Der Bayerische Landesbeauftragte
für den Datenschutz

und das

Bayerische Landesamt für
Datenschutzaufsicht

Leitfaden

Auftragsdatenverarbeitung bei der Aktenverwaltung in bayerischen öffentlichen und privaten Krankenhäusern

Stand 22.06.2016

Bayerische Landesbeauftragte für den Datenschutz	Hausanschrift Wagmüllerstr. 18 80538 München	Postanschrift Postfach 221219 80502 München	Tel. 089.212672-0 Fax 089.212672-50	www.datenschutz-bayern.de E-Mail: poststelle@datenschutz-bayern.de
Bayerisches Landesamt für Datenschutzaufsicht	Hausanschrift Promenade 27 91522 Ansbach	Postanschrift Postfach 606 91511 Ansbach	Tel. 0981.53-1300 Fax 0981.53-5300	www.lda.bayern.de E-Mail: poststelle@lda.bayern.de

Inhaltsverzeichnis

0 Einleitung 3

1 Prüfungsübersicht 4

2 Art. 27 BayKrG, Gewahrsam des Klinikums 5

3 Geeignete und ungeeignete Verfahrensweisen 7

3.1 ..... Serverstandort 7

3.2 ..... Wartung, Fernwartung 8

3.3 ..... Backup und elektronische Archivierung 9

3.4 ..... Externer Dienstleister bei der Verwaltung des Papierarchivs 9

3.5 ..... Externer Scandienstleister 10

3.6 ..... Externe Entsorgung 11

0 Einleitung

Immer wieder ist zu hören, dass Art. 27 Abs. 4 Bayerisches Krankenhausgesetz (BayKrG) in Zeiten von Cloud Computing und Big Data veraltet und unbrauchbar sei, da er einer Auftragsdatenverarbeitung im Bereich der Krankenhäuser zu enge Grenzen setze.

Gleichzeitig entstehen gerade in Krankenhäusern zunehmend große Mengen an Daten, die die Gesundheit der Patientinnen und Patienten und damit deren intimsten Lebensbereich betreffen. Für diese Daten ist es durchaus angemessen, höhere Schutzmaßnahmen als in anderen Bereichen zu fordern.

Durch die Beteiligung externer Stellen wird der Kreis derer, die mit sensiblen medizinischen Daten in Berührung kommen, größer. Gleichzeitig sinken die direkten Einflussmöglichkeiten der Krankenhäuser auf den Umgang mit den Daten ihrer Patienten. Das kann das Risiko von Datenmissbrauch und Datenverlust in einem besonders sensiblen Bereich erhöhen.

Deshalb hat Art. 27 Abs. 4 BayKrG aus Sicht der beiden bayerischen Datenschutzbehörden auch weiterhin seine Berechtigung. Er sorgt dafür, dass externe Dienstleister nur mit zusätzlichen Sicherheitsmaßnahmen zum Einsatz kommen dürfen. Wie später ausführlich dargestellt, darf eine elektronische Archivierung beispielsweise nur erfolgen, wenn die Daten im Krankenhaus verschlüsselt werden oder die Papierentsorgung bei einem externen Entsorger von Klinikmitarbeitern begleitet wird. Dies sorgt dafür, dass die Daten jederzeit unter Aufsicht und im Gewahrsam des Klinikums stehen.

Dass es möglich ist, die strengen Anforderungen des Art. 27 Abs. 4 BayKrG einzuhalten, hat eine flächendeckende Prüfung im Jahr 2015 gezeigt. Zwar wurden in den Krankenhäusern Mängel bei der Umsetzung gefunden, gleichzeitig konnte jedoch auch festgestellt werden, dass es für alle Konstellationen sehr wohl datenschutzgerechte Lösungen gibt. Zur Unterstützung der Krankenhäuser wurden die Ergebnisse der Prüfung daher in diesem Leitzfaden zusammengefasst.

1 Prüfungsübersicht

Anfragen und Einzelfallprüfungen haben in der Vergangenheit gezeigt, dass Auftragsdatenverarbeitung ein zunehmend wichtiges Thema für Krankenhäuser ist und hier verschiedenste Ansätze zum Tragen kommen. Gleichzeitig sind die Möglichkeiten zur Auftragsdatenverarbeitung für bayerische Krankenhäuser durch Art. 27 Abs. 4 BayKrG eingeschränkt.

