Der Diözesandatenschutzbeauftragte

des Erzbistums Hamburg
der Bistümer Hildesheim, Osnabrück und
des Bischöflich Münsterschen Offizialats in Vechta i.O

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

Leitfaden

zur Aktenverwaltung in Krankenhäusern
von Trägern der katholischen Kirche
im Erzbistum Hamburg,
den Bistümern Hildesheim und Osnabrück
und dem Bischöflich Münsterschen Offizialat in Vechta i.O.

Stand: 01.04.2017

Herausgegeben vom

Diözesandatenschutzbeauftragten
des Erzbistums Hamburg
der Bistümer Hildesheim, Osnabrück und
des Bischöflich Münsterschen Offizialats in Vechta i.O.

Schwachhauser Heerstraße 67
28211 Bremen

Tel.: 0421 / 16 30 19 25
Mobil: 0151 / 41 97 57 58
Mail: info@datenschutz-katholisch-nord.de

Diesen Leitfaden können Sie auch auf unserer Internetseite abrufen unter:
https://www.datenschutz-kirche.de/

Inhalt

1. Einleitung

Für Ärzte gilt schon seit fast dreitausend Jahren die ärztliche Verschwiegenheitspflicht. Sie hat in Deutschland durch Festlegung in § 203 des Strafgesetzbuchs (StGB) ihren Niederschlag und ihre rechtliche Absicherung gefunden. Um sie auch im Strafverfahren zu schützen sieht der § 53 Abs. 1 Zi. 3 der Strafprozessordnung (StPO) ein Aussageverweigerungsrecht für *Ärzte, Zahnärzte, Psychologische Psychotherapeuten, Kinder- und Jugendlichenpsychotherapeuten, Apotheker und Hebammen* vor. In Ergänzung hierzu gilt auch ein Beschlagnahmeverbot für schriftliche Mitteilungen, Aufzeichnungen und andere Gegenstände, insbesondere ärztliche Untersuchungsbefunde nach § 97 Abs. 1 StPO. Allerdings müssen sich zur Anwendbarkeit dieser Vorschrift nach dem zweiten Absatz die Informationen im Gewahrsam des Arztes oder einer Krankenanstalt oder eines Dienstleisters befinden, der für die Ärzte personenbezogene Daten erhebt, verarbeitet oder nutzt. Für die Berufshelfer ist in § 97 Abs. 3 eine entsprechende Anwendung vorgesehen. Bei dem Begriff „Dienstleister" sind nur solche Personen oder Stellen gemeint, die selbst ebenfalls der Verschwiegenheitspflicht nach § 203 StGB unterliegen, wie zum Beispiel privatärztliche Verrechnungsstellen, die in Absatz 1, Ziffer 6 benannt werden.

Eine Aktenverwaltung, muss die Verschwiegenheitspflicht, das Zeugnisverweigerungsrecht und das Beschlagnahmeverbot zu Gunsten des Patienten und seines Vertrauens zu den Ärzten der Klinik ausreichend berücksichtigen und darf Patientendaten nicht in fahrlässiger Weise dem Zugriff von Ermittlungsbehörden aussetzen. Für Krankenhäuser ergeben sich daher folgende wesentliche Anforderungen, die eingehalten werden müssen:

1. Die Patientenakte ist immer im Krankenhaus zu verwalten. Das gilt unabhängig davon, ob sie elektronisch oder nach wie vor in Papierform geführt wird. Nach der Formulierung des Gesetzes „…im Gewahrsam einer Krankenanstalt" können die elektronischen Daten auch in einer anderen Krankenanstalt gespeichert werden, solange das auftraggebende Krankenhaus den alleinigen Zugriff auf diesen Datenbestand hat (sogenannte „Mandantenfähigkeit" des eingesetzten Verwaltungssystems). Die Benutzung eines klinikfremden Systems, etwa der Cloud eines fremden Dienstleisters wird dieser Forderung nur dann gerecht, wenn der Auftragnehmer keine Möglichkeit hat, auf die gespeicherten Daten inhaltlich Zugriff zu nehmen, auch nicht bei einer Fernwartung. Dies lässt sich nur durch eine Verschlüsselung erreichen, die nicht nur den Übertragungsweg schützt sondern auch die Speicherung in der Cloud selbst. Der Schlüssel darf dem Dienstleister nicht bekannt sein.

2. Die gleichen Anforderungen gelten auch für die Archivierung von abgeschlossenen Behandlungsfällen, wie auch für die Speicherung von Bildern aus den Bereichen der Radiologie, Nuklearmedizin, Endoskopie, Kardiologie, Pathologie und Mikrobiologie, im Rahmen von PACS- oder RIS-Systemen.
3. Problematisch sind auch die Fälle, bei denen Hilfsdienstleistungen zur Verwaltung der Akten von Drittanbietern in Anspruch genommen werden sollen. Das gilt insbesondere für das Einscannen von Unterlagen und das Vernichten von nicht mehr aufbewahrungspflichtigen Akten. Auch in diesen Fällen müssen die Patientendaten im Gewahrsam des Krankenhauses verbleiben, was ein Tätigwerden dritter Personen auf dem Gelände der Klinik, unter der Aufsicht von Klinikmitarbeitern nahelegt.

