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: Bestandsaufnahme

IT-Bestandsaufnahme

Besteht bereits ein Qualitätsmanagementsystem nach § 4 GBA QM Richtlinie nach § 135 ff SGB V (z.B. QEP, ISO 9001 etc.)?

Besteht bereits ein Qualitätsmanagementsystem?

Referenz: Ein Qualitätsmanagementsystem (QMS) ist nach der QM Richtlinie gem. § 135ff SGB V für die Praxen, die an der kassenärztlichen Versorgung teilnehmen, verpflichtend.
Im Qualitätsmanagement spielt die Informationssicherheit eine wichtige Rolle.
Im QEP System (Qualität und Entwicklung in Praxen) wird Informationssicherheit in Kapitel 4.5.1 behandelt.

Ja: Wenn es im QMS bereits Regelungen zur Informationssicherheit und Cyberschutz gibt, werden 10 Punkte notiert.

IT-Bestandsaufnahme

Besteht bereits ein Datenschutz-managementsystem (DSMS) nach DSGVO und BDSG neu?

Besteht bereits ein Datenschutzmanagementsystem nach DSGVO und BDSG neu?

Referenz: Datenschutz nach dem Bundesdatenschutzgesetz (BDSG) und der EU-Datenschutz-Grundverordnung (DSGVO) sind eng mit den Anforderungen für Informationssicherheit und Cyberschutz in der Praxis verbunden. In einem professionellen DSMS nach BDSG/DSGVO sind die wesentlichen Anforderungen an die Informationssicherheit geregelt.

Ja: Wenn ein DSMS mit globalen Regelungen für Informationssicherheit und Cyberschutz besteht und „gelebt“ wird, werden 10 Punkte dokumentiert.

IT-Bestandsaufnahme

Ist bereits ein QM-Beauftragter und / oder Datenschutzbeauftragter (intern oder extern) bestellt?

Ist bereits ein QM-Beauftragter und / oder Datenschutzbeauftragter (intern oder extern) bestellt?

Referenz: Das BDSG (Bundesdatenschutzgesetz) regelt in § 22 den Einsatz von Datenschutzbeauftragten in medizinischen Einrichtungen. Werden personenbezogene Daten in großem Umfang digital verarbeitet (beispielsweise Elektronische Patientenakte / Papierlose Praxis) muss ein interner oder externer Datenschutzbeauftragter eingesetzt werden. Ab 20 Mitarbeitern ist diese Verpflichtung in jedem Fall bindend. Der DSB ist auch für Informationssicherheit und Cyberschutz verantwortlich.

Ja: Ist ein DSB eingesetzt und nimmt er die Aufgaben nach Gesetz wahr, werden 15 Punkte gutgeschrieben.

IT-Bestandsaufnahme

Gibt es einen QM- und / oder Datenschutzkoordinator, der intern die Anforderungen an Rechtskonformität koordiniert?

Gibt es einen QM- und / oder Datenschutzkoordinator, der intern die Anforderungen an Rechtskonformität koordiniert?

Referenz: Sowohl im Qualitätsmanagement (nach § 135ff SGB V und §4 (1) Absatz 3 QM Richtlinie) als auch nach den geltenden Datenschutzbestimmungen besteht die Verpflichtung Verantwortungsbereiche und Rollen festzulegen. Ein / eine Datenschutzkoordinator(in) ist eine wichtige Rolle für die Umsetzung aller internen Regelungen für Datenschutz- und Informationssicherheits-Maßnahmen.

Ja: Ist ein / eine Datenschutzkoordinator(in) eingesetzt und wird diese Rolle verantwortlich ausgeübt, werden 15 Punkte gutgeschrieben

IT-Bestandsaufnahme

Werden regelmäßig QM-Jahresberichte nach der GBA QM-Richtlinie erstellt?

Werden regelmäßig QM-Jahresberichte nach der GBA QM-Richtlinie erstellt?

Referenz: Nach § 4 – § 6 GBA QM-Richtlinie sind die Ergebnisse der Selbstbewertung regelmäßig zu dokumentieren. In dem QM-Jahresbericht (§ 5) ist auch der Status der Informationssicherheit und des Cyberschutzes zu dokumentieren.

Ja: Wenn aktuelle Jahresberichte mit Dokumentation der Entwicklung der Informationssicherheit und Cyberschutz vorliegen, werden 10 Punkte gutgeschrieben.

IT-Bestandsaufnahme

Werden regelmäßig Datenschutz-Jahresberichte nach DSGVO / BDSG (neu) erstellt?

Werden regelmäßig Datenschutz-Jahresberichte nach DSGVO / BDSG neu erstellt?

Referenz: Nach § 5 und § 24 DSGVO bestehen Nachweis- und Rechenschaftspflichten, die in einem Jahresbericht dokumentiert werden können. Darin sind vorhandene Risiken und Maßnahmen zur Gewährleistung der Informationssicherheit und zum Cyberschutz zu dokumentieren.

Ja: Wenn ein aktueller Jahresbericht besteht, in dem Informationssicherheits-Maßnahmen dokumentiert sind, werden 10 Punkte gutgeschrieben.

IT-Bestandsaufnahme

Wird regelmäßig eine Risikoanalyse zur Informationssicherheit und zum Cyberschutz durchgeführt?

