Schulungskompendium

Fragen und Antworten zum Datenschutz in der IT und Administration

Einführung in das MCSS Schulungskompendium

Das digitale MCSS Schulungs- und Einweisungs-System 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 2: Datenschutz in der IT und Administration

Teil 2: Datenschutz in der IT und Administration

Welche Datenverarbeitungs-prozesse sind unter Datenschutz-Gesichtspunkten besonders sensibel?

Welche Datenverarbeitungsprozesse sind unter Datenschutz-Gesichtspunkten besonders sensibel?

In den meisten Praxen und Kliniken werden IT Anwendungen intensiv eingesetzt.
Viele medizinische Einrichtungen arbeiten bereits mit papierlosen Patientenakten.
Diese Entwicklung stellt an den Datenschutz besonders hohe Ansprüche und deshalb ist die Analyse der digitalen Datenverarbeitungsprozesse an den Anfang der DSGVO-Umsetzung zu stellen.

Teil 2: Datenschutz in der IT und Administration

Welche rechtlichen Rahmenbedingungen gelten insbesondere auch für den Datenschutz bei Einsatz digitaler Datenverarbeitung?

Welche rechtlichen Rahmenbedingungen gelten insbesondere auch für die digitale Datenverarbeitung?

Die folgenden rechtlichen Rahmenbedingungen sind bei dem Datenschutzmanagement in medizinischen Versorgungseinrichtungen 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)
- Empfehlungen der Bundesärztekammer und KBV zur digitalen Datenverarbeitung (im Bereich der Kassenmedizin)

Teil 2: Datenschutz in der IT und Administration

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

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

Verantwortlich im Sinn der DSGVO ist grundsätzlich der leitende Arzt, auch für die Informationstechnologie. Er kann die Verantwortung nicht delegieren / übertragen.
Wenn ein Datenschutzbeauftragter berufen ist, sollte dieser unbedingt IT-Kompetenz haben und Schulungen / Einweisungen durchführen. Im Bereich der IT ist dies besonders kritisch, da häufig die Kompetenz im eigenen Team für IT und Datenschutz fehlen.

Teil 2: Datenschutz in der IT und Administration

Welche IT Bereiche sind im Kontext des Datenschutzes besonders sensibel?

Welche IT Bereiche sind im Kontext des Datenschutzes besonders sensibel?

Die folgenden Prozesse sind nach DSGVO besonders zu analysieren:

- Schnittstellen und Datenübertragungen zwischen mehreren internen Systemen (z.B. digitaler Terminkalender, Medizintechnik Schnittstellen, interne Messenger Systeme etc.)
- Prozesse der Datensicherung inkl. der geschützten langfristigen Aufbewahrung
- Externe Datenübertragungen (z.B. PVS, Qualitätssicherungsprojekte, besondere Abrechnungsverfahren [ambulante Chirurgie, Ärztenetze und MVZ Strukturen]).
- Rekonstruktion von Datenbanken bei Störfällen mit Datenverlusten

Im Regelfall sind Experten (mit AV Verträgen) in den Analyse Prozess einzubeziehen, wenn die Leitung und der DSB nicht über die erforderliche IT-Qualifikation verfügen (siehe IT-Koordinator).

Teil 2: Datenschutz in der IT und Administration

Wie sind interne systemübergreifende Datenverarbeitungsprozesse nach DSGVO zu behandeln?

Wie sind interne systemübergreifende Datenverarbeitungs-prozesse nach DSGVO zu behandeln?

In vielen Praxen und Kliniken werden IT-Systeme von unterschiedlichen Anbietern eingesetzt, die intern personenbezogene Daten austauschen (z.B. EPA und Terminkalender und Medizin-technik / Bildverarbeitung und EPA etc.). Nach den Vorgaben der DSGVO sind die Prozesse und die Datenkategorien (Stammdaten, Befunde, Diagnosen, Therapien) genau zu analysieren und zu dokumentieren:

- Welche internen Datenübertragungen sind im Einsatz?
- Welche Daten werden übertragen (medizinisch, administrativ)?

