Schulungskompendium

Fragen und Antworten

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 3,0 – 5,0 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.

Status-Check: Informationssicherheitsvoraussetzungen

Informationssicherheitsvoraussetzungen

Besteht eine vollständige Bestandsaufnahme für alle Strukturen, die für Informationssicherheit relevant sind (Praxis-Computer, Internet-Kommunikation, Telekommunikation und Medizintechnik)?

Besteht eine vollständige Bestandsaufnahme für alle Strukturen, die für Informationssicherheit relevant sind?

Referenz: Die Bestandsaufnahme ist eine zentrale Anforderung nach QM RL § 3 und § 4 Absatz 2 „Erhebung des Ist-Zustands“.

Ja: Um 25 Punkte zu erreichen sind alle IT-Systeme und -Strukturen ausführlich zu dokumentieren.

Informationssicherheitsvoraussetzungen

Besteht in allen Bereichen ein aktueller Schutz gegen Schadsoftware (Virenschutz, Firewall)?

Besteht in allen Bereichen ein aktueller Schutz gegen Schadsoftware (Virenschutz, Firewall)?

Referenz: Technische Anlage zu Empfehlungen der BÄK / KBV Kapitel 2.3 „Einsatz von Virenschutzprogrammen“.

Ja: Alle Schutzsysteme sind zu bewerten. Sind alle möglichen Sicherungen realisiert werden 20 Punkte gutgeschrieben. Da im Regelfall Lücken bestehen, werden anteilige Punkte (5,10 oder 15) gutgeschrieben.

Informationssicherheitsvoraussetzungen

Wird der Schutz gegen Schadsoftware regelmäßig überprüft und gegebenenfalls aktualisiert?

Wird der Schutz gegen Schadsoftware regelmäßig überprüft und gegebenenfalls aktualisiert?

Referenz: Technische Anlage zu Empfehlungen der BÄK / KBV Kapitel 2.3 „Einsatz von Virenschutzprogrammen“ und 3.1.1 „Virenschutz“ und 3.1.3 „Firewalls“.

Ja: Wenn eine regelmäßige Prüfung stattfindet und dokumentiert wird, wird die volle Punktzahl (20) gutgeschrieben. Ansonsten erfolgt eine anteilige Gutschrift (5, 10, 15 Punkte).

Informationssicherheitsvoraussetzungen

Werden alle relevanten Sicherheits-Updates der eingesetzten Software (insbesondere auch Betriebs-systeme) regelmäßig eingespielt?

Werden alle relevanten Sicherheits-Updates der eingesetzten Software regelmäßig eingespielt?

Referenz: Technische Anlage zu Empfehlungen der BÄK / KBV Kapitel 2.3 „Einsatz von Virenschutzprogrammen“ und 3.1.1 „Virenschutz“ und 3.1.3 „Firewalls“.

Ja: Wenn eine regelmäßige Aktualisierung nachprüfbar ist, werden 15 Punkte dokumentiert.

Informationssicherheitsvoraussetzungen

Werden die genannten Updates dokumentiert?

Werden diese genannten Updates dokumentiert?

Referenz: QM RL § 5 „Dokumentation“ und § 4 Absatz 14 „Fehlermanagement und Fehlermeldesysteme“.

Ja: Liegen alle Dokumentationen zu Updates vor, werden 10 Punkte zugerechnet.

Informationssicherheitsvoraussetzungen

Sind Rechner im Praxisnetz getrennt von Arbeitsplätzen mit Internet-Zugang?

Sind Rechner im Praxisnetz getrennt von Arbeitsplätzen mit Internet-Zugang?

Referenz: Technische Anlage zu Empfehlungen der BÄK / KBV Kapitel 3.2 „Internet“. Die BÄK / KBV stellen hohe Ansprüche an die Trennung von Internet-Rechnern und dem Praxisnetz mit digitalen Patientendaten.

Ja: Die volle Punktzahl kann dokumentiert werden, wenn die Rechner mit Internetanschluss physikalisch getrennt sind. Bei struktureller Trennung im gleichen physikalischen Netzwerk sind bei den sicheren Trennungsmaßnahmen 15 Punkte anzusetzen.

