

bvitg-Stellungnahme zum Entwurf eines Krankenhausgesetzes für das Land Schleswig-Holstein – Landeskrankenhausgesetz – (LKHG)

Kontakt:
Chris Berger
Referent Politik
chris.berger@bvitg.de

www.bvitg.de

- Zu § 35 Allgemeine Bestimmungen, Begriffsbestimmungen
- Zu § 36 Datenverarbeitung im Krankenhaus
- Zu § 37 Datenverarbeitung im Auftrag
- Zu § 38 Verarbeiten von Patientendaten im Rahmen von Forschungsvorhaben
- Zu § 39 Auskunft und Akteneinsicht
- Zu § 40 Löschen von Patientendaten und Einschränkung der Verarbeitung
- Ergänzende Einschränkung von Betroffenenrechten



Die Landesregierung von Schleswig-Holstein möchte mit dem vorliegenden Gesetzesentwurf (Stand: 09.10.2019) das Landeskrankenhausgesetz um den Patientendatenschutz ergänzen. Die Einführung datenschutzrechtlicher Regelungen in das Landeskrankenhausgesetz begrüßt der bvitg, da somit auch die europarechtlichen Vorgaben der Datenschutz-Grundverordnung (DS-GVO) auf Landesebene konkretisiert und umgesetzt werden.

Der bvitg sieht am vorliegenden Gesetzesentwurf allerdings noch erheblichen Anpassungsbedarf, um eine innovative und vernetzte Versorgung zu ermöglichen und um einen Flickenteppich an Regulierungen zum Nachteil der Krankenhäuser zu verhindern.

An einigen Stellen fehlen Konkretisierungen und Klarstellungen von Verarbeitungsprozessen, die für Rechtsunsicherheit in der Verarbeitung mit Gesundheitsdaten führen. Die vorgesehenen Regelungen zur Speicherung von Patientendaten vor Ort in den Krankenhäusern sind eine nicht nachvollziehbare Einschränkung von innovativen Diensten. Eine umfassende Auskunftspflicht zum physischen Speicherort von Akten und Daten steht einer vernetzten Versorgung diametral entgegen. Bei den Ausführungen zur Auftragsverarbeitung sollte die Vernetzung der Gesundheitsversorgung nicht unnötig behindert werden. Ebenfalls sollte die Forderung nach Schriftform bei der Einwilligung angepasst werden. Im Sinne einer praxis- und zukunftsorientierten Datenschutzregelung sollte eine elektronische Einwilligung, die ggf. auch schriftlich erfolgen kann, im vorliegenden Gesetzestext ergänzt werden. Auf Bundesebene ist dies durch das Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz EU (2. DSAnpUG-EU) bereits geschehen.

Um die Forschung und Versorgungsforschung der Krankenhäuser in Schleswig-Holstein gegenüber anderen Bundesländern nicht zu benachteiligen, empfiehlt der Verband die Aufnahme zusätzlicher Tatbestände zur Aufnahme und Durchführung von medizinischer Forschung.

Der bvitg als Vertretung der IT-Anbieter im Gesundheitswesen bedankt sich für die Gelegenheit zur Kommentierung des Entwurfes und nimmt zum LKHG wie folgt Stellung:

Zu § 35 Allgemeine Bestimmungen, Begriffsbestimmungen

Im vorliegenden Gesetzesentwurf der Landesregierung wird u.a. in §36 Abs. 1 oder § 38 Abs. 2 auf die Nutzung von „anonymisierten Daten“ verwiesen, allerdings ohne eine Konkretisierung und rechtliche Klarstellung der Frage, ab wann Patientendaten als anonymisiert einzustufen sind. Die daraus resultierende Rechtsunsicherheit für die Verarbeitung von Gesundheitsdaten für Auftragsverarbeiter und Krankenhäuser ist nicht zielführend für eine innovative Nutzung von Daten.

Da § 35 Begriffsbestimmungen zur Datenschutz-Grundverordnung (DS-GVO) enthält, empfiehlt der Verband eine ergänzende Definition zur Anonymisierung in Anlehnung an § 12 Abs. 3 S. 4 Hamburgisches Krankenhausgesetz durch den Gesetzgeber, um Rechtssicherheit herzustellen:

Gesetzesentwurf der Landesregierung	Neufassung
<p>[...] (2) Patientendaten im Sinne dieses Gesetzes sind Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter und bestimmbarer Patientinnen und Patienten eines Krankenhauses. Als Patientendaten gelten auch personenbezogene Daten von Angehörigen oder anderen Bezugspersonen der Patientinnen und Patienten sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit einer Behandlung bekannt werden. Als Krankenhäuser im Sinne dieses Teils gelten auch stationäre und teilstationäre Einrichtungen der medizinischen Rehabilitation</p>	<p>(2) Patientendaten im Sinne dieses Gesetzes sind Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter und bestimmbarer Patientinnen und Patienten eines Krankenhauses. Als Patientendaten gelten auch personenbezogene Daten von Angehörigen oder anderen Bezugspersonen der Patientinnen und Patienten sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit einer Behandlung bekannt werden. Als Krankenhäuser im Sinne dieses Teils gelten auch stationäre und teilstationäre Einrichtungen der medizinischen Rehabilitation.</p> <p>(3) Personenbezogenen Daten sind anonym, wenn sie keine personenbezogenen Daten im Sinne der Verordnung (EU) 2016/679 darstellen.</p> <p>(4) Anonymisierung ist die Verarbeitung von personenbezogenen Daten, sodass nach der Verarbeitung Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr einer identifizierten oder identifizierbaren natürlichen Person zugeordnet werden können.</p>

