Schulungskompendium

Fragen und Antworten zum Datenschutz Teil 3

Einführung in das MCSS Schulungskompendium

Das digitale MCSS Schulungs- und Einweisungssystem basiert auf den jeweils aktuellen Rahmenbedingungen für die Rechtskonformität in medizinischen Einrichtungen. Für die Anwendung der innovativen didaktischen Schulungen gelten folgende Richtlinien.

- Pro Frage sind etwa 1,5 – 2,0 Minuten aufzuwenden.
- Zuerst wird die Frage reflektiert und überlegt, welche Antworten gegeben werden können (evtl. mit schriftlichen Notizen).
- Anschließend werden die Überlegungen/Notizen mit den richtigen Antworten verglichen.
- Nach ca. 45 Minuten (ca. 20 Fragen und Antworten) sollte eine Konzentrationspause eingelegt werden.

Die Anwendung wird in MCSS protokolliert und die Anwendungsstatistik gilt als Nachweisdokument für die rechtlichen Audit Anforderungen.

Teil 3: Datenschutz in der Leitung

Teil 3: Datenschutz in der Leitung

Welche Rahmenbedingungen definieren die Datenschutzanforderungen in medizinischen Einrichtungen?

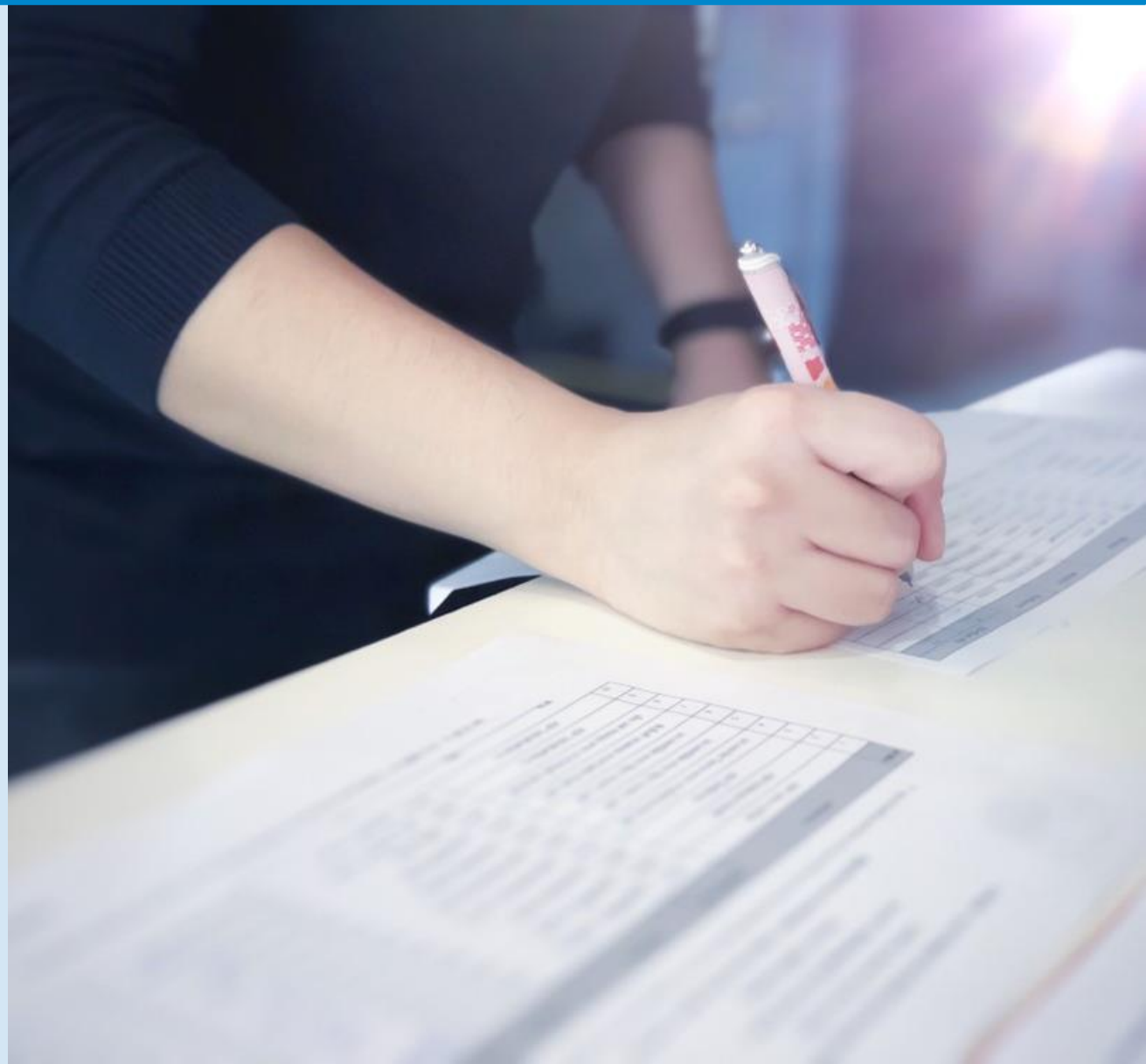
Welche Rahmenbedingungen definieren die Datenschutzanforderungen in medizinischen Einrichtungen?