Wird regelmäßig eine Risikoanalyse zur Informationssicherheit und zum Cyberschutz durchgeführt?

Referenz: Risikomanagement spielt eine zentrale Rolle für Informationssicherheit und Cyberschutz. Generell ist Risikomanagement für Arztpraxen verpflichtend nach § 135ff SGB V, QM-RL § 4 Absatz 13 „Risikomanagement“. Im Bereich Datenschutz werden Risikoanalysen im DSK (Datenschutzkommission) Kurzpapier Nr. 18 beschrieben.

Ja: Wenn eine vollständige Risikoanalyse, z.B. nach ISO 27001, durchgeführt wird, werden 25 Punkte gutgeschrieben. Bei Risikoanalysen in Teilbereichen (z.B. nur Datenschutz) können 10 Punkte dokumentiert werden.

IT-Bestandsaufnahme

Bestehen zu allen Risiken technische und organisatorische Maßnahmen zur Schadensvermeidung und -minimierung?

Bestehen zu allen Risiken TOMs u. zur Schadensvermeidung und -minimierung?

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.

Ja: Wenn technische und organisatorische Maßnahmen (TOM) zur Informationssicherheit / Datensicherheit nach den gesetzlichen Regelungen vorliegen (z.B. Interne Regelungen nach QEP, Verfahrensanweisungen nach ISO werden 20 Punkte dokumentiert. Bei teilweise vorliegenden TOM Dokumenten werden z.B. 10 Punkte gutgeschrieben.

Status-Check: Dokumentationen und Schulungen

Dokumentationen und Schulungen

Besteht ein Schulungsplan (Curriculum) für alle Mitarbeiter für ein Halbjahr / ein Jahr?

Besteht ein Schulungsplan (Curriculum) für alle Mitarbeiter für ein Halbjahr / ein Jahr?

Referenz: Das Schulungsmanagement ist nach § 135ff SGB V QM RL §4 Absatz 10 „Fortbildungs- und Schulungsmaßnahmen“ geregelt. Es gilt für alle Bereiche der Praxis- und Klinikorganisation.

Ja: Wenn für alle Mitarbeiter ein Schulungsplan mit Ausbildungszielen (Curriculum) besteht, werden die vollen 20 Punkte dokumentiert. Sind Fortbildungen nur nach Bedarf vorgesehen, werden je im Bereich Informationssicherheit / Cyberschutz 5-10 Punkte gutgeschrieben.

Dokumentationen und Schulungen

Werden regelmäßig (z.B. 4 x jährlich) Teamschulungen außerhalb der medizinischen Fortbildungen durchgeführt?

Werden regelmäßig Teamschulungen (exkl. medizinischen Fortbildungen) durchgeführt?

Referenz: Die Verpflichtungen zu regelmäßigen Schulungsmaßnahmen außerhalb von medizinischen Fortbildungen (Informationssicherheit, Datenschutz, Qualitätsmanagement etc.) ergeben sich aus QM RL § 4 Absatz 10 „Fortbildungs- und Schulungsmaßnahmen“.

Ja: Die volle Punktzahl wird erreicht, wenn regelmäßig Schulungen durchgeführt werden und so der notwendige Kenntnisstand aller Mitarbeiter gewährleistet werden kann.

Dokumentationen und Schulungen

Finden regelmäßig Teambesprechungen zu organisatorischen und technischen Maßnahmen in der medizinischen Einrichtung statt?

Finden regelmäßig Teambesprechungen zu TOMs in der medizinischen Einrichtung statt?

Referenz: Regelmäßige Gespräche aller Mitarbeiter sind nach QM RL § 4 Absatz 9 „Teambesprechungen“ verpflichtend.

Ja: Volle Punktzahl (10) wird erreicht, wenn regelmäßig Teambesprechungen zur Informationssicherheit und zum Cyberschutz stattfinden und diese auditfähig dokumentiert werden.

Dokumentationen und Schulungen

Enthalten die Mitarbeiterverträge alle rechtlichen Verpflichtungen zum Qualitätsmanagement, Datenschutz und zu Informationssicherheit und Cyberschutz?

Mitarbeiterverträge inkl. QS, DS, IS und Cyberschutz?

Referenz: QM RL § 3 und § 4 Absatz 3 „Regelung von Verantwortlichkeiten und Zuständigkeiten“.

Ja: Sind alle 3 Bereiche im Mitarbeitervertrag enthalten, werden 10 Punkte dokumentiert. Bei 2 erfassten Bereichen werden 5 Punkte angesetzt.

Dokumentationen und Schulungen

Bestehen genaue Regelungen zur Informationssicherheit und Cyberschutz bei Einstellung neuer Mitarbeiter und Ausscheiden von Teammitgliedern?

Bestehen Regelungen zur IS und Cyberschutz bei Einstellung und Ausscheiden von Mitarbeitern?

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

Ja: Wenn es eine Verfahrensanweisung mit Checkliste für den Personalbereich gibt, der die Anforderungen an Datenschutz und Informationssicherheit regelt, werden 10 Punkte gutgeschrieben. Wenn die Regelungen nur teilweise abgebildet werden, sind anteilige Punkte zu notieren.