

Inhaltsübersicht

<i>Vorwort</i>	V
<i>Bearbeiterverzeichnis</i>	VII
<i>Inhaltsverzeichnis</i>	XI
<i>Abkürzungsverzeichnis</i>	XXV
<i>Gesamtliteraturverzeichnis</i>	XXIX
1. Kapitel Cyberbedrohungslage im Gesundheitswesen (<i>Dochow</i>)	1
2. Kapitel Rechtsgrundlagen der Cybersicherheit im Gesundheitswesen (<i>Dittrich/Dochow/Ippach</i>)	17
3. Kapitel Technische Grundlagen (<i>Hansen</i>)	45
4. Kapitel Krankenhäuser (<i>Monsees/Gehrmann</i>)	65
5. Kapitel Medizinprodukte (<i>Kohoutek</i>)	93
6. Kapitel Arzneimittel (<i>Monschke/Copeland</i>)	107
7. Kapitel Laborbereich (<i>Dittrich/Ippach</i>)	119
8. Kapitel Telematikinfrastruktur (<i>Dochow/Herpers</i>)	127
9. Kapitel Ambulante Gesundheitsversorgung (<i>Grzesiek</i>)	159
10. Kapitel Pflege (<i>Staufer/Kirsch</i>)	179
11. Kapitel Rettungsdienste, Katastrophenschutz und Notrufleitstellen (<i>Staufer/Kirsch</i>)	185
12. Kapitel Digitale Gesundheitsanwendungen und Health Apps (<i>Kohoutek</i>)	199
13. Kapitel Telemedizin (<i>Hahn/Schüller</i>)	209
14. Kapitel Sozialdatenverwaltung (<i>Kircher</i>)	227
15. Kapitel Gesundheitsforschung (<i>Weichert</i>)	235
16. Kapitel Register des Gesundheitswesens (<i>Stollmann/Stenzel</i>)	251
17. Kapitel Cybersicherheit im öffentlichen Gesundheitsdienst (<i>Franck</i>)	263
18. Kapitel Compliance und Cybersicherheitsmanagement (<i>Müller/Dittrich</i>)	281
19. Kapitel Cybercrime im Gesundheitswesen (<i>S. T. Vogel</i>)	303
20. Kapitel Patientenschäden und Cybersicherheit: Haftung der Behandlerseite (<i>Vogeler</i>)	325
21. Kapitel Künstliche Intelligenz und Cybersicherheit im Krankenhaus (<i>P. Vogel</i>)	339
22. Kapitel Versicherungslösungen für Cybergefahren (<i>Grieger</i>)	345
23. Kapitel Anforderungen an die Vertragsgestaltung (<i>Ziegler</i>)	359
24. Kapitel Cyber Incident – Legal-Checkliste (<i>Adelberg/Dittrich</i>)	381
<i>Stichwortverzeichnis</i>	399

Inhaltsverzeichnis

<i>Vorwort</i>	V
<i>Bearbeiterverzeichnis</i>	VII
<i>Inhaltsübersicht</i>	IX
<i>Abkürzungsverzeichnis</i>	XXV
<i>Gesamtliteraturverzeichnis</i>	XXIX

1. Kapitel

Cyberbedrohungslage im Gesundheitswesen

A. Einführung	1
B. Lageberichte zur IT-Sicherheit in Deutschland	2
C. Bedrohungslage aus Sicht von Cyberkriminellen	4
D. Bedrohungslage nach Sektoren und anderen Bereichen	4
I. Stationärer Gesundheitssektor	4
1. Lukas-Krankenhaus Neuss 2016	5
2. DRK-Kliniken Südwest 2019	6
3. Universitätsklinikum Düsseldorf 2020	6
4. Klinikum Bremen 2023	7
5. Universitätsklinikum Frankfurt 2023	7
6. Krankenhaus Esslingen 2023	7
7. Betroffene Kliniken im Jahr 2024	8
II. Ambulanter Sektor	8
1. Angriffe auf Arztpraxen	8
2. Angriffe auf Dienstleister	9
III. Krankenversicherungen	9
IV. Telematikinfrastruktur	10
V. Medizinprodukte	13
VI. Arzneimittelbereich und Apotheken	13
VII. Gesundheits-Apps	14
VIII. Einrichtungen der Gesundheits- und Selbstverwaltung	14
E. Fazit	15