Nach der allgemein anerkannten „Zwei-Schranken-Theorie“ haben Krankenanstalten darüber hinaus auch die Bestimmungen der allgemeinen Datenschutzordnungen und der bereichsspezifischen Festlegungen durch Patientendatenschutzordnungen einzuhalten. Für kirchliche Krankenhäuser im Bereich der (Erz-)Bistümer Hamburg, Hildesheim, Osnabrück und im Offizialatsbezirk Vechta sind dies die „Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern (KrhDSO)“ und die „Anordnung über den kirchlichen Datenschutz (KDO)“. Wesentlich sind hier besonders die Grundsätze:

- Patientendaten sind nach Maßgabe der §§ 9, 10 KDO im Krankenhaus zu erheben, zu verarbeiten und zu nutzen (§ 2 Abs. 1 KrhDSO). Da es sich hier um besondere Arten personenbezogener Daten handelt, sind darüber hinaus auch die Festlegungen aus § 10 Abs. 5 und 6 KDO zu beachten.
- Auch hier gilt das Erforderlichkeitsprinzip (§ 9 Abs. 1 KDO) und der Grundsatz der Unmittelbarkeit der Datenerhebung (§ 9 Abs. 2 KDO).
- Verschiedene Fachabteilungen sind bei der Nutzung der Daten als Dritte anzusehen und somit ist die Einsichtnahme in die Patientenakte durch weitere Ärzte nur mit Einverständnis des Betroffenen möglich (§ 3 Abs. 2 KrhDSO).
- Auftragsdatenverarbeitungen sind nur zulässig, wenn sie die Anforderungen nach § 8 KDO erfüllen und zudem die Verpflichtung zur Verschwiegenheit und die Voraussetzungen für das Bestehen des Beschlagnahmeverbots gewahrt sind.
- Krankenhäuser sind nach den Landeskrankenhausplänen Einheiten, die mit einem einheitlichen Institutskennzeichen nach § 293 SGB V und zudem einer einheitlichen ärztlichen Leitung ausgestattet sind. Sie sind rechtlich selbstständig, mit der Folge, dass auch eine Zusammenarbeit mit dem Träger (Beispiel: Rechenzentrum) eine Auftragsdatenverarbeitung darstellt und entsprechend rechtlich abgesichert werden muss.

Der Arzt und seine berufsmäßig tätigen Gehilfen unterliegen strafrechtlich folgenden Verpflichtungen:

- Privatgeheimnisse der Patienten nicht zu offenbaren;
- diese Schweigepflicht gilt auch anderen Ärzten und Fachstationen gegenüber!
- Zu verhindern, dass Dritte durch eigene Handlungen vom Inhalt der Patientenakte Kenntnis erlangen können;
- Diese gilt insbesondere auch für externe Mitarbeiter oder externe Gehilfen.
- Eigenen Gewahrsam an den Akten sicherzustellen, um sie vor Beschlagnahme zu schützen.
- Über die Verhältnisse des Patienten nur Angaben zu machen, wenn er hierfür vom Betroffenen von der ärztlichen Verschwiegenheitspflicht entbunden wurde. Das gilt auch für die Überlassung von Unterlagen an Ermittlungsbehörden.

2. Geplante Neuregelung des § 203 StGB

Nach einem Regierungsentwurf vom 15. Februar 2017 soll die Zahl der geheimnispflichtigen Personen erweitert werden. Dabei wird ausgeführt, dass im Zeitalter der Digitalisierung in weiterem Umfang als bisher Unterstützungstätigkeiten erforderlich seien, die nicht durch eigenes Personal erbracht werden könnten. Für die Einrichtung, den Betrieb und die Wartung informationstechnischer Anlagen sei die Einbeziehung von externen Dienstleistern erforderlich, die aber nach dem geltenden Recht nicht die Möglichkeit besitzen dürften, von den geschützten Geheimnissen Kenntnis zu erlangen. Das würde für alle Beteiligten ein hohes strafrechtliches Risiko bedeuten.

Abhilfe schafft hier die geplante Änderung des Absatzes 3, der in Zukunft folgenden Wortlaut haben soll:

> *„(3) Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen. Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weite-*

rer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken."