Um einen Überblick über die Bereiche und Formen der Auftragsdatenverarbeitung zu bekommen, wurde an die bayerischen Krankenhäuser bzw. Krankenhausverbünde in öffentlicher Trägerschaft ein Fragebogen verschickt. Die Ergebnisse werden im Folgenden in allgemeiner Form zusammengefasst und aus Datenschutzsicht bewertet, um den angefragten Krankenhäusern einen Handlungsleitfaden an die Hand zu geben.

2 Art. 27 BayKrG, Gewahrsam des Klinikums

Art. 27 Abs. 4 Satz 6 BayKrG sieht vor, dass sich ein Krankenhaus zur Verarbeitung von Patientendaten, die nicht zur verwaltungsmäßigen Abwicklung der Behandlung der Patienten erforderlich sind (medizinische Patientendaten), nur anderer Krankenhäuser bedienen darf.

Sinn und Zweck des Art. 27 Abs. 4 Satz 6 BayKrG ist insbesondere, den Kreis der Personen, die mit sensiblen medizinischen Daten in Berührung kommen, möglichst eng und die Qualifikation der betreffenden Personen möglichst hoch zu halten. Die Aufsichtsbefugnisse der Krankenhäuser auch während der Datenverarbeitung sollen gestärkt, die Kenntnisnahme durch Unbefugte soll vermieden und die missbräuchliche Verwendung medizinischer Patientendaten damit soweit wie möglich ausgeschlossen werden.

Art. 27 Abs. 4 Satz 6 BayKrG ist nach der Entscheidung des Bayerischen Verfassungsgerichtshofs vom 06.04.1989 (Az.: Vf. 2-VII-87) verfassungsgemäß. Die gegen diese Entscheidung gerichtete Verfassungsbeschwerde wurde vom Bundesverfassungsgericht im Beschluss vom 25.09.1990 nicht zur Entscheidung angenommen (Az.: 1 BvR 1555/87).

Allerdings hat der Bayerische Verfassungsgerichtshof unter anderem ausgeführt, dass es den Krankenhäusern nicht verwehrt sei, medizinische Daten in einer dem Art. 26 Abs. 4 Satz 5 BayKrG a.F. (jetzt: Art. 27 Abs. 4 Satz 6 BayKrG) entsprechenden Ausgestaltung innerhalb des Krankenhauses durch Dritte mikroverfilmen (archivieren) zu lassen. Dem Gesetzgeber sei es entscheidend darauf angekommen, dass die medizinischen Patientendaten nicht aus dem Gewahrsam des Krankenhauses herausgegeben werden.

Eine Beteiligung externer Dienstleister ist demnach möglich, wenn die Datenverarbeitung im Gewahrsam des Klinikums stattfindet oder diese keine Kenntnis von den Daten nehmen können (z.B. durch Verschlüsselung). Gewahrsam bedeutet dabei nicht nur die räumliche Zuordnung zum Krankenhaus (z.B. Nutzung von Räumen auf dem Gelände des Krankenhauses), sondern auch die ausschließliche Verfügungsgewalt über die Patientendaten. Z.B. muss die Schlüsselgewalt beim Krankenhaus verbleiben, eine Wei-

sungsbefugnis gegenüber den Mitarbeitern des Dienstleisters bestehen und eine regelmäßige Kontrolle bzw. Aufsicht von Seiten des Klinikums durchgeführt werden. Die entsprechenden Punkte müssen ausdrücklich in einem schriftlichen Vertrag zur Auftragsdatenverarbeitung geregelt werden.

Die hier verwendete Definition von Krankenhaus richtet sich nach den Festlegungen der Orientierungshilfe KIS. Danach ist ein Krankenhaus ein zusammengehörender Funktionskomplex im Sinne von § 107 SGB V. Welche Einrichtungen als zusammengehörig betrachtet werden, kann nach den jeweiligen Landeskrankenhausplänen, dem Auftreten unter einheitlichem Institutskennzeichen nach § 293 SGB V und der Existenz einer einheitlichen ärztlichen Leitung beurteilt werden.