Die folgenden Anforderungen sind bei dem Datenschutzmanagement in medizinischen Versorgungseinrichtungen „parallel“ zu beachten:

- Ärztliche Schweigepflicht nach § 9 Abs. 1 MBO-Ä und korrespondierende Regelungen der Berufsordnungen (Landesärztekammern)
- Datenschutz-Grundverordnung DSGVO nach EU Recht
- Bundesdatenschutzgesetz neu (BDSG neu) nach deutschem Recht
- Qualitätsmanagement Richtlinie des Gemeinsamen Bundesausschusses GBA-QMRL (im Bereich der Kassenmedizin)

Teil 3: Datenschutz in der Leitung

Wer ist in einer Praxis oder Klinik verantwortlich für den Datenschutz nach DSGVO und BDSG?



Wer ist in einer Praxis oder Klinik verantwortlich für den Datenschutz nach DSGVO und BDSG?

Verantwortlich im Sinn der DSGVO ist grundsätzlich der leitende Arzt. Er kann die Verantwortung nicht delegieren / übertragen. In einer Gemeinschaftspraxis können die Ärzte einen Kollegen als Hauptverantwortlichen und auch einen Stellvertreter benennen.

Der / die Datenschutzbeauftrage hat keine Weisungsbefugnis und ist nur verpflichtet, die Leitung laufend und zeitnah zu unterrichten.

Teil 3: Datenschutz in der Leitung

Welche Risiken sind mit Verstößen gegen Datenschutz-Rahmenbedingungen inkl. Schweigepflicht verbunden?

Welche Risiken sind mit Verstößen gegen Datenschutz-Rahmenbedingungen inkl. Schweigepflicht verbunden?

Die ärztliche Schweigepflicht ergibt sich auch als Zusatzpflicht aus dem zwischen Arzt und Patient geschlossenen Behandlungsvertrag, der seit dem Inkrafttreten des Patientenrechtegesetzes in den §§ 630a ff. Bürgerliches Gesetzbuch (BGB) geregelt ist. Mit der ärztlichen Schweigepflicht korrespondiert das durch § 203 des Strafgesetzbuches (StGB) geschützte Patientengeheimnis, das entsprechende Verstöße des Arztes gegen die Verschwiegenheitspflicht strafrechtlich sanktioniert. Nach § 203 Abs.1 StGB wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wer unbefugt ein fremdes „Geheimnis“, das ihm als Arzt anvertraut worden ist preisgibt.

Nach DSGVO können bei Datenschutzverstößen relativ hohe Strafen verhängt werden. Diese richten sich nach der Schwere der „Datenpannen“ und nach den Umsatzgrößen der Einheit. Liegt kein Datenschutzmanagementsystem (DSMS) vor, so fallen die Sanktionen höher (Artikel 83 d) aus.

Höhere Risiken stellen mögliche Schadensersatzansprüche geschädigter Patienten dar.

Teil 3: Datenschutz in der Leitung

Welche Risiken stellen Schadensersatzansprüche von Patienten dar?

Welche Risiken stellen Schadensersatzansprüche von Patienten dar?

Werden Datenschutzrechte von Patienten verletzt, so können diese Schadensersatzansprüche nach DSGVO einklagen. Neu ist dabei, dass neben materiellen auch immaterielle Ansprüche geltend gemacht werden können. Da es noch keine umfassende Rechtsprechung gibt, können bislang keine Prognosen zu der Höhe möglicher Ersatzansprüche gemacht werden.

Mit entsprechenden Haftpflichtversicherungen können Schadensersatzansprüche im Regelfall mit Selbstbeteiligungen abgemildert werden.

Teil 3: Datenschutz in der Leitung

Welche Versicherungen gibt es bei Schäden aus Verstößen gegen Datenschutz Verletzungen?

Welche Versicherungen gibt es bei Schäden aus Verstößen gegen Datenschutz Verletzungen?