Informationssicherheitsvoraussetzungen

Sind Internet-Rechner, falls mit dem Praxisnetz verbunden, durch geprüfte technische Maßnahmen gegen Schadsoftware gesichert?

Sind Internet-Rechner durch geprüfte technische Maßnahmen gegen Schadsoftware gesichert?

Referenz: Technische Anlage zu Empfehlungen der BÄK / KBV Kapitel 3.2 „Internet“.

Ja: Siehe 3.6. Sind die Rechner physikalisch getrennt, kann ebenfalls unter 3.7. die volle Punktzahl notiert werden.

Informationssicherheitsvoraussetzungen

Sind Administratorenrechte nur für qualifizierte und autorisierte Administratoren zugänglich (auch gegenüber IT-Partnern)?

Sind Administratorenrechte nur für qualifizierte und dokumentierte Administratoren zugänglich?

Referenz: Technische Anlage zu Empfehlungen der BÄK / KBV Kapitel 2.5 „Beschränkung der Arbeit mit Administratorenrechten“.

Ja: Die volle Punktzahl wird notiert, wenn ein Autorisierungsmanagement für alle Administratoren-Funktionen schriftlich festgelegt ist.

Informationssicherheitsvoraussetzungen

Hat jeder Nutzer eine eigene Zugangskennung mit einem individuellen Passwort?

Hat jeder Nutzer eine eigene Zugangskennung mit einem individuellen Passwort?

Referenz: Technische Anlage zu Empfehlungen der BÄK / KBV Kapitel 2.4 „Begrenzung von Programmprivilegien“.

Ja: Ist gewährleistet, dass ALLE Mitarbeiter eine eigene Kennung haben und nutzen, werden 20 Punkte gutgeschrieben.

Informationssicherheitsvoraussetzungen

Bestehen professionelle Vorgaben für die Anwendung sicherer Passworte?

Bestehen professionelle Vorgaben für die Anwendung sicherer Passworte?

Referenz: Technische Anlage zu Empfehlungen der BÄK / KBV Kapitel 2.1 „Umgang mit Passwörtern“.

Ja: Sind alle Passworte sicher (Checkliste mit Empfehlungen) wird die Punktzahl 20 erreicht.

Informationssicherheitsvoraussetzungen

Wird regelmäßig eine Datensicherung der elektronischen Patientenakte durchgeführt?

