VA QM Abstimmung und laufende Synchronisierung zwischen Qualitätsmanagement (QMS) und ISMS/DMS

Übersicht

Diese VA dient der internen Unterstützung der QM-, Datenschutz- Beauftragten und -Koordinatoren (QMB/DSB/DSK/ISB) in medizinischen Einrichtungen wie Arztpraxen, Zahnarztpraxen, Kliniken, MVZ, speziell bei der rechtskonformen Umsetzung der IT-Sicherheitsrichtlinie und den Datenschutz-Rahmenbedingungen.

Ziel und Zweck

Die Verfahrensanweisung hat das Ziel, die Abläufe und allgemeinen Regelungen zur Informationssicherheit, zum Datenschutz in strukturierten Prozessen und Verfahren transparent umzusetzen und gut verständlich darzustellen. Ziel dieser Beschreibung ist die Vereinheitlichung der Abläufe und die Sicherstellung der Vollständigkeit und Qualität.

Zentrales Ziel dieser VA ist es insbesondere, die gesetzlich geforderten Einrichtungen von Qualitätsmanagement nach SGB V, Informationssicherheit nach DVG (§75b SGB V) und Datenschutz nach DSGVO und BDSG neu zu harmonisieren und zu synchronisieren.

Anwendungsbereich

Diese Anweisung gilt für die Einrichtung und Nutzung eines QMS (Qualitätsmanagementsystem), eines ISMS (Informationssicherheits-Management Systems) und eines DSMS (Datenschutz Managementsystem).

Der Anwendungsbereich ist unabhängig von den Standorten der Einheiten und ist definiert für alle Bereiche, in denen personenbezogene Daten, erfasst, verarbeitet, übertragen und gespeichert und IT-Systeme eingesetzt werden.

Verantwortung

Verantwortlich für die einzelnen Segmente des Verfahrens sind dazu beauftragte Personen, insbesondere:

- Leitung/Mitglieder der Leitung (ärztlich und organisatorisch)
- Informationssicherheits-Beauftragte (ISB)
- Datenschutz Beauftragte (DSB) und Datenschutz Koordinatoren (DSK)
- Externe Dienstleister, soweit rechtlich geregelt

Die individuellen Verantwortungsbereiche sind in Protokollen, falls vorgesehen, zu dokumentieren.

Prozesse

Die gesetzlich vorgeschriebenen QMS und ISMS/DSMS überschneiden sich in ihren Anforderungen und Umsetzungen. Bei bestehenden Qualitätsmanagementsystemen werden bereits ca. 40% der Anforderungen an ein ISMS/DSMS abgedeckt. Die

Synchronisierung und parallele Umsetzung ist deshalb abhängig von der individuellen Situation in Praxis bzw. Klinik.

Alternative 1:

Die Praxis / Klinik setzt bislang weder ein QMS noch ein ISMS/DSMS ein.

Alternative 2:

Die Praxis / Klinik setzt ein Qualitätsmanagementsystem (QMS) aber noch kein ISMS/DSMS ein.

Alternative 3:

Die Praxis / Klinik setzt in einem QMS bereits Teile eines DSMS für den Datenschutz ein.

Alternative 1 (kein QMS und kein DSMS)

Mit Einführung eines ISMS/DSMS können auch die Grundlagen eines QMS realisiert werden. Folgende Prozesse werden umgesetzt:

- Das ISMS/DSMS wird mit den Minimalanforderungen eingerichtet. Dazu gehören insbesondere:
    - Planung des Systems
    - Definition der Rollen und Verantwortungsbereiche
    - Umsetzung der Mindestanforderungen des DSGVO nach Vorlagen
    - Schulungen der Mitarbeiter im Bereich Datenschutz
    - Einführung eines PDCA Systems für die laufende Optimierung

- Zu einem späteren Zeitpunkt wird das ISMS/DSMS zum Qualitätsmanagementsystem erweitert. Dazu werden zusätzlich zu den Bereichen Datenschutz und Datensicherheit Verfahren im Bereich Patientensicherheit, Notfallplan, Patientenaufklärung etc. nach QM-Gesichtspunkten aufgenommen.
  Die Erweiterung des Systems erfolgt nach den Mindestanforderungen nach §136 ff SGB V

Alternative 2 (QMS ja, ISMS/DSMS nein)

Es bestehen grundsätzlich zwei Möglichkeiten der Einführung von ISMS/DSMS Anforderungen bei bestehendem QMS:

- Das ISMS/DSMS wird als Subsystem des QMS geführt. Im QMS wird in den entsprechenden Kapiteln zum Datenschutz und Datensicherheit auf ein ISMS/DSMS als Subsystem referenziert.
  Es bestehen analog und digital zwei voneinander getrennte Systeme (zwei getrennte Ordner bzw. zwei getrennte Software-Applikationen).

- Das ISMS/DSMS wird voll in das QMS integriert. Das bedeutet, dass die für die Vorgaben für den Datenschutz in das bestehende QMS voll integriert werden. Dazu werden in den entsprechenden Kapiteln die nach DVG/DSGVO erforderlichen Verfahrensanweisungen, Checklisten und Vorlagen integriert werden.

Alternative 3 (QMS enthält einen Teil der IS/DS-Anforderungen)

Es besteht ein umfangreiches Qualitätsmanagementsystem, gegebenenfalls mit Zertifizierung (z.B. ISO, QEP).

Erforderliche Maßnahmen:

- Die für den Datenschutz relevanten Dokumente werden auf Vollständigkeit und Kompatibilität mit der DSGVO und dem BDSG neu sowie dem DVG (IT-Sicherheitsrichtlinie nach § 75b SGB V) überprüft.
- Lücken im IT-Sicherheits- und Datenschutzbereich werden durch zusätzliche Verfahrensanweisungen und Checklisten ausgefüllt. Im Regelfall wird hierzu eine 2-Jahres-Planung umgesetzt, um nach dieser Frist ein synchrones System für Qualitätsmanagement und Datenschutz realisiert zu haben.

Zeitplanung

Die individuelle Umsetzung von QMS und DSMS richtet sich nach den bestehenden Voraussetzungen:

Alternative 1 – 48 bis 72 Monate

Alternative 2 – 24 – 48 Monate

Alternative 3 – 24 Monate

Mitgeltende Dokumente:

- DVG, insbesondere Richtlinie nach § 75b SGB V
- QM-Standardnormen nach QEP und/oder ISO 900x
- Bestimmungen zur Ärztlichen Schweigepflicht nach BGB und StGb
- Bundesdatenschutz Gesetz (BDSG) insbesondere § 64
- Datenschutz Grundverordnung (DSGVO) insbesondere Art. 32
- § 136 SGB V QM Richtlinie des GBA (GBA-RL) insbesondere §4
- Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis der BÄK & KBV
- Technische Anlage zu den BÄK/KBV Empfehlungen
- Curriculum 24 Monate