Krankenhäuser sind als rechtlich selbständige Einheiten auch unabhängig von ihrem Träger / Kommunalverband etc., so dass dieser nicht als Krankenhaus gewertet werden kann. Er gilt daher in der Bewertung der Zulässigkeit der Auftragsdatenverarbeitung wie ein externer Dritter, der kein Krankenhaus ist. Ähnliches gilt für Tochtergesellschaften von Krankenhäusern. Diese werden in der Regel geschaffen, um nicht Teil des Krankenhauses zu sein und selbständig agieren zu können. Daher können auch sie nicht als Auftragnehmer mit Krankenhauseigenschaft angesehen werden.

3 Geeignete und ungeeignete Verfahrensweisen

3.1 Serverstandort

Die Server und Serverräume befinden sich in der Regel im eigenen Klinikum, was den Anforderungen des Datenschutzes entspricht. Bei einem Klinikum mit mehreren Standorten kann hierbei die IT auch zentral an einem Standort zusammengeführt werden. Allerdings muss der Betreiber des Serverraums / Rechenzentrums weiterhin ein Krankenhaus sein, um die Anforderungen des BayKrG zu erfüllen. Eine Dienstleistungs-GmbH des Krankenhauses kann nicht als Krankenhaus angesehen werden. Sie kann aber in den Räumen des Krankenhauses als Auftragnehmerin tätig werden, wenn der Gewahrsam sichergestellt ist. Gleiches gilt für andere externe IT-Dienstleister.

Es besteht auch die Möglichkeit, Serverräume und IT-Dienstleistungen eines anderen Krankenhauses zu nutzen. Hier muss beachtet werden, dass für das Auftragnehmer-Krankenhaus kein Behandlungszusammenhang besteht und somit das Personal des Auftragnehmer-Krankenhauses (abgesehen von dem im Rahmen der beauftragten Administration erforderlichen Maß) keine Einsicht in die Daten des Auftraggeber-Krankenhauses nehmen darf. Zudem muss zumindest eine logische Trennung der Datenbestände erfolgen, d.h. für jedes Krankenhaus muss ein eigener Mandant eingerichtet werden.

Dies gilt auch für Klinikkonzerne, die aus mehreren rechtlich selbständigen Krankenhäusern und diversen Tochterunternehmen im Servicebereich bestehen. Es ist möglich, die IT in einem der Krankenhäuser des Konzerns zu zentralisieren. In diesem Fall müssen Verträge zur Auftragsdatenverarbeitung mit diesem Krankenhaus als Auftragnehmer geschlossen werden. Sollen in dieser Konstellation beim Auftragnehmer-Krankenhaus weitere Dienstleister beteiligt werden, die kein Krankenhaus sind, kann dies über ein Unterauftragsverhältnis erfolgen: Im Vertrag zwischen den Krankenhäusern wird die Einbeziehung von Unterauftragnehmern grundsätzlich geregelt und das Auftragnehmer-Krankenhaus schließt einen entsprechenden Vertrag zur Auftragsdatenverarbeitung mit dem gewünschten externen Dienstleister ab. Dabei gelten jedoch weiterhin die Anforderungen an den Gewahrsam des Krankenhauses, d.h. der Serverbetrieb erfolgt auf dem Gelände und unter Aufsicht des Auftragnehmer-Klinikums. Eine

direkte Beauftragung des Unterauftragnehmers durch die Auftraggeber-Krankenhäuser ist wegen Art. 27 Abs. 4 Satz 6 BayKrG nicht möglich.
Verwaltungsdaten und der Betrieb entsprechender Systeme (z.B.SAP ish) können nach Art. 27 Abs. 4 Satz 5 BayKrG an externe Dienstleister ausgelagert werden. Allerdings muss sichergestellt sein, dass tatsächlich keine medizinischen Daten enthalten sind.

Räumlichkeiten des Krankenhausträgers können genutzt werden, wenn nur das Krankenhaus einen Zugang dazu hat. Darüber hinausgehende IT-Dienstleistungen des Trägers sind kritisch zu sehen und wie die eines sonstigen externen Dienstleisters zu behandeln, d.h. es müssen Maßnahmen ergriffen werden, um den Gewahrsam des Krankenhauses sicherzustellen, indem z.B. eine Aufsicht der Arbeiten durch das Krankenhaus erfolgt.