In diesem Kontext sind Diagnosen oder Diagnose Codes besonders sensibel zu behandeln (z.B., wenn der Termin als Besuchsgrund eine sensible Diagnose enthält).

Teil 2: Datenschutz in der IT und Administration

Welche Vorkehrungen sind bei allen Datensicherungsprozessen im Rahmen der TOM Anforderungen zu realisieren?

Welche Vorkehrungen sind bei allen Datensicherungsprozessen im Rahmen der TOM Anforderungen zu realisieren?

Alle Praxen und Kliniken müssen ihre personenbezogenen digitalen Daten nach den besten verfügbaren technischen Möglichkeiten sichern (z.B. nach der rechtlich-bindenden Aufbewahrungspflicht). In den meisten medizinischen Einrichtungen stellen diese Datensicherungsprozesse die größten Risiken für „Datenpannen“ dar. Vielfach wird empfohlen, die Datensicherungen außerhalb der gesicherten Praxisräume aufzubewahren.
Damit werden hohe Ansprüche an die Sicherung während des Transports und auch an die Aufbewahrungsräume (z.B. Tresor in Privaträumen) gestellt.

Teil 2: Datenschutz in der IT und Administration

Wie können Datensicherungen geschützt und rechtskonform aufbewahrt werden?

Wie können Datensicherungen geschützt und rechtskonform aufbewahrt werden?

Die technischen Möglichkeiten der Datensicherungen hängen stark von der vorhandenen IT-Infrastruktur ab. Im Rahmen der DSGVO Umsetzung werden die unterschiedlichen Datensicherungsstrategien mit dem oder den IT-Partnern zu eruieren sein.
Die verschiedenen Alternativen haben alle Vor- und auch Nachteile (z.B. cloudbasierte Sicherung gegenüber traditionellen Speichermedien). Diese sind in einem Auswahlverfahren zu dokumentieren, in das Datenschutzmanagement aufzunehmen und in den Rechenschaftsbericht zu integrieren. Bei Einsatz eines QMS sind die relevanten Verfahrensanweisungen mit Priorität zu erstellen.

Teil 2: Datenschutz in der IT und Administration

Welche externen Datenübertragungen sind Standard und welche Prozesse sind datenschutzrechtlich sensibel (AV Verträge)?

Welche externen Datenübertragungen sind Standard und welche Prozesse sind datenschutzrechtlich sensibel (AV Verträge)?

Datenübertragungen und die Verarbeitung personenbezogener Daten im Rahmen der Abrechnung für Standardbehandlungen der Kassen- und Privatpatienten sind nach den Anforderungen der DSGVO nicht relevant für AV Verträge. Das Gleiche gilt für Überweisungen von Patienten an andere Fachärzte.

Davon zu unterscheiden sind z.B. Datenaustausch-Prozesse für wissenschaftliche Studien, Qualitätssicherungsprojekte, MVZ - und DZ - Kooperationen und Disease Management Projekte (DMP).

Teil 2: Datenschutz in der IT und Administration

Sind im Sinn der DSGVO die Kassenärztlichen Vereinigungen Auftragsverarbeiter?

Sind im Sinn der DSGVO Kassenärztliche Vereinigungen Auftragsverarbeiter?

Die KBV ist kein Auftragsverarbeiter im Sinn der DSGVO, da die personenbezogenen Daten auf der Grundlage von gültigen Rechtsvorschriften zur Aufgabenerfüllung Dritter erfolgt.

Der Vollständigkeit halber wird empfohlen diesen Sachverhalt in die Liste der Auftragsdatenverarbeitung (ADV) ohne AV Vertrag aufzunehmen.

Teil 2: Datenschutz in der IT und Administration

Sind Laborpraxen Auftragsverarbeiter?

Sind Laborpraxen Auftragsverarbeiter?

