

ISMS nach VdS 10000 und 100010

Kombiniertes Managementsystem für Cybersicherheit, Datenschutz und QM in Krankenhäusern

(§ 75c SGB V kompatibel)

Inhalt

<u>1</u>	<u>Allgemeine Grundlagen</u>	13
<u>1.1</u>	<u>Anwendungsgrundlagen</u>	13
<u>1.1.1</u>	<u>Anwendungsgrundlagen Informationssicherheit</u>	13
<u>1.1.2</u>	<u>Anwendungsgrundlagen Datenschutz</u>	13
<u>1.2</u>	<u>Anwendungs- und Geltungsbereich</u>	14
<u>1.3</u>	<u>Gültigkeit und Anwendungsbereiche</u>	14
<u>1.4</u>	<u>Anleitung zur Anwendung</u>	14
<u>1.4.1</u>	<u>Analoges Handbuch</u>	14
<u>1.4.2</u>	<u>Digitales Kompendium</u>	14
<u>1.4.3</u>	<u>Einführung und Sensibilisierung</u>	14
<u>1.4.4</u>	<u>Standard Planung</u>	15
<u>1.4.5</u>	<u>Planung ISMS nach B3S-Systematik (ab EMRAM Stufe 4/5)</u>	15
<u>1.4.6</u>	<u>Umsetzung mit Curriculum (Einführungs- und Zielplanung)</u>	15
<u>1.4.7</u>	<u>Modulare Anwendung</u>	16
<u>1.4.8</u>	<u>Grundsätze der Anwendung</u>	16
<u>2</u>	<u>Normen</u>	18
<u>2.1</u>	<u>Normen Informationssicherheit</u>	18
<u>2.2</u>	<u>Normen Datenschutz</u>	18
<u>3</u>	<u>Glossar</u>	19
<u>4</u>	<u>Organisation</u>	62
<u>4.1</u>	<u>Verantwortlichkeiten</u>	62
<u>4.1.1</u>	<u>Verantwortlichkeiten Informationssicherheit</u>	62
<u>4.1.2</u>	<u>Verantwortlichkeiten Datenschutz</u>	62
<u>4.1.3</u>	<u>Zuweisung Dokumentation</u>	62
<u>4.1.3.1</u>	<u>Zuweisung und Dokumentation Informationssicherheit</u>	62
<u>4.1.3.2</u>	<u>Zuweisung und Dokumentation Datenschutz</u>	63
<u>4.1.4</u>	<u>Funktionstrennungen</u>	63
<u>4.1.4.1</u>	<u>Funktionstrennungen Informationssicherheit</u>	63

4.1.4.2	<u>Funktionstrennungen Datenschutz</u>	63
4.1.5	<u>Zeit-Ressourcen</u>	63
4.1.5.1	<u>Zeit-Ressourcen Informationssicherheit</u>	63
4.1.5.2	<u>Zeit-Ressourcen Datenschutz</u>	63
4.1.6	<u>Aufgaben-Delegierung</u>	64
4.1.6.1	<u>Aufgaben-Delegierung Informationssicherheit</u>	64
4.1.6.2	<u>Aufgaben-Delegierung Datenschutz</u>	64
4.2	<u>Klinikleitung</u>	64
4.3	<u>Beauftragte</u>	64
4.3.1	<u>Informationssicherheitsbeauftragter (ISB)</u>	65
4.3.2	<u>Datenschutzbeauftragter</u>	65
4.4	<u>Teams</u>	66
4.5	<u>Verantwortliche</u>	66
4.5.1	<u>IT-Verantwortliche</u>	66
4.5.2	<u>Datenschutz-Verantwortliche</u>	67
4.6	<u>Besondere Verantwortungsbereiche</u>	67
4.6.1	<u>Administratoren Informationssicherheit</u>	67
4.6.2	<u>Eigentümer einer Datenverarbeitung im Datenschutz</u>	67
4.7	<u>Team-Leiter / Vorgesetzte</u>	68
4.8	<u>Mitarbeiter</u>	68
4.8.1	<u>Mitarbeiteraufgaben Bereich Informationssicherheit</u>	68
4.8.2	<u>Mitarbeiteraufgaben Bereich Datenschutz</u>	68
4.9	<u>Projektverantwortliche</u>	68
4.9.1	<u>Projektverantwortliche Informationssicherheit</u>	68
4.9.2	<u>Projektverantwortliche Datenschutz</u>	68
4.10	<u>Externe Partner</u>	69
4.10.1	<u>Externe Partner Informationssicherheit</u>	69
4.10.2	<u>Externe Partner Datenschutz</u>	69
5	<u>Leitlinien</u>	70
5.1	<u>Anforderungen allgemein</u>	70
5.1.1	<u>Anforderungen Informationssicherheit (IS-Leitlinie)</u>	70
5.1.2	<u>Anforderungen Datenschutz (DS-Leitlinie)</u>	70
5.2	<u>Inhalte</u>	70
5.2.1	<u>Inhalte Informationssicherheit</u>	70
5.2.2	<u>Inhalte Datenschutz</u>	70
5.3	<u>Beispiel Leitlinie</u>	71