3.2 Wartung, Fernwartung

Wie oben bereits dargestellt dürfen der Serverbetrieb und die Wartung vor Ort nur durch das Krankenhaus selbst oder ein anderes Krankenhaus erfolgen, soweit es sich um medizinische Daten handelt. Unterauftragnehmer können auch hier nur dann eingesetzt werden, wenn der Gewahrsam und die Kontrolle des Krankenhauses sichergestellt ist.

Die Fernwartung ist regelmäßig weder ein Fall der Auftragsdatenverarbeitung, noch ein Fall der Datenübermittlung und wird von Art. 27 BayKrG nicht erfasst. Gemäß § 11 Abs. 5 BDSG gelten die Vorschriften über die Auftragsdatenverarbeitung in § 11 Absätze 1 bis 4 BDSG jedoch entsprechend.

Im Interesse klarer Verhältnisse für Patienten und Krankenhäuser wird empfohlen, für die externe Fernwartung die Einwilligung der Patienten über eine Klausel im Krankenhaus-Aufnahmevertrag einzuholen. Nur durch eine wirksame Einwilligung können die strafrechtlichen Risiken der Fernwartung für Krankenhäuser ausgeräumt werden (Kenntnisnahme im Rahmen der Fernwartung ist Offenbarung i.S.d. § 203 StGB). Voraussetzung dafür, dass den Patienten eine Klausel im Aufnahmevertrag zugemutet werden kann, ist jedoch, dass die Kenntnisnahme von personenidentifizierenden Angaben auf das notwendige Maß eingeschränkt wird. Auch bei Aufnahme einer entsprechenden Klausel im Aufnahmevertrag sind daher bei der Fremdwartung alle vertretbaren technisch-organisatorischen Sicherungsmöglichkeiten zu aktivieren, mit denen die

Zahl der Fälle reduziert werden kann, in denen personenbezogene Patientendaten überhaupt zur Kenntnis der Wartungsfirma gelangen können (vgl. ausführlich 14. Tätigkeitsbericht des BayLfD 1992 (Nr. 2.2) und 18. Tätigkeitsbericht des BayLfD 1998 (Nr. 3.3.4), sowie 6. Tätigkeitsbericht des BayLDA 2013/2014 (Nr. 16.2)).

3.3 Backup und elektronische Archivierung

Konkret wurden im Rahmen der Prüfung zwei Anwendungsbereiche für eine externe elektronische Archivierung gefunden, zum einen Radiologiedaten und zum anderen gescannte Akten. Bei den Radiologiedaten kann unterschieden werden zwischen Langzeitarchivierung bzw. Backup verschlüsselter Daten bei einem externen Dienstleister und der (unverschlüsselten) Mitnutzung der Infrastruktur eines anderen Krankenhauses oder einer niedergelassenen Arztpraxis.

Eine Auslagerung elektronischer Daten an einen Dienstleister, der kein Krankenhaus ist, ist nur möglich, wenn der Dienstleister keine Einsichtsmöglichkeiten in die Daten hat. Dies ist nach derzeitigem Stand der Technik nur durch eine Verschlüsselung der Daten im Krankenhaus vor Abgabe an den Dienstleister zu erreichen. Die Schlüssel dürfen dem Dienstleister nicht bekannt oder beispielsweise durch Fernwartung zugänglich sein, genaueres siehe 21. Tätigkeitsbericht des Bayerischen Landesbeauftragten für den Datenschutz Kap. 22.2.3.2. Es ist somit nicht ausreichend, wenn Daten nur während der Übermittlung in das Rechenzentrum des Dienstleisters verschlüsselt werden. Weder eine Speicherung im Klartext, noch eine Verschlüsselung im Rechenzentrum mit einem Schlüssel des Dienstleisters sind ausreichend. Denkbar ist eine Schlüsselverwaltung über einen externen Treuhänder, der in Bezug auf den Dienstleister nicht weisungsabhängig ist und keine gleichzeitige Zugriffsmöglichkeit auf medizinische Daten hat.