Wird ein Labor oder ein ähnlicher Dienstleister in Anspruch genommen, so werden von dem Dienstleister eigene Leistungen unter der alleinigen Verantwortung erbracht. Dadurch entfallen AV Verträge für Labor-Untersuchungen. Diese Rechtsauffassung entspricht dem Kenntnisstand von September 2019.

Teil 2: Datenschutz in der IT und Administration

Sind Steuerberater, Wirtschaftsprüfer, Banken etc. Auftragsverarbeiter im DSGVO Kontext?

Sind Steuerberater, Wirtschaftsprüfer, Banken etc. Auftragsverarbeiter im DSGVO Kontext?

Eine Gruppe von Dienstleistern für Ärzte erbringen fremde Fachleistungen mit eigener Verantwortlichkeit. Dazu gehören z.B. Steuerberater, Wirtschaftsprüfer, Anwälte, Inkasso-Unternehmen usw. (siehe Artikel 6 DS GVO).

Auch in diesen Fällen werden keine AV Verträge benötigt.

Teil 2: Datenschutz in der IT und Administration

Wann ist eine steuerliche Betriebsprüfung DSGVO relevant?

Wann ist eine steuerliche Betriebsprüfung DSGVO relevant?

Unter bestimmten Voraussetzungen haben Steuerberater, Anwälte Notare, Wirtschaftsprüfer und Ärzte ein Auskunftsverweigerungsrecht (BFH, 28.10.2009 VIII R 78/05 BStBl 2010 II S 455). Insoweit können sich also Ärzte bei steuerlichen Betriebsprüfungen auf die Schweigepflicht berufen, wenn es um die Offenlegung von Patientenunterlagen geht.
Allerdings ist eine rechtliche Beurteilung in jedem individuellen Einzelfall notwendig.

Teil 2: Datenschutz in der IT und Administration

Wann ist eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen?

Wann ist eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen?

Die DSFA ist ein wichtiger Bestandteil des neu eingeführten Konzepts des „risikoorientierten Ansatzes" im Datenschutz, der sich durch die DSGVO wie ein roter Faden zieht. Eine DSFA soll gerade bei Verarbeitungen von sensiblen personenbezogenen Daten (Gesundheitsdaten), bei denen ein hohes Risiko für die von der Verarbeitung betroffenen Personen besteht, eine Risikominimierung bewirken (z.B. bei Praxisaufgaben und -zusammenlegungen).

Allgemein gilt, dass für jede Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, die aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte natürlicher Personen zur Folge hat, vorab eine Datenschutz-Folgenabschätzung durchgeführt werden muss (Beispiel DMP Brustkrebs).

Teil 2: Datenschutz in der IT und Administration

Inwieweit ist die Praxis / Klinik für die Sicherheit der Telematikinfrastruktur verantwortlich?

Inwieweit ist die Praxis / Klinik für die Sicherheit der Telematikinfrastruktur verantwortlich?

Nach einer Stellungnahme des Bundesbeauftragten für den Datenschutz (BfDI) vom 30.06.2018 endet die Verantwortung der Praxis / Klinik am Telematik-Konnektor in der Praxis.

Für die externe Telematikinfrastruktur liegt die Verantwortung des Datenschutzes bei der BÄK, der KBV und den Landeskrankenversicherungen.

Teil 2: Datenschutz in der IT und Administration

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 rechtlich relevant, 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 2: Datenschutz in der IT und Administration

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 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 (TOM) 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 2: Datenschutz in der IT und Administration

Welcher Zusammenhang besteht im Bereich Informationstechnologie zwischen Qualitätsmanagement und Datenschutz?

Welcher Zusammenhang besteht im Bereich IT zwischen QM 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 der Systeme durchzuführen, um Überschneidungen und widersprüchliche Anweisungen auszuschließen.

Teil 2: Datenschutz in der IT und Administration

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 dem BDSG neu und der Verpflichtung zur 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 2: Datenschutz in der IT und Administration

Wie ist ein QM System nach QEP zu aktualisieren?