Nach der Begründung des Gesetzentwurfs liegt nach wie vor kein unbefugtes Offenbaren vor, wenn die Geheimnisse an unmittelbar in die Sphäre des Schweigepflichtigen eingebundenen Personen weitergegeben werden. Der zweite Satz gestattet in Zukunft auch die Weitergabe an Personen, die durch Hilfsleistungen an der beruflichen Tätigkeit des Geheimnisträgers mitwirken, wenn diese Inanspruchnahme erforderlich ist. Hierdurch würden notwendige technische Hilfestellungen dem Strafbarkeitsrisiko entzogen. Wesentlich ist aber dabei, dass die externen Dienstleister in die Verpflichtung zur Verschwiegenheit einbezogen werden und wissen, dass auch sie sich nach § 203 StGB strafbar machen können. Dies wird künftig durch den Wortlaut von Absatz 4 festgelegt, der bestimmt, dass ebenso bestraft wird, wer *„nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, zur Geheimhaltung verpflichtet wurde;…".* Insoweit müssen vertragliche Regelungen mit dem Dienstleister hierzu eine eindeutige Vereinbarung enthalten. Nach Absatz 4, Ziffer 2 gilt dieses auch für den Auftragnehmer bei einer eventuellen Weitergabe an weitere Personen (Unterauftragsverhältnisse). Geplant ist die Verabschiedung der Neuregelung noch in dieser Legislaturperiode.

3. Durchgeführte Untersuchung der Aktenverwaltung in Krankenhäusern der katholischen Kirche in Norddeutschland

Auf dieser rechtlichen Basis ist eine Befragung aller in unseren Zuständigkeitsbereich fallender Krankenhäuser vorgenommen worden. Bereits im 3. Jahresbericht wurde die Nutzung externer Dienstleister in Krankenhäusern angesprochen und darauf hingewiesen, dass an 40 Kliniken ein Fragebogen verteilt worden ist, der nach Rücklauf zu einer Gesamtauswertung der bestehenden Situation führen sollte. Im weiteren Verlauf stellte sich heraus, dass ein Krankenhaus seinen Betrieb zum 30. September 2016 eingestellt hat und vier weitere Kliniken inzwischen in die Trägerschaft des päpstlichen Ordens der Alexianerbrüder übergegangen sind, so dass die Verantwortung hierfür beim Datenschutzbeauftragten des Ordens liegt. Die Aufsicht des Diözesandatenschutzbeauftragten umfasst daher zurzeit 35 Krankenanstalten.

Bis Ende 2016 hatten bereits 27 Kliniken eine Rückmeldung abgegeben. Die weiteren Einrichtungen wurden noch einmal angeschrieben, mit dem Ziel, eine möglichst vollständige Auswertung vornehmen zu können. Hierauf sind zunächst weitere sieben und nach einer zweiten Erinnerung auch die restlichen fünf Rückmeldungen eingegangen.

Abgeschlossen wurde die Befragung daher Anfang März 2017. Aus dem vollständigen Rücklauf wurden 35 Fragebögen zur Auswertung herangezogen. Die vier Alexianer Kliniken und selbstverständlich das geschlossene Krankenhaus wurden nicht berücksichtigt.

Die Ergebnisse dieser Befragung werden in den folgenden Abschnitten dargestellt und unter datenschutzrechtlichen Gesichtspunkten bewertet. Hierdurch sollen allen Verantwortlichen für die Datenverarbeitung in den Krankenanstalten wichtige Hinweise zu einer ordnungsgemäßen Organisation gegeben werden.

Für viele Einzelfragen, die in diesem Rahmen nicht angesprochen werden können, steht nach wie vor die gemeinsam mit den Arbeitskreisen Technik und Gesundheit und Soziales der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitete Orientierungshilfe Krankenhausinformationssysteme in der zweiten Auflage zur Verfügung. Sie steht in allen Ausführungen im Einklang mit dem von der Kirche erlassenen Recht.

Für das Verfahren der Datenlöschung und Vernichtung von Papierunterlagen sollte zudem die vom Deutschen Institut für Normung, unter Mitarbeit des Bundesbeauftragten für den Datenschutz (BfDI) und des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entwickelte DIN 66399 Teile 1 bis 3 SPEC beachtet werden. Die Anwendung dieser Norm in der Praxis wird in unserem Muster MV 204 „Mustervertrag zur Vernichtung von Datenträgern mit sensiblen personenbezogenen Daten nach DIN 66399“ dargestellt. Zwar sind solche DIN-Normen nicht allgemein verbindlich und ihre Einhaltung geschieht daher freiwillig, in dem konkreten Fall ist jedoch zu berücksichtigen, dass bei ihrer Beachtung der Vorwurf der Verschwiegenheitsverletzung rechtlich nicht aufrechterhalten werden kann. Es dient somit der strafrechtlichen und datenschutzrechtlichen Sicherheit der beteiligten Stellen.