3.4 Externer Dienstleister bei der Verwaltung des Papierarchivs

Die meisten Häuser verwalten ihr Papieraktenarchiv selbst auf dem Gelände des Klinikums. Teilweise werden Räume außerhalb des Klinikums angemietet. Diese können ebenfalls als Räume des Klinikums betrachtet werden, wenn sichergestellt ist, dass der Vermieter keinen Zugang hat.

Teilweise sind externe Dienstleister an der Archivverwaltung mit Transportdiensten (verschlossen und unverschlossen) und dem Einsortieren / Ausgeben von Akten beteiligt. Dies ist nur akzeptabel, wenn das Klinikum die Arbeiten beaufsichtigt und die Mitarbeiter des Dienstleisters auf Weisung des Klinikums tätig sind. Der Transport auf dem Gelände des Klinikums darf hierbei nur mit verschlossenen Behältern erfolgen und der Schlüssel muss beim Krankenhaus verbleiben, so dass der Dienstleister während des Transports keine Einsicht nehmen kann. Ist für den Transport ein Verlassen des Klinikgeländes nötig, so muss der Transport von Mitarbeitern des Krankenhauses begleitet werden. Dies gilt auch für Tochterunternehmen des Klinikums, die nicht als Krankenhaus oder dem Krankenhaus zugehörig gelten.

In Einzelfällen werden auch Räumlichkeiten bei einem externen Dienstleister zur Aktenlagerung genutzt. Handelt es sich hierbei nicht um ein Krankenhaus, entspricht dies nicht den Anforderungen des Datenschutzes, auch wenn die Lagerung in verschlossenen Containern, Umschlägen etc. erfolgt und diese nicht mit Namen beschriftet sind. Die Akten verlassen den Gewahrsam des Krankenhauses, was den Forderungen des Art. 27 BayKrG widerspricht. Verschlossene Kisten sind auch nicht mit einer Verschlüsselung gleichzusetzen, da bei einer Verschlüsselung die Daten umgerechnet und damit unkenntlich gemacht werden. Bei verschlossenen Containern sind die Akten in lesbarer Form weiterhin im Container enthalten und könnten eventuell zur Kenntnis genommen werden. Die technischen Sicherheitsmaßnahmen sind somit deutlich schwächer und damit nicht ausreichend.

Die Lagerung von Papierakten bei einem externen Dienstleister ist daher nur unter folgenden Bedingungen zulässig: Auf dem Gelände des Dienstleisters werden vom Klinikum Räumlichkeiten angemietet und räumlich abgetrennt. Der Schüssel befindet sich beim Klinikum. Mitarbeiter des Dienstleisters, die mit der Verwaltung der Akten beschäftigt sind, werden vom Krankenhaus als Mitarbeiter übernommen. Der behördliche/betriebliche Datenschutzbeauftragte des Krankenhauses führt regelmäßig Kontrollen vor Ort durch.

3.5 Externer Scandienstleister

Im Idealfall werden die Patientenakten im Krankenhaus durch eigenes Personal eingescannt. Ein externer Dienstleister kann beteiligt werden, wenn dieser in den Räumlich-

keiten des Krankenhauses arbeitet und der Gewahrsam des Klinikums über die Patientendaten sichergestellt ist. Wie im 19. Tätigkeitsbericht des Bayerischen Landesbeauftragten für den Datenschutz Kap. 3.4.2 bezüglich der Mikroverfilmung näher dargestellt, ist es hierzu erforderlich, dass die Schlüsselgewalt beim Krankenhaus verbleibt und die Arbeiten unter der Aufsicht des Krankenhauses stattfinden. Dies beinhaltet regelmäßige und auch unangekündigte Kontrollen durch das Klinikum und den behördlichen/betrieblichen Datenschutzbeauftragten. Die mit der Aufsicht beauftragten Mitarbeiter müssen uneingeschränkte Betretungsrechte haben. Insbesondere darf der Dienstleister als Auftragnehmer keine schriftliche Datenschutzerklärung des Auftraggebers als Voraussetzung für das Betreten der Räume einfordern, da damit die Schlüssel- und Kontrollgewalt untergraben wird. Die Tätigkeiten der Mitarbeiter des externen Dienstleisters dürfen nur auf Weisung des Klinikums erfolgen.