5.3.1	<u>Leitlinie zur Informationssicherheit</u>	71
5.3.2	<u>Beispiel Leitlinie zum Datenschutz</u>	72
6	<u>Richtlinien</u>	74
6.1	<u>Anforderungen allgemein</u>	74
6.1.1	<u>Anforderungen Informationssicherheit</u>	74
6.1.2	<u>Anforderungen Datenschutz</u>	74
6.2	<u>Inhalte</u>	74
6.2.1	<u>Inhalte Informationssicherheit</u>	75
6.2.2	<u>Inhalte Datenschutz</u>	75
6.3	<u>Regelungen für Anwender</u>	75
6.3.1	<u>Regelungen für Anwender Informationssicherheit</u>	75
6.3.2	<u>Regelungen für Anwender Datenschutz</u>	77
6.4	<u>Regelungen allgemein</u>	77
6.4.1	<u>Regelungen allgemein Informationssicherheit</u>	77
6.4.2	<u>Regelungen allgemein Datenschutz</u>	78
6.5	<u>Weitere Regelungen und Richtlinien</u>	78
6.5.1	<u>Weitere Richtlinien Informationssicherheit</u>	78
6.5.2	<u>Weitere Richtlinien und Regelungen für den Datenschutz</u>	79
7	<u>Human Resources</u>	80
7.1	<u>Vor Tätigkeitsaufnahme</u>	80
7.1.1	<u>Vor Tätigkeitsaufnahme Informationssicherheit</u>	80
7.1.2	<u>Vor Tätigkeitsaufnahme Datenschutz</u>	80
7.2	<u>Tätigkeitsaufnahme</u>	80
7.2.1	<u>Tätigkeitsaufnahme Informationssicherheit</u>	80
7.2.2	<u>Tätigkeitsaufnahme Datenschutz</u>	81
7.3	<u>Tätigkeitsbeendigung oder -wechsel</u>	81
7.3.1	<u>Tätigkeitsbeendigung oder -wechsel Informationssicherheit</u>	81
7.3.2	<u>Tätigkeitsbeendigung oder -wechsel Datenschutz</u>	81
8	<u>Wissensmanagement</u>	82
8.1	<u>Aktualität des Wissens</u>	82
8.1.1	<u>Aktualität des Wissens Informationssicherheit</u>	82
8.1.2	<u>Aktualität des Wissens Datenschutz</u>	82
8.2	<u>Sensibilisierung und Schulung</u>	83
8.2.1	<u>Sensibilisierung und Schulung Informationssicherheit</u>	83
8.2.2	<u>Sensibilisierung und Schulung Datenschutz</u>	84
8.3	<u>Curriculum und Fortbildung</u>	84