Zu § 36 Datenverarbeitung im Krankenhaus

In Absatz 1 listet der Gesetzgeber verschiedene Zwecke auf, bei denen Patientendaten verarbeitet werden dürfen. Aus Sicht des bvityg sollte Absatz 1 um eine Klarstellung ergänzt werden, dass zu diesen Zwecken eine Verarbeitung von Daten auch ohne Einwilligung der Patienten erfolgen darf, da diese entweder für abrechnungsrelevante Sachverhalte benötigt werden oder zur Wahrung der Patientensicherheit vorgeschrieben sind.

Gesetzesentwurf der Landesregierung	Neufassung
<p>[...] (1) Patientendaten dürfen auch verarbeitet werden, soweit dies durch eine andere Rechtsvorschrift zugelassen ist oder soweit dies erforderlich ist.</p>	<p>[...] (1) Patientendaten dürfen ohne Einwilligung der betroffenen Personen auch verarbeitet werden, soweit dies durch eine andere Rechtsvorschrift zugelassen ist oder soweit dies erforderlich ist.</p>

Laut aktueller Rechtslage gibt es über die in §36 Absatz 1 genannten Tatbestände hinaus Fälle die eine Verarbeitung von Patientendaten erlauben. Das Arzneimittelgesetz und die Medical Device Regulation (MDR) verpflichten zum Beispiel Hersteller von Medikamenten oder Medizinprodukten zur Marktbeobachtung, insbesondere auch hinsichtlich von auftretenden Nebenwirkungen. Eine entsprechende Rechtsgrundlage zur Weitergabe der Informationen in diesem Kontext durch das medizinische Personal im klinischen Umfeld an die Hersteller existiert nicht. Aus Sicht des Verbandes ist eine Ergänzung auf Landesebene eine sinnvolle Maßnahme zur Wahrung der Patientensicherheit und Weiterentwicklung der Medizinprodukte.

Zur Weiterentwicklung der Versorgungsforschung sollten Krankenhäuser für Forschungszwecke die Möglichkeit erhalten, entlassene Patienten zu kontaktieren und zu informieren. Besonders chronisch erkrankte Patienten haben ein hohes Interesse daran, sich an Forschungsvorhaben zur Verbesserung ihrer Behandlung zu beteiligen. Eine Ergänzung um diesen Tatbestand im vorliegenden Gesetzentwurf liegt somit sowohl im Interesse der Patienten als auch der forschenden Institutionen.

Teile von Krankenhäusern werden häufig über Spenden finanziert, wie zum Beispiel Kinderhospize oder Kinderonkologien. Eine Rechtsgrundlage zur Kontaktaufnahme mit ehemaligen Patienten bezüglich Spendenaufrufen für die Krankenhäuser sichert somit weiterhin die Finanzierungsgrundlage dieser Einrichtungen.

Der bvitg empfiehlt vor diesem Hintergrund den Absatz 1, § 36 um folgende Tatbestände zur Verarbeitung von Patientendaten zu ergänzen:

Gesetzentwurf der Landesregierung	Neufassung
<p>[...] 13. zur Aus-, Fort- und Weiterbildung,</p>	<p>[...] 13. zur Aus-, Fort- und Weiterbildung, 14. zur Information entlassener Patienten hinsichtlich neuer Erkenntnisse bezüglich ihrer Erkrankungen, 15. zur Information entlassener Patienten bezüglich ihrer Erkrankung betreffende Forschungsvorhaben des Krankenhauses verbunden mit der Möglichkeit, diese Forschungsvorhaben gegebenenfalls durch Teilnahme zu unterstützen, 16. zur Information entlassener Patienten über Spendenaufrufe des Krankenhauses,</p>

Das im Bundestag in 2./3. Lesung verabschiedete Gesetz für bessere und unabhängige Prüfungen (MDK-Reformgesetz) sieht eine Änderung im § 17c KHG vor, die Krankenhäuser ab dem 01. Januar 2020 verpflichtet, eine einzel-fallbezogene Erörterung mit den Krankenkassen vor Klageerhebung durchzuführen. Nach § 17c Abs. 2b S. 3 KHG dürfen Krankenhäuser zur Erörterung der Rechtmäßigkeit von Abrechnungen im erforderlichen Umfang Patientendaten verarbeiten, jedoch müssen in diesem Zuge den Krankenkassen ebenfalls Patientendaten zur Verfügung gestellt werden.

Die aktuelle Begriffsbestimmung der DS-GVO zur „Verarbeitung“ ist zwar gesetzlich weit gefasst, allerdings wäre in diesem Zuge eine Klarstellung der Landesregierung aus Gründen der Rechtssicherheit wünschenswert.

