen auf Grundlage der im Entwurf aufgeführten Sicherheitsstandards und vergleichbare Nachweise über die Wirksamkeit von Maßnahmen ausreichen, um nach dem 1. Juli 2025 ein zu einem C5-Typ2-Testat vergleichbares Sicherheitsniveau belegen zu können.

Weiterer gesetzlicher Handlungsbedarf

Gesundheitsdaten im Sinne von § 393 SGB V definieren

Bei Umsetzung der Anforderungen aus dem § 393 SGB V treten immer wieder Unsicherheiten auf, weil unterschiedliche Sozial- und Gesundheitsdaten in Art. 4 DSGVO einbezogen sind und damit bei Nutzung von Cloud-Diensten C5-Testate gefordert werden. Es sollte eine Klarstellung in § 393 SGB V ergänzt werden, die festlegt, dass die Cloud-Verarbeitung von anonymisierten und pseudonymisierten Sozial- und Gesundheitsdaten sowie von GKV-Routinedaten im Forschungskontext mit Personenbezug von den Beschränkungen der § 393 Absatz 3 Nummer 2 und 3 SGB V ausgenommen sind. Anderenfalls wird die Wirkung von Gesetzen, die den Forschungsstandort Deutschland stärken sollen (z. B. Bayerisches Universitätsklinikagesetz) ausgehebelt.

Cloud-Computing-Dienste für Medizinprodukte abgrenzen

Im Krankenhaus werden umfangreich Medizinprodukte eingesetzt, z. B. in der Bildgebung, die u. a. Updates über Cloud-Dienste eingespielt bekommen oder Wartungsdaten über Cloud-Dienste austauschen. Für den Betreiber ist nicht ohne Weiteres erkennbar, ob die dabei eingesetzten Cloud-Computing-Dienste den Regelungen des § 393 SGB V unterfallen oder nicht. Es ist eine Klarstellung zu ergänzen, die Hersteller von Medizinprodukten, die mit der Medical Device Regulation (MDR) auf EU-Ebene bereits umfangreich reguliert sind, von den zusätzlichen Auflagen des § 393 SGB V ausnimmt.

Alternative prüfende Stellen nicht ausschließen

Neben alternativen Sicherheitsstandards zu C5-Testaten, wie sie die C5-Äquivalenz-Verordnung einführt, sollten ebenso alternative Nachweisverfahren für C5-Testate ergänzt werden. An Stelle der Beschränkung auf Testate von Wirtschaftsprüfern sollte § 384 Satz 1 Ziffer 6 SGB V herangezogen werden, nach dem ein C5-Testat definiert ist als „das positive Prüfergebnis über einen sicheren Cloud-Computing-Dienst anhand des Kriterienkatalogs C5 (…)“. Weitere prüfende Stellen neben Wirtschaftsprüfern sollten nicht ausgeschlossen werden.

Klarstellung zu Eigenbetrieb von Cloudlösungen ergänzen

Es bestehen Unsicherheiten bei der Auslegung des § 393 SGB V in Bezug auf den Eigenbetrieb von Cloud-Lösungen. In § 384 Satz 1 Nummer 5 SGB V ist ein Cloud-Computing-Dienst als digitaler Dienst bezeichnet, der nicht von einem Eigenbetrieb abgegrenzt wird. Diese

Abgrenzung sollte in § 384 Satz 1 Nummer 5 SGB V ergänzt und damit vom Pflichtbereich der C5-Testate ausgenommen werden.

Klarstellung zu Institutionen im Gesundheitswesen ergänzen

Institutionen im Gesundheitswesen verarbeiten umfangreich personenbezogene Sozial- und Gesundheitsdaten, z. B. für die Erstellung der Qualitätsberichte. Diese Verarbeitung gehört nicht zu dem beabsichtigten Wirkbereich der C5-Testate und ist daher ausdrücklich von der Verpflichtung des § 393 SGB V auszunehmen.

Klarstellung zum Beschlagnahmeschutz der Cloud-Daten ergänzen

Nicht nur bei Cloud-Computing-Diensten, sondern z. B. auch bei der elektronischen Patientenakte gemäß § 341 SGB V spielt die Frage, ob die Daten vor einer Beschlagnahmung geschützt sind, für die Wahrung des Berufsgeheimnisses eine entscheidende Rolle. Im § 393 SGB V ist eine Klarstellung zu ergänzen, dass Betreiber von Cloud-Computing-Angeboten durch die Erfüllung der Kriterien aus dem Kriterienkatalog Cloud Computing nicht dazu angehalten werden, Behörden Zugriff auf Daten zu gewähren, die dem Berufsgeheimnis unterliegen oder auf die gemäß Auftragsverarbeitungsvertrag kein Zugriff gewährt werden darf.

Deutsche Krankenhausgesellschaft (DKG)

Bundesverband der Krankenhausträger
in der Bundesrepublik Deutschland

Wegelystraße 3
10623 Berlin

Tel. (030) 3 98 01-0
Fax (030) 3 98 01-3000
E-Mail dkgmail@dkgev.de

FAIR

DEUTSCHE KRANKENHAUS GESELLSCHAFT DKG