Addendum zur Technischen Anlage

Dieses Addendum ergänzt die Technische Anlage der Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, die im Mai 2008 veröffentlicht wurde.

1. Elektronische Dokumentation und Archivierung (ersetzt Kap. 11 der Technischen Anlage)

1.1. Elektronische Dokumentation

Die elektronische Dokumentation wird durch das „Gesetz zur Verbesserung der Rechte von Patientinnen und Patienten“ in BGB § 630f nur allgemein geregelt.

Im Fall der elektronisch geführten Patientenakte ist durch den Einsatz einer geeigneten Softwarekonstruktion sicherzustellen, dass nachträgliche Änderungen automatisch kenntlich gemacht werden (Vgl. Gliederungspunkt 4.4 der Empfehlung). Ein Übergangszeitraum wurde durch den Gesetzgeber nicht eingeräumt. Aus Sicht des Anwenders ist es daher dringend geboten, ein Praxisverwaltungssystem einzusetzen, welches über die geforderte Funktionalität verfügt. Alternativen zur Verwendung einer IT gestützten Änderungsdokumentation, die gleichermaßen rechtssicher sind, sind aus dem Gesetz nicht ableitbar. Dennoch sollen an dieser Stelle Vorgehensweisen dargestellt werden, die die Position des Anwenders in einem Haftungsprozess möglicherweise verbessern können.

Technische Vorkehrungen

Der Mangel, der durch technische Maßnahmen ausgeglichen werden soll, ist das Löschen, Ersetzen oder Verändern des ursprünglichen Inhalts der Patientenakte sowie die mögliche Manipulation des Zeitpunkts eines Eintrags.

Folgende Maßnahmen könnten geeignet sein:

- häufige, am besten tägliche, Datensicherung der hinzugefügten Daten (technisch: sog. inkrementelles Backup). Vorausgesetzt ist, dass es ein vollständiges Datenbackup gab. Zu verwenden sind nicht-veränderbare Speichermedien (z. B. CD- oder DVD-ROM).
- Die Datenträger müssen sicher aufbewahrt werden. Durch Backuplösungen kann jedoch die vom Gesetzgeber beabsichtigte Manipulationssicherheit nicht vollständig erreicht werden, da Änderungen zwischen zwei Sicherungen nicht erfasst werden.
- Integritätssicherung der innerhalb eines Tages hinzugefügten Daten mit einer qualifizierten elektronischen Signatur oder einem qualifizierten elektronischen Zeitstempel. Der Vorteil dieses Verfahrens ist, dass die tägliche Datensicherung auch mit Speichermedien, die eine nachträgliche Veränderung zulassen (Festplatte, Band, externer Dienstleister), erfolgen kann. Wird ein qualifizierter Zeitstempel verwendet, kann außerdem der Zeitpunkt, zu dem die Daten

vorgelegen haben, zweifelsfrei nachgewiesen werden (SigG). Das Problem der fehlenden Lückenlosigkeit zwischen den Sicherungen besteht aber weiterhin.

Organisatorische Vorkehrungen

Durch die zuvor aufgeführten Maßnahmen wird keine lückenlose bzw. rechtssichere Dokumentation gewährleistet. Aus diesem Grund können weitere Maßnahmen ergriffen werden. Hierbei wird zugrunde gelegt, dass nachträgliche Änderungen der Patientenakte in der Regel nicht sehr häufig vorkommen.

Wenn der Anwender einen nachträglichen Änderungsbedarf erkennt und eine Software zur Änderungsdokumentation noch nicht zur Verfügung steht, kann die Änderung protokolliert werden: Im Dokumententext der elektronischen Patientenakte erfolgt, ohne Streichung des bisherigen Textes, die notwendige Änderung mit Zeit- und Datumszusatz. In einem Änderungsprotokoll in Papierform wird der Änderungsgrund dargelegt. Das unterzeichnete Änderungsprotokoll wird zur Patientenakte genommen.

Wie einleitend klargestellt, handelt es sich bei den dargestellten Maßnahmen nicht um rechtssichere Alternativen zum Einsatz einer geeigneten Software zur Änderungsdokumentation.

