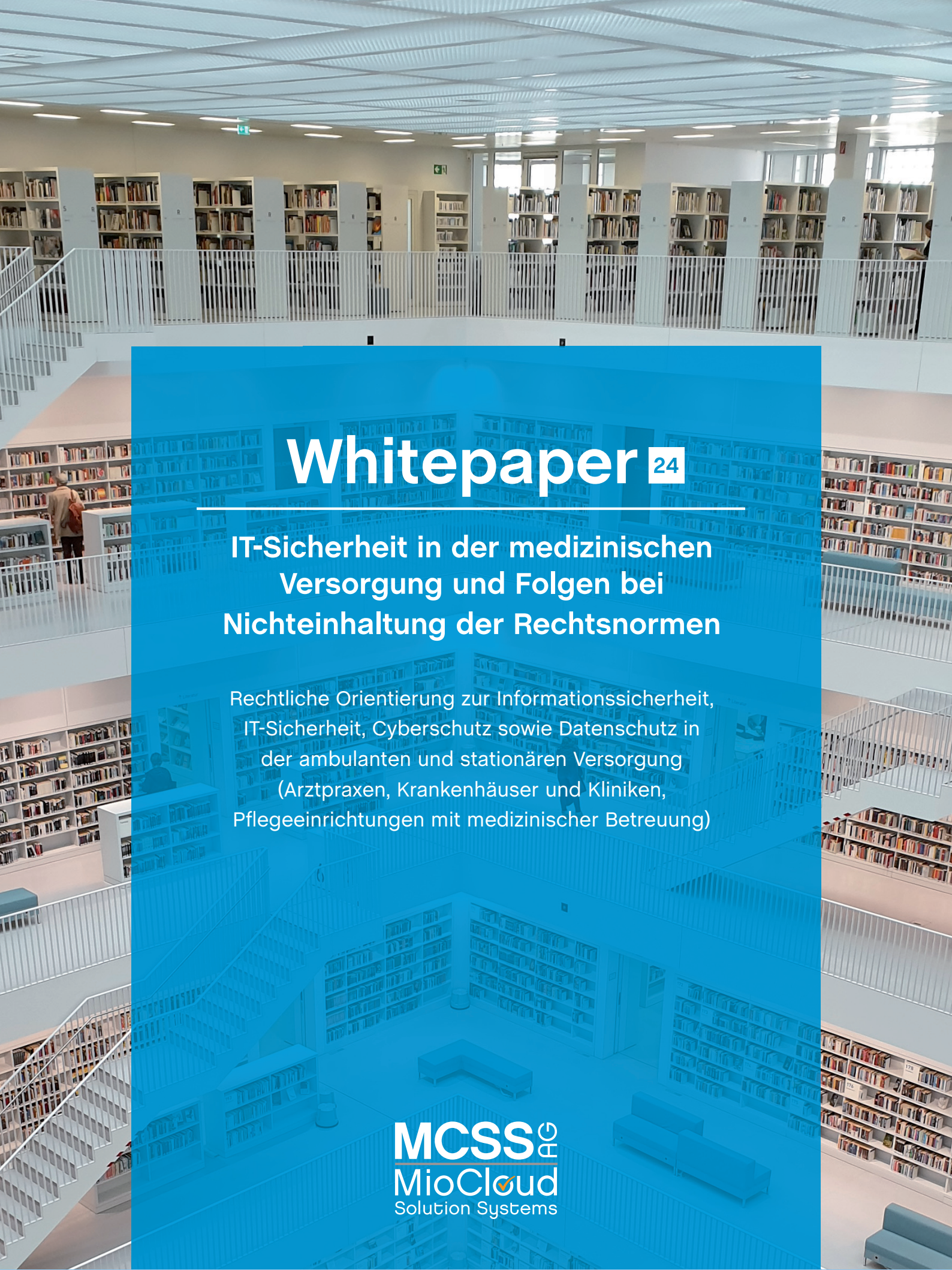


# Whitepaper 24

## IT-Sicherheit in der medizinischen Versorgung und Folgen bei Nichteinhaltung der Rechtsnormen

Rechtliche Orientierung zur Informationssicherheit, IT-Sicherheit, Cyberschutz sowie Datenschutz in der ambulanten und stationären Versorgung (Arztpraxen, Krankenhäuser und Kliniken, Pflegeeinrichtungen mit medizinischer Betreuung)

MCSS AG
MioCloud
Solution Systems

Sicherheit durch Technologie.

Sicherheit durch Technologie

# INHALT

# 1 Extrakt

Die rechtlichen Anforderungen zur Informationssicherheit, IT-Sicherheit, Cyberschutz sowie Datenschutz in der ambulanten und stationären Versorgung, werden durch verschiedene Gesetze, Verordnungen und Richtlinien definiert.
Im Wesentlichen sind dies:

- Art. 32 DSGVO
- Art. 34 DSGVO
- § 75b und § 75c SGB V (Digitale-Versorgung-Gesetz) inkl. Richtlinien
- Qualitätsmanagement nach § 135ff SGB V und QM-Richtlinie
- § 8a Absatz 1/8b BSIG (KRITIS-Krankenhäuser)
- § 203 StGB iVm ärztlicher Schweigepflicht

Die o.g. Normen sind rechtsverbindlich und verpflichtend für die Verantwortlichen. In der ambulanten Versorgung sind dies die verantwortlichen Ärzte/-innen und in der stationären Versorgung die rechtlichen Vertreter/-innen und die medizinischen Leiter/-innen.

Die entsprechenden Risiken, sowie die rechtlichen und wirtschaftlichen Konsequenzen bei Nichteinhalten oder Nichterfüllung der verbindlichen Normen sind komplex und abhängig von vielen Kriterien. Vertiefende Hinweise können den folgenden Veröffentlichungen entnommen werden:

- Dittrich / Ippach „IT-Sicherheit betrifft nicht nur Großkrankenhäuser – die Regulierung der IT-Sicherheit im ambulanten und stationären Bereich“, GesR 2021, 285 ff.
- Prölss / Martin: Versicherungsvertragsgesetz: VVG, 31., überarbeitete Auflage. 2021

Wegen der Komplexität der relevanten Rechtsnormen und den daraus abzuleitenden technischen und organisatorischen Maßnahmen, sieht der Gesetzgeber die Risikoübertragung sowie die Umsetzung der relevanten rechtlichen Verpflichtungen in der Präambel der Richtlinie nach § 75b SGB V an externe Dritte vor:

> *„Bei der Umsetzung (der Richtlinie nach § 75b SGB V) können Risiken auch an Dritte, wie IT-Dienstleister oder Versicherungen, übertragen werden.“*

In diesem Kontext sind auch die Anforderungen für Risikoübertragungen an Dritte, wie Dienstleistende und z.B. Cyber-Versicherer, in die aktuelle rechtliche Bewertung einzubeziehen.