8.3.1	<u>Curriculum und Fortbildung Informationssicherheit</u>	84
8.3.2	<u>Curriculum und Fortbildung Datenschutz</u>	84
9	<u>Ressourcen IT-Infrastruktur</u>	85
9.1	<u>Prozesse</u>	85
9.1.1	<u>Prozesse Informationssicherheit</u>	85
9.1.2	<u>Prozesse Datenschutz</u>	85
9.2	<u>Informationen und Daten</u>	86
9.3	<u>Ressourcen</u>	87
9.3.1	<u>IT-Ressourcen</u>	87
9.3.2	<u>Personenbezogene Daten Datenschutz</u>	87
10	<u>IT-Systeme</u>	88
10.1	<u>Bestandsaufnahme und Inventarisierung</u>	88
10.2	<u>Statusanalyse nach EMRAM</u>	88
10.2.1	<u>EMRAM Stufenmodell</u>	89
10.2.2	<u>Erläuterung des EMRAM Stufenkonzepts</u>	90
10.2.3	<u>ISMS Anforderungen nach EMRAM Stufen</u>	91
10.2.4	<u>EMRAM Einordnung in Deutschland</u>	92
10.3	<u>Lebenszyklus der Systeme</u>	94
10.3.1	<u>Inbetriebnahme und Änderung</u>	95
10.3.2	<u>Ausmusterung und Wiederverwendung</u>	95
10.4	<u>Basisschutz</u>	95
10.4.1	<u>Software</u>	96
10.4.2	<u>Beschränkung des Netzwerkverkehrs</u>	96
10.4.3	<u>Protokollierung und Dokumentation</u>	97
10.4.4	<u>Externe Schnittstellen und Laufwerke</u>	97
10.4.5	<u>Schadsoftware</u>	97
10.4.6	<u>Starten von fremden Medien</u>	97
10.4.7	<u>Authentifizierung</u>	98
10.4.8	<u>Zugänge und Zugriffe</u>	98
10.5	<u>Mobile IT-Systeme</u>	99
10.5.1	<u>IS-Richtlinie</u>	99
10.5.2	<u>Schutz der Informationen</u>	99
10.5.3	<u>Verlust der Informationen</u>	100
10.6	<u>Kritische IT-Systeme</u>	100
10.6.1	<u>Risikoanalyse und Behandlung</u>	100
10.6.2	<u>Notbetriebsmanagement</u>	100

10.6.3	<u>Robustheit</u>	100
10.6.4	<u>Externe Schnittstellen und Laufwerke</u>	101
10.6.5	<u>Änderungsmanagement</u>	101
10.6.6	<u>Dokumentation</u>	101
10.6.7	<u>Datensicherung und -rekonstruktion</u>	101
10.6.8	<u>Überwachung und Kontrolle</u>	102
10.6.9	<u>Ersatzsysteme und Verfahren</u>	102
10.6.10	<u>Kritische Individualsoftware</u>	102
10.7	<u>IT-Spezialanwendungen in Medizinischen Versorgungseinrichtungen</u> ..	102
10.7.1	<u>Telematikinfrastuktur (TI)</u>	102
10.7.2	<u>Abrechnungsprogramme</u>	103
10.7.2.1	<u>KV-Abrechnung</u>	103
10.7.2.2	<u>Privatliquidation</u>	103
10.7.2.3	<u>IGeL Abrechnung</u>	103
10.7.3	<u>Elektronische Patientenakte (ePA)</u>	103
10.7.4	<u>Medizintechnik</u>	104
10.7.4.1	<u>Medizintechnik mit Speicherung von Patientendaten</u>	104
10.7.4.2	<u>Medizintechnik ohne Speicherung von Patientendaten</u>	104
10.7.5	<u>Terminmanagement-SW</u>	104
10.7.5.1	<u>Lokaler Terminkalender</u>	104
10.7.5.2	<u>Web-Terminkalender</u>	106
10.7.6	<u>Web-Anwendungen</u>	106
10.7.6.1	<u>Homepage / Portal</u>	106
10.7.6.2	<u>Videosprechstunde nach DVG</u>	106
10.7.6.3	<u>Gesundheits-APPS nach DVG</u>	106
10.7.7	<u>Datenschnittstellen medizinische Anwendungen</u>	107
10.7.7.1	<u>DICOM Schnittstellen</u>	107
10.7.7.2	<u>HL7 Schnittstellen</u>	107
10.7.7.3	<u>GDT-Schnittstellen</u>	107
10.7.7.4	<u>Andere Schnittstellen</u>	107
10.7.8	<u>Qualitätssicherungs- und Forschungsprojekte</u>	108
10.7.9	<u>Schnittstellen zu Gesundheits-Apps nach DVG</u>	108
11	<u>Netzwerke und Verbindungen</u>	109
11.1	<u>Netzwerkplan</u>	109
11.2	<u>Aktive Netzwerk-Komponenten</u>	109
11.3	<u>Netzübergänge</u>	109