4. Verfahren bei dem Einsatz von Klinikinformationssystemen

Der überwiegende Teil der befragten Krankenhäuser betreibt das Krankenhausinformationssystem (KIS) alleine, auf eigenen Rechnern und betreut es auch durch eigene Mitarbeiter. Festzustellen ist aber weiterhin, dass ergänzend auch externe Dienstleister eingebunden werden. Dabei handelt es sich überwiegend um Mitarbeiter der applikationsliefernden Firmen, die teilweise einen Vollzugriff auf das System haben, in anderen Fällen auf einen Remote-Zugriff beschränkt sind. Nur in wenigen Fällen wird die Hilfestellung innerhalb des Krankenhauses erbracht, wobei ein interner Mitarbeiter die Aufsicht führt. Die Möglichkeit vollständig auf das System Zugriff zu nehmen ist sicherlich

nicht mit der Verpflichtung aus § 203 StGB vereinbar, die jeden Arzt zwingt, auch die Möglichkeit der Kenntnisnahme von Patientendaten durch Unberechtigte auszuschließen. Auch nach der geplanten Gesetzesänderung, die es erlauben würde Dritte einzuschalten, soweit dies für die Inanspruchnahme ihrer Tätigkeit erforderlich ist, dürfte eine solche Lösung kaum rechtlichen Bestand haben. Ein Remote-Zugriff, der die Preisgabe eines Passworts für den vorübergehenden, zeitlich begrenzten Zugriff auf das System unter Mitwirkung eines internen Mitarbeiters ermöglicht, kann auch unter den jetzigen Anforderungen rechtmäßig sein und wird nach der beschrieben Reform des § 203 StGB unproblematisch durchgeführt werden können, wenn der Externe zuvor auf seine gesetzliche Verschwiegenheitsverpflichtung hingewiesen wurde. Eine Bereitstellung und Wartung der Hardware geschieht allgemein ohne die Möglichkeit zur Einsicht in medizinische Daten.

Die eingesetzten Krankenhausinformationssysteme werden zurzeit nur von einem geringen Teil, der befragten Kliniken gemeinsam betrieben. Das ist vor allem dann der Fall, wenn mehrere Einrichtungen eines Trägers hierdurch Kostenvorteile erstreben. Dies ist dann nicht zu beanstanden, wenn sich das gemeinsam genutzte Rechenzentrum in einem der beteiligten Krankenhäuser befindet und sichergestellt ist, dass jede Klinik nur auf die von ihr angelegten Akten Zugriff hat. Zwingende Voraussetzung ist also der Einsatz eines Systems, das eine mandantenbezogene Speicherung durchführen kann. Darüber hinaus sollte die Übertragung der Daten technisch abgesichert sein, wozu in der Regel eine Transportverschlüsselung erforderlich ist. Die Betreuung der technischen Systeme wird durch ein zentrales IT-Management für die beteiligten Krankenhäuser gewährleistet, das in die Klinikstruktur eingebunden ist. Externe Dienstleister werden darüber hinaus nicht eingesetzt. Zum Teil bestehen dabei auch noch eigene Serverräume in den Krankenhäusern, die ebenfalls von der zentralen IT-Stelle betreut werden. Backups werden dann sowohl auf dem Zentralrechner, wie auch in eingeschränkter Form auf dem lokalen Server erstellt. Angesichts der Tatsache, dass Krankenhäuser in jüngster Zeit mehrfach Opfer von erpresserischen Hacker-Attacken geworden sind, ist auch ein Schutz vor Ransomware durch eine eingehende Backup-Versorgung notwendig. Das kann, wie in einem der vorliegenden Fälle dadurch geschehen, dass die Backup-Versorgung zweigleisig gefahren wird.

In einem Falle werden zur Wartung des KIS auch Mitarbeiter des Herstellers eingesetzt. Die Durchführung der Fernwartung erfolgt jedoch nur nach telefonischer Absprache. Eine Einsichtnahme in medizinische Daten ist dabei möglich und nach dem jetzt geltenden Recht äußerst problematisch. Hier könnte die geplante Änderung des § 203 StGB eine wesentliche Entlastung bringen. Ein Auftragsdatenverarbeitungsvertrag liegt vor.

Die Einbindung von Rechenzentren außerhalb des Krankenhauses entspricht nur dann den strafrechtlichen/strafprozessualen Vorschriften, wenn sichergestellt ist, dass Mitarbeiter des Auftragnehmers keinen Zugriff auf die medizinischen Daten nehmen können. Das gilt auch dann, wenn der Krankenhausträger eine eigene Gesellschaft gründet, die Dienstleistungen für seine Kliniken übernehmen soll. Die Schaffung einer eigenen Firma kann in solchen Fällen nur so verstanden werden, dass dieser Bereich eben nicht Teil des Krankenhauses sein soll (Outsourcing). Technisch ist hierfür eine verschlüsselte Datenübertragung und ebenso eine verschlüsselte Datenspeicherung erforderlich, wobei der Auftragnehmer nicht über eine Zugangsberechtigung verfügen darf, selbst dann nicht, wenn nur Wartungsarbeiten am System vorzunehmen sind. Hier sollte mit einem fiktiven Satz an Testdaten gearbeitet werden, die keinen Zugriff auf die Realdaten ermöglichen. Zur rechtlichen Absicherung ist auch hier ein Vertrag zur Auftragsdatenverarbeitung nach § 8 KDO erforderlich. Nur wenige Kliniken machen hiervon bisher Gebrauch. Die Erfüllung der rechtlichen Grundlagen, wie auch die der technischen Absicherung ist nach den hierzu gemachten Angaben sehr fraglich.