Folglich sollte Absatz 1 §36 mit einem Satz 2 wie folgt ergänzt werden:

Gesetzentwurf der Landesregierung	Neufassung
<p>[...] soweit diese Zwecke mit anonymisierten oder pseudonymisierten Daten nicht erreicht werden können und im Einzelfall überwiegende schutzwürdige Interessen der Betroffenen nicht entgegenstehen.</p>	<p>[...] soweit diese Zwecke mit anonymisierten oder pseudonymisierten Daten nicht erreicht werden können und im Einzelfall überwiegende schutzwürdige Interessen der Betroffenen nicht entgegenstehen. Patientendaten dürfen an Dritte weitergegeben werden, soweit dies erforderlich ist: (a) zur Klärung der Rechtmäßigkeit der Abrechnung erbrachter Leistungen der Patientenversorgung sowie zur Durchführung entsprechender Erörterungen mit den dafür zuständigen Leistungsträgern, (b) zur Übermittlung von beobachteten Nebenwirkungen beim Einsatz von Arzneimitteln oder Medizinprodukten an die jeweiligen Hersteller in anonymisierter Form.</p>

§ 36 Abs. 1 Ziff. 10 LKHG erlaubt die Nutzung von Patientendaten des Krankenhauses auch zu statistischen Zwecken. Viele Analysen und Statistiken können auch ohne jeden konkreten Personenbezug vorgenommen werden. Bereits heute nutzen medizinische Fachgesellschaften dieses Vorgehen für eine spezifische Darstellung der Versorgungsqualität, z. B. im Rahmen der onkologischen Behandlung oder bei der Notfallversorgung. Nach herrschender Meinung stellt eine Anonymisierung aber spätestens mit der sehr weiten Darstellung nach Art. 4 Ziff. 2 DS-GVO einen Verarbeitungsprozess dar, der einen Erlaubnistatbestand voraussetzt. Der vorliegende Gesetzestext sollte deshalb um einen entsprechenden Erlaubnistatbestand ergänzt werden, sodass Krankenhäuser ihre Patientendaten für statistische Zwecke anonymisieren dürfen.

Laut Empfehlungen der Datenschutzkonferenz zieht die Pseudonymisierung von Patientendaten die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung aufgrund des hohen Risikos mit sich. Dementsprechend muss das Krankenhaus den Nachweis bezüglich der Anonymität der Daten erbringen.

Folgende Ergänzungen des § 36 LKHG werden deshalb aus Sicht des bvitg empfohlen:

Gesetzentwurf der Landesregierung	Neufassung
<p>[...]</p>	<p>[...] (1a) Krankenhäuser dürfen Patientendaten ohne Einwilligung der jeweiligen Patienten anonymisieren und diese anonymisierten Daten für andere Zwecke verwenden. Das Krankenhaus muss einen Nachweis über die Anonymität der Daten führen.</p>

Die in § 36 Abs. 2 geforderte Schriftformerfordernis bei der Einwilligung ist vor dem Hintergrund der Anpassungen aller bereichsspezifischen Gesetze durch das Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz EU (2. DSAn-pUG-EU) nicht nachvollziehbar. Im Zuge der voranschreitenden Digitalisierung des Gesundheitssystems besteht deshalb aus Sicht des bvitg redaktioneller Anpassungsbedarf, um neben einer schriftlichen Einwilligung zusätzlich die elektronische Übermittlung des Einverständnisses der Versicherten zu ermöglichen. Um das Effizienzpotenzial der Digitalisierung in der Versorgung zu nutzen, gilt es von daher grundsätzlich zu prüfen, welche Dokumentationsprozesse digital abgewickelt werden können. Die Nutzung der elektronischen und nicht schriftlichen Form muss im vorliegenden Gesetz dringend ergänzt werden:

Gesetzentwurf der Landesregierung	Neufassung
<p>[...] (2) Die Einwilligung der Patientin oder des Patienten in die Verarbeitung von Daten im Sinne des Artikels 9 Absatz 1 der Datenschutz-Grundverordnung in der Geltung seit dem 25. Mai 2018 Verordnung Nr. 2016/679 des Europäischen Parlaments und Rates vom 27.04.2016 (Amtsblatt L 119 vom 4.5.2016 S. 1 ber. Amtsblatt L 314 vom 22.11.2016, S 7, Amtsblatt L 127 vom 23.5.2018 S. 2), bedarf grundsätzlich der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Wird die Einwilligung mündlich erteilt, ist sie aufzuzeichnen. Die Patientin oder der Patient ist über Art, Umfang und Zweck der beabsichtigten Verarbeitung zu unterrichten und aufzuklären.</p>	<p>[...] (2) Die Einwilligung der Patientin oder des Patienten in die Verarbeitung von Daten im Sinne des Artikels 9 Absatz 1 der Datenschutz-Grundverordnung in der Geltung seit dem 25. Mai 2018 Verordnung Nr. 2016/679 des Europäischen Parlaments und Rates vom 27.04.2016 (Amtsblatt L 119 vom 4.5.2016 S. 1 ber. Amtsblatt L 314 vom 22.11.2016, S 7, Amtsblatt L 127 vom 23.5.2018 S. 2), erfolgt grundsätzlich schriftlich oder elektronisch bedarf grundsätzlich der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Wird die Einwilligung mündlich erteilt, ist sie aufzuzeichnen. Die Patientin oder der Patient ist über Art, Umfang und Zweck der beabsichtigten Verarbeitung zu unterrichten und aufzuklären.</p>