Gegen Sanktionen / Strafen der Aufsichtsbehörden gibt es keine Versicherungen. Die beste Absicherung ist ein professionelles DSMS. Nach Artikel 83 DSGVO werden die Sanktionen nach einem Bewertungskatalog festgelegt. Fahrlässigkeit und das Fehlen eines Datenschutzmanagementsystems (DSMS) erhöhen die Strafzahlungen.

Bei Schäden aus Schadenersatzansprüchen kann eine erweiterte Berufshaftpflichtversicherung ganz oder teilweise eine Deckung darstellen.

Teil 3: Datenschutz in der Leitung

Welches sind die wichtigsten Maßnahmen und in welcher Reihenfolge sollten sie umgesetzt werden?

Welches sind die wichtigsten Maßnahmen und in welcher Reihenfolge sollten sie umgesetzt werden?

An den Anfang sollte eine Analyse zu den Datenschutzanforderungen der Praxis gestellt werden. Dabei ist es wichtig, ob die Praxis bereits ein Qualitätsmanagementsystem (QMS) einsetzt. Ist dies der Fall, wird eine Ist-Analyse erstellt, nach der die DS Maßnahmen QM-kompatibel definiert werden (z.B. nach ISO 9001, QEP etc.). Wird noch kein QMS eingesetzt, ist ein Datenschutz Projektplan auf der Grundlage einer Analyse zu erstellen:

- Erstellung des Verzeichnisses der Verarbeitungstätigkeiten
- Analyse und Planung der „Technischen und Organisatorischen Maßnahmen“
- Prüfung vorhandener Strukturen im QMS (falls im Einsatz nach ISO oder QEP)
- Erfüllung der Rechenschaftspflicht (Rechenschaftspflicht-Bericht)

Ab 20 Ärzten / Mitarbeitern sind die Regelungen zur Berufung der Datenschutzbeauftragten zu berücksichtigen

Teil 3: Datenschutz in der Leitung

Was bedeutet die
Rechenschaftspflicht nach DSGVO?

Was bedeutet die Rechenschaftspflicht nach DSGVO?

Die Rechenschaftspflicht bedeutet, dass der Verantwortliche (Arzt) nachweisen und belegen können muss, dass er – bspw. im Fall von Art. 5 DSGVO – die Grundsätze des Art. 5 DSGVO einhält und – im Fall von Art. 24 DSGVO – die Verarbeitung personenbezogener Daten entsprechend der Grundverordnung befolgt. Dazu gehört auch angemessene technische und organisatorische Maßnahmen zu ergreifen.

Nachweisen bedeutet, dass die Praxis auf Nachfrage der Aufsichtsbehörde belegen kann, dass sie die Vorgaben der DSGVO erfüllt. Praxen sollten einen Rechenschaftsbericht vorbereiten und auf Anforderung der Aufsichtsbehörde die entsprechende Dokumentation vorlegen können.

Teil 3: Datenschutz in der Leitung

In welcher Form sollten Patienten informiert werden?

In welcher Form sollten Patienten informiert werden?

Die Praxisleitung hat die Patientenaufklärungsstrategie festzulegen (Patientenaufklärungsmanagement) und entsprechende Prozesse einzuleiten bzw. zu delegieren. Aushänge oder gedruckte Merkblätter sind zu entwickeln und den Patienten zu den häufigsten Fragestellungen zur Verfügung zu stellen.

Ebenfalls sollten alle Mitarbeiter in der Patientenversorgung professionell geschult werden, damit eine qualifizierte Kommunikation (insbesondere auch zum Datenschutz) gewährleistet wird.

Teil 3: Datenschutz in der Leitung

Welcher Zusammenhang besteht zwischen Qualitätsmanagement und Datenschutz

Welcher Zusammenhang besteht zwischen Qualitätsmanagement und Datenschutz

Nach der QM-Richtlinie des GBA (GBA-QMRL) sind Kassenärzte verpflichtet, ein Qualitätsmanagementsystem einzurichten und zu pflegen. Die meisten niedergelassenen Ärzte und alle Kliniken setzen dadurch bereits seit Jahren QM ein. Damit werden von aktuellen QM-Systemen bereits viele DSGVO Anforderungen formal erfüllt. Allerdings ist in jedem Fall eine Synchronisierung durchzuführen, um Überschneidungen und widersprüchliche Anweisungen auszuschließen.

Teil 3: Datenschutz in der Leitung

Welches System hat einen höheren Stellenwert: QMS oder DSMS?

Welches System hat einen höheren Stellenwert: QMS oder DSMS?