2. Kapitel

Rechtsgrundlagen der Cybersicherheit im Gesundheitswesen

A. Einführung	18
B. Verfassungsrecht und Grundrechte (Überblick)	19
C. Europarecht	22
I. EU-Grundrechte-Charta	22
II. NIS-Richtlinie	23
III. NIS-2-Richtlinie	23

IV. Resilienz-Richtlinie	25
V. DSGVO	26
1. Grundsätze und Anforderungen	27
2. Technische und organisatorische Maßnahmen	28
3. Meldungen von Datenschutzverletzungen	31
VI. Europäischer Gesundheitsdatenraum und weitere Vorhaben	31
D. Nationales Recht	32
I. BSIG mit BSI-KritisV	33
II. BSIG-E aufgrund NIS2UmsuCG	34
III. KRITIS-DachG-E	38
IV. SGB V	39
1. Cybersicherheit nach den Richtlinien gemäß § 390 SGB V	40
2. Cybersicherheit nach § 391 SGB V	40
3. Cybersicherheit in der Telematikinfrastruktur	41
V. Cybersicherheit und Berufsgeheimnisschutz	41
E. Fazit und Ausblick	42

3. Kapitel

Technische Grundlagen

A. Einführung	47
B. Begriff der Cybersicherheit	48
C. Anforderungen an die Cybersicherheit	49
I. Schutzziele der Cybersicherheit	49
1. Klassische Schutzziele	49
2. Authentizität als ableitbares Schutzziel	51
3. Bedeutung von Resilienz	51
4. Die Gewährleistungsziele des Standard-Datenschutzmodells	52
II. Stand der Technik	54
D. Bedrohungen	54
I. Schwachstellen	54
II. Angriffsarten von Cyberkriminellen	56
E. Maßnahmen zur Gewährleistung des Schutzes	57
I. Allgemeine Schutzmaßnahmen	57
II. Verschlüsselung	58
III. Authentifizierung, Autorisierung, Signaturen	58
IV. Absicherung von Kommunikationsnetzen	59
V. Anonymisierung, Pseudonymisierung und Löschen	59
VI. Umgang mit Sicherheitsvorfällen	60
F. Standards im Bereich Cybersicherheit	60
I. Allgemeine Cybersicherheitsstandards	60
II. Spezifische Cybersicherheitsstandards für den Gesundheitsbereich	62
G. Fazit und Ausblick	63

4. Kapitel

Krankenhäuser

A. Krankenhäuser	65
I. Bedeutung der Cybersicherheit im Krankenhausbereich	65
II. Grundlegende Regelungssystematik für Krankenhäuser	66
III. Anforderungen für Krankenhäuser als Kritische Infrastrukturen nach dem BSIG	69
1. Umsetzung der OTV mit B3S	69
2. Nachweispflichten	72
3. Meldepflicht	74
4. Kooperations- und sonstige Pflichten	76
5. Sanktionen	77
IV. Anforderungen für Krankenhäuser nach § 391 SGB V	78
1. Regelungsgeschichte und Anwendungsbereich	78
2. Umsetzung der OTV mit Empfehlung für B3S	79
3. Rechtsfolgen mangelhafter Umsetzung	79
V. Cybersicherheit nach der DSGVO	80
1. Besonderheiten im Krankenhaus	80
a) Öffentliche Träger	82
b) Private Träger	85
c) Freigemeinnütziger Träger	85
2. Meldepflichten nach der DSGVO	86
3. Umsetzungshinweise von Behörden	87
4. Sanktionen nach der DSGVO	87
5. Vorfälle aus Datenschutzberichten/Praxis	89
VI. Förderung von Cybersicherheit (KHZG u.a.) und Förderungsbedarf	90
B. Fazit und Ausblick	92

5. Kapitel

Medizinprodukte

A. Einführung	93
B. Kritische Infrastrukturen nach dem BSIG	93
I. Versorgung mit Medizinprodukten	94
II. Sicherheit in der Informationstechnik	95
III. Umsetzung der OTV bzw. TOM mit B3S	96
IV. Weitere Rechtspflichten und Sanktionen	97
C. Cybersicherheit nach Medizinprodukterecht	97
I. Einleitung	97
II. „Secure by Design“	99
III. Dokumentation und Gebrauchsanweisung	101
IV. Überwachung nach dem Inverkehrbringen und Vigilanz	103
V. Betrieb und Anwendung von Medizinprodukten	103

