Maßnahmen zum Datenschutz

Ärztliche Schweigepflicht

Alle Angestellten sind per ihrem Arbeitsvertrag zur ärztlichen Schweigepflicht aufgeklärt und verpflichtet. Im Rahmen des Mikroqualitätsmanagements wird dies tagtäglich geprüft.

Konstante Weiterbildung

Im täglichen Umgang mit verschiedensten datenschutzrechtlichen Situationen in der Arzpraxis erfolgt die Liveanalyse von Vorgängen, entsprechenden Grenzsituationen und die Aufklärung über die rechtliche Grundlage. Damit geht, wie im Mikroqualitätsmanagement beschrieben, die Denkweise vom Hauptakteur, dem Arzt, auf die Angestellten über. Dies sorgt für eine interne Kontrolle.

Papieraktenprinzip

Es wird grundsätzlich eine Papierakte verwendet. In der Papierakte findet sich alle Dokumentation und der Briefverkehr bezüglich des Patienten. Elektronische Zwischenspeicherungen (z.B. Fax) werden ausgedruckt und unverzüglich in die Papierakte eingefügt. Die Zwischenspeicherungen werden entsprechend der Fristen aus dem Datenverarbeitungskatalog vorgehalten, falls ein eventueller weiterer Briefverkehr stattfindet, damit die Wirtschaftlichkeit gewahrt wird. Die Vernichtung der Papierakten erfolgt noch DIN-Norm.

Faxempfang

Beim Faxempfang werden die Faxe gesichtet. Wenn Patientendaten in einem Fax vorhanden sind, wird das Fax ausgedruckt und in die Papierakte eingefügt. Die Speicherfristen der Faxe sind im Katalog angegeben.

E-Mail

Patienten werden darauf hingewiesen, dass eine Kommunikation per E-Mail grundsätzlich verschlüsselt erfolgen soll. Eine initiale und unverschlüsselte Übermittlung des Patienten entspricht einer einer Einwilligung durch den Patienten für diese E-Mail und zur Weiterverarbeitung. Der Verkehr wird in die Papierakte eingefügt.

Abrechnung

Für die Abrechnung mit den einzelnen Kostenstellen sind wir gezwungen Daten elektronisch zu übertragen. Dazu haben die einzelnen Kostenstellen gesetzliche Grundlagen. Näheres ist dem Dossier der Bundesärztekammer zum Datenschutz zu entnehmen, besonders die einzelnen Gesetze mit entsprechenden Zitaten. Der Einfachheit halber sind diese hier nicht aufgeführt. Für die Buchhaltung der Privatrechnungen sind die Vorgaben der GOÄ zu beachten, die in der Rechnungsführung auch z.B. die Angaben der Diagnosen verlangen.

Laboranforderungen

Bei Anforderungen von Laborleistungen ist eine gesetzlich vorgeschriebene Identifizierung für die Analyse der Proben erforderlich. Hier erfolgt die Überweisung zwischen Ärzten in einer Laborgemeinschaft, die allesamt der ärztlichen Schweigepflicht unterliegen. Mit dem Einverständnis zur Blutabnahme erfolgt das Einverständnis in die Analyse. Die zu analysierenden Parameter erfordern eventuell weitere Einverständnisse (z.B. bei Genanalysen), über die der Patient separat aufgeklärt wird. Die Labore führen ihr jeweils eigenes Datenschutzmanagement durch.

Open Source

In der Praxis wird grundsätzlich Software mit offenem Quelltext verwendet. Nur mit einem offenen Quelltext ist die Vertifizierung der Kryptographiealgorithmen gegeben. Bei den eingesetzten Open-Source-Komponenten ist dies durch anerkannte Forscher durch das Vielaugenprinzip erfolgt. Wenn wir gezwungen sind lizenzierte und damit geschlossene Software zu verwenden, verweisen wir auf die Datenschutzmaßnahmen dieser Softwarehersteller. Hier ist eine Überprüfung durch uns nicht möglich. Insbesondere ist dies bei der DMP-Software und dem Praxisinformationssystem gegeben. Eine Überprüfung der Kryptographie kann daher durch uns nicht erfolgen und ist grundsätzlich anzuzweifeln. Die Philosophie der KV-Verwaltung ist hier leider 20 Jahre hinter dem aktuellen Stand der Softwareentwicklung und nicht uns anzulasten.