Es gibt Bestrebungen einiger Krankenhäuser, externe Scan-Dienstleister nicht im eigenen Haus einzusetzen, sondern zentralisiert in einem anderen Krankenhaus. Dies ist nur möglich, wenn alle Krankenhäuser mit dem Krankenhaus, bei dem das Einscannen erfolgen soll, einen Vertrag zur Auftragsdatenverarbeitung abschließen. Dieses Krankenhaus kann dann den gewünschten Dienstleister als Unterauftragnehmer mit obigen Bedingungen einsetzen. Direkte Verträge zur Auftragsdatenverarbeitung zwischen den auftraggebenden Krankenhäusern und dem Dienstleister sind nicht möglich, da dieser kein Krankenhaus ist. Zudem muss ein gesicherter Transport der Akten in verschlossenen Behältern vom Krankenhaus zum Scannen erfolgen, beim Verlassen des Geländes des Klinikums mit Begleitung durch Mitarbeiter des Krankenhauses. Der Dienstleister muss die Akten der verschiedenen Krankenhäuser getrennt halten. Die Vorort-Aufsicht über den Dienstleister liegt beim beauftragten Krankenhaus und muss auch tatsächlich wahrgenommen werden. Zudem haben die auftraggebenden Krankenhäuser Kontrollrechte.

3.6 Externe Entsorgung

Vorzugswürdig aus Datenschutzsicht ist die datenschutzgerechte Vernichtung durch das Krankenhaus selbst. Danach können die Wertstoffe an einen beliebigen Entsorger weitergegeben werden.

Als Vernichtung durch das Krankenhaus selbst kann auch angesehen werden, wenn Mitarbeiter des Klinikums die Akten selbst zur Vernichtung bringen, z.B. zur kommunalen Müllverbrennungsanlage und der Vernichtung beiwohnen. Hierbei muss auf einen Transport in verschlossenen Behältern geachtet werden, um beispielsweise bei einem Unfall einen Verlust oder die Einsicht in Unterlagen für Unbefugte zu verhindern.

Der Gewahrsam des Klinikums wäre dagegen nicht mehr gewährleistet, wenn das kommunale Entsorgungsunternehmen die Akten abholen würde, ohne dass diese vorab bereits unkenntlich gemacht worden wären. Das kommunale Entsorgungsunternehmen des gleichen Trägers zählt nicht als zum Krankenhaus gehörig. Gleiches gilt, wenn die Akten von einem externen Dienstleister abgeholt und vernichtet werden. Die Abgabe einer Vernichtungsbestätigung und eine Zertifizierung nach DIN oder BDSG etc. reichen nicht aus, um die Anforderungen des BayKrG umzusetzen. Eine derartige externe Entsorgung wäre nur möglich, wenn jeder Transport lückenlos bis zum Abschluss des gesamten Vernichtungsprozesses von einem Mitarbeiter des Krankenhauses begleitet und überwacht würde oder es sich nicht mehr um personenbezogene Daten handeln würde. Dies kann z.B. dadurch erreicht werden, dass Festplatten vorab datenschutzgerecht gelöscht werden oder medizinische Unterlagen vorab anonymisiert werden.

Eine akzeptable Möglichkeit wäre, dass der Dienstleister mit einer mobilen Aktenvernichtungsanlage auf das Gelände des Klinikums kommt und dort entweder unter Aufsicht von Mitarbeitern des Klinikums die Akten vernichtet oder aber die Mitarbeiter des Klinikums selbst die Akten vernichten und der Dienstleister nur technische Unterstützung bietet.

Es ist auch vorstellbar, dass der Scandienstleister die datenschutzgerechte Entsorgung übernimmt. Dies ist unproblematisch soweit dies auf dem Gelände und unter Aufsicht des Klinikums mit einer technischen Anlage des Dienstleisters erfolgt. Verlassen die Akten das Gelände, so gelten die üblichen Gewahrsamsanforderungen (insbesondere Begleitung und Überwachung durch das Krankenhaus). Dies gilt auch, wenn für die Entsorgung ein Unterauftragnehmer hinzugezogen werden soll.

Vor der Vernichtung von Patientenakten nach Ablauf der Aufbewahrungsfristen müssen vom Krankenhaus archivrechtliche Vorschriften abgeklärt werden.