D. Cybersicherheit und Produkthaftung 104

 I. Haftung nach dem ProdHaftG 104

 II. Deliktische Haftung 105

E. Cybersicherheit nach der DSGVO 105

F. Fazit und Ausblick 106

6. Kapitel
Arzneimittel

A. Einleitung 107

 I. Kritische Infrastrukturen nach dem BSIG 108

 1. Anwendungsbereich 108

 a) Herstellung 109

 b) Vertrieb 110

 c) Abgabe durch Apotheken 110

 2. Umsetzung der OTV mit B3S 111

 3. Weitere Rechtspflichten und Sanktionen 111

 4. Ausblick auf die Umsetzung der NIS-2-RL und die CER-Richtlinie 112

 II. Cybersicherheit im nationalen Arzneimittelrecht 113

 III. Cybersicherheit nach der DSGVO 114

 1. Begriff der Gesundheitsdaten als besondere Kategorie personenbezogener Daten 114

 2. Rechtliche Einordnung und Besonderheiten 114

 IV. Geschäftsgeheimnisschutz in der Pharmaforschung 115

 V. Das E-Rezept 116

B. Fazit und Ausblick 116

7. Kapitel
Laborbereich

A. Einführung 119

B. Labormedizin im Anwendungsbereich des BSIG 120

 I. Anwendungsbereich der BSI-KritisV seit 2017 120

 II. Anwendungsbereich der BSI-KritisV seit 2021 121

 III. Labormedizin als Kritische Infrastruktur in den nächsten Jahren 122

 IV. Pflichtenprogramm und drohende Sanktionen aus dem BSIG 123

C. Anwendungsbereich des KRITIS-Dachgesetzes 124

D. DSGVO 125

E. Fazit und Ausblick 126

8. Kapitel

Telematikinfrastruktur

A. Einführung: Bedeutung der Telematikinfrastruktur	127
B. Grundlagen zur Telematikinfrastruktur	128
I. Rechtliche Einordnung	128
II. Definitionen und Begriffe	130
III. Anwendungen im Überblick	132
IV. Sicherheitsarchitektur und Sicherheitsleistungen der TI	133
1. Sichere Anbindung an das Netz der TI	133
2. Digitale Identitäten	135
a) Smartcards und PKI	135
b) Kartenunabhängige Identitäten und Identity Provider	137
3. Ver- und Entschlüsselung	138
4. Elektronische Signaturen	139
C. Regulierung der Cybersicherheit	140
I. Rolle und Aufgaben der gematik	141
II. Betriebsverantwortung der gematik	143
III. Nachweis von Produktsicherheit	144
1. Auftragsvergabe und Zulassung von Betriebsleistungen	145
2. Zulassung von Komponenten und Diensten	146
3. Zulassung von Herstellern und Anbietern	147
4. Bestätigung von weiteren Diensten und Anwendungen	148
IV. Überwachung von Funktionsfähigkeit und Sicherheit	149
1. Meldepflichten und Maßnahmen zur Gefahrenabwehr (§ 329 SGB V)	149
a) Meldepflichten	149
b) Gefahrenabwehrmaßnahmen	151
2. Vorkehrungen zur Vermeidung von Störungen (§ 330 SGB V)	151
3. Maßnahmen zur Betriebsüberwachung (§ 331 SGB V)	152
4. Anforderungen an Dienstleister (§ 332 SGB V)	154
5. Überprüfung durch das BSI (§ 333 SGB V)	155
V. Zugriffskonzept	155
VI. Sanktionen	156
D. Fazit und Ausblick	157

9. Kapitel

Ambulante Gesundheitsversorgung

A. Steigende Bedrohung der ambulanten Gesundheitsversorgung durch Cyberattacken	159
B. § 390 SGB V und KBV-Richtlinie	161
I. Rechtliche Grundlagen nach § 390 SGB V	161
II. Anwendungsbereich der IT-Sicherheitsrichtlinien	162
III. Pflichten nach der KBV-Richtlinie zur IT-Sicherheit	163
1. Grundlegende Anforderungen an alle Arztpraxen	163
2. Weitere Anforderungen	164
IV. Rechtsfolgen mangelhafter Umsetzung	164