Wie ist ein QM System nach QEP zu aktualisieren?

Informationstechnologie und Datenschutz werden im QEP System (Qualität und Entwicklung in Praxen) in den Kapiteln 4.5.1 und 4.5.2 behandelt. Allerdings müssen wesentliche Anforderungen zusätzlich erfüllt werden. Die KBV stellt dazu Informationen und Vorlagen zur Verfügung.

QMS und DSMS sollten unbedingt synchronisiert werden.

Teil 2: Datenschutz in der IT und Administration

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 nach DSGVO einen Datenschutz-Beauftragten einstellen müssen, entscheiden sich für externe Beauftragte. Damit ist der Kündigungsschutz der internen DSB ausgeschlossen und die internen Kapazitäten können für andere Aufgaben geschont werden.

Achtung: Externe DSB sollten in jedem Fall Referenzen aus dem Bereich der Arztpraxen und Kliniken nachweisen, da die DS Anforderungen für Ärzte sehr spezifisch sind.

Teil 2: Datenschutz in der IT und Administration

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 2: Datenschutz in der IT und Administration

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 2: Datenschutz in der IT und Administration

Welche Maßnahmen sind bei Datenpannen im IT-Bereich zu veranlassen?

Welche Maßnahmen sind bei Datenpannen im IT-Bereich 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 2: Datenschutz in der IT und Administration

Wie häufig müssen Datenschutz Schulungen im IT-Bereich durchgeführt werden?

Wie häufig müssen Datenschutz Schulungen im IT-Bereich 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 aktuellen Anlässen und bei Veränderungen werden Trainings alle 6 Monate empfohlen.

Teil 2: Datenschutz in der IT und Administration

Darf die Praxis Auskunft an Krankenkassen und Gesundheitsämtern geben?

Darf die Praxis Auskunft an Krankenkassen und Gesundheitsämtern geben?

Patientendaten dürfen nur basierend auf einer klar definierten Rechtsgrundlage weitergegeben werden. Entweder muss die Einwilligung des Patienten mit Entbindung der Schweigepflicht erfolgen, oder es besteht eine ausdrückliche Rechtsnorm.

Vertragsärztliche Anforderungsformulare basieren auf Rechtsnormen.
Wenn kein Formular vorliegt, muss die Rechtsgrundlage schriftlich angegeben werden.

Anders verhalten sich Mitteilungen an Gesundheitsämter bei meldepflichtigen Diagnosen (z.B. IFSG).

Teil 2: Datenschutz in der IT und Administration

Wie sind Anfragen von Apotheken zu Rezepten zu behandeln?

Wie sind Anfragen von Apotheken zu Rezepten zu behandeln ?

Anfragen zu Rezepten, die von der Praxis ausgestellt wurden, können Mitarbeitern einer Apotheke telefonisch beantwortet werden.