1.2. Archivierung elektronisch signierter Dokumente

Für die rechtssichere langfristige Archivierung elektronisch signierter Dokumente müssen die Vorgaben des SigG und der SigV beachtet werden. Dies können PVS- oder Archivsoftware-Hersteller z. B. durch die Umsetzung der Technischen Richtlinie BSI-TR-03125 („Beweiswerterhaltung kryptographisch signierter Dokumente“, BSI-TR-ESOR) sicherstellen.

2. Ersetzendes Scannen

Sollen einkommende Papierdokumente (z. B. Arztbriefe von Kollegen) eingescannt werden, um diese elektronisch zu verwalten und das Original zu vernichten, wird dieser Vorgang als „Ersetzendes Scannen“ bezeichnet. Aus technischer Sicht empfiehlt die Richtlinie BSI-TR-03138 (BSI-TR-RESISCAN) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) technische Maßnahmen für das Ersetzende Scannen. Diese Richtlinie beschreibt, welche Maßnahmen durchgeführt werden müssen, damit der Beweiswert des elektronisch erfassten Dokuments (Scanprodukt) möglichst nah an den des Originaldokuments angenähert wird. Zitat aus der Richtlinie: „Ziel ist es, die mit einer Vernichtung des Originaldokuments stets einhergehende Verringerung des Beweiswerts für den jeweiligen Anwender durch einen an das Original möglichst weit angenäherten Beweiswert des – in einem nachweisbar ordnungsgemäßen Prozess erstellten – Scanproduktes selbst auszugleichen, zu minimieren oder sichtbar zu machen.“

Für Experten: Die Technische Richtlinie BSI-TR-03138 des BSI definiert das Ersetzende Scannen als den „Vorgang des elektronischen Erfassens von Papierdokumenten mit dem Ziel der elektronischen Weiterverarbeitung und Aufbewahrung des hierbei entstehenden elektronischen Abbildes (Scanprodukt) und der späteren Vernichtung des papiergebundenen Originals“.

Die rechtliche Anwendbarkeit der Technischen Richtlinie BSI-TR-03138 für die ärztliche Dokumentation in der Patientenakte ist nach Ansicht des BSI gegenwärtig nur für Röntgenbilder und diesbezügliche Aufzeichnungen ausdrücklich geregelt. Für sonstige Papierdokumente der Patientenakte existiert keine gesetzliche Bestimmung, die es gestattet oder verbietet, die Originaldokumente nach dem Scannen zu vernichten (Anlage R, Abschnitt R.1.2.4., S. 21). Ärzte, die beabsichtigen, Papierdokumente nach der Digitalisierung zu vernichten, müssen diese unklare Rechtslage berücksichtigen und sich ggfs. beraten lassen. Wird ein sehr hoher Beweiswert der Scanprodukte angestrebt, wären die „zusätzlichen Maßnahmen bei sehr hohen Integritätsanforderungen“ der Richtlinie zu berücksichtigen (Gliederungspunkt 4.3.3 der Technischen Richtlinie).

Etwas differenzierter sind die von TR-RESISCAN empfohlenen Maßnahmen zur Vertraulichkeit und Verfügbarkeit zu betrachten. Die Richtlinie trifft hierzu unter anderem folgende Aussage: „Die Vertraulichkeitsanforderungen haben keinen Einfluss auf den Beweiswert des Scanprodukts“[1]. Gescannte Dokumente werden Teil der elektronischen Dokumentation in der Arztpraxis. Zur Sicherstellung der Vertraulichkeit und Verfügbarkeit wird daher die Einhaltung derselben Maßnahmen empfohlen, die auch sonst für die elektronische Dokumentation in der Arztpraxis vorgesehen sind und in der vorliegenden Technischen Anlage beschrieben sind.