C. Cybersicherheit nach der DSGVO	165
I. Besonderheiten in der vertrags(zahn)ärztlichen Versorgung	165
II. Privatärztlicher Bereich	165
1. Abstrakte Anforderungen nach der DSGVO	166
2. Berufsrecht	166
3. Umsetzungshinweise von Behörden	167
III. Zusammenarbeit mit externen Dienstleistern	167
IV. Meldepflichten nach der DSGVO	170
D. Das Digital-Gesetz	170
I. Die Einrichtung der elektronischen Patientenakte	171
II. Beratung und Unterstützung durch den sog. Digitalbeirat	172
III. Verbesserung der Interoperabilität	172
IV. Erhöhung der Cybersicherheit	172
1. IT-Sicherheit in der vertrags(zahn)ärztlichen Versorgung	173
2. IT-Sicherheit in Krankenhäusern	173
3. IT-Sicherheit in gesetzlichen Krankenkassen	173
4. Cloud-Einsatz im Gesundheitswesen	173
E. Rechtsfolgen und Sanktionen	174
1. Zivilrechtlicher Schadenersatz	174
2. Datenschutzrechtliche Sanktionen	175
3. Strafrechtliche Risiken	175
F. Basis-IT-Sicherheitskonzept	177
G. Fazit und Ausblick	177

10. Kapitel
Pflege

A. Allgemeine Anmerkungen	179
B. Cybersicherheit in der Pflege	180
I. Übersicht, Aufgaben und Ziele der Pflege	180
II. Gesetzliche Grundlagen der Cybersicherheit	181
III. Cybersicherheit von Pflegeeinrichtungen in Gesundheitskonzernen	183
IV. Cybersicherheit bei Herstellern	184
C. Fazit	184

11. Kapitel
Rettungsdienste, Katastrophenschutz und Notrufleitstellen

A. Allgemeine Anmerkungen	185
B. Cybersicherheit im Rettungsdienst	188
I. Übersicht	188
II. Gefahrenlage im Rettungsdienst bei Digitalisierung und Vernetzung	189

III. Gesetzliche Bestimmungen zur Cybersicherheit	190
1. Baden-Württemberg	190
2. Bayern	190
3. Berlin	190
4. Brandenburg	191
5. Bremen	191
6. Hamburg	191
7. Hessen	191
8. Mecklenburg-Vorpommern	191
9. Niedersachsen	192
10. Nordrhein-Westfalen	192
11. Rheinland-Pfalz	192
12. Saarland	192
13. Sachsen	192
14. Sachsen-Anhalt	193
15. Schleswig-Holstein	193
16. Thüringen	193
IV. Cybersicherheit in der Luftrettung	194
V. Reformbedarf bei Änderung der Notfallversorgung	194
C. Cybersicherheit bei Notrufleitstellen und Lagezentren	195
I. Übersicht, Aufgaben und Rechtsgrundlagen	195
II. Gefahrenlage für Notrufleitstellen und Lagezentren	196
III. Reformbedarf und Gesetzgebungskompetenzen	197
D. Fazit und Ausblick	197

12. Kapitel

Digitale Gesundheitsanwendungen und Health Apps

A. Digitale Gesundheits- und Pflegeanwendungen	199
I. Hintergrund und Anwendungsgebiete von DiGA	199
II. Zulassungsverfahren mit Schwerpunkt Cybersicherheit	200
1. Fast-Track-Verfahren	200
2. Streichung aus DiGA-Verzeichnis wegen Cybervorfällen	203
III. Datenschutz im Zulassungsverfahren	203
IV. Digitale Pflegeanwendungen nach dem SGB XI	205
B. Cybersicherheit nach der DSGVO	206
C. Cybersicherheit nach der MDR	206
D. Fazit und Ausblick	207