Teil 2: Datenschutz in der IT und Administration

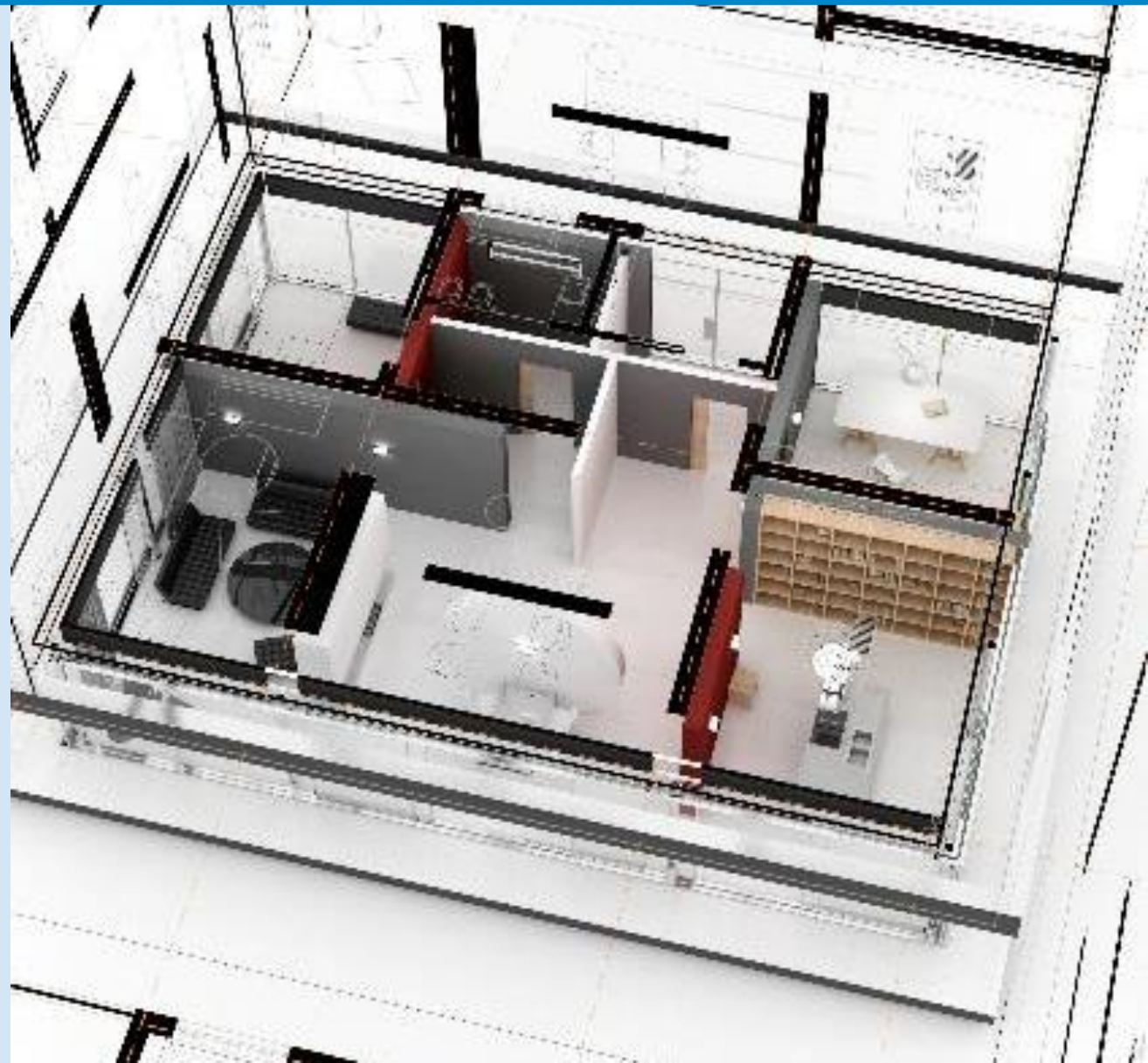
Dürfen Patienten weiterhin mit Namen aus den Wartezonen aufgerufen werden?

Dürfen Patienten weiterhin mit Namen aus den Wartezonen aufgerufen werden?

Auch nach Inkrafttreten der DSGVO sind Patienten mit Namen zur Behandlung aufzurufen. Allerdings sollten weitergehende Aufforderungen an Patienten (beispielsweise zu besonderen Untersuchungen) nur diskret kommuniziert werden.

Teil 2: Datenschutz in der IT und Administration

Muss das Verzeichnis der Verarbeitungstätigkeiten nur einmalig erstellt werden oder in regelmäßigen Abständen?



Muss das Verzeichnis der Verarbeitungstätigkeiten nur einmalig erstellt werden oder in regelmäßigen Abständen?

Das Verzeichnis soll immer auf dem aktuellen Stand gehalten werden. Bei neuen Projekten oder veränderten Prozessen muss das Verzeichnis aktualisiert werden. Im jährlichen Audit sollte ebenfalls eine Überprüfung der Aktualität erfolgen.