In Erwartung der geplanten Gesetzesänderung besteht die Frage, ob sich in diesem Bereich tatsächlich eine Änderung ergeben wird. Der geplante neue § 203 Abs. 3 StGB spricht nur davon, dass externe Mitarbeiter, die an der beruflichen Tätigkeit des Schweigepflichtigen mitwirken, Kenntnis von den personenbezogene Daten haben dürfen, soweit dies für ihre Tätigkeit erforderlich ist. Für ein Rechenzentrum dürfte keine Mitwirkung an der beruflichen Tätigkeit bestehen. Die Mitarbeit an der Anlage einer Patientenakte, zu deren Führung der Arzt verpflichtet ist, ergibt sich nur aufgrund der Tätigkeit des KIS-Programmherstellers, nicht aber aus der Tätigkeit des Rechenzentrums. Darüber hinaus ist auch die Erforderlichkeit für eine Mitkenntnis dieser Daten nicht gegeben.

5. Nutzung elektronischer Archivsysteme

Für elektronische Archivsysteme, in denen Altakten aufbewahrt und verwaltet werden, gelten die gleichen Voraussetzungen, wie sie für die Bearbeitung der aktuellen Akten ausgeführt worden sind. Die Tatsache, dass dieser Punkt hier speziell erwähnt wird, hat damit zu tun, dass hier in einem wesentlich höheren Maße, als es beim Einsatz eines KIS erfolgt, außenstehende Dienstleister einbezogen werden. Bedenkt man, dass in den Krankenhäusern üblicherweise Patientenakten für einen Zeitraum von 30 Jahren nach Abschluss der Behandlung aufbewahrt werden und sich damit eine große Fülle an Unterlagen ergibt, mag das vom Mengengerüst her gesehen, verständlich sein. Zur Erinnerung sei hier aber noch einmal darauf hingewiesen, dass die ärztliche Schweigepflicht auch nach Abschluss der Behandlung, sogar auch nach dem Tod des Patienten

weiter fortbesteht (§ 203 Abs. 4 StGB)! Auch archivierte Daten sind in gleichem Maße zu schützen, wie die aktuellen Patientendaten.

In etlichen Fällen ist dabei das Einscannen der Unterlagen mit einer Langzeitarchivierung durch den gleichen Dienstleister verbunden. Gerade hier bestehen große Probleme mit dem Schutz der Patientenrechte, wenn das Einscannen der Unterlagen außerhalb der Klinik passiert, wie in den weit überwiegenden Fällen, die Mitarbeiter des Dienstleisters somit die Möglichkeit haben, sich auch vom medizinischen Inhalt Kenntnis zu verschaffen und zudem die Speicherung auf einem fremden Server mit Administratorrechten des Anbieters erfolgt, der dann vollen Zugriff auf den Inhalt der Patientenakten nehmen kann. Ein unberechtigter Zugriff kann nur durch eine sehr stringente technische Gestaltung vorgenommen werden. In vielen Fällen ist diese nicht vorhanden oder doch in erheblichem Maße zweifelhaft.

Weiterhin zu beachten ist der Umstand, dass in vielen Fällen archivierte Akten wieder aufgenommen werden müssen, weil der Patient sich zu einer neuen Behandlung einfindet. Kein Problem besteht dann, wenn der vorbehandelnde Arzt die weggelegte Akte wieder beizieht. Er darf auf alle Informationen Zugriff nehmen, die er durch seine Tätigkeit erfahren hat. Anders ist die Sache jedoch zu beurteilen, wenn auf die Vorbehandlungsdaten eines anderen Arztes oder einer anderen Fachstation zugegriffen werden soll. Dies ist nach allgemeiner Meinung, wie sie auch in § 3 Abs. 2 und entsprechender Anwendung von § 4 Abs. 1 KrhDSO zum Ausdruck gekommen ist, nur mit Einwilligung des Betroffenen zulässig. Im Einzelnen geht hierauf die unter Ziffer 3 im vorletzten Absatz dieses Leitfadens aufgeführte Orientierungshilfe Krankenhausinformationssysteme ein, auf die an dieser Stelle verwiesen werden kann. Bei dem Einsatz eines externen Servers darf es allein der Verwaltung des Krankenhauses möglich sein, eine weggelegte Akte wieder zu aktivieren und erneut in das KIS einzufügen, wenn die Voraussetzung hierfür durch die Zustimmung des Patienten gegeben ist. Der Dienstleister kann hier nur durch „blinde“ Übermittlung der Akte auf den Klinikserver beteiligt sein. Werden auch hier Verschlüsselungstechniken bei der Speicherung und Übertragung der Daten eingesetzt, dürfte der Schutz des Patienten zu gewährleisten sein.