3. Umgang mit externen Speichermedien

Es gibt zunehmend Angebote der Industrie für elektronische Patientenakten auf externen Speichermedien (USB-Sticks). Diese sollen in der Arztpraxis angeschlossen werden, um Daten auszulesen oder neue Daten darauf zu speichern. Von außen ist nicht erkennbar, ob sich auf dem USB-Stick Schadsoftware befindet, die – sogar durch bloßes Stecken – den Rechner des Arztes infizieren und z. B. Patientendaten löschen, manipulieren oder stehlen kann[2].

Auch wenn einige kommerzielle USB-Sticks spezielle Sicherheitsmechanismen gegen Schadsoftware implementieren, kann in der Regel ein sicherer USB-Stick eines renommierten Anbieters nicht von einer Fälschung unterschieden werden.

Die Nutzung eines fremden externen Speichermediums ist einer Kommunikation mit einem unsicheren externen Netz (Internet) gleichzusetzen. Es gelten demnach die gleichen Voraussetzungen, wie für die Anbindung eines Praxisrechners an ein unsicheres Netz (Internet).

Fremde Speichermedien dürfen nicht direkt mit einem Patientendaten führenden System verbunden werden. Die Nutzung fremder Speichermedien darf nur an einem Rechner oder einer speziellen Hardwarekomponente geschehen, welche speziell im Voraus gehärtet wurde und Sicherheitsmechanismen zur Abwehr von Angriffen implementiert. Ein Mindestmaß an Sicherheit bietet zudem die regelmäßige Aktualisierung des Betriebssystems mit Updates in Kombination mit einer aktuellen Anti-Viren-Software.

4. Maßnahmen bei Einsatz von Chipkarten-Terminals und Konnektoren

Für das Einlesen der elektronischen Gesundheitskarte werden Chipkarten-Terminals eingesetzt. Es dürfen grundsätzlich nur

[1] Zitat aus BSI-TR-RESISCAN Anlage R Kap. R.1.2.4 Tab. 8 Fußnote 26

[2] Ein praktisches Beispiel für Schadsoftware, welche sich durch bloßes Stecken des USB-Sticks den Rechner infiziert, ist „Stuxnet“ im Jahr 2010, mit mehreren Millionen befallenen Rechnern weltweit. Damit konnten auch Rechner in hochsensiblen Industrieanlagen, die nicht mit dem Internet verbunden waren, infiziert werden.

von der gematik zugelassene Kartenterminals verwendet werden. Die Kartenterminals können teilweise auch für die Erstellung und Prüfung von qualifizierten elektronischen Signaturen sowie für weitere Anwendungen, bspw. im sicheren Netz der KVen (KV-Safenet), eingesetzt werden. Die Empfehlungen und Auflagen der Hersteller der jeweiligen Produkte sollten für den sicheren Einsatz in der Arztpraxis berücksichtigt werden.

5. Vernetzung in der Arztpraxis durch das Stromnetz (Powerline) (Ergänzung zu Kap. 4 der Technischen Anlage)

Es ist möglich, eine Vernetzung in der Arztpraxis über das Stromnetz mit Hilfe sogenannter Powerline-Adapter zu realisieren. Vorteil einer solchen Vernetzung ist es, dass keine weiteren Datenleitungen verlegt werden müssen. Nachteil einer solchen Vernetzung ist, dass sich die Datensignale auch in das Stromnetz von benachbarten Wohnungen oder Gebäuden ausbreiten können, so dass der Netzwerkverkehr abgehört oder manipuliert werden kann. Eine effektive und sichere Filterung am Stromzähler kann nicht vorausgesetzt werden. Eine Vernetzung über das Stromnetz wird aus diesem Grund grundsätzlich nicht empfohlen. Ist aus bautechnischen Gründen eine Vernetzung über LAN-Kabel nicht möglich, kann die Vernetzung über das Stromnetz nur mit besonderen Sicherheitsmaßnahmen erwogen werden. Es muss sichergestellt werden, dass die Powerline-Adapter verschlüsselt kommunizieren. Die Verschlüsselung mit einem werkseitigen Default-Schlüssel ist in der Regel nicht sicher. Ein individueller Schlüssel muss nach der Dokumentation des Herstellers in allen Powerline-Adaptern generiert und eingestellt werden. Es wird empfohlen, die korrekte Funktion der Verschlüsselung regelmäßig zu prüfen und den Schlüssel regelmäßig zu ändern.