Gehärtete Betriebssysteme

Auf den Computern der Praxis werden gehärtete Linuxsysteme eingesetzt.

Sichere Interne Netzwerkkommunikation

Die einzelnen Terminals, Server und Arbeitsplätze kommunizieren grundsätzlich über SSH per Public-Key-Authentifizierung. Alternativpasswörter entsprechen den Vorgaben des BSI. Wenn aufgrund der rückständigen proprietären Entwicklungsphilosophie von Komponenten (Drucker, Medizingeräte) eine solche Kommunikation nicht gesichtet und kontrolliert werden kann, so ist sichergestellt, dass in diesen Netzwerksegmenten der gesamte Netzwerkverkehr auf unsicheren Verkehr kontrolliert wird.

Datensicherung

Jeden Tag werden die relevanten Daten gesichert auf einem Server, der in der Praxis in einem separat physisch abgesicherten Raum steht.

Zugriffskontrolle

Vor jeden Zugriff auf die Rechner erhielten und erhalten die Mitarbeiter eine entsprechende Einführung über die Nutzung und den Umgang mit den möglichen anfallenden Daten. Die Server für die Datensicherung sind nur durch den Datenverantwortlichen zugänglich. Im täglichen Praxisbetrieb sind bei Anwesenheit von Patienten immer Mitarbeiter in Sichtweite der Arbeitsplätze und kontrollieren Zugriffe. Im Sprechzimmer sind die Wechsel zwischen den Patienten so kurz gehalten, dass eine Einarbeitung und damit Informationsgewinnung im Praxisinformationssystem praktisch nicht möglich sind.

Telefongespräche

Die Gegenüber bei Telefongesprächen werden immer nach Ihrer Identität gefragt. Bei fehlender Identifizierung erfolgt keine Übertragung von eventuell zu schützenden Informationen. Auskünfte von Patienteninformationen erfolgen nur im Ausnahmefall. Grundsätzlich ist ein persönliches Vorbeikommen des Patienten erforderlich.

Privatsphäre im Praxisalltag

Arzt-Patienten-Gespräche finden grundsätzlich in abgetrennten Räumen statt. Am Empfang werden Patienten gebeten die von ihnen begonnen Gespräch in die Sprechzimmer zu verlegen.

Arztwechsel

Bei einem Arztwechsel wird grundsätzlich die Papierakte an den weiterbehandelnden Arzt versandt. Dies dient der Wirtschaftlichkeit und Vereinfachung der rechtlichen Komplexität (Grundsatzforderung der DSGVO).

Befundauskunft

Die Befundauskunft erfordert die Entbindung von der ärztlichen Schweigepflicht, die schriftlich vorliegen muss. Ausnahmen sind im Dossier der Bundesärztekammer zu lesen (u.a. Infektionsschutzgesetz).

Recht auf Vergessen

In der Praxis liegen die Hinweise für das Recht auf Vergessensein aus. Dies überschneidet sich mit den Vorgaben der Dokumentations- und Aufbewahrungspflicht des Arztes. Die Fristen sind im Katalog beschrieben.

Datenänderung

Siehe hierzu das Dossier der Bundesärztekammer, welches auch die Feinheiten der einzelnen Möglichkeiten und Unmöglichkeiten der Datenänderung durch den Patienten beschreibt.

Webseite

Die Webseite www.arztpraxis-lohmann.de speichert keine Logdateien im Interesse der Freiheit der Besucher.

Datenschutzverletzungen

Datenschutzverletzungen sind dem Geschäftsführer zu melden. Dieser bearbeitet mit dem Datenschutzverantwortlichen den Vorfall. Innerhalb von 72 Stunden (außer bei Wochenendverzug) wird durch den Datenschutzbeauftragten der Vorfall an die zusätzliche Datenschutzbehörde gemeldet:

Sächsischer Datenschutzbeauftragter
Bernhard-von-Lindenau-Platz 1, 01067 Dresden

Stand: 2018-06-13

gez.

Datenverantwortlicher