Das Segment der Cyber-Policen wird im Jahr 2021 zu einem der Aufsichtsschwerpunkte der Versicherungsaufsicht (BaFin). Neben einer inhaltlichen Analyse des am Markt angebotenen Versicherungsschutzes soll dabei auch die Tragfähigkeit der Produkte im Mittelpunkt stehen.

# 2 Definitionen und Geltungsbereich

## 2.1 IT-Sicherheit, Informationssicherheit und Cybersicherheit

### IT-Sicherheit

Die IT-Sicherheit bezieht sich in der medizinischen Versorgung auf den Schutz der IT-Infrastruktur von Arztpraxen, Kliniken und Krankenhäusern etc. mit dem Ziel, wirtschaftlichen Schaden und Datenschutzverstöße zu verhindern. Es finden Werkzeuge wie Antivirenprogramme, Spamfilter und Passwortmanager ihre Anwendung.

### Informationssicherheit

Die Informationssicherheit beinhaltet die IT-Sicherheit, erweitert diesen Begriff jedoch um die Sicherheit von nicht technisch gespeicherten und elektronisch verarbeiteten Daten. Um das Erreichen von Informations- und IT-Sicherheit messbar zu machen, werden sogenannte Schutzziele definiert.

**Allgemeine Schutzziele sind dabei:**

- Die Vertraulichkeit von Daten, dass keine Daten von unberechtigten Personen gelesen oder verändert werden dürfen, beispielsweise durch Richtlinien, Nutzergruppen und der Anwendung des sogenannten Need-to-know-Prinzips.
- Die Integrität von Daten, dass keine Daten unbemerkt verändert werden dürfen und jede Veränderung beispielsweise durch Logs nachvollziehbar belegt werden kann. Auch die Konsistenz von Daten, also der Abhängigkeit der Daten untereinander zählt zum Schutzziel Integrität.
- Die Verfügbarkeit von Daten, die in definierten Zeiträumen gewährleistet sein muss (beispielsweise Aufbewahrungsfristen medizinischer Daten und Informationen). Dieses Schutzziel wird unter anderem durch das Erstellen von regelmäßigen Datensicherungen (Backups), redundanter Datenhaltung und Langzeit-Archivierung erreicht.

### Cyber-Sicherheit

Die Cyber-Sicherheit wird häufig entweder der Informationssicherheit gleichgesetzt oder dieser übergeordnet. Sie beinhaltet dann nicht nur die Sicherheit von Daten und der IT-Infrastruktur einer einzelnen Organisation, sondern bezeichnet den Sicherheitsbegriff umfassender bis hin zur nationalen oder globalen Sicherheit. Damit ist Cyber-Sicherheit als Prozess zur Implementierung von Kontrollen zu verstehen, mit dem die Eintrittswahrscheinlichkeit von Datenschutzverletzungen aus einem Cyber-Angriff reduziert werden kann.

**Zusammenfassung für den Bereich der medizinischen Versorgung:**

IT-Sicherheit bezieht sich auf ein soziotechnisches System, in dem Informationen mit Hilfe von Informationstechnik (IT) erfasst, gespeichert und verarbeitet werden. IT-Sicherheit erhält durch die Einführung der elektronischen Patientenakte (ePA) eine deutlich größere Bedeutung. Dagegen ist Informationssicherheit umfassender definiert und umfasst auch auf Papier dokumentierte Daten und Informationen.

## Übergeordnete Definitionen

***Art. 32 DSGVO***

***Sicherheit der Verarbeitung***

*„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:*

*a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;*

*b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;*

*c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;*

*d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.“*

### Stand der Technik

Der Terminus „Stand der Technik“ unterliegt einer ständigen Entwicklung. In der Rechtsprechung existieren verschiedene Definitionen wie z.B. in

***§ 3 Abs. 10 GefStoffV***

*„Der ‚Stand der Technik’ ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Gesundheit und zur Sicherheit der Beschäftigten gesichert erscheinen lässt. Bei der Bestimmung des Standes der Technik sind insbesondere vergleichbare Verfahren, Einrichtungen oder Betriebsweisen heranzuziehen, die mit Erfolg in der Praxis erprobt worden sind.“*

### Implementierungskosten

Als Implementierungskosten werden die Gesamtaufwendungen für die Einführung eines meist digitalen Systems bezeichnet. In der Betriebswirtschaftslehre werden darunter auch die TCO Aufwendung (Total Cost of Ownership) verstanden:

**TCO = (Konzeptionskosten + Investitionskosten): Nutzungszeitraum + Betriebskosten**

Bei Nutzung innovativer SaaS Systemen entfallen die Investitionskosten:

**TCO = (Konzeptionskosten: Nutzungszeitraum) + Betriebskosten inkl. SaaS**

### Art des Umfangs, der Umstände und Zwecke der Verarbeitung

Art, Umfang und Zweck der Verarbeitung ergibt sich aus der Anwendung in der medizinischen und sozialen Versorgung:

- **Art der Verarbeitung**
  Die Art bezieht sich auf die Verwaltung von persönlichen und gesundheitsbezogenen Patientendaten
- **Umfang der Verarbeitung**
  Die Größe der Versorgungseinrichtung und die fachärztliche Ausrichtung bestimmen den Umfang der Datenverarbeitung in medizinischen und sozialen Organisationen.
  Der Umfang der Verarbeitung hängt auch von der Organisation der medizinischen Dokumentation (digital v/s analog) ab.
- **Zweck der Verarbeitung**
  Der Zweck der Verarbeitung ergibt sich aus den jeweiligen Versorgungsverträgen zwischen Ärzten, Einrichtungen und den Patienten/Personen

### Eintrittswahrscheinlichkeit und Schwere des Risikos

Bei der Risikobetrachtung in der Informationssicherheit ist die Sichtweise der Patienten und Patientinnen einerseits und die der Verantwortlichen andererseits zu betrachten:

- **Risiken für Patienten/-innen**
  - Risiken der Patientensicherheit
  - Risiken der Versorgungsqualität
  - Risiken der Verletzung der Privatsphäre
- **Risiken für die Verantwortlichen (Ärzte/-innen und Krankenhausmanager/-innen)**
  - Vertragsärztliche Risiken
  - Datenschutzrechtliche Risiken
  - Berufsrechtliche Risiken
  - Versicherungsrelevante Risiken

## Spezifische Risikobereiche für Ärzte/-innen

Die exponentiell gestiegenen digitalen Anwendungen in der Medizin haben die Risikosituation hinsichtlich Cyberangriffen und IT-Störfällen extrem erhöht. Folgende Bereiche konnten in einer Studie der **MCSS AG** identifiziert werden:

- Einsatz der Telematikinfrastruktur (verpflichtend) für alle Kassenärzte/-innen in Deutschland
- Medizintechnik mit digitaler Speicherung und digitalen Schnittstellen
- Anwendungen des elektronischen Rezepts (eRezept)
- Einsatz von Video-Sprechstunden mit Spezialsoftware für Telekonsultation
- Verordnung von Gesundheits-Apps in der Arztpraxis
- eArztbrief als Ablösung der analogen Kommunikation zwischen Ärzten/-innen
- Anwendung von digitalen Studien und Qualitätssicherungsprojekten (Pharma-Studien etc.)
- Medizinische Großgeräte
- Elektronische Notfalldaten für Patienten/-innen
- E-Behandlungsplan mit kompletten Therapieinformationen
- Elektronisches Terminmanagement über Web-Kalender

### POTENTIAL DER MINIMIERUNG VON CYBERRISIKEN IN DER MEDIZINISCHEN VERSORGUNG

(bestätigte Rechtskonformität mit IT-Sicherheitsrichtlinie nach § 75b / 75c SGB V)

| Cyber- und IT-Sicherheitsrisiken in Arztpraxen | Gesamtrisiko von 100% | Rechtliche Referenzen |
|---|---|---|
| **Anwendungen in der Arztpraxis** | | |
| Telematikinfrastruktur (TI) (z.B. e-AU etc.) | **10,5%** | § 75b Anl. 5 Ziffer 1–7 |
| Medizintechnik Datenschnittstellen (HL7, DICOM, GDT) | **10,5%** | § 75b Anl. 4 Ziffer 1–6 |
| Qualitätssicherungsprogramme, DMP etc. | **7,5%** | QM RL § 135ff SGB V / DVG |
| Webbasierte Terminkalender | **8,5%** | § 75b Anl. 1 Ziffer 7–11 |
| Video-Sprechstunden | **6,5%** | § 75b Anl. 1 Ziffer 7–11 |
| e-Rezept (ab 07/2022) | **8,5%** | § 75b Anl. 5 Ziffer 1–2 |
| e-Arztbrief | **6,0%** | § 75b Anl. 5 Ziffer 1–2 |
| ePA (elektronische Patientenakte) (ab 2022) | **9,5%** | § 75b Anl. 1 Ziffer 7–11 |
| Forschungsprojekte | **4,5%** | QM RL § 135ff SGB V / DVG |
| Gesundheits-Apps | **6,5%** | § 75b Anl. 1 Ziffer 7–11 |
| E-Mail-Phishing | **2,5%** | BSI Grundschutz |
| Cyber-Attacken global | **2,5%** | BSI Grundschutz |
| Sabotage intern | **1,5%** | BSI Grundschutz |
| IT-Crashes | **3,5%** | BSI Grundschutz |
| Andere Risiken | **12,0%** | BSI allgemein |
| **GESAMT** | **100%** | |

Etwas 78% der IT-Sicherheitsrisiken in Arztpraxen sind nach der Einführung der Telematik-Infrastruktur branchenspezifisch (Hochrechnung der Risikoanalyse)

## Fälle aus der IT-Sicherheitspraxis

Im Rahmen einer Studie wurden IT-Sicherheitsvorfälle gesammelt und in klassischen Risikobewertungen katalogisiert.

### Dazu hier einige Beispiele:

- In einer Praxis wurde der TI-Konnektor (TI) falsch installiert. Über offene Ports erhielten Cyberkriminelle Zugang zu der elektronischen Kartei einer Praxis (Facharzt für Orthopädie).
- In einer Augenarztpraxis wurde ein digitales Diagnosesystem (OCT) unzureichend geschützt mit dem PVS (Praxisverwaltungssystem) verbunden. Die Daten waren über Wartungsverbindung mit dem OCT Hersteller offen zugänglich.
- In einer Praxis wurde das elektronische Rezept getestet, ohne dass die Mitarbeitenden ausreichend geschult waren. Es wurden Therapiedaten zu einem falschen Patienten bzw. einer falschen Patientin übertragen (Konfliktsituation durch Kontraindikation).
- In einer Praxis wurde zu Beginn der Pandemie eine Video-Sprechstunde angeboten. Das Telekonsultationssystem war mit der PVS (Praxisverwaltungssystem) ungeschützt verbunden und Daten konnten von außen durch Unbefugte eingesehen werden.
- Eine Schmerztherapiepraxis bot den Patienten/-innen die Einweisung in eine Schmerztagebuch-App an. Dabei wurden ungeschützte Verbindungen zwischen dem PVS und dem Internet angewendet. Sensible Daten konnten von außen abgerufen werden.
- Etwa ein Viertel aller Arztpraxen nehmen an fachlichen Studien und Qualitätssicherungsprojekten (z.B. DMP – Disease Management Programm) teil Die Übertragung der Patientendaten erfolgte unvorschriftsmäßig, weil Mitarbeitenden keine Aufklärung und Schulung erhalten hatten. Über den Zugang wurden durch Cyberkriminelle sensible Patientendaten abgerufen.
- Eine radiologische Praxis setzt medizinische Großgeräte ein und hat das System über das Internet mit einem digitalen Archiv verbunden. Beim Austausch eines Kommunikationsadapters kommt es zu einer falschen Installation und der Zugang auf radiologische Untersuchungsergebnisse ist für Cyberkriminelle sofort zu entschlüsseln. Die Mitarbeitenden haben die einfachsten Sicherheitstests zusammen mit dem Servicetechniker unterlassen.
- Eine Praxis setzt für das Terminmanagement einen Kalender im Internet ein. Die Anbindung ist direkt mit dem Praxisverwaltungssystem (PVS) verbunden. Über die nicht geschützte Verbindung haben Unbefugte Zugriff auf Patientendaten (Termindaten mit Diagnosen im Klartext).
- Eine dermatologische Praxis verwendet ein Antwortformular zur Kommunikation mit Patienten bzw. Patientinnen über das Web. Die Mitarbeitenden sind nicht über den Regelbetrieb aufgeklärt und so kommt es zu Cyber-Attacken mit direktem Zugriff auf das Patientenverwaltungssystem (PVS) und dem unberechtigten Zugriff von Kriminellen auf sensible Patientendaten.
- Eine ophthalmologische Praxis setzt eine digitale Untersuchungssuite ein und überträgt die Daten per USB-Stick in das Lasersystem und die elektronische Patientenkartei (PVS). Über unsachgemäße Verwendung des Übertragungsmediums wird ein zerstörerisches Schadprogramm über die Untersuchungssuite in das gesamte IT-Netzwerk importiert.
- Eine gynäkologische Praxis hat einen Hardware-Crash (Festplatte). Die Datensicherung enthält nur die GKV-Abrechnungsdaten, da das Back-up-System nicht wie vorgeschrieben durch Rekonstruktion geprüft war. Alle medizinischen Patientendaten gehen verloren.