13. Kapitel

Telemedizin

A. Telemedizin in Deutschland	211
I. Einführung	211
II. (Zulässige) Anwendungsmöglichkeiten	212

B. Cybersicherheit nach der DSGVO	214
I. Grundsätze der Datensicherheit	214
II. Pflichten des Verantwortlichen	215
III. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellung	215
IV. Sicherheit der Verarbeitung	216
1. Grundsätzliches	216
2. Technische und organisatorische Maßnahmen (TOM)	216
V. Datenschutz-Folgenabschätzung	218
1. Erforderlichkeit	218
2. Zeitpunkt der Durchführung	219
C. Telemedizin und Anforderungen an die Cybersicherheit nach SGB V, BMV-Ä, BMV-Z und weiteren Vereinbarungen	219
I. Vereinbarung über telemedizinische Leistungen in der vertragsärztlichen Versorgung (Anlage 31 BMV-Ä)	219
II. Konsiliarische Befundbeurteilung von Röntgenaufnahmen (§ 364 SGB V)	220
III. Videosprechstunde in der vertrags(zahn)ärztlichen Versorgung (§§ 365 und 366 SGB V)	221
IV. Telemedizinische Konsilien (§ 367 SGB V)	224
V. Telemedizinisches Monitoring (§ 367a SGB V)	224
VI. Versorgung mit Hebammenhilfe im Wege der Videobetreuung (§ 134a Abs. 1d S. 1 Nr. 1 und 2 SGB V)	224
VII. Ambulante Behandlung in stationären Pflegeeinrichtungen (§ 119b Abs. 2b SGB V)	225
D. Fazit und Ausblick	226

14. Kapitel
Sozialdatenverwaltung

A. IT-Sicherheitsrecht in der Sozialdatenverwaltung	227
B. Cybersicherheit im Sozialrecht (Regelungen im SGB X)	228
C. Kranken- und Pflegeversicherungen (einschl. KRITIS-Sektor nach BSIG und BSI- KritisV)	231
D. Fazit und Ausblick	234

15. Kapitel
Gesundheitsforschung

A. Verfassungsrechtliche Vorgaben für die Forschung	235
B. Forschung in der DSGVO	237
I. Zweckbindung	237
II. Betroffenenrechte	237
C. Weitere EU-Regelungen	238
D. Nationalgesetzliche Regelungen	238
I. Datenschutz- und Medizinrecht	239

II. Allgemeine Regelungen	239
1. Einwilligung	239
2. Gesetzliche Abwägungsregelungen	240
III. Spezifische Regelungen	240
E. Spezifische Garantien	241
I. Verarbeitungsverbote	241
II. Personelle Anforderungen	241
III. Prozedurale Anforderungen	242
IV. Weitere formelle Anforderungen	243
V. Insbesondere Datenminimierung	243
VI. Treuhänder	244
VII. Forschungsprozesse	245
VIII. Transparenz und Betroffenenrechte	245
IX. Technisch-organisatorische Vorkehrungen	246
X. Register und Biobanken	246
XI. Forschungsdateninfrastruktur	248
F. Ausblick	248

16. Kapitel

Register des Gesundheitswesens

A. Besondere Rechtsvorschriften bei Registern	251
I. Ausgangslage	251
II. Registerlandschaft in Deutschland	253
1. Transplantationsregister	253
2. Implantate Register	256
3. Klinische Krebsregister	257
B. Cybersicherheit nach der DSGVO	259
C. Fazit und Ausblick	261

17. Kapitel

Cybersicherheit im öffentlichen Gesundheitsdienst

A. Einführung	263
B. Informationssicherheitsrecht(e) der öffentlichen Verwaltung	264
I. Verwaltungsverfahrensgesheimnis	264
II. Datenschutzrecht	265
III. IT-Sicherheitsrecht	267
IV. Geheimschutzrecht	268
C. Cybersicherheitsrecht(e) der Gesundheitsämter in den Ländern	269
I. Baden-Württemberg	269
II. Bayern	270
III. Berlin	271
IV. Brandenburg	271
V. Bremen	272

VI. Hamburg	272
VII. Hessen	273
VIII. Mecklenburg-Vorpommern	273
IX. Niedersachsen	274
X. Nordrhein-Westfalen	274
XI. Rheinland-Pfalz	275
XII. Saarland	275
XIII. Sachsen	276
XIV. Sachsen-Anhalt	276
XV. Schleswig-Holstein	277
XVI. Thüringen	277
D. Pakt für den Öffentlichen Gesundheitsdienst	278
E. Zusammenfassung und Ausblick	279