Zu § 37 Datenverarbeitung im Auftrag

Die in § 37 Absatz 1 genannte grundsätzliche Begrenzung der Datenverarbeitung der Patientendaten auf die Krankenhäuser, ist aus Sicht des bvitg kritisch zu betrachten. Die intelligente Verarbeitung von Forschungs- und Gesundheitsdaten sowohl innerhalb als auch außerhalb der Krankenhäuser bietet enorme Chancen für die Verbesserung der Patientenversorgung und Steigerung der Effizienzen im Gesundheitssystem. Das Ziel sollte eine Harmonisierung der diversen Regelungen für eine sichere Vernetzung und vertrauenswürdige Nutzung von Daten sein. Dies würde z.B. die klinische Forschung und die translationale Medizin in Deutschland entscheidend stärken. Von einer Standortbegrenzung gilt es daher grundsätzlich abzusehen.

Die medizinische Versorgung im klinischen Kontext findet primär im Krankenhaus statt, allerdings gibt es viele Situationen, in denen eine elektronische Verarbeitung der Patientendaten nicht im Krankenhaus erfolgen muss oder kann. Die in § 37 Abs. 2 S.2 LKHG genannten Ausnahmen sind nur drei der vielen Beispiele, stellen aber keine abschließende Betrachtung dar.

Eine externe Speicherung der Patientendaten kann in vielen Fällen eine höhere IT-Sicherheit gewährleisten als eine Speicherung vor Ort. Professionelle Rechenzentrumsanbieter haben im Vergleich zu einem Krankenhaus eine Vielzahl an technischen und organisatorischen Maßnahmen, um IT-Sicherheit zu gewährleisten. Externe Zertifizierung und Auditierung sowie nachweislich geprüfte Sicherheitsmaßnahmen, wie z.B. nach der ISO Norm 27001 oder DIN EN 50600-x, gewährleisten einen hohen Schutz von Patientendaten. Ein 24-Stunden-Support durch entsprechend qualifizierte und auf dem aktuellen Stand der Technik geschulte Mitarbeiter ist ein weiterer Vorzug, der nicht wesent-

licher Bestandteil einer allgemeinen Krankenhaus-IT-Infrastruktur ist.

Die Datenverarbeitung durch externe Dienstleister kann in Einzelfällen kostenintensiver als die Vor-Ort Verarbeitung sein. Aufgrund der hohen Schutzwürdigkeit der in Art. 9 Abs. 1 DS-GVO genannten Daten, sollte dies allerdings kein Ausschlusskriterium für eine externe Datenverarbeitung sein.

Gesetzentwurf der Landesregierung	Neufassung
<p>[...]</p> <p>(1) Patientendaten sind grundsätzlich im Krankenhaus zu verarbeiten. Das Krankenhaus kann sich zur Verarbeitung von Patientendaten anderer Personen oder Stellen bedienen, wenn</p> <ol style="list-style-type: none"> 1. Störungen im Betriebsablauf sonst nicht vermieden werden können, 2. die Datenverarbeitung dadurch erheblich kostengünstiger gestaltet werden kann oder 3. das Krankenhaus seinen Betrieb einstellt 	<p>[...]</p> <p>(1) Patientendaten sind grundsätzlich im Krankenhaus zu verarbeiten. Das Krankenhaus kann sich zur Verarbeitung von Patientendaten anderer Personen oder Stellen bedienen, wenn dies für eine optimierte Patientenversorgung, aus wirtschaftlichen Gründen oder zur Etablierung eines hohen Niveaus der IT-Sicherheit, erforderlich erscheint. Das Sicherheitsniveau muss bei einer Verarbeitung von Patientendaten durch andere Personen oder Stellen mindestens dem Standard des Krankenhauses selbst entsprechen, die in § 22 Absatz 2 des Bundesdatenschutzgesetzes genannten Anforderungen müssen von eingesetzten Dienstleistern erfüllt sowie deren Erfüllung bei Bedarf nachgewiesen werden.</p> <ol style="list-style-type: none"> 1. Störungen im Betriebsablauf sonst nicht vermieden werden können, 2. die Datenverarbeitung dadurch erheblich kostengünstiger gestaltet werden kann oder 3. das Krankenhaus seinen Betrieb einstellt.

§ 37 Abs. 2 im vorliegenden Gesetzentwurf verlangt eine Anonymisierung bei einer Datenverarbeitung im Auftrag. Erwägungsgrund 26 der DS-GVO sieht allerdings eine klare Begrenzung der Anwendbarkeit datenschutzrechtlicher Vorgaben auf anonymisierte Daten vor. Eine Auftragsverarbeitung im Sinne der DS-GVO liegt nur vor, sofern mit personenbezogenen Daten und nicht mit anonymisierten Daten gearbeitet wird. Die Zielstellung der vorliegenden Formulierung in § 37 Abs. 2 LKHG ist dem Verband nicht eindeutig ersichtlich und vor dem Hintergrund der Vorgaben der DS-GVO nicht nachvollziehbar. Nach Auffassung des bviti ist die vorliegende Regelung aus rechtlicher Sicht deshalb nicht haltbar.

Während bei einem Update eines eingesetzten Datenbankmanagementsystems durch den Dienstleister keine personenbezogenen Daten verarbeitet werden, benötigen Systemhersteller im Supportfall in Krankenhäuser Zugriff auf personenbezogene Daten, um die Zuordnung der Patientendaten zu ermöglichen. In diesen Fällen können weder pseudonymisierte, noch anonymisierte Patientendaten genutzt werden. Dies ist weder praxistauglich noch rechtlich erforderlich.