### Technische und Organisatorische Maßnahmen (TOM)

TOM sind durch die DSGVO (Datenschutz-Grundverordnung) vorgeschriebene Maßnahmen, die die Sicherheit der Verarbeitung personenbezogener Daten gewährleisten sollen. TOM umfassen eine strukturierte Liste an Instrumenten, mit denen die medizinischen und pflegenden Versorgungseinrichtungen den Datenschutz und die Datensicherheit (Informationssicherheit) gewährleisten müssen. Eine professionelle Dokumentation ist dabei für den Verantwortlichen verpflichtend (ISMS, DSMS, QMS). Die wesentlichen Anforderungen dieser Verpflichtung ergeben sich aus Art. 25 DSGVO.

## 2.2 Datenschutz und ärztliche Schweigepflicht

Datenschutz in der medizinischen Versorgung und der Pflege ist eng verbunden mit der beruflichen Schweigepflicht.

Der Datenschutz ist auf EU-Ebene durch die DSGVO und auf nationaler Ebene durch das BDSG geregelt. Für die medizinische und pflegende Versorgung gelten besondere gesetzliche Anforderungen. Im Art. 9 der DSGVO wird die „Verarbeitung besonderer Kategorien personenbezogener Daten“, zu denen alle Gesundheitsdaten gehören, geregelt.

## 2.3 Qualitätsmanagement in der medizinischen Versorgung

Nach §§ 135 ff. SGB V ist die Anwendung eins internen Qualitätsmanagements in der vertragsärztlichen Versorgung verpflichtend. Seit 2005 sind Qualitätsmanagementsysteme in inzwischen mehr als 80% der Arztpraxen eingeführt. Dazu werden unterschiedliche Qualitätsmanagementsysteme (QMS) eingesetzt. Die Systeme mit der größten Verbreitung sind QEP (Qualität und Entwicklung in Praxen) und ISO 9001. Nach beiden Normen sind Regelungen für Informationssicherheit und Datenschutz mit entsprechenden Kapiteln integriert. In diesem Kontext hat die Kassenärztliche Bundesvereinigung (KBV) in den Verhandlungen zur Einführung der IT-Sicherheitsrichtlinie nach § 75b SGB V, festgestellt, dass über die QM-Umsetzung bereits bis zu 60% der Anforderungen nach § 135ff. SGB V umgesetzt sind.

Im 2. Halbjahr 2021 soll eine neue Generation des QEP Systems eingeführt werden, welches zentrale Elemente der IT-Sicherheit und des Datenschutzes nach der DSGVO enthalten soll. Arztpraxen, die ein strukturiertes QMS einsetzen, können somit die Anforderungen nach § 75b SGB V und nach der DSGVO über eine Erweiterung des QMS wirtschaftlich umsetzen.

Arztpraxen, die kein QMS einsetzen, obwohl dies nach dem Beschluss des Gemeinsamen Bundesausschusses (GBA) verpflichtend ist, gehen forensische Risiken ein. Kommen Patienten/-innen in der medizinischen Versorgung zu Schaden und die medizinische Versorgungseinrichtung kann kein QMS nachweisen, kann es zur Beweislastumkehr gegen den/die Vertragsarzt/-ärztin kommen. Insofern ist die Etablierung eines QMS bei der Risikobewertung von Berufshaftpflicht und Betriebsunterbrechungsversicherungen zu berücksichtigen.

Die konkreten Anforderungen an ein QMS in der medizinischen Versorgung werden in § 4 des GBA der QM-Richtlinie definiert:

### Messen und Bewerten von Qualitätszielen

- Informationssicherheit: Festlegung der Ziele der IT-Sicherheit und des Cyberschutzes (z.B. nach § 75b SGB V)
- Datenschutz: Festlegung der Datenschutz-Ziele nach der DSGVO und des BDSG

### Erhebung des Ist-Zustandes und Selbstbewertung

- Informationssicherheit: IT-Infrastruktur Inventarisierung
- Datenschutz: Umsetzungsstatus DSGVO/BDSG

### Regelung von Verantwortlichkeiten und Zuständigkeiten

- Informationssicherheit: Informationssicherheitsbeauftragter (ISB)
- Datenschutz: Datenschutzbeauftragter (DSB)

### Prozess- bzw. Ablaufbeschreibungen

- Informationssicherheit: Verfahrensanweisungen (ISO), Interne Regeln (QEP)
- Datenschutz: Verfahrensanweisungen (ISO), Interne Regeln (QEP)

### Schnittstellenmanagement

- Informationssicherheit: Definition Datenaustausch
- Datenschutz: Definition Informationsaustausch

### Checklisten

- Informationssicherheit: Übersicht IT-Sicherheits-Maßnahmen (TOM)
- Datenschutz: Übersicht Datenschutz-Maßnahmen (TOM)

### Fortbildungs- und Schulungsmaßnahmen

- Informationssicherheit: IT-Sicherheits-Coaching/Schulungsplan (Curriculum)
- Datenschutz: DS-Coaching/Schulungsplan (Curriculum)

### Risikomanagement

- Informationssicherheit: IT-Sicherheits-Risikoanalyse und TOM
- Datenschutz: Datenschutz-Risikoanalyse und TOM

### Fehlermanagement und Fehlermeldesysteme

- Informationssicherheit: PDCA Strategien
- Datenschutz: PDCA Strategien

**Notfallmanagement**

- Informationssicherheit: Definition von Maßnahmen im IS-Notfall
- Datenschutz: Definition von Maßnahmen im DS-Notfall

**Dokumentation**

- Informationssicherheit: IT-Sicherheits-Vorlagen für Mitarbeitende
- Datenschutz: Datenschutz-Vorlagen für Mitarbeitende

Ärzte/-innen, die das Qualitätsmanagement rechtskonform nach § 4 der QM-Richtlinie nach §§ 135ff SGB V anwenden, erfüllen bereits die Anforderungen für Informationssicherheit und Datenschutz in hohem Maße. Zum Qualitätsmanagement gehört als primäre Verpflichtung die Einhaltung aller relevanter gesetzlicher Regelungen.

# 3 Die IT-Sicherheitsrichtlinie nach § 75b SGB V

Am 1. April 2021 trat die erste Stufe (Anlage 1 der Richtlinie) für medizinische Versorgungseinrichtungen in Kraft. In der Richtlinie werden zusätzlich zu den Regelungen des Datenschutzes nach DSGVO und BDSG und ergänzend zur QM-Richtlinie des GBA umfassende technische und insbesondere organisatorische Maßnahmen festgeschrieben.

Die vorliegende Richtlinie kam nach ausführlichen Verhandlungen zwischen dem BSI und den ärztlichen Bundesvereinigungen zustande. Es ist nach Aussagen der Verantwortlichen ein angemessener Kompromiss zwischen erwünschten Maßnahmen und pragmatischen Möglichkeiten, insbesondere unter Berücksichtigung zusätzlicher Belastungen der medizinischen Versorgung.