6. Kryptographische Algorithmen (Aktualisierung zu Kap. 5 der Technischen Anlage)

Für Experten: Für die langfristige Sicherheit von verschlüsselten Daten werden statt AES128 nun stärkere symmetrische Algorithmen empfohlen, z. B. AES256. Für die Eignung von kryptographischen Algorithmen allgemein gilt die Technische Richtlinie BSI-TR-03116–1 des BSI. In dieser werden entsprechende Empfehlungen je nach Anwendungsbereich (z. B. Verschlüsselung von Patientendaten, Signatur usw.) gegeben.

7. Voice over IP (VoIP) und Videotelefonie über das Internet (Ergänzung zu Kap. 4 der Technischen Anlage)

In den letzten Jahren hat sich Telefonie über VoIP (also über technische Internet-Protokolle) weit verbreitet und verdrängt mittlerweile die klassische Telefonie über dedizierte Telefonleitungen. Viele etablierte Telefongesellschaften bieten inzwischen bei Neuverträgen sogar nur noch VoIP-Anschlüsse an.

Die Anbieter müssen gemäß § 109 des Telekommunikationsgesetzes Maßnahmen, zum Schutz der übermittelten personenbezogenen Daten, auf dem aktuellen Stand der Technik treffen. Bei Anbietern, welche bei der Bundesnetzagentur registriert sind,[3] kann davon ausgegangen werden, dass die Vertraulichkeit der Kommunikation nach dem Stand der Technik gewahrt ist. Eventuelle Sicherheitsauflagen des Anbieters müssen dabei eingehalten werden. Insbesondere müssen evtl. vom Anbieter mitgeteilte Zugangsdaten für VoIP von den Nutzern geheim gehalten werden.

Anders sind internetbasierte Telefonie- oder Videotelefonie-Dienstleistungen zu bewerten, deren Anbieter nicht bei der Bundesnetzagentur registriert sind. In diesem Fall muss vom Anbieter verbindlich zusichert werden, dass die Vertraulichkeit der Kommunikation technisch hinreichend gewährleistet ist. Bei Bedarf muss der Anwender selbst für eine effektive Verschlüsselung sorgen, falls diese technisch möglich ist.

Nicht empfohlen wird die Kommunikation von Patientendaten mit Hilfe von (Video-)Telefonie über VoIP, wenn diese mit Hilfe von Software auf einem gewöhnlichen Rechner in der Arztpraxis, der direkt mit dem Internet verbunden ist, realisiert wird. Es kann nicht ausgeschlossen werden, dass dieser Rechner mit Schadsoftware infiziert und der Inhalt der Kommunikation abgehört wird. Wird Videotelefonie z. B. im Rahmen einer telemedizinischen Anwendung realisiert, muss die Kommunikation in einem sicheren Intranet nach Kap. 3.3 der Technischen Anlage übertragen werden.

8. Nutzung von schnurlosen Telefonen (Telefone nach dem DECT-Standard) (Ergänzung zu Kap. 4 der Technischen Anlage)

Die Nutzung der weit verbreiteten schnurlosen Telefonen nach dem DECT-Standard (Digital Enhanced Cordless Telecommunication) für die telefonische Kommunikation von Patientendaten wird aktuell nicht empfohlen[4]. Die Verschlüsselung des DECT-Standards gilt als gebrochen[5], so dass jedermann mit überschaubarem Aufwand und Ausrüstung aus einiger Entfernung unbemerkt Gespräche abhören kann.

9. Auslagerung der Speicherung der medizinischen Dokumentation (Datensicherung) an externe Firmen (Ergänzung zu Kap. 6 der Technischen Anlage)

Die externe Sicherung von Patientendaten außerhalb des eigenen Praxisverwaltungssystems ist aus technischer Sicht nur unter sehr strengen Vorgaben zulässig. Ziel ist es dabei, dass nur der Anwender Zugriff auf seine extern gespeicherten Daten haben kann. Insbesondere darf auch der Dienstleister nicht in der Lage sein, auf den Klartext der Daten zuzugreifen.