Beauftragt ein Krankenhaus z.B. einen externen Scandienstleister zur systematischen Erfassung von analogen Patientenakten bedingt dies den uneingeschränkten Zugriff auf die personenbezogenen Patientendaten, sonst kann keine sinnvolle Zuordnung der Patientendaten im Anschluss der Digitalisierung erfolgen. Eine anonyme pseudonyme Auftragsverarbeitung von Patientendaten ist unmöglich. Eine pseudonyme Verarbeitung ist in den meisten Fällen nicht ohne eine Gefährdung des Patientenwohls durchführbar.

Artikel 5 Abs. 1 lit. b DS-GVO erlaubt nur die Nutzung erforderlicher personenbezogenen Daten. Die Anforderungen in § 37 Abs. 2 S. 1 LKHG sind somit überflüssig, da diese bereits ausreichend in der DS-GVO geregelt sind.

Art. 32 Abs. 1 DS-GVO verlangt die Ergreifung geeigneter technischer und organisatorischer Maßnahmen (TOMS), um ein dem Risiko angemessenes Schutzniveau bei der Verarbeitung von personenbezogenen Daten zu gewährleisten. Da TOMS Maßnahmen wie die Pseudonymisierung als Anforderung einschließt, ist die Anforderung im vorliegende Gesetzesentwurf nach § 37 Absatz 1 Satz 2 zur expliziten Pseudonymisierung ebenfalls redundant.

Der Verband empfiehlt die komplette Streichung des § 37 Abs. 2 LKHG oder schlägt alternativ folgende Anpassung vor:

Gesetzesentwurf der Landesregierung	Neufassung
<p>[...] (2) Dem Auftragsverarbeiter dürfen Patientendaten nur offenbart werden, soweit dies für die Auftrags- erfüllung erforderlich ist. Der Krankenhausträger hat, soweit dies für den Auftragszweck ausreichend ist, dem Auftragsverarbeiter anonymisierte Daten zur Verfügung zu stellen; ist eine Anonymisierung nicht möglich, müssen die Daten pseudonymisiert werden.</p>	<p>[...] (2) Dem Auftragsverarbeiter dürfen Patientendaten nur offenbart werden, soweit dies für die Auftrags- erfüllung erforderlich ist. Der Krankenhausträger hat, soweit dies für den Auftragszweck ausreichend ist und die Patientenversorgung nicht unangemes- sen beeinträchtigt und insbesondere das Patien- tenwohl nicht gefährdet, dem Auftragsverarbeiter pseudonymisierte anonymisierte Daten zur Ver- fügung zu stellen; ist eine Anonymisierung nicht möglich, müssen die Daten pseudonymisiert wer- den.</p>

Absatz 3 § 37 LKHG begrenzt den physikalischen Speicherort auf Standorte innerhalb der Europäischen Union. Auch hier ist die Zielstellung des Gesetzgebers unklar, da eine derartige Anforderung nicht vor den Zugriff von Dritten außerhalb der EU schützt. So könnte in Zukunft der Clarifying Lawful Overseas Use of Data Act in Fällen mit strafrechtlicher Relevanz einen Zugriff von U.S. Strafverfolgungsbehörden auf Cloud-Daten von US-amerikanischen Firmen ermöglichen. Sollte die Zielsetzung der Gesetzgebung eine Beschränkung des Zugriffs ausländischer Strafverfolgungsbehörden auf die in der EU gespeicherten Daten sein, so ist diese Regel unwirksam. Die vorliegende Formulierung in § 37 Absatz 3 LKHG ist deshalb aus Sicht des bvitg irrelevant, da diese zu keiner Steigerung der Sicherheit der Patientendaten beiträgt und somit gestrichen werden sollte.

Artikel § 37 Abs. 3 LKHG schreibt eine Auskunftspflicht von Auftragsverarbeitern gegenüber den Krankenhäusern zum physikalischen Ort der Speicherung vor. Zielstellung des Landesgesetzgebers laut Gesetzesbegründung ist es Cloud-Services und Cloud-Computing Dienste zu unterbinden.

Diese Forderung ist im Zuge der voranschreitenden Digitalisierung und Nutzung von innovativen Diensten zur Speicherung von Patientendaten nicht nachvollziehbar.

Neben der Sinnhaftigkeit dieser Regelung ist die praktische Umsetzung ebenfalls schwierig. Anbieter von Rechenzentren betreiben aus Gründen der IT-Sicherheit und Praktikabilität in mehreren Städten gesicherte Rechenzentren. So wird sichergestellt, dass bei einem Ausfall eines Standortes die Integrität und Funktionalität anderer Speicherorte gewährleistet ist. So können Patientendaten von einem Krankenhaus in mehreren Rechenzentren liegen. Die Speicherung an mehreren Standorten ermöglicht eine geringe Latenzzeit und hohe Verfügbarkeit der Patientendaten.