6. Einsatz von PACS- und RIS-Systemen

Fast alle Kliniken setzen ein Picture Archiving and Communication System (PACS) sowie Radiologieinformationssysteme (RIS) zur Dokumentation, Verwaltung und Prozesssteuerung ihrer Bilddateien ein. Unterschiede gibt es darin, welche Bilddateien erfasst werden können. Der Betrieb solcher Systeme setzt einen hohen Grad bei der Bestandsicherheit voraus. Ein Ausfall des Systems würde praktisch sämtliche Fachabteilungen

in ihrer Arbeit behindern, da in diesem Falle auch die Bilddateien nicht mehr von den Wiedergabegeräten angezeigt werden und daher zeitweilig nicht mehr für Zwecke der Diagnose und Behandlung herangezogen werden könnten. Die Befürchtung, dass diese Funktion „outgesourced“ wird, um sie professionellen Rechenzentren zu übertragen, hat sich weitgehend nicht bestätigt. Nur in wenigen Ausnahmefällen werden Auftragsdatenverarbeiter in Anspruch genommen. Die generelle Problematik ergibt sich auch hier wieder daraus, dass die Speicherung nicht im Krankenhaus vorgenommen wird und möglicherweise Zugriffsmöglichkeiten des Dienstleisters auf die medizinischen Daten bestehen, die nicht hinnehmbar sind. Das gilt auch dann, wenn der Dienstleister eine vom Träger gegründete Gesellschaft ist. Es muss auf jeden Fall sichergestellt sein, dass nur das Krankenhaus auf die Bilddateien Zugriff nehmen darf und auch eine Offenbarung für Servicemaßnahmen nicht statthaft ist. Hier wird auf unsere Ausführungen zu Punkt 4 dieses Leitfadens verwiesen.

Die Speicherung der Daten in einem anderen Krankenhaus des gleichen Trägers erfolgt unter den gleichen Bedingungen, wie bei den Ausführungen zum KIS bereits angegeben. Auch Wartungsarbeiten an diesen Systemen werden vom technischen Personal der KIS-Systeme vorgenommen. Insoweit kann auf die vorhergehenden Ausführungen Bezug genommen werden.

7. Ungeeignete Verfahrensweisen beim Einscannen von Patientenakten

Die Anforderungen beim Einscannen von Patientenakten sind hoch. Dies wird noch lange nicht in allen Krankenhäusern berücksichtigt. Der weit überwiegende Teil der befragten Einrichtungen hat mit diesen Arbeiten einen externen Dienstleister beauftragt. Das setzt aber rechtlich voraus, dass das Krankenhaus seinen Gewahrsam an den Unterlagen sichert, die Schlüsselgewalt über die Akten behält und die Arbeiten beaufsichtigt. Daher kann nur eine Ausführung der Arbeiten auf einem Gelände, das zur Klinik gehört, unter regelmäßigen und unangekündigten Kontrollen durch den betrieblichen Datenschutzbeauftragten und eventuell weitere beauftragte Mitarbeiter erfolgen. Dabei ist auch sicherzustellen, dass außerhalb des festgelegten Verfahrens keine weiteren Kopien gefertigt werden dürfen.

Eine Herausgabe der Akten an den Dienstleister, der sie auf seinem Gelände einliest und anschließend auch noch vernichtet, wird der Forderung nach § 203 StGB, dass die zur Verschwiegenheit verpflichtete Person auch sicherstellen muss, dass andere Personen nicht durch eine eigene unzulässige Handlung vom Inhalt der Akte Kenntnis nehmen **können** nur schwer gerecht. Hierfür reicht es nicht aus, wenn vertraglich zugesichert wird, dass man von dieser Möglichkeit keinen Gebrauch machen werde, weil

hierdurch die Gefahren möglicherweise zwar reduziert aber keineswegs vollständig ausgeschlossen werden. Das wiegt umso schwerer, als in diesen Fällen auch keine effektive Kontrollmöglichkeit durch Mitarbeiter der Klinik besteht. Darüber hinaus besteht auch kein Gewahrsam der Klinik mehr, so dass die Unterlagen nicht mehr nach § 97 StPO vor Beschlagnahme geschützt sind.