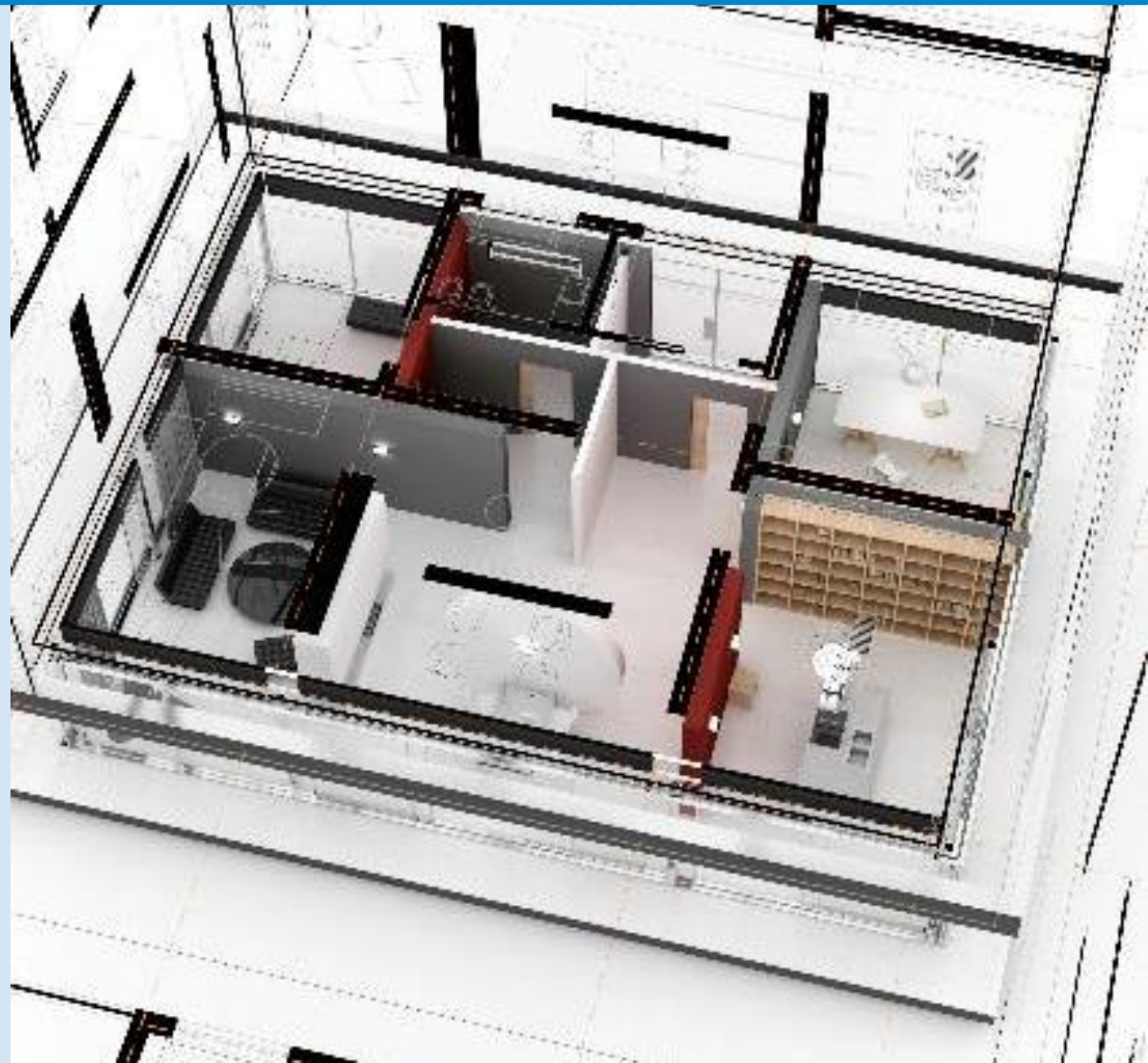
Wird regelmäßig eine Datensicherung der elektronischen Patientenakte durchgeführt?

Referenz: Technische Anlage zu Empfehlungen der BÄK / KBV Kapitel 6. „Datensicherung (Backup)“.

Ja: Die regelmäßige Datensicherung der Patientendokumentation wird mit 15 Punkten bewertet.

Informationssicherheitsvoraussetzungen

Werden regelmäßig Datensicherungen für alle anderen Software-Anwendungen z.B. Privatliquidation, Terminkalender, Qualitätssicherungssoftware etc., durchgeführt?



Datensicherungen aller Software-Anwendungen ?

Referenz: Technische Anlage zu Empfehlungen der BÄK / KBV Kapitel 6. „Datensicherung (Backup)“.

Ja: Volle Punktzahl (15) kann erfasst werden, wenn eine Liste der Systeme (inkl. Medizintechnik) vorliegt und Datensicherungen regelmäßig erfolgen.

Informationssicherheitsvoraussetzungen

Werden alle Datensicherungen räumlich getrennt und vor Schäden gesichert (z.B. gegen Feuer) aufbewahrt?

Werden alle Datensicherungen räumlich getrennt und vor Schäden gesichert (z.B. Feuerschutz) aufbewahrt?

Referenz: Technische Anlage zu Empfehlungen der BÄK / KBV Kapitel 6. „Datensicherung (Backup)“.

Ja: Werden die Datensicherungen räumlich gesichert aufbewahrt, sind 15 Punkte zu dokumentieren.

Informationssicherheitsvoraussetzungen

Ist der Transport der Datensicherung vom Server-System zum Aufbewahrungsort gesichert und separat dokumentiert?