Durch die Ratifizierung der DSGVO in Kombination mit BDSG und der ärztlichen Schweigepflicht stellt ein Datenschutzmanagementsystem eine höhere Anforderung an Praxen und Kliniken. Der Datenschutz mit den komplexen Rahmenbedingungen hat in jedem Fall rechtlich gesehen Vorrang vor dem Qualitätsmanagement. Allerdings kann aus einem professionellen QMS (ISO 9001 oder QEP) mit geringerem Aufwand auch ein DSMS entwickelt werden.

Teil 3: Datenschutz in der Leitung

Welche Auswirkungen hat die DSGVO auf Zertifizierungen nach ISO 9001:2015?

Welche Auswirkungen hat die DSGVO auf Zertifizierungen nach ISO 9001:2015?

Die ISO 9001 Qualitätsnorm fordert Aufzeichnungen über das wirksame Funktionieren des Qualitätsmanagementsystems. Der Datenschutz regelt darin die Voraussetzungen und Folgen einer personenbezogenen Erhebung und Verwendung von Daten. Datenschutz schützt nicht die Daten, sondern bewahrt natürliche Personen vor dem Missbrauch ihrer persönlichen Daten. Das ISO basierte QM-System ist nach den neuen Anforderungen der DSGVO zu aktualisieren. Die TOM (technischen und organisatorischen Maßnahmen im Sinne der DSGVO) sind im Kontext von ISO 9001:2015 Verfahrensanweisungen, z.B. zu der Erhebung der Anamnese, zur Schulung zu DSGVO etc.

Teil 3: Datenschutz in der Leitung

Wie ist ein QM System nach QEP zu aktualisieren?

Wie ist ein QM System nach QEP zu aktualisieren?

Datenschutz wird im QEP-System (Qualität und Entwicklung in Praxen) in Kapitel 4.5.2 qualifiziert behandelt. Allerdings müssen wesentliche Anforderungen zusätzlich erfüllt werden. Die KBV stellt dazu Informationen und Vorlagen zur Verfügung.

In jedem Fall sollten QMS und DSMS synchronisiert werden.

Teil 3: Datenschutz in der Leitung

Wann muss ein Datenschutzbeauftragter berufen werden?

Wann muss ein Datenschutzbeauftragter berufen werden?

Ein Datenschutzbeauftragter ist grundsätzlich dann zu berufen, wenn Datenschutz-Folgenabschätzungen in Praxis oder Klinik notwendig sind. Dies ist immer dann der Fall, wenn besondere Datenverarbeitungen (früher Verarbeitung sensibler Daten) angenommen werden müssen. Formulierung: Ein DSB ist erforderlich, wenn die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten“ besteht. Dazu gehören Nach Art. 9 DSGVO auch „Gesundheitsdaten“.

Als Faustregel gilt: ab 3 Ärzten in einer Praxis sollten die Bedingungen nach Artikel 37 ff DSGVO individuell geprüft werden.

Außerdem ist die Berufung eines DSB zwingend vorgeschrieben bei Erreichen der 20 Personen Grenze (Ärzte und alle Mitarbeiter, die mit personenbezogenen Daten in Berührung kommen).

Teil 3: Datenschutz in der Leitung

Wie wird der DSB berufen und registriert?

Wie wird der DSB berufen und registriert?

Der Datenschutzbeauftragte wird offiziell von der Leitung schriftlich berufen.
Anschließend wird er zwingend und zeitnah der zuständigen Aufsichtsbehörde gemeldet.
Dies ist die jeweilige Landes-Datenschutzbehörde.

Teil 3: Datenschutz in der Leitung

Wer kann DSB sein?

Wer kann DSB sein?

Die Praxis kann einen internen DSB (Mitarbeiter) berufen, wenn dieser die Voraussetzungen erfüllt. Dieser ist dann weisungsfrei und muss von der Praxisleitung unterstützt werden.

Die Berufung eines externen DSB ist eine praktische Alternative.
Er muss ebenfalls der Landesbehörde für den Datenschutz gemeldet werden.

Teil 3: Datenschutz in der Leitung

Kann der interne DSB gekündigt werden?

Kann der interne DSB gekündigt werden?

Gem. Art. 38 Absatz 3 DSGVO dürfen Datenschutzbeauftragte wegen der Erfüllung ihrer Aufgaben weder abberufen noch benachteiligt werden. §§ 38 Absatz 2, 6 Absatz 4 BDSG n.F. erweitert diesen Schutz noch über das DSGVO hinaus. Für interne Datenschutzbeauftragte gilt somit ein besonderer Kündigungsschutz nach dem BDSG. Demnach ist eine Kündigung des Arbeitsverhältnisses grundsätzlich unzulässig.