18. Kapitel
Compliance und Cybersicherheitsmanagement

A. Cybersicherheit als Pflicht der Unternehmensleitung	282
I. Gesetzliche Grundlagen für Compliance-Pflichten und Anforderungen für Geschäftsleitungen	283
1. Leitungspflichten aus dem Gesellschaftsrecht	283
a) Einleitung zu den Leitungspflichten	283
b) Rechtsprechung zu den gesellschaftsrechtlichen Compliance-Pflichten ...	284
2. Compliance-Pflichten aus dem OWiG	285
a) Organisationsverschulden nach § 130 OWiG	286
b) Verbandsgeldbuße nach § 30 OWiG	286
c) Panzerhaubitzen-Entscheidung des BGH vom 9.5.2017	286
d) Rechtspolitische Erwägungen	286
3. Compliance-Pflichten aus der DSGVO	287
4. Compliance-Pflichten aus dem Geschäftsgeheimnisschutzgesetz	288
5. Compliance-Pflichten aus dem BSIG	289
a) Stand des BSIG vor dem NIS2UmsuCG	289
b) Exkurs: Referentenentwurf zum NIS2UmsuCG	289
II. Wirkung von Compliance auf Bußgelder und andere Sanktionen	292
1. Folgen von Rechtsverstößen für die Geschäftsführung	292
2. Folgen von Rechtsverstößen für das Unternehmen	293
3. Bußgeldmindernde Wirkung eines Compliance-Management-Systems	293
B. Umsetzungsmaßnahmen zur Cybersicherheits-Compliance	294
I. Allgemeine Hinweise zum Compliance-Management	294
II. Hinweisgebersysteme bei Cybergefahren	296
1. Hinweisgebersystem nach dem Hinweisgeberschutzgesetz	297
a) EU-Whistleblowerrichtlinie	297
b) IT-Sicherheit im HinSchG	297
c) Sanktionsrelevanz des HinSchG	298
2. Hinweisgebersysteme außerhalb des HinSchG	298

III. Internal Investigations	299
IV. Standards im Bereich Compliance und Cybersicherheit	300
V. Kooperation mit Behörden und Dritten	300
C. Fazit und Ausblick	301

19. Kapitel

Cybercrime im Gesundheitswesen

A. Cybercrime-Tatbestände bei Cyberangriffen und anderen Vorfällen	304
I. Straftatbestände nach dem StGB	304
II. Die Verletzung von Geschäftsgeheimnissen nach § 23 GeschGehG	306
1. Betrachtung aus Sicht der Täter	306
2. Strafbarkeitsrisiken für die Leistungserbringer	307
B. Körperverletzungs- und Tötungsdelikte im Zusammenhang mit Cyberangriffen ...	307
I. Betrachtung aus Sicht der Täter	308
II. Strafbarkeitsrisiken für die Leistungserbringer	310
C. Strafbarkeit der Lösegeldzahlung	312
I. Einführung	312
II. Empfehlungen contra Lösegeldzahlungen	312
III. Strafbarkeit bei der Zahlung von Lösegeld	312
1. Unterstützung einer kriminellen Vereinigung, § 129 Abs. 1 S. 2 StGB	313
2. Terrorismusfinanzierung	317
3. Geldwäsche	317
4. Verstöße gegen das Außenwirtschafts- und EU-Sanktionsrecht	318
5. Untreue	318
IV. Strafbarkeit von Versicherern	319
D. Strafbare Schweigepflichtverletzung durch Unterlassen	319
E. Strafanzeige bei Cybercrime als Mittel der Wahl	321
F. Behördliche Ermittlungsmaßnahmen bei Cybercrime mit Auswirkungen auf die Leistungserbringer	322
I. Durchsuchung	322
II. Beschlagnahme und Sicherstellung	323
III. Ermittlungen infolge von Hinweisen durch Whistleblower	323
G. Fazit und Ausblick	324

20. Kapitel

Patientenschäden und Cybersicherheit: Haftung der Behandlerseite

A. Problemstellung und Haftungsgrundlagen	326
I. Inkorporierung des Cybersicherheitsrechts in das allgemeine Arzthaftungsrecht	326
1. Ausgangslage: Nichterbringung des Facharztstandards	326
2. „Cybersicherheit“ – dogmatische Einordnung	327
3. Aufklärungsfehlerhaftung?	328
II. Weitere mögliche Anspruchsgrundlagen	328