Gesicherter Transport der Datensicherung?

Referenz: Technische Anlage zu Empfehlungen der BÄK / KBV Kapitel 6. „Datensicherung (Backup)“.

Ja: Wenn zu diesem Prozess eine Verfahrensanweisung/interne Regelung besteht und diese den Verantwortlichen bekannt ist und eingehalten wird, ist die volle Punktzahl (15) zu dokumentieren.

Informationssicherheitsvoraussetzungen

Werden die Datensicherungen mindestens 1x jährlich rekonstruiert, um die Qualität und Vollständigkeit der gesicherten Daten zu gewährleisten?

Rekonstruktion der Datensicherungen mindestens 1x jährlich?

Referenz: Technische Anlage zu Empfehlungen der BÄK / KBV Kapitel 6. „Datensicherung (Backup)“.

Ja: Volle Punktzahl (20) wird erreicht, wenn innerhalb der letzten 12 Monate eine erfolgreiche Sicherungs-Rekonstruktion durch geführt und dokumentiert wurde.

Informationssicherheitsvoraussetzungen

Besteht eine Cyber-Versicherung, die eigene Schadensfälle ausreichend abdeckt?

Besteht eine Cyber-Versicherung, die eigene Schadensfälle ausreichend abdeckt?

Referenz: In den Empfehlungen BÄK / KBV Kapitel 3.11. mit Verweis auf Art. 32 DSGVO werden die Anforderungen für technische und organisatorische Maßnahmen dokumentiert. Für die Informationssicherheit / Datensicherheit sind Art. 24 und 32 DSGVO relevant. Eine Versicherung zur Begrenzung finanzieller Schäden gehört zu den wichtigen organisatorischen Maßnahmen, insbesondere durch die Einhaltung der Versicherungsbedingungen.

Ja: Die volle Punktzahl (25) kann vergeben werden, wenn die Cyber-Versicherung den Maximalschutz regelt. Dazu gehören auch Schäden an Hardware-Komponenten und die Deckung von Risiken bei Sanktionen und Bußgeldern. **Achtung:** die Leitung muss allen Anforderungen an die Mitwirkungspflichten der Versicherten nachkommen (beispielsweise hohe Punktzahl bei dieser Checkliste).

Informationssicherheitsvoraussetzungen

Besteht ein umfassendes Sicherheitskonzept für alle webbasierten Anwendungen wie die Homepage, Web-Terminkalender, Videosprechstunden, Verordnung von Gesundheits-Apps etc. (siehe separate Checkliste)?

Sicherheitskonzept für alle webbasierten Anwendungen?

Referenz: Technische Anlage zu Empfehlungen der BÄK / KBV Kapitel 3.1.6 „Umgang mit Web-Browsern und E-Mail-Programmen)“ sowie Richtlinien DVG nach § 75b (vor Veröffentlichung) und DSGVO sowie TMG.

Ja: Die Anforderungen im Bereich Informationssicherheit und Cyberschutz für alle Aktivitäten im Web müssen nach einer separaten Checkliste abgearbeitet werden. Je nach positiven Beurteilungen einzelner Bereiche können anteilige Punktzahlen dokumentiert werden: z.B. 12 Punkte (von 20) wenn geschätzt 60% der Anforderungen erfüllt werden.

Informationssicherheitsvoraussetzungen

Besteht eine Cyber-Haftpflichtversicherung, die fremde Schäden und Sanktionen (Bußgelder) ausreichend abdeckt?

Besteht eine Cyber-Haftpflichtversicherung, die fremde Schäden und Sanktionen ausreichend abdeckt?

Referenz: In den Empfehlungen BÄK / KBV Kapitel 3.11. mit Verweis auf Art. 32 DSGVO werden die Anforderungen für technische und organisatorische Maßnahmen dokumentiert. Für die Informationssicherheit / Datensicherheit sind Art. 24 und 32 DSGVO relevant. Eine Versicherung zur Begrenzung finanzieller Schäden gehört zu den wichtigen organisatorischen Maßnahmen, insbesondere durch die Einhaltung der Versicherungsbedingungen.