Der bvitg empfiehlt somit die Streichung des letzten Satzes in Absatz 3 § 37 LKHG wie folgt:

Gesetzentwurf der Landesregierung	Neufassung
[...]	[...] (3) Im Falle der elektronischen Datenverarbeitung durch den Auftragsverarbeiter hat der Krankenhaussträger sicherzustellen, dass sich der Ort der physikalischen Speicherung innerhalb der Europäischen Union befindet und der Auftragsverarbeiter dem Krankenhaussträger jederzeit genaue Auskunft über den Ort beziehungsweise die Orte der physikalischen Speicherung geben kann.

Zu § 38 Verarbeiten von Patientendaten im Rahmen von Forschungsvorhaben

In § 38 LKHG fehlt die Privilegierung der Eigenforschung, die bereits in allen Landesgesetzen vorhanden ist. Bei der Forschung mit den im eigenen Krankenhaus erhobenen Patientendaten entstehen für Patienten aus datenschutzrechtlicher Sicht keine neuen Gefahren. Berechtigte forschende Institutionen unterliegen sowohl der Geheimhaltung des Datenschutzes als auch der Verpflichtung zur Nicht-Offenbarung von Patientengeheimnissen nach § 203 StGB.

Um forschende Krankenhäuser in Schleswig-Holstein nicht zu benachteiligen und eine Harmonisierung der landesdatenschutzrechtlichen Anforderungen voranzutreiben, empfiehlt der bvity die Ergänzung des Absatzes 1 § 38 um einen Absatz 1a, in Anlehnung an bereits bestehende Landesgesetze:

Gesetzentwurf der Landesregierung	Neufassung
[...]	[...] (1a) Ergänzend zu den Vorschriften der Verordnung (EU) 2016/679 darf ein Krankenhaus oder eine Krankenhausgruppe die dort im Zusammenhang mit der Behandlung der Patientin oder des Patienten erhobenen Patientendaten ohne Einwilligung für eigene wissenschaftliche Forschung weiterverarbeiten und -sammeln, und zwar auch dann, wenn das Krankenhaus diese Patientendaten zuvor für wissenschaftliche Forschungszwecke an Dritte weitergegeben hat und sie dort erneut erhebt. Darüber hinaus darf ein Krankenhaus besondere Kategorien personenbezogener Daten ohne Einwilligung für wissenschaftliche Forschung dann verarbeiten und sammeln, wenn die Verarbeitung und Sammlung zu diesem Zweck erforderlich ist und das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schützenswerten Interessen der betroffenen Person überwiegt. Sätze 1 und 2 gelten auch für das Verarbeiten und Sammeln von Proben zu wissenschaftlichen Forschungszwecken und für die Übernahme bereits vorhandener Proben. Einer Einwilligung bedarf es auch dann nicht, wenn die behandelnde Krankenhauseinheit die Patientendaten und die zu Behandlungszwecken aufbewahrten Proben vor der Weitergabe zu einer Sammlung anonymisiert. Dies gilt auch für Proben, die bei klinischen und rechtsmedizinischen Sektionen entnommen wurden. § 22 Absatz 2 des Bundesdatenschutzgesetzes gilt entsprechend.

Der bviti empfiehlt in diesem Zuge die Ergänzung des Absatzes 1 § 38 um einen Absatz 1b zur Schaffung einer Rechtsgrundlage für eine Zusammenarbeit mit „Dritten“ im Rahmen von Forschungsvorhaben, um Kooperationen mit Institutionen, wie dem KI-Institut, zu ermöglichen.

Im Bereich der medizinischen Forschung arbeiten Krankenhäuser oft mit privaten Forschungseinrichtungen, zum Beispiel der Fraunhofer-Gesellschaft, der Helmholtz-Gemeinschaft, der Leibniz-Gemeinschaft oder der Max-Planck-Gesellschaft zusammen. Da es im Datenschutzrecht kein Konzernprivileg gibt, zählen auch Universitäten oder An-Institute einer Universitätsklinik als datenschutzrechtliche „Dritte“. Eine Kooperation mit Instituten, wie dem Institut für Künstliche Intelligenz in der Medizin der Universität Duisburg Essen, wäre somit aus datenschutzrechtlicher Perspektive eine Zusammenarbeit mit „Dritten“ und nur unter erschwerten Bedingungen für das Krankenhaus durchführbar.

Folgende Ergänzungen zum Absatz 1 § 38 schlägt der bviti vor:

Gesetzentwurf der Landesregierung	Neufassung
[...]	[...] (1b) Eine Weitergabe von Patientendaten zu Forschungszwecken an Dritte ist grundsätzlich nur anonymisiert zulässig. Erfordert der Zweck der Forschung die Möglichkeit einer Zuordnung, ist die Weitergabe von pseudonymisierten Patientendaten statthaft, wenn die Merkmale, mit denen ein Personenbezug hergestellt werden kann, ausschließlich im Krankenhaus gespeichert werden und dort nur den unter § 203 Absatz 1 des Strafgesetzbuches genannten Personenkreisen zugänglich sind. Werden Patientendaten in pseudonymisierter Form an Dritte zu Forschungszwecken übermittelt, so müssen die Patienten über die Empfänger informiert werden, ausgenommen ein Ausnahmetatbestand gemäß Artikel 14 Absatz 5 der Verordnung (EU) Nr. 2016/679 liegt vor.