11.4	<u>Basis-Schutz</u>	110
11.4.1	<u>Netzwerkanschlüsse</u>	110
11.4.2	<u>Segmentierung</u>	111
11.4.3	<u>Fernzugang</u>	111
11.4.4	<u>Netzwerkkopplung</u>	111
11.5	<u>Kritische Verbindungen</u>	112
12	<u>Mobile Datenträger</u>	113
12.1	<u>IS-Richtlinie</u>	113
12.2	<u>Schutz der Informationen</u>	113
12.3	<u>Kritische mobile Datenträger</u>	113
13	<u>Umgebung / Infrastruktur</u>	114
13.1	<u>Server und aktive Netzwerk-Komponenten</u>	114
13.2	<u>Datenleitungen</u>	114
13.3	<u>Kritische IT-Systeme</u>	114
14	<u>IT-Outsourcing und Cloud-Computing</u>	116
14.1	<u>IS-Richtlinie</u>	116
14.2	<u>Vorbereitung</u>	116
14.3	<u>Vertragsgestaltung</u>	116
14.4	<u>Kritische IT-Ressourcen</u>	117
15	<u>Zugänge und Zugriffsrechte</u>	119
15.1	<u>Managementzugänge und -zugriffe</u>	119
15.2	<u>Kritische IT-Systeme und Informationen</u>	119
16	<u>Datensicherung, Sicherungstransport, Archivierung</u>	120
16.1	<u>IS-Richtlinie</u>	120
16.2	<u>Archivierung</u>	120
16.3	<u>Planung und Verfahren</u>	120
16.4	<u>Weiterentwicklung</u>	121
16.5	<u>Basis-Schutz</u>	121
16.5.1	<u>Speicherorte</u>	122
16.5.2	<u>Server</u>	122
16.5.3	<u>Aktive Netzwerk-Komponenten</u>	122
16.5.4	<u>Mobile IT-Systeme</u>	122
16.6	<u>Kritische IT-Systeme</u>	122
16.6.1	<u>Risikoanalyse</u>	122
16.6.2	<u>Verfahrensweisungen</u>	123
17	<u>Störungen und Ausfälle</u>	124

17.1	<u>IS-Richtlinie</u>	124
17.2	<u>Reaktionen</u>	125
17.3	<u>Kritische IT-Systeme</u>	125
17.3.1	<u>Wiederanlaufpläne</u>	125
17.3.2	<u>Abhängigkeiten IT-Systeme</u>	126
18	<u>Sicherheitsvorfälle</u>	127
18.1	<u>IS-Richtlinie</u>	127
18.2	<u>Erkennen von Sicherheitsvorfällen</u>	127
18.3	<u>Reaktionen auf Sicherheitsvorfälle</u>	128
19	<u>Individualdokumentation</u>	129
19.1	<u>Verfahrensanweisungen</u>	129
19.2	<u>Risikoanalyse und Behandlung</u>	129
19.2.1	<u>Risikoanalyse</u>	130
19.2.2	<u>Risikobehandlung</u>	130
19.2.3	<u>Wiederholung und Anpassung</u>	130
20	<u>Verarbeitungen im Rahmen des Datenschutzes</u>	131
20.1	<u>Verarbeitungsprozesse</u>	131
20.2	<u>Lebenszyklus</u>	131
20.2.1	<u>Etablierung und Änderungen</u>	131
20.2.2	<u>Einstellung / Beendigung</u>	131
20.3	<u>Zweck</u>	132
20.4	<u>Beschreibung</u>	132
20.5	<u>Gemeinsam Verantwortliche</u>	132
20.6	<u>Eigentümer/Verantwortlicher</u>	132
20.7	<u>Rechtsgrundlage</u>	132
20.8	<u>Personenbezogene Daten</u>	133
20.8.1	<u>Datenkategorien</u>	133
20.8.2	<u>Datenübermittlung</u>	133
20.9	<u>IT-Systeme, mobile Datenträger</u>	134
20.10	<u>Risikoanalyse und -behandlung</u>	134
20.11	<u>Datenschutz-Folgeabschätzung (DSFA)</u>	135
20.12	<u>Betroffenenrechte</u>	136
20.12.1	<u>Anfrage und Reaktion</u>	136
20.12.2	<u>Erfüllung</u>	136
20.13	<u>Überprüfung</u>	138
21	<u>Informationssicherheit (Verweis auf Kapitel 1-9)</u>	139