Für Krankenhäuser steht heute immer mehr der Kostenfaktor im Vordergrund. Denkbar wäre deshalb auch, dass eine Klinik die Möglichkeiten zentralisiert für mehrere Krankenhäuser zur Verfügung stellt. Hierfür wäre dann ein Vertrag über Auftragsdatenverarbeitung zwischen den beteiligten Häusern erforderlich. In diesem Vertrag müsste auch der Einsatz eines bestimmten externen Dienstleisters gestattet werden. Die beauftragte Klinik müsste zudem den Gewahrsam an den Unterlagen übernehmen, was rechtlich zulässig ist (siehe die grundlegenden Ausführungen im 1. Abschnitt) und die Durchführung der Arbeiten beaufsichtigen.

In jedem Fall zu beachten:

- Scannen innerhalb der eigenen Klinik (Gewahrsamssicherung)
- Beim Einsatz externer Mitarbeiter: Regelmäßige und unangekündigte Kontrollen
- Durchführung technischer Sicherheitsmaßnahmen, beispielsweise zur Vermeidung unautorisierter Kopien
- Das Scannen außerhalb der Klinik verletzt das Schweigegebot!
- Das Scannen außerhalb der Klinik hebelt das Beschlagnahmeverbot aus!
- Übertragung der Arbeiten an ein anderes Krankenhaus muss durch Vertrag abgesichert werden

8. Verwaltung des Papierarchivs

Die Verwaltung des Papierarchivs erfolgt bei den befragten Kliniken zu einem weit überwiegenden Teil ohne die Beteiligung Dritter. Ebenso werden sie, von nur wenigen Fällen abgesehen, direkt vor Ort im Krankenhaus verwaltet.

Die teilweise vorgenommene Auslagerung bezieht sich allein auf Altakten, wobei in einem Fall auch der Zeitraum genau angegeben wird (z.B. Akten bis 2008). In einem weiteren Fall werden nur gescannte Akten ausgelagert. Dabei wird angegeben, dass die Lagerung in verschlossenen Behältern erfolgt und die Schlüsselgewalt und Weisungs-

befugnis allein beim Krankenhaus liege. Der Schlüssel werde im Sekretariat der Geschäftsleitung und beim Technischen Dienst aufbewahrt.

Eine Auslagerung von Patientenakten muss selbstverständlich so erfolgen, dass keine unautorisierten Personen Einblick nehmen können und das Krankenhaus zudem den Gewahrsam an den Unterlagen aufrechterhält. Eine Auslagerung ist daher an folgende Voraussetzungen gebunden:

1. Die angemieteten Räume müssen räumlich abgetrennt sein.
2. Zu den Räumen dürfen nur Mitarbeiter des Krankenhauses Zugang haben. Ein Zugang des Vermieters und seiner Mitarbeiter muss ausgeschlossen sein.
3. Die Verwahrung der Akten muss dabei in einer gesicherten Weise erfolgen, die einen Zugriff fremder Personen ausschließt (z.B. gesicherte Container).
4. Wird eine Akte wieder benötigt, müssen die Herausgabe und das dabei angewendete Verfahren genau festgelegt sein.
5. Sollen Mitarbeiter des Dienstleisters mit der Verwaltung der Akten betraut werden, so sind sie in ein Anstellungsverhältnis mit dem Krankenhaus zu übernehmen.

Zum Begriff des Gewahrsams ein kleiner Exkurs:

Das Wort „Gewahrsam“ wird im strafrechtlichen Bereich als die tatsächliche und von einem Herrschaftswillen getragene Herrschaftsgewalt über eine Sache definiert. Der Gewahrsamsinhaber muss zu jeder Zeit Zugriff auf die Sache haben und bestimmen können was mit ihr passiert. Eine räumliche Trennung führt zur einer Lockerung des Gewahrsams, solange dabei kein Fremdgewahrsam besteht. So hat beispielsweise ein Mieter auch dann Gewahrsam an den Gegenständen in seiner Wohnung, wenn er in Urlaub fährt. Gibt er aber bestimmte Sachen zur Aufbewahrung an eine andere Person, erfolgt ein Gewahrsamsübergang.

„Mitgewahrsam“ besteht in solchen Fällen, in denen mehrere Personen zu gleicher Zeit auf eine Sache einwirken können. Klassischer Fall: Die gemeinsam in einem Fachbereich tätigen Ärzte, die ihre Akten in einem einheitlichen System verwalten, haben jeweils Mitgewahrsam. Jeder von ihnen ist in der Lage die Akte zu nutzen und zu bearbeiten.

Einen „mittelbaren Gewahrsam“ kennt das Strafrecht nicht (im Gegensatz zu dem zivilrechtlichen Begriff des „mittelbaren Besitzes“). Das bedeutet, dass eine Person ihren

Gewahrsam an einer Sache verliert, wenn sie diese einem Dritten aushändigt und ihm die tatsächliche Herrschaftsmacht überträgt. Das ist dann der Fall, wenn beispielsweise die Herausgabe einer Akte, die wieder benötigt wird, nur unter Mitwirkung des Gewahrsamsinhabers möglich ist.