Die Wahrnehmung von Betroffenenrechten kann in einigen Forschungsvorhaben die Erreichung des Forschungszieles verhindern. Beispielsweise kann in einer Doppel-Blind-Studie den Probanden keine Auskunft gegeben werden, ob das zu testende Medikament oder ein anderes Produkt verabreicht wurde, ohne die Studie ad absurdum zu führen. Betroffenenrechte sollten in diesen Fällen in Anlehnung an § 22 Abs. 2 BDSG eingeschränkt werden:

Gesetzentwurf der Landesregierung	Neufassung
[...]	[...] <p>(5) Die in den Artikeln 15, 16 18 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte der betroffenen Person können beschränkt werden, wenn diese Rechte voraussichtlich die Verwirklichung der Forschungszwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der Forschungszwecke notwendig ist. Die Gründe für die Beschränkung sind der zuständigen Aufsichtsbehörde mitzuteilen, welche dann unter Abwägung der Betroffenenrechte eine Entscheidung hinsichtlich der gewünschten der Beschränkung trifft. Die Entscheidung sowie die Gründe für die Entscheidung werden von der Aufsichtsbehörde schriftlich festgehalten und der beantragenden Forschungsstelle bekanntgegeben.</p>

In § 38 Abs. 4 wird auf § 36 Abs. 4,5 LKHG verwiesen („gilt § 36 Absatz 4 und 5 entsprechend“), jedoch beinhaltet § 36 LKHG keine Absätze 4 und 5. Der Verband bittet hier um eine Klarstellung.

Zu § 39 Auskunft und Akteneinsicht

§ 39 Absatz 1 adressiert die Auskunfts- und Einsichtsansprüche medizinischer Daten nach Art. 15 DS-GVO. Laut vorliegendem Gesetzentwurf soll die Aushändigung der Daten nur durch eine Ärztin/Arzt, Psychotherapeutin/Psychotherapeut oder Krankenkasse erfolgen.

Der Auskunftsanspruch nach Art. 15 Abs. 3 DS-GVO erstreckt sich lediglich auf die Kopie der Patientendaten, nicht die Einsichtnahme vor Ort. Die Aushändigung auf die oben genannten Leistungserbringer bzw. Leistungsträger zu begrenzen, erscheint vor diesem Hintergrund nicht praxistauglich.

Folgende Anpassungen werden empfohlen:

Gesetzentwurf der Landesregierung	Neufassung
[...] <p>(1) Soweit die Auskunfts- und Einsichtsansprüche medizinische Daten betreffen, sollen sie durch eine Ärztin oder einen Arzt oder eine Psychotherapeutin oder einen Psychotherapeuten des Krankenhauses erfüllt werden.</p>	[...] <p>(1) Soweit die Auskunfts- und Einsichtsansprüche medizinische Daten betreffen, sollen sie durch eine Ärztin oder einen Arzt oder eine Psychotherapeutin oder einen Psychotherapeuten des Krankenhauses erfüllt werden, sofern therapeutische Gründe dies erfordern.</p>

§ 39 Abs. 3 LKHG sieht die Einsichtnahme in Patientenunterlagen durch Dritte vor. Patientendaten stehen auch unter dem Offenbarungsverbot von § 203 StGB, daher bedarf der Gesetzestext folgender Anpassungen:

Gesetzentwurf der Landesregierung	Neufassung
<p>[...]</p> <p>(3) Die Absätze 1 und 2 gelten entsprechend, soweit Dritte Auskunft über die zu ihrer Person gespeicherten Daten verlangen und schutzwürdige Belange der Patientinnen und Patienten nicht entgegenstehen.</p>	<p>[...]</p> <p>(3) Die Absätze 1 und 2 gelten entsprechend, soweit Dritte Auskunft über die zu ihrer Person gespeicherten Daten verlangen und schutzwürdige Belange der Patientinnen und Patienten nicht entgegenstehen und durch die Einsichtnahme keine unbefugte Offenbarung im Sinne des § 203 des Strafgesetzbuches StGB erfolgt.</p>

Zu § 40 Löschen von Patientendaten und Einschränkung der Verarbeitung

Nach Artikel 18, Absatz 1 DS-GVO hat die betroffene Person das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird. Dies hat zur Folge, dass ein Krankenhaus die Daten für den Zeitraum der Prüfung nicht verarbeiten darf.

Dies kann einerseits die Patientenbehandlung gefährden, andererseits auch weitergehende Verarbeitungen einschränken. § 40 sollte vor diesem Hintergrund um Absatz 3 ergänzt werden:

Gesetzentwurf der Landesregierung	Neufassung
<p>[...]</p>	<p>[...]</p> <p>(3) Werden Daten gemäß Artikel 18 der Verordnung (EU) 2016/679 in ihrer Verarbeitung eingeschränkt, dürfen die Daten trotzdem verarbeitet werden, wenn</p> <ul style="list-style-type: none"> • die Verarbeitung für die Durchführung einer Behandlung erforderlich ist, • die Verarbeitung mit der die frühere Behandlung in einem medizinischen Sachzusammenhang steht, oder • zur Erfüllung der Zwecke aus § 36 erforderlich ist oder • wenn die Patientin oder der Patient einwilligt. <p>Die Aufhebung der Einschränkung der Verarbeitung ist zu begründen und in der Krankenunterlage zu vermerken. Wurde die Einschränkung der Verarbeitung von einer betroffenen Person erwirkt, ist Artikel 18 Absatz 3 der Verordnung (EU) 2016/679 zu genügen.</p>