Ja: Deckt die Cyber-Versicherung alle möglichen Risiken, werden 25 Punkte zugerechnet.

Informationssicherheitsvoraussetzungen

Bestehen vollständige Verfahrensanweisungen zur Zugangskontrolle, Zutrittskontrolle und Zugriffskontrolle?

Bestehen vollständige VAs zur Zugangskontrolle, Zutrittskontrolle und Zugriffskontrolle?

Referenz: In den Empfehlungen BÄK / KBV Kapitel 3.11. mit Verweis auf Art. 32 DSGVO werden die Anforderungen für technische und organisatorische Maßnahmen dokumentiert. Für die Informationssicherheit / Datensicherheit sind Art. 24 und 32 DSGVO relevant. Die Anforderungen an Datenzugriffsmöglichkeiten sind in der Technischen Anlage zu den BÄK / KBV Empfehlungen unter Kapitel 2.4 „Begrenzung der Datenzugriffsmöglichkeiten“ definiert.

Ja: Die Verfahrensanweisungen / internen Regelungen müssen alle Anforderungen des sicheren Zugangs, Zutritts und Zugriffs auf Daten der Praxis gewährleisten, um die Punktzahl von 20 zu erreichen.

Informationssicherheitsvoraussetzungen

Sind die Verfahrensanweisungen für Zugangskontrolle, Zutrittskontrolle und Zugriffskontrolle dem Team bekannt und die Einweisung aktuell dokumentiert?

Sind die VAs dem Team bekannt u. Einweisungen dokumentiert?

Referenz: Die Anforderungen an Datenzugriffsmöglichkeiten sind in der Technischen Anlage zu den BÄK / KBV Empfehlungen unter Kapitel 2.4 „Begrenzung der Datenzugriffsmöglichkeiten“ definiert.
Die Schulungsverpflichtungen ergeben sich aus QM RL § 4 Absatz 10 „Fortbildungs- und Schulungsmaßnahmen“.

Ja: Wenn Einweisungsprotokolle zu den 3 Z-Prozessen vorliegen (mit Unterschrift der Mitarbeiter) werden 20 Punkte gutgeschrieben.

Informationssicherheitsvoraussetzungen

Bestehen AV-Verträge (nach DSGVO) mit allen Dienstleistern für Software, Hardware, Telekommunikation und Medizintechnik?

Bestehen AV-Verträge nach DSGVO mit allen Dienstleistern für SW, HW, TK und Medizintechnik?

Referenz: Die Anforderungen an Datenzugriffsmöglichkeiten sind in der in den BÄK / KBV Empfehlungen unter Kapitel 3.6 „“Auftragsverarbeitung“ definiert.

Ja: Sind alle AV Verträge speziell im IT-Bereich aktuell vorhanden, so können 15 Punkte erfasst werden.

Informationssicherheitsvoraussetzungen

Besteht ein Notfallplan für alle Störfälle und Schadenssituationen im Bereich Informationssicherheit und Cyberschutz?

Besteht ein Notfallplan für alle Störfälle und Schadenssituationen im Bereich Informationssicherheit und Cyberschutz?

Referenz: Die Etablierung eines Notfallmanagements für Störfälle in der Informationsverarbeitung ergibt sich aus den Grundsätzen der Informationssicherheits- und Datenschutzgesetzgebung. U.a. ergeben sich Richtlinien aus § 42 a BDSG, Art. 32 der DSGVO und nach BSI Standard 100-4 (Notfallmanagement) und BÄK / KBV Empfehlungen Kapitel 3.10.

Ja: Die volle Punktzahl von 20 Punkten wird erreicht, wenn alle Anforderungen durch ein entsprechendes Notfallkompendium nach BSI Standards vorliegt. Ist ein Notfallplan nach DSGVO (z.B. zur Behandlung von Datenpannen nach Art. 33 DSGVO) vorhanden, können 10 Punkte dokumentiert werden.