## 3.1 Die Struktur der IT-Sicherheitsrichtlinie nach § 75b SGB V

Die Struktur der Richtlinie wurde spezifisch für die medizinische Versorgung entwickelt und steht nicht in einem direkten Kontext mit bisherigen Veröffentlichungen des BSI (z.B. zum Grundschutz) und bezieht ebenfalls die bereits bestehende Richtlinie zum Qualitätsmanagement nach §§ 135 ff. SGB V nicht mit ein. Bereits veröffentlichte Empfehlungen der Bundesärztekammer (BÄK) inklusive der technischen Anlage wurden berücksichtigt.

## 3.2 Präambel (der Richtlinie nach § 75b SGB V)

In der Präambel wird ausdrücklich auf die Regelung des Artikel 32 DSGVO Bezug genommen. Die Richtlinie soll insbesondere zur Vereinheitlichung speziell im Gesundheitswesen beitragen.

In den Verhandlungen der Ärztevertretungen mit dem Bundesamt wurde deutlich, dass z.B. Arztpraxen nicht mit den Strukturen kleiner und mittlerer Unternehmen (KMU) vergleichbar sind. Deshalb wurde auch in die Präambel aufgenommen, dass bei der Umsetzung der Richtlinie Risiken an Dritte, wie an IT-Dienstleister oder Versicherungen übertragen werden können.

## 3.3 Geltungsbereich (der Richtlinie nach § 75b SGB V)

Es wurde eine IT-Sicherheitsrichtlinie durch die KBV für den Geltungsbereich der vertragsärztlichen und vertragspsychotherapeutischen Versorgung veröffentlicht. Eine weitere identische Richtlinie erstellte die KZBV für die kassenzahnärztliche Versorgung. Soweit in dieser gutachterlichen Stellungnahme die IT-Sicherheitsrichtlinie benannt wird, bezieht sie sich auf alle drei Geltungsbereiche.

Ausdrücklich wird im Geltungsbereich der Richtlinie festgelegt, dass der bzw. die Praxisinhaber für die Einhaltung der Anforderungen der Richtlinie verantwortlich sind. Bei Berufsausübungsgemeinschaften werden demzufolge alle Gesellschafter gleichermaßen in die Verantwortung einbezogen.

## 3.4 Praxisgrößen und Anforderungskategorien (nach Richtlinie § 75b SGB V)

Wegen der unterschiedlichen Strukturen und Prozesse von Praxen unterschiedlicher Größe unterscheidet die Richtlinie nach drei Größen:

- Einzelpraxis mit bis zu 5 ständig mit der Datenverarbeitung betrauten Personen
- Gemeinschaftspraxis (mittlere Praxis) mit 6 – 20 Mitarbeitenden
- Großpraxis oder Praxis mit Datenverarbeitung in erheblichem Umfang mit über 20 ständig mit der Datenverarbeitung betrauten Personen. In diese Kategorie fallen auch ein Groß-MVZ mit krankenhausähnlichen Strukturen oder medizinische Labore.

## 3.5 Anforderungen zur Gewährleistung der IT-Sicherheit in Praxen (nach Richtlinie § 75b SGB V)

Erfahrungsgemäß sind die IT-Strukturen und -Prozesse abhängig von der Größe einer Praxis und dem Umfang der Datenverarbeitung. Anlage 1 stellt die Anforderungen an eine Einzelpraxis und gleichzeitig den Standard für alle Praxen dar. Hinzu kommt der Anforderungskatalog im Zusammenhang mit dem Einsatz der Telematikinfrastruktur nach Anlage 5.

Ein weiterer Anforderungskatalog ergibt sich aus Anlage 4 für medizinische Großgeräte wie Computertomographen, Magnetresonanztomographen, Positronenemissionstomographen und Linearbeschleuniger. In Analogie kann angenommen werden, dass vergleichbare Anforderungen für die Nutzung von Medizintechnik mit Datenspeicherung gelten.

In Ziffer 5 der Anforderungen wird ein kontinuierlicher Verbesserungsprozess, wie er aus den Anforderungen des Qualitätsmanagements in medizinischen Versorgungseinrichtungen bekannt ist, eingeführt. Ebenfalls vorgesehen ist eine jährliche Evaluationspflicht, aus der ein Jahresbericht wie er im Qualitätsmanagement und im Datenschutz nach der DSGVO definiert ist, abgeleitet werden kann.

## 3.6 Inkrafttreten und Geltung (der Richtlinie nach § 75b SGB V)

Die Basisanforderungen gemäß Anlage 1, Anforderungen für Praxen, gelten ab 01.04.2021. In den Anlagen 1 – 5 sind die jeweiligen Module mit Daten zum Inkrafttreten belegt. Die zentralen Anforderungen aus den Anlagen 2 – 5 treten zum 01.01.2022 in Kraft.

## 3.7 Anlagen zur IT-Sicherheitsrichtlinie nach § 75b SGB V

Die Anlagen zur Richtlinie sind nach Praxisgröße (Anlage 1–3) und nach technischen Anwendungsbereichen (Anlage 4 und 5) gegliedert.
Die Anlagen 1–3 sind nach folgenden Zielobjekten differenziert:

- Mobile Anwendungen
- Office-Produkte
- Internet-Anwendungen
- Endgeräte und IT-Systeme
- Endgeräte mit dem Betriebssystem Windows
- Smartphones und Tablets
- Mobiltelefone
- Wechseldatenträger und Speichermedien
- Netzwerksicherheit

Anlage 4 bezieht sich auf die Nutzung medizinischer Großgeräte und Anlage 5 auf dezentrale Komponenten der TI.

## 3.8 Zielgruppen der Richtlinie

### 3.8.1 Arztpraxen

Die Regelungen nach § 75b SGB V gelten für alle Praxen, die an der vertragsärztlichen Versorgung teilnehmen. Sie gelten auch für Ärzte/-innen, die an der hausarztzentrierten Versorgung teilnehmen.

### 3.8.2 Zahnarztpraxen

Die Kassenzahnärztliche Vereinigung hat eine eigene IT-Sicherheitsrichtlinie veröffentlicht, die aber identische Inhalte zur Version der KBV (siehe 3.1.) dokumentiert.

### 3.8.3 Medizinische Versorgungszentren (MVZ)

MVZ sind eigenständige Leistungserbringer, in denen mehrere ambulant tätige Ärztinnen beziehungsweise Ärzte kooperativ unter einem Dach zusammenarbeiten.

Im Gegensatz zu den klassischen Teilnahmeformen (Einzelpraxis, Berufsausübungsgemeinschaft), bei denen die Praxisinhaber die ärztliche Tätigkeit in der Regel persönlich auszuüben haben, zeichnen sich MVZ insbesondere durch eine organisatorische Trennung der Inhaberschaft von der ärztlichen Behandlungstätigkeit aus.