Die Aktualität ist auch Teil der Rechenschaftspflicht im Kontext des DSGVO.

Teil 2: Datenschutz in der IT und Administration

Wann sind Provider von Websites auch Auftragsverarbeiter?

Wann sind Provider von Websites auch Auftragsverarbeiter?

Das Hosten einer Website ist in Standardfällen keine Auftragsverarbeitung, da keine personenbezogenen Daten übermittelt werden.

Das ändert sich, wenn die Website auch eine Kommunikationsplattform zur Verfügung stellt und personenbezogen Daten übermittelt oder gespeichert werden (z.B. digitale Terminkalender).

(Quelle: KBV.de)

Teil 2: Datenschutz in der IT und Administration

Dürfen Bilder von Patienten in der elektronischen Patientenakte gespeichert werden?

Dürfen Bilder von Patienten in der elektronischen Patientenakte gespeichert werden?

Bilder von Patienten, die nur dem Wiedererkennen für das Praxisteam dienen, können nur auf der Grundlage einer Einwilligung des Patienten erfolgen.

Medizinische Fotos sind dagegen Bestandteil der ärztlichen Dokumentation und sind auch ohne Einwilligung (z.B. zur Befundsicherung) zu speichern.

Teil 2: Datenschutz in der IT und Administration

Was ist bei der Nutzung des Internets in der Praxis zu beachten?

Was ist bei der Nutzung des Internets in der Praxis zu beachten?

Die Verbindung des Praxisnetzwerks (EPA) mit dem Internet ist unter dem Gesichtspunkt möglicher Datenpannen genau zu prüfen. Die sicherste Variante ist die Trennung der EPA Anwendung von Internet-Rechnern. In der Praxis ist aber häufig aus Informationsgründen die Verbindung sinnvoll. Dazu gibt es verschiedene technische Möglichkeiten, die 2 lokale und unabhängige Netzwerke sicher verwalten.

Eine weitere Alternative stellt die getrennte Nutzung von Tablet-Computern für Internet Anwendungen (z.B. Patientenaufklärung, QMS etc.) dar.

Teil 2: Datenschutz in der IT und Administration

Was hat sich durch die Änderung des § 203 StGB hinsichtlich der geregelten Auftragsverarbeitung geändert?

Was hat sich durch die Änderung des § 203 StGB hinsichtlich der geregelten Auftragsverarbeitung in der Praxis geändert?

In § 203 StGB wird die Strafe bei Verletzung von Privatgeheimnissen, z.B. durch Bruch der ärztlichen Schweigepflicht, geregelt.

Personen, die an beruflichen Tätigkeiten des Arztes mitwirken, können wenn notwendig auch Zugang zu personenbezogenen Daten erhalten, falls dies zur ärztlichen Leistungserbringung geboten ist. Zu diesem Personenkreis gehört auch IT-Service-Personal. Der Zugang externer Personen zu Daten ist in einer separaten Dokumentation zu speichern (IT-Service-Buch).

Teil 2: Datenschutz in der IT und Administration

Welche Anforderungen gelten für Datenübertragungen bei Praxisübernahmen und Zusammenschlüssen von Praxen?

Welche Anforderungen gelten für Datenübertragungen bei Praxisübernahmen und Zusammenschlüssen von Praxen?

Datenübertragungen zwischen 2 oder mehreren IT-Systemen sind in jedem Fall kritische Auftragsverarbeitungen. Es empfiehlt sich dringend eine komplexe Projektplanung inkl. Datenschutz-Folgenabschätzung (DSFA). Werden Daten von einem Arzt auf einen anderen übertragen, sind dazu besondere Einwilligungen notwendig. Es ist zu empfehlen zu solchen Projekten qualifizierte Fachleute hinzuzuziehen, um das Risiko von Datenpannen und Datenschutz-Verstößen zu minimieren.