9. Verfahren der Vernichtung von Papierakten

Für die Vernichtung von Patientenakten und anderer Unterlagen sollte die im Jahre 2012 geschaffene DIN-Norm 66399 in den Teile I – III SPEC beachtet werden. Eine genaue Beschreibung des Verfahrens ist in unserem Entwurf eines Mustervertrages zur Vernichtung von Datenträgern mit sensiblen personenbezogenen Daten zu entnehmen. Das Unabhängige Landeszentrum für Datenschutz in Schleswig-Holstein hat eine Reihe von Anbietern zertifiziert und ihnen ein Gütesiegel verliehen. Es ist empfehlenswert die dort genannten Auftragnehmer zu bevorzugen. Die Anwendung der genannten DIN-Norm durch sie kann sowohl rechtlich, wie auch in technischer Hinsicht erfolgen.

Fast alle Einrichtungen, mit nur wenigen Ausnahmen haben externe Aktenvernichtungsunternehmen beauftragt. Ideal wäre es, wenn das beauftragte Unternehmen mit Spezialfahrzeugen auf das Klinikgelände fährt und die zu vernichtenden Unterlagen vor Ort in die Vernichtungsmaschine einfüllt. Ein Mitarbeiter des Krankenhauses ist dabei und überzeugt sich, dass schon vor Ort mit der Vernichtung der Unterlagen begonnen wurde. Wenn die weiteren Rahmenbedingungen stimmen, also die Sammlung auf dem Gelände der Einrichtung in einem gesicherten Container erfolgt, der wiederum nur durch das Spezialfahrzeug geöffnet werden kann, dann ist jedes Risiko für eine Verletzung der Schweigepflicht ausgeschlossen.

Dieses Verfahren wird jedoch bisher bei weitem nicht von den befragten Krankenhäusern eingesetzt. Vielmehr werden die zu vernichtenden Unterlagen zwar in gesicherten Containern gesammelt, dann aber dem Dienstleister zur Mitnahme und zur Vernichtung in seinen eigenen Räumen überlassen. Auch in diesen Fällen sollte technisch sichergestellt sein, dass das Material nur durch das Einfüllen in die Vernichtungsanlage aus dem Container entnommen werden kann. Nur auf diese Weise kann sichergestellt werden, dass ein unautorisierter Einblick in das Material ausgeschlossen ist. Anderenfalls ist in jedem Fall eine Begleitung und Überwachung des Transports durch einen Mitarbeiter des Krankenhauses bis zum Einfüllen in die Vernichtungsanlage erforderlich.

Vor der Einbeziehung von Dokumenten in die zu vernichtenden Unterlagen sind noch archivrechtliche Aspekte zu berücksichtigen. Die Übergabe von Patientenakten oder

anderer Gegenstände an das Bistumsarchiv entspricht nach § 2 Abs. 3 der Kirchlichen Archivanordnung (KAO) einer ordnungsgemäßen Entsorgung, wenn dabei das Persönlichkeitsrecht der Person nicht verletzt wird. Diese Voraussetzung wird durch die Schutzfristen des § 9 KAO regelmäßig gewährleistet. Kirchliche Krankenhäuser unterliegen auch der Archivierungspflicht nach § 4 KAO.

10. Durchführung externer Leistungsabrechnung bei Privatpatienten

Die Vornahme einer externen Leistungsabrechnung bei Privatpatienten ist nur mit Einwilligung der Betroffenen statthaft. Alle befragten Kliniken machen hiervon Gebrauch. Die Zustimmung des Patienten wird dabei entweder im Behandlungsvertrag, durch eine Wahlleistungsvereinbarung oder durch eine separate schriftliche Einwilligungserklärung herbeigeführt.

Erforderlich ist zudem eine vertragliche Regelung der Auftragsdatenverarbeitung nach § 8 KDO. Hierin ist im Einzelnen festzulegen, welche Leistungen in welcher Form erbracht werden, wie das beauftragte Unternehmen die zur Abrechnung erforderlichen Daten übermittelt bekommt und wie mit den Daten nach Erstellung der Rechnung, bzw. deren Bezahlung zu verfahren ist. Auch Fragen der Haftung und eventuell notwendiger Korrekturen am Abrechnungsverfahren sind im Vorhinein zu klären. Dabei unterliegen die beauftragten Unternehmen nach § 203 Abs. 1 Ziffer 6 StGB ebenso der gesetzlichen Schweigepflicht, so dass im Rahmen der Erforderlichkeit keine unbefugte Offenbarung stattfindet.

Die Befragung hat auch ergeben, dass in einigen Fällen die Chefärzte ein Recht zu Privatliquidation besitzen, so dass in diesen Fällen diese Regelungen allein von ihnen getroffen werden. Auch sie haben in diesem Fall sicherzustellen, dass die oben genannten Voraussetzungen erfüllt werden.