<u>22</u>	<u>Auftragsverarbeitung</u>	140
<u>22.1</u>	<u>Als Auftraggeber</u>	140
<u>22.1.1</u>	<u>Datenschutz-Richtlinie</u>	140
<u>22.1.2</u>	<u>Vorbereitung</u>	140
<u>22.1.3</u>	<u>Eignung des Auftragsverarbeiters</u>	140
<u>22.1.4</u>	<u>Vertragsgestaltung</u>	140
<u>22.1.5</u>	<u>Überprüfung</u>	142
<u>22.2</u>	<u>Als Auftragnehmer</u>	143
<u>22.2.1</u>	<u>Datenschutz-Richtlinie</u>	143
<u>22.2.2</u>	<u>Zertifizierungen</u>	143
<u>23</u>	<u>Datenschutzvorfälle</u>	144
<u>23.1</u>	<u>Richtlinie</u>	144
<u>23.2</u>	<u>Erkennen</u>	144
<u>23.3</u>	<u>Reaktion</u>	145
<u>24</u>	<u>Datenmanagement</u>	146
<u>24.1</u>	<u>Löschen</u>	146
<u>24.2</u>	<u>Anonymisieren, Pseudonymisieren, Kryptieren (Verschlüsseln)</u>	146
<u>25</u>	<u>Technische und organisatorische Maßnahmen (TOM)</u>	147
<u>25.1</u>	<u>Technische Maßnahmen</u>	148
<u>25.2</u>	<u>Organisatorische Maßnahmen</u>	148
<u>26</u>	<u>Datenschutzberichte</u>	149
<u>26.1</u>	<u>Jahresbericht</u>	149
<u>26.2</u>	<u>Rechenschaftsbericht</u>	150
<u>27</u>	<u>Optimierungsmanagement (PDCA)</u>	151
<u>27.1</u>	<u>Planung (plan)</u>	151
<u>27.2</u>	<u>Realisierung (do)</u>	151
<u>27.3</u>	<u>Überprüfung (check)</u>	151
<u>27.4</u>	<u>Optimierung (act)</u>	152
<u>28</u>	<u>Richtlinien für Dienstleister vor Ort (DLO)</u>	153
<u>28.1</u>	<u>Zweck</u>	153
<u>28.2</u>	<u>Geltungsbereich und Zielgruppen</u>	153
<u>28.3</u>	<u>Informationssicherheitsprozess</u>	154
<u>28.3.1</u>	<u>Geregelter Sicherheitsprozess zur Steuerung und Verbesserung der Informationssicherheit</u>	154
<u>28.3.2</u>	<u>Ansprechpartner für Informationssicherheit</u>	154
<u>28.3.3</u>	<u>Mitarbeiter und Dienstleister</u>	154