### 3.8.4 Stationäre Pflegeeinrichtungen mit vertragsärztlicher Versorgung

Nach § 119b SGB V „Ambulante Behandlung in stationären Pflegeeinrichtungen“ behandeln Vertragsärzte/-innen auch Patienten/-innen in Pflegeheimen. Für diese Einrichtungen gelten ebenfalls alle Regelungen zur IT-Sicherheit nach § 75b SGB V.

# 4 Rechtsfolgen bei Nichteinhaltung der Rechtsnormen

## 4.1 Vertragsärztliche Rechtsfolgen

Werden die Pflichten nach § 75b SGB V missachtet, bestehen unterschiedliche mögliche Rechtsfolgen für den/die Vertragsarzt/-ärztin.

### 4.1.1 Verwarnungen und Verweise

In geringfügigen Fällen kann die zuständige Kassenärztliche Vereinigung Verwarnungen oder Verweise nach Einleitung eines Disziplinarverfahrens aussprechen. Diesen gehen im Regelfall Beratungen zur rechtskonformen Umsetzung der Informationssicherheit voraus.

### 4.1.2 Geldbußen

In schwereren Fällen können nach § 81 Abs. 5 SGB V i.V.m. den korrespondierenden Disziplinarordnungen Geldbußen, die sich nach der Schwere des Verstoßes richten, verhängt werden. Die Höchstgrenze der Geldbußen liegt einmalig bei 50.000 Euro. Die Geldbuße kann durch Honorarkürzung und damit über Verrechnung eingezogen werden.

### 4.1.3 Ruhen der Zulassung

Der Disziplinarausschuss kann darüber hinaus auch das Ruhen der Zulassung bzw. der vertragsärztlichen Beteiligung für bis zu zwei Jahre anordnen.

### 4.1.4 Zulassungsentziehung

In schwerwiegenden Fällen kann der zuständige Zulassungsausschuss auf Antrag nach § 95 Abs. 6 SGB V die vertragsärztliche Zulassung ganz oder zum Teil entziehen. Dies ist auch bei der Verletzung wichtiger Organisationspflichten, wie der zur IT-Sicherheit und dem Datenschutz möglich.

### 4.1.5 Zusammenfassung zu vertragsärztlichen Rechtsfolgen

Nach üblichen Klassifizierungen im Risikomanagement ist die Eintrittswahrscheinlichkeit ernster vertragsärztlicher Sanktionen eher gering. In besonders schweren Fällen können die Auswirkungen allerdings existenzbedrohend sein (z.B. Entziehung der Kassenzulassung). Die Vermeidung negativer vertragsärztlicher Sanktionen ist dagegen durch einfache Organisationsmaßnahmen und Delegieren an externe Dienstleister zu realisieren.

## 4.2 Datenschutzrechtliche Folgen

Die negativen Rechtsfolgen aus Datenschutzverstößen aufgrund von Missachtung der Regelungen nach § 75b SGB V sind wahrscheinlicher als die Rechtsfolgen nach Vertragsarztrecht. Die Abschreckung steht häufig im Vordergrund der Begründung.

In der Präambel der Richtlinie nach § 75b SGB V wird ausdrücklich darauf hingewiesen, dass die Regelungen auch der Konkretisierung der Pflichten nach Art. 32 DSGVO dienen (siehe 2.1. Definitionen und Geltungsbereiche).

### 4.2.1 Bußgeldverfahren nach Art. 83 DSGVO

Bei Verstößen gegen Art. 32 DSGVO im Kontext der Richtlinie nach § 75b SGB V können erhebliche Bußgelder verhängt werden. Nach Art. 83 der DSGVO können Bußgelder bis zu 2% des Jahresumsatzes der medizinischen oder pflegenden Einrichtung verhängt werden. Das sind für eine Einzelpraxis maximal 10.000 Euro und für eine große Gemeinschaftspraxis mit 5 Mio. Euro Jahresumsatz bis zu 100.000 Euro. Die maximale Höhe beträgt 10 Millionen Euro, was aber in der ambulanten und stationären medizinischen Versorgung nicht relevant ist.

Gegen Krankenhäuser wurden bereits Bußgelder über 100.000 Euro wegen organisatorischer Versäumnisse verhängt.

### 4.2.2 Schadensersatzzahlungen nach Art. 82 DSGVO

Eine unzureichende IT-Sicherheit nach § 75b SGB V in Praxen und nach § 75c SGB V in Krankenhäusern kann zu erheblichen Schadensersatzzahlungen an Patienten/-innen führen. Nach Art. 82 der DSGVO können durch Datenschutzverstöße geschädigte Patienten/-innen Schadensersatzansprüche geltend machen. Dies gilt sowohl für materielle wie auch für immaterielle Schadensereignisse.

Fachleute sehen in den potenziellen Schadensersatzforderungen erhebliche Gefahren. Dabei wird darauf hingewiesen, dass die zivilrechtlichen Ansprüche im Kontext der EU-Datenschutz-Grundverordnung abschreckende Wirkungen erzielen sollen. Da bislang keine gefestigte Rechtsprechung vorliegt, ist die Bandbreite der Zahlungen schwer einzuschätzen bzw. zu limitieren.

Ein weiteres Risiko ergibt sich aus der möglichen Beweislastumkehr, die Juristen im Kontext der Rechenschaftspflicht nach Art. 5 DSGVO als wahrscheinlich ansehen.

**Fazit:**

Die Eintrittswahrscheinlichkeit ist nicht zu unterschätzen und auch die Schadenshöhe aus Sicht des Arztes/ der Ärztin ist schwer kalkulierbar. Mit den konkreten Anforderungen nach § 75b SGB V ist eine Missachtung der Anforderungen an die IT-Sicherheit grob fahrlässig und damit mit sehr konkreten Risiken verbunden.

### 4.2.3 Meldepflichten nach Art. 33 DSGVO

Ein weiteres finanzielles Risiko ergibt sich aus Art. 33 DSGVO. Danach müssen die Verantwortlichen eine konkrete Datenschutzverletzung innerhalb von 72 Stunden nach Kenntnisnahme der zuständigen Datenschutz-Aufsichtsbehörde melden.

Bei der Meldepflicht einer Datenschutzverletzung kommt es nicht darauf an, ob der Arzt/die Ärztin für einen Vorfall selbst verantwortlich ist. Ist ein Auftragsverarbeiter (z.B. der Dienstleister für die externe Datensicherung) involviert, so muss dieser unverzüglich die Meldung des Vorfalls an den Arzt veranlassen. Somit kommt es auf die Schuldfrage bei der Meldepflicht nicht an.

Für die Meldeprozesse sind genaue Vorschriften veröffentlicht. Die Anforderungen ergeben sich aus Art. 34 DSGVO. Hinzu kommt die Regelung zur Benachrichtigung der betroffenen Patienten/-innen. Unterschieden wird nach einer Einzelbenachrichtigung und nach einer öffentlichen Benachrichtigung (z.B. in der Tagespresse). Aus letzterer kann sich ein erheblicher Reputationsschaden ergeben, der nur sehr schwer kalkuliert werden kann.