Ergänzende Einschränkung von Betroffenenrechten

Es erscheint sinnvoll, dass die in Art. 13 und 14 DS-GVO genannten Informationspflichten des Krankenhauses zu

bestimmten Zwecken eingeschränkt werden, z.B. bei der Weitergabe von Patientendaten an die Polizei oder andere staatliche Organe. Da es sich bei diesen Weitergaben regelhaft um Zweckänderungen handelt, müssten Patienten nach Art. 13 Abs. 3 resp. Art. 14 Abs. 4 DS-GVO über die Weitergabe informiert werden, was ggf. dem Ermittlungserfolg der staatlichen Organe entgegensteht. Art. 23 Abs. 1 DS-GVO sieht für derartige Zwecke die Möglichkeit der Einschränkung der Betroffenenrechte vor. Der bvitg empfiehlt die Ergänzung einer Regelung analog zu §§ 32,33 BDSG in einem neuen Paragraphen einzuführen:

Gesetzentwurf der Landesregierung	Neufassung
[...]	<p>[...]</p> <p>§ 40a Informationspflichten hinsichtlich Verarbeitung von Patientendaten</p> <p>(1) Die Pflicht zur Information der betroffenen Person gemäß Artikel 13 Absatz 3 der Verordnung (EU) 2016/679 besteht ergänzend zu der in Artikel 13 Absatz 4 der Verordnung (EU) 2016/679 genannten Ausnahme dann nicht, wenn die Erteilung der Information über die beabsichtigte Weiterverarbeitung</p> <ul style="list-style-type: none"> • die Information die öffentliche Sicherheit gefährden würde, • die Tatsache der Verarbeitung nach einer Rechtsvorschrift oder wegen der Rechte und Freiheiten anderer Personen geheim zu halten ist, • dies zur Verfolgung von Straftaten und Ordnungswidrigkeiten erforderlich ist, • die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigen würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen oder • eine vertrauliche Übermittlung von Daten an öffentliche Stellen gefährden würde. <p>(2) Die Pflicht zur Information der betroffenen Person gemäß Artikel 14 Absatz 1, 2 und 4 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 unter den in Absatz 1 genannten Bedingungen ebenfalls nicht.</p> <p>(3) Wird von einer Information der betroffenen Person entsprechend Absatz 1 oder Absatz 2 abgesehen, hat der Verantwortliche die Gründe hierfür zu dokumentieren.</p> <p>(4) Unterbleibt die Benachrichtigung in den Fällen des Absatzes 1 oder Absatzes 2 wegen eines vorübergehenden Hinderungsgrundes, kommt der Verantwortliche der Informationspflicht unter Berücksichtigung der spezifischen Umstände der Verarbeitung innerhalb einer angemessenen Frist nach Fortfall des Hinderungsgrundes, spätestens jedoch innerhalb von zwei Wochen, nach.</p>

Analog zu den Informationspflichten kann auch eine Benachrichtigung hinsichtlich einer Verletzung des Schutzes personenbezogener Daten gemäß Art. 34 DS-GVO die Arbeit öffentlicher Organe, wie beispielsweise Ermittlungen der Polizei, behindern. Das Hamburger Krankenhausgesetz sieht eine entsprechende Einschränkung vor. Da in Art. 34 Abs. 1 DS-GVO eine „unverzügliche“ Benachrichtigung verlangt wird und „unverzüglich“ nach § 121 Abs. 1 BGB „ohne schuldhaftes Zögern“ bedeutet, kann der deutsche Bundes- und Landesgesetzgeber entsprechende Regelungen erlassen, da es hierbei seitens des Verantwortlichen zu keinem schuldhaften Verzögern kommt:

Gesetzentwurf der Landesregierung	Neufassung
<p>[...] (3) Die Absätze 1 und 2 gelten entsprechend, soweit Dritte Auskunft über die zu ihrer Person gespeicherten Daten verlangen und schutzwürdige Belange der Patientinnen und Patienten nicht entgegenstehen.</p>	<p>[...] § 40b Beschränkung der Benachrichtigungspflicht (1) Der Verantwortliche kann von der Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person gemäß Artikel 34 der Verordnung (EU) 2016/679 absehen, soweit und solange die Benachrichtigung die öffentliche Sicherheit gefährden würde, oder dies zur Verfolgung von Straftaten oder Ordnungswidrigkeiten erforderlich ist, oder dazu führen würde, dass Sachverhalte, personenbezogene Daten oder die Tatsache ihrer Verarbeitung, die nach einer Rechtsvorschrift oder wegen der Rechte und Freiheiten anderer Personen geheim zu halten sind, aufgedeckt würden. (2) Wenn nach Absatz 1 von einer Benachrichtigung abgesehen wird, ist die oder der zuständige Beauftragte für Datenschutz und Informationsfreiheit zu informieren.</p>

Der bvityg steht als Branchenverband der Hersteller von IT-Systemen im Gesundheitswesen bei der weiteren Ausarbeitung des Landeskrankenhausgesetzes, der Ausarbeitung untergesetzlicher Normen sowie technischer Richtlinien gerne als fachlicher Dialogpartner zur Verfügung.

Berlin, 29.11.2019