B. (Haftungserhebliche) Standards der Cybersicherheit	330
I. Standard und Verkehrspflichten	330
II. Konkrete Cybersicherheitsstandards	331
C. Auswirkungen auf die Darlegungs- und Beweislast	332
I. Sekundäre Darlegungslast	333
II. Cybersicherheit als voll beherrschbares Behandlungsrisiko	334
III. Cybersicherheit und grober Behandlungsfehler	335
IV. Anscheinsbeweis	336
D. Mithaftung Dritter und die Auswirkung auf die Haftung	337
I. Cyberkriminelle	337
II. Fehlverhalten von Angestellten	337
III. Externe Dienstleister	337
E. Fazit und Ausblick	338

21. Kapitel

Künstliche Intelligenz und Cybersicherheit im Krankenhaus

A. Einführung	339
B. Chancen und Risiken des Einsatzes von KI im Krankenhaus	341
C. Regulatorischer Rahmen für den Einsatz von KI im Hinblick auf Cybersicherheit	342
I. DSGVO	342
II. KI-VO-E	343
D. Fazit und Ausblick	344

22. Kapitel

Versicherungslösungen für Cybergefahren

A. Cyberversicherungen nach AVB Cyber	346
I. Inhalt von Cyberversicherungen	346
II. Patientenschäden und Versicherungslösungen	347
B. Obliegenheiten im Versicherungsverhältnis	349
I. Vor Abschluss der Versicherung	349
II. Nach Abschluss der Versicherungen mit Rechtsfolgen bei Verletzungen	349
1. Umsetzung gesetzlicher Vorgaben zur IT-Sicherheit	349
2. Umsetzung vertraglicher Vorgaben zur IT-Sicherheit	350
3. Anzeigepflicht und Schadensverminderungspflicht	353
C. Unterstützung durch Versicherungsgeber bei IT-Vorfall	354
D. Fazit und Ausblick	355

23. Kapitel

Anforderungen an die Vertragsgestaltung

A. Einleitung	360
B. Verträge mit IT-Dienstleistern	362
I. Pflichten des medizinischen Leistungserbringers	362
1. Anschluss an die Telematikinfrastruktur	362
2. Vorgaben zur IT-Sicherheit in der vertrags(zahn)ärztlichen Versorgung gemäß § 390 SGB V	363
3. Vorgaben zur IT-Sicherheit in Krankenhäusern gemäß § 391 SGB V	364
4. Vorgaben zur IT-Sicherheit für den Einsatz von Cloud-Diensten gemäß § 393 SGB V	365
II. IT-Dienstleister als Verantwortlicher	365
1. Gesetzliche Verantwortlichkeit	365
2. Vertragliche Verantwortlichkeit	366
III. Möglichkeiten der Vertragsgestaltung	367
1. Konkretisierung des Leistungsgegenstands	367
2. Anforderungen an das Personal	369
3. Mangelfreiheit der Leistungserbringung	370
4. Haftung im Innenverhältnis und Freistellung	371
5. Vertragsstrafe	372
C. Aspekte der Cybersicherheit bei Kooperationen von medizinischen Einrichtungen	373
I. Gesetzliches Rücksichtnahmegebot und Verantwortlichkeiten	373
II. Möglichkeiten der Vertragsgestaltung	374
1. Proaktiv wirkende vertragliche Instrumente	374
2. Vertragliche Instrumente in Bezug auf die Durchführung einer Kooperation	375
3. Vertragliche Regelungen in Bezug auf den Umgang mit unerwünschten IT-Sicherheitsvorfällen	376
D. Aspekte von Kooperationen mit internationalen Vertragspartnern	377
I. Datenschutzrecht	377
II. Anwendbares Recht und Rechtswahlklausel	377
III. Gerichtsstandvereinbarungen	378
E. Fazit	379

24. Kapitel

Cyber Incident – Legal-Checkliste

A. Einführung zu Cyber Incident Plänen	381
B. Die vorbereitende Arbeit mit der Legal-Checkliste	382
C. Die Arbeit mit der Legal-Checkliste im Notfall	384
D. Anhang: Legal-Checkliste (als Übersicht)	385
<i>Stichwortverzeichnis</i>	399