Im Fall einer orthopädischen Gemeinschaftspraxis in Celle wurde die Veröffentlichung aus der lokalen Presse durch überregionale Medien aufgegriffen, wodurch es zu einem eheblichen Reputationsschaden kam.

### Zusammenfassung:

Meldepflichtverletzungen bei einer Datenschutzverletzung sind nicht selten. Bei Verlusten großer Mengen von Patientendaten, beispielweise werden Datensicherungsmedien mit medizinischen Daten öffentlich zugänglich, können Schäden im 6-stelligen Euro-Bereich entstehen.

## 4.3 Versicherungsrelevante Rechtsfolgen

Im Bereich der IT-Sicherheit sind 3 Versicherungsbereiche relevant:

- Cyber-Versicherung
- Haftpflicht- und Berufshaftpflichtversicherung
- Betriebsunterbrechungs-Versicherung (BU)

Die steigende Gefährdung der Informationssicherheit im Gesundheitswesen leitet einen Paradigmenwechsel auch für Versicherungen in der medizinischen Versorgung ein. Im Mittelpunkt steht die Digitalisierung mit den neuen Errungenschaften der medizinischen Versorgung aber auch mit zusätzlichen Risiken für IT-Sicherheit und Datenschutz.

Verstößt der/die Versicherungsnehmer/-in gegen Verpflichtungen aus dem Versicherungsvertrag, so kann der/die Versicherer/-in Schadenszahlungen reduzieren oder ganz verweigern. Im Einzelfall kommt es auf den konkreten Vertrag an.

Unterschieden wird dabei nach vertraglichen und gesetzlichen Obliegenheiten:
Obliegenheiten sind Normen, die dem/der Versicherungsnehmer/-in auferlegen, sich in einer bestimmten Weise zu verhalten. Das einem/einer Versicherungsnehmer/-in obliegende Verhalten kann ein Tun oder auch ein Unterlassen sein. Der/die Versicherer/-in kann zwar von dem/der

Versicherungsnehmer/-in nicht verlangen, sich entsprechend einer Obliegenheit zu verhalten. Beachtet der/die Versicherungsnehmer/-in eine Obliegenheit jedoch nicht, kann der/die Versicherer/-in nach § 28 Absatz 2 VVG seine/ihre Leistung ganz oder teilweise kürzen.

Verstöße gegen Obliegenheiten können den/die Versicherer/-in im Schadenfall zu Leistungskürzungen berechtigen. In der Sachversicherung spielt die Einhaltung von Sicherheitsvorschriften eine große Rolle. Die Regulierungspraxis zeigt, dass Versicherer/-innen den Einwand der Verletzung von Sicherheitsvorschriften (z.B. § 75b SGB V) erheben können, um die Einigungsbereitschaft von Versicherten in Verhandlungen zu erhöhen. Um Auseinandersetzungen zu vermeiden, sollten Ärzte/-innen deshalb die Einhaltung des Art. 32 DSGVO und der Richtlinie nach § 75b SGB V jederzeit dokumentieren können.

### Mögliche Folgen für Versicherte:

#### Kündigung

Verletzt der/die Versicherungsnehmer/-in vorsätzlich oder grob fahrlässig eine Obliegenheit, die er vor Eintritt des Versicherungsfalls gegenüber dem/der Versicherer/-in zu erfüllen hat, so kann der/die Versicherer/-in innerhalb eines Monats, nachdem er/sie von der Verletzung Kenntnis erlangt hat, den Vertrag fristlos kündigen.

Der/die Versicherer/-in hat kein Kündigungsrecht, wenn der/die Versicherungsnehmer/-in nachweist, dass er/sie die Obliegenheit weder vorsätzlich noch grob fahrlässig verletzt hat.

#### Leistungsfreiheit bei Obliegenheitsverletzungen

Verletzt der/die Versicherungsnehmer/-in eine Obliegenheit vorsätzlich, so ist der/die Versicherer/-in von der Verpflichtung zur Leistung frei. Bei grob fahrlässiger Verletzung der Obliegenheit ist der/die Versicherer/-in berechtigt, seine/ihre Leistung in dem Verhältnis zu kürzen, das der Schwere des Verschuldens des/der Versicherungsnehmers/-in entspricht.

Verletzt der/die Versicherungsnehmer/-in eine nach Eintritt des Versicherungsfalls bestehende Auskunfts- oder Aufklärungsobliegenheit, ist der/die Versicherer/-in nur dann vollständig oder teilweise leistungsfrei, wenn er/sie den/die Versicherungsnehmer/-in durch gesonderte Mitteilung in Textform (z.B. E-Mail, Telefax oder Brief) auf diese Rechtsfolge hingewiesen hat.

## 4.4 Weitere mögliche Rechtsfolgen

### 4.4.1 Förderrechtliche Folgen

Förderrechtliche Folgen aus Verpflichtungen zur IT-Sicherheit können sich aus dem Krankenhauszukunftsgesetz (KHZG) ergeben. Im Rahmen dieses Gesetzes werden Investitionen in die Digitalisierung der Krankenhäuser mit mehr als 4 Milliarden Euro gefördert. Nach § 14a Abs. 3 Satz 5 KHZG sind 15% der beantragten Fördermittel für Maßnahmen zur IT-Sicherheit zu verwenden. Damit stehen über 600 Millionen Euro Fördermittel, für die genaue Förderrichtlinien, zur Verfügung.

Bei Nichteinhaltung der geforderten Mittelrelationen sind Rückzahlungen und Sanktionen bei nicht korrekter Verwendung vorgesehen

### 4.4.2 Folgen nach § 8b BSIG

Nach § 8b Abs. 3 BSIG müssen Krankenhäuser, die den KRITIS-Sicherheitsstandard erfüllen müssen, eine jederzeit erreichbare Kontaktstelle einrichten. Damit verbunden ist eine Verpflichtung zur Meldung von möglichen Risiken und Störfällen.

Konkret ergibt sich hieraus die Einführung eines BCMS (Business-Continuity-Management-System).

# 5 Erfüllung der Rechtsnormen

In der medizinischen Versorgung sind u.a. folgende Rechtsnormen in drei Bereichen zu erfüllen:

- Rechtsnormen in der Informationssicherheit, der IT-Sicherheit und des Cyberschutzes (z.B. § 75b und § 75c SGB V)
- Rechtsnormen des Datenschutzes nach DSGVO und BDSG sowie Berufsrecht (Berufliche Schweigepflicht)
- Rechtsnormen des Qualitätsmanagements nach §§ 135 ff. SGB V (bzw. § 72 SGB V für die Hausärztliche Versorgung) siehe auch **2.3**

## 5.1 Definitionen

Zur Erfüllung der Rechtsnormen werden den Verantwortlichen (Ärzte/-innen und Management von Krankenhäusern) unterschiedliche Unterstützungen angeboten. In der Präambel der IT-Sicherheitsrichtlinie (§ 75 b SGB V) wird erstmals ausdrücklich die Möglichkeit der Übertragung von Risiken auf Dienstleister und Versicherungen dokumentiert. Unabhängig von den professionellen Angeboten, bieten ärztliche Fachverbände, Fachgesellschaften und Kassenärztliche Vereinigungen sowie die Bundesärztekammer und die Landesärztekammern Informationen und Schulungen für Ärzte/-innen und ihre Mitarbeitenden an.