Eine Ausnahme ist nur dann möglich, wenn Tatsachen vorliegen, die eine Kündigung aus wichtigem Grund notwendig machen. Für die Kündigung gelten dann die sehr strengen Voraussetzungen des § 626 BGB.

Teil 3: Datenschutz in der Leitung

Kann der externe DSB gekündigt werden?

Kann der externe DSB gekündigt werden?

Externe Datenschutzbeauftragte genießen keinen Kündigungsschutz. Sie stehen in keinem Arbeitsverhältnis mit dem Unternehmen, dies unterscheidet sie von den internen Datenschutzbeauftragten, für die wiederum der Kündigungsschutz gilt. Wenn ein externer Datenschutzbeauftragter abberufen werden soll, muss seine Benennung widerrufen werden. Dann kann der Dienstleistungsvertrag gekündigt werden.

Teil 3: Datenschutz in der Leitung

Was ist zu empfehlen: Interner oder externer Datenschutzbeauftragter?

Was ist zu empfehlen: Interner oder externer Datenschutzbeauftragter?

Die Wahl zwischen einem internen oder externen DSB ist nur nach individuellen Gesichtspunkten zu entscheiden. Die meisten medizinischen Einrichtungen, die einen nach DSGVO einen Datenschutzbeauftragten einstellen müssen, entscheiden sich für externe Beauftragte. Damit ist der Kündigungsschutz ausgeschlossen und die internen Kapazitäten können für andere Aufgaben geschont werden.

Teil 3: Datenschutz in der Leitung

Welche Aufgaben haben Datenschutzbeauftragte?

Welche Aufgaben haben Datenschutzbeauftragte?

Die wichtigsten Aufgaben des DSB:

- Entwicklung eines DSMS unter Berücksichtigung aller DS-Rahmenbedingungen
- Regelmäßige Schulungen der Leitung und aller Mitarbeiter
- Überwachung der wichtigen TOM
- Berichte an die Leitung und Unterstützung bei der Erfüllung der Rechenschaftspflicht
- Durchführung der regelmäßigen Audits

Zusätzlich sollte der DSB seine Aufgaben mit dem QM-Beauftragten synchronisieren, um Kapazitäten zu schonen und Synergien zu nutzen.

Teil 3: Datenschutz in der Leitung

Wie wird der Empfangsbereich nach Datenschutz Rahmenbedingungen organisiert?

Wie wird der Empfangsbereich nach Datenschutz Rahmenbedingungen organisiert?

Am Empfang ist eine sogenannte Diskretionszone einzurichten. Dazu gehört eine Markierung, die die Patienten deutlich erkennen können und entsprechend Abstand halten können.

Die Bildschirme sind so auszurichten, dass nur die Mitarbeiter Einsicht auf Patientendaten haben. Außerdem gehören keine Papierakten oder Laufzettel mit Personendaten an die Rezeption.

Die Mitarbeiter am Empfang sind speziell in die diskrete Kommunikation einzuweisen. Wird am Empfang auch mit Patienten telefoniert, sind besondere technische und organisatorische Maßnahmen zu definieren (TOM).

Teil 3: Datenschutz in der Leitung

Welche Maßnahmen sind bei Datenpannen zu veranlassen?

Welche Maßnahmen sind bei Datenpannen zu veranlassen?

Wird eine Datenpanne festgestellt, muss diese der zuständigen Datenschutzbehörde (das Landesamt für die Datenschutzaufsicht) innerhalb von 72 Stunden angezeigt werden.

Bei der betroffenen Person bzw. dem betroffenen Unternehmen gelten andere zeitliche Vorgaben. Hierbei ist man dazu verpflichtet, die Meldung unverzüglich durchzuführen. „Unverzüglich“ bedeutet, dass die Meldung so schnell wie nur möglich durchzuführen ist.

Faustregel: Je risikobehafteter die Datenschutzverletzung ist, desto schneller sollte die Meldung erfolgen.

Teil 3: Datenschutz in der Leitung

Wie häufig müssen Datenschutz Schulungen durchgeführt werden?

Wie häufig müssen Datenschutz Schulungen durchgeführt werden?

Es besteht die gesetzliche Schulungspflicht nach Artikel 39 Abs. 1 a) DSGVO.
Die Überwachung der Sensibilisierung und Schulung von Mitarbeitern wird als Aufgabe des Datenschutzbeauftragten angesehen (Artikel 39 Abs. 1 lit. b) DSGVO) und sollte auch fester Bestandteil des Datenschutzmanagements im Unternehmen sein.
Im Regelfall reicht eine nachgewiesene Schulung alle 12 Monate aus.
Aus aktuellen Anlässen und bei Veränderungen werden Trainings alle 6 Monate empfohlen.