28.3.4	<u>Anforderungen zum Stand der Technik</u>	155
28.3.5	<u>Datenschutz</u>	155
28.4	<u>Technische und organisatorische Bestimmungen</u>	156
28.4.1	<u>Softwareentwicklung (sofern in der Zusammenarbeit relevant)</u>	156
28.4.2	<u>Zugriffs- und Zutrittsschutz</u>	156
28.4.3	<u>Kennwortanforderungen</u>	157
28.4.4	<u>Netzwerksicherheit</u>	157
28.4.5	<u>Schadsoftwareschutz</u>	157
28.4.6	<u>Systemhärtung, Schwachstellen und Patch-Management</u>	157
28.4.7	<u>Administration von Systemen und Anwendungen</u>	158
28.5	<u>Umgang mit klassifizierten Informationen</u>	158
28.5.1	<u>Verarbeitung sensibler Informationen</u>	159
28.5.2	<u>Zugriffsschutz, Speicherung und Entsorgung</u>	159
28.5.3	<u>Übermittlung in Netzwerken</u>	159
28.6	<u>Anforderungen an die Wartungsprozesse</u>	160
28.6.1	<u>Allgemeines</u>	160
28.6.2	<u>Sichere Systemkonfiguration von Wartungskomponenten</u>	160
28.6.3	<u>Fernwartung</u>	161
28.7	<u>Spezielle Anforderungen der Telematikinfrasturktur (TI)</u>	161
28.8	<u>Meldung von Informationssicherheitsvorfällen</u>	161
29	<u>Qualitätsmanagement</u>	162
29.1	<u>Übersicht der medizinischen Versorgungseinheit/Klinik</u>	162
29.2	<u>Mission, Vision und Politik</u>	162
29.2.1	<u>Mission</u>	162
29.2.2	<u>Vision</u>	163
29.3	<u>Ressourcen und Prozesse</u>	164
29.3.1	<u>Technische Ressourcen</u>	164
29.3.2	<u>IT-Infrastruktur</u>	164
29.3.3	<u>Medizintechnik</u>	164
29.3.4	<u>Qualifikation und Kompetenz</u>	165
29.3.5	<u>Patientenversorgung (Fortbildung)</u>	165
29.3.6	<u>Qualitätsmanagement und Rechtskonformität</u>	165
29.3.7	<u>Kommunikation</u>	165
29.3.8	<u>Kommunikation mit Patienten</u>	165
29.3.9	<u>Kommunikation im Team</u>	166
29.4	<u>Messung, Analyse und Optimierung</u>	166

29.4.1	<u>Befragungen</u>	166
29.4.2	<u>Patienten</u>	166
29.4.3	<u>Mitarbeiter/Kollegen</u>	166
29.4.4	<u>Partner und Lieferanten</u>	166
29.4.5	<u>Statistiken und Auswertungen</u>	166
29.4.6	<u>Audit</u>	167
29.5	<u>Anwendungsbereich (Patientenversorgung)</u>	167
29.6	<u>Rechtliche Anforderungen nach SGB V QM RL §4 (vertragsärztliche Versorgung)</u>	168
29.6.1	<u>Messen und Bewerten von Qualitätszielen</u>	168
29.6.2	<u>Erhebung des Ist-Zustandes und Selbstbewertung</u>	168
29.6.3	<u>Regelung von Verantwortlichkeiten und Zuständigkeiten</u>	168
29.6.4	<u>Prozess- bzw. Ablaufbeschreibungen</u>	168
29.6.5	<u>Schnittstellenmanagement</u>	168
29.6.6	<u>Checklisten</u>	169
29.6.7	<u>Teambesprechungen</u>	169
29.6.8	<u>Fortbildungs- und Schulungsmaßnahmen</u>	169
29.6.9	<u>Patientenbefragungen</u>	169
29.6.10	<u>Mitarbeiterbefragungen</u>	169
29.6.11	<u>Beschwerdemanagement</u>	170
29.6.12	<u>Patienteninformation und -aufklärung</u>	170
29.6.13	<u>Risikomanagement</u>	170
29.6.14	<u>Fehlermanagement und Fehlermeldesysteme</u>	170
29.6.15	<u>Notfallmanagement</u>	171
29.6.16	<u>Hygienemanagement</u>	171
29.6.17	<u>Arzneimitteltherapiesicherheit</u>	171
29.6.18	<u>Schmerzmanagement</u>	171
29.6.19	<u>Maßnahmen zur Vermeidung von Stürzen bzw. Sturzfolgen</u>	171
29.6.20	<u>Dokumentation</u>	172
30	<u>Anhang Rechtsvorschriften für Ärzte</u>	173
31	<u>Anhang Aufbewahrungsfristen</u>	174
32	<u>Anhang individuell</u>	179