Folgende Betriebsarten der externen Datenverarbeitung und -archivierung werden nicht empfohlen:

- Die Auslagerung der Datenverarbeitung außerhalb der Arztpraxis:
  Dies ist der Fall, wenn das Computerprogramm des PVS bei einem externen Dienstleister („in der Cloud"), außerhalb der Praxis betrieben wird. Damit wäre der Zugang des Dienstleisters zu den Patientendaten potentiell technisch möglich.
- Die Auslagerung der Datenhaltung außerhalb der Arztpraxis:
  Dies ist der Fall, wenn das PVS in der Praxis betrieben wird, die Daten allerdings extern gespeichert werden. Selbst bei der Verwendung einer sicheren verschlüssel-

[3] Verzeichnis der gemeldeten Unternehmen gemäß §6 Abs. 4 TKG. Link (Abruf am 03.12.2013): http://www.bundesnetzagentur.de/cln_1911/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/Meldepflicht/meldepflicht.html?nn=268208

[4] s. auch Sicherheitshinweis des BSI vom 14.02.2012: Sicherheit von schnurlosen Telefonen nach DECT-Standard, Link (Abruf 03.12.2013): https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Sicherheitshinweise/2012–02–14_Sicherheitshinweis_DECT_pdf.pdf?__blob=publicationFile

[5] Vgl. heise.de, Artikel v. 30.12.2009, Link (Abruf 03.12.2013): http://heise.de/-893693

ten Speicherung wäre dies mit dem Risiko einer verminderten Verfügbarkeit verbunden (z. B. Unterbrechung der Netzleitung, technischer Defekt, Insolvenz des Dienstleisters).

Eine externe Datenhaltung älterer Datenbestände z. B. zu Archivierungszwecken, ist mit zusätzlichen Sicherheitsmaßnahmen (organisatorische und technische Redundanz, Notfallkonzepte) möglich, die das Risiko einer verminderten Verfügbarkeit ausschließen.

Für Experten: Die folgenden technischen Empfehlungen beschreiben Schutzmaßnahmen im Sinne von Mindeststandards, die zum Zeitpunkt der Veröffentlichung dieses Dokuments als geeignet für den Schutz der Daten gelten. Die Schutzmaßnahmen müssen vom externen Anbieter nach dem Stand der Technik weiterentwickelt werden, so dass der technische Schutz der Daten zu jeder Zeit effektiv gewährleistet wird. Eine externe Speicherung von Daten einer Praxis wird aktuell unter den folgenden Bedingungen als zulässig betrachtet:

- Übertragung der Daten
  - Die Daten werden bereits in der Praxis ausreichend verschlüsselt, d. h. bevor sie verschickt werden. Eine Entschlüsselung darf ebenfalls nur in der Praxis erfolgen können.
  - Die Übertragung der verschlüsselten Daten zwischen Arztpraxis und Anbieter muss über einen verschlüsselten Kanal erfolgen.
  - Beide Endpunkte der Kommunikation (d. h. Arztpraxis und Dienstleister) müssen sich gegenseitig authentifizieren. Es müssen dabei Verfahren zur „starken Authentifizierung“ mit Hilfe kryptographischer Algorithmen zum Einsatz kommen. Die Authentifizierung allein mit Username und Passwort ist dabei nicht ausreichend.
  - Die Integrität und Authentizität der Daten müssen gewährleistet werden, z. B. mit Einsatz einer technischen Signatur.
- Generierung und Verwendung von Schlüsseln
  - Die Schlüssel für die Entschlüsselung müssen in der alleinigen Kontrolle des Arztes liegen.
  - Sie müssen durch Soft- oder Hardware in der Praxis generiert werden.
  - Sie dürfen nicht vom externen Dienstleister vorgegeben oder zur Verfügung gestellt werden.
  - Schlüsselgenerierung, Verschlüsselungsalgorithmen und Schlüssellängen müssen dem jeweils aktuellen Stand der Technik und Wissenschaft entsprechen, gemäß der jeweils aktuellen Version der BSI-TR-03116–1. Es muss bei Bedarf die Möglichkeit bestehen, die Verschlüsselung der Daten durch stärkere Algorithmen und Schlüsseln zu erneuern. (s. BSI-TR-03116–1 Kap. 4.4.1).
  - Schlüsselgenerierung und Verschlüsselung/Entschlüsselung dürfen nur auf Rechner erfolgen, die vor Angriffen aus dem Internet ausreichend geschützt sind. Die Maßnahmen entsprechen den Regelungen dieser Technischen Anlage Kap. 3.1.3 und Kap. 3.1.5.
- Getrennte Datenhaltung beim Dienstleister
  - Der Dienstleister muss verschlüsselte medizinische Daten getrennt von anderen Datenarten speichern, um den Beschlagnahmeschutz gem. § 97 Abs. 2 StPO zu gewährleisten.
- Vertrauenswürdigkeit des Dienstleisters
  - Der Dienstleister sollte vertrauenswürdig sein und über ein funktionierendes IT-Sicherheitsmanagement verfügen. Um dies zu beurteilen sind Zertifizierungen hilfreich, wie z. B. nach ISO27001, vom TÜV-IT, vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein. □