Einen zunehmend wichtigen Anteil nehmen Assistance Services der Versicherer ein. Mit ihnen sollen Präventionsmaßnahmen und damit Risikoreduzierungen erreicht werden.

In Versicherungsverträgen werden außerdem die Mitwirkungspflichten der Versicherten mit sogenannten Obliegenheiten definiert. Dies gilt insbesondere für das Segment der Cyber-Versicherungen.

Da Cyber-Versicherungen erst seit etwa 4 Jahren gezielt am Markt angeboten werden, sind die Vertragsbedingungen noch nicht sehr strukturiert ausgebildet. Das gilt insbesondere auch für den Bereich der medizinischen Versorgung. Der Verband der Versicherer (GDV) hat zur Unterstützung einer Standardisierung der Obliegenheiten einen Fragenkatalog mit über 50 Maßnahmen entwickelt. Daraus wählen die führenden Cyber-Versicherer je nach strategischer Ausrichtung zwischen 6 und 20 Fragen und Anforderungskomplexe aus. Diese Anforderungen an technische und organisatorische Maßnahmen (im Sprachgebrauch der DSGVO = TOM) stellen dann Obliegenheiten dar, an denen sich Versicherte und Versicherer hinsichtlich der Leistungsverpflichtung im Schadensfalle orientieren.

## 5.2 Erfüllung der Normen nach Art. 32 DSGVO

### 5.2.1 Auswahl nach „Stand der Technik“

Der unbestimmte Rechtsbegriff “Stand der Technik” erhielt in den letzten Jahren vermehrt Aufmerksamkeit. Unbestimmte Rechtsbegriffe bestimmen zu erfüllende Anforderungen, legen jedoch nicht fest, wie diese Anforderungen im Einzelfall auszugestalten sind. Unbestimmte Rechtsbegriffe sind grundsätzlich gerichtlich uneingeschränkt überprüfbar und nach ständiger Rechtsprechung ist ihre Verwendung grundsätzlich verfassungsrechtlich unbedenklich (BVerfG, 19.04,1978 – 2 BvL 2/75). Das Anforderungsniveau beim „Stand der Technik“ liegt zwischen dem Anforderungsniveau „allgemein anerkannte Regeln der Technik“ und „Stand von Wissenschaft und Technik“.

Der Begriff „Stand der Technik“ ist insoweit keine Besonderheit der Cyber-Security. Er wird verwendet, um die verschiedenen Technologiestände vorzugeben, die von den Adressaten zumeist abhängig vom Gefährdungsgrad einzuhalten sind (Kipker, Cybersecurity, 3, 3).

Der Stand der Technik in den Jahren 2021/2022 ist durch innovative und teilweise öffentlich geförderte IT-Anwendungen gekennzeichnet.

**Stand der Technik Schutzmaßnahmen u.a.:**

- Virenschutz-Software
- Firewall Systeme
- Cloudbasierte Datensicherungen (inkl. Rekonstruktionstests)
- Kryptierungen in den Primäranwendungen

**Stand der Technik Organisationsmaßnahmen:**

- Cloudbasierte Sicherheitsmanagementsysteme (ISMS)
- E-Learning Anwendungen (z.B. Webinare, digitale Erklär-Videos)
- Digitale Coaching Systeme (nach Schulungsplan und Curriculum)
- Digitale Statusanalysen mit Benchmarking (z.B. nach Fragenkatalog des GDV)
- Digitale Alarmnachrichten (z.B. auf mobile Endgeräte)

Der „Stand der Technik“ verändert sich natürlich dynamisch. Insofern ist ein integrierter Update-Service für Software und Nachrichten von wesentlicher Bedeutung für die Gewährleistung der Informationssicherheit und den Cyberschutz.
Dem wachsenden Druck auf die Absicherung von Daten und Informationen können Verantwortliche von Behörden und Unternehmen durch die Etablierung eines Informationssicherheitsmanagementsystems begegnen. Dafür kann auf die anerkannten Standards (BSI 200-2/3, ISO 27001, VdS 10000 ) zurückgegriffen werden.

### 5.2.2 Kalkulation der „Implementierungskosten“

Die Implementierungskosten sind nicht rechtsverbindlich definiert (siehe auch 2.1.). Somit sind die Implementierungskosten direkt abhängig vom „Stand der Technik“. Digitale Organisationsmittel sind im Regelfall deutlich wirtschaftlicher als traditionelle analoge Systeme.

Im Vergleich zu serverbasierten lokalen IT-Systemen sind cloudbasierte Informationssicherheits-managementsysteme deutlich wirtschaftlicher. Einerseits werden Investitionen in Server-Hardware gespart und andererseits entfallen Software-Investitionen, da die cloudbasierten Anwendungen fast ausschließlich als „Software as a Service“ (SaaS) Leistungen angeboten werden.

Werden Systeme nach dem „Stand der Technik“ (cloudbasierte digitale Organisationsmittel und E-Learning) eingesetzt, können die laufenden Gesamtaufwendungen für die IT-Nutzung mit ca. 0,5% vom Umsatz der Versorgungseinrichtung angesetzt werden. Diese Infrastruktur (cloudbasiert und SaaS finanziert) kann dann auch gleichzeitig zur Umsetzung von Datenschutz nach DSGVO und Qualitätsmanagement nach §§ 135ff SGB V genutzt werden.

#### ZEITAUFWENDUNGEN FÜR DIE DIGITALISIERUNG MIT CYBERSCHUTZ, INFORMATIONS-SICHERHEIT UND DATENSCHUTZ IN ARZTPRAXEN 2021 (2 ÄRZTE / 8 MITARBEITENDE)

| Anwendungen in der Arztpraxis | Std. Ärzte (2) | Std. Koordinatoren (2) | Std. Mitarbeiter (6) | Std.Gesamt |
|---|---|---|---|---|
| Telematikinfrastruktur (TI) (z.B. e-AU etc.) | 12,0 | 36,0 | 72,0 | **120,0** |
| Medizintechnik Datenstellen | 8,0 | 12,0 | 0,0 | **20,0** |
| Qualitätssicherungsprogramme, DMP etc. | 8,0 | 24,0 | 18,0 | **50,0** |
| Webbasierte Terminkalender | 0,0 | 36,0 | 18,0 | **54,0** |
| Video-Sprechstunden | 12,0