Medizinische Fortbildungstage Thüringen

vom 25. bis 28. Juni in Erfurt

Veranstalter: Landesärztekammer Thüringen, Kassenärztliche Vereinigung Thüringen

Tagungspräsident: Prof. Dr. med. Stein, Jena

Themen: Berufspolitisches Forum; Plenarthema „Konservative oder operative Behandlung?“; Seminare zu Psychosomatik, regenerativer Medizin, Transition, Notfallmanagement, Balint, Schweigepflicht, Geriatrie, Update Hygiene, Versorgung von Patienten mit Trachealkanülen, Niederlassung und Praxisabgabe, besonderes Angebot für junge Mediziner; Fortbildungsangebote für Praxis- und Pflegepersonal und MTA

Auskunft zum Programm/Anmeldung: Akademie für ärztliche Fort- und Weiterbildung der Landesärztekammer Thüringen, Postfach 10 07 40, 07707 Jena, Telefon: 03641 614-142, Fax: 03641 614-149, E-Mail: info@medizinische-fortbildungstage.org, Internet: www.medizinische-fortbildungstage.org □

46. Internationaler Seminarkongress in Grado/Italien

vom 24. bis 29. August

Collegium Medicinae Italo-Germanicum
in Zusammenarbeit mit der Bundesärztekammer

Die Veranstaltung wurde von der Bayerischen Landesärztekammer mit insgesamt 33 Fortbildungspunkten zertifiziert, pro Tag gibt es 6 Fortbildungspunkte.

Die Österreichische Ärztekammer erkennt diese Veranstaltung als Fortbildungsmaßnahme an.

Eröffnungsvortrag (24. 8., 16.00 Uhr): „Die Kunst, Arzt zu sein“ (Prof. Dr. Friedemann Nauck, Göttingen)

Schwerpunktthemen der Seminare (25.–29. 8.): Arbeits- und Umweltmedizin (Prof. Dr. Axel Buchter, Homburg/Saar); Impfseminar (Dr. Sigrid Ley-Köllstadt, Marburg); Notfallmanagement – Theorie (Prof. Dr. Peter Sefrin, Würzburg); Pädiatrie für Allgemeinmediziner (Teil 2) (PD Dr. Lothar Schrod, Frankfurt/M.); Palliativmedizin (Prof. Dr. Friedemann Nauck, Göttingen); interdisziplinäre Gespräche – **Kurse (mit Zusatzgebühr)**

Programmanforderung: Bundesärztekammer, Frau Del Bove, Herbert-Lewin-Platz 1, 10623 Berlin, Telefon: 030 400456-415, Fax: -429, E-Mail: cme@baek.de, im Internet unter http://www.bundesaerztekammer.depage.asp?his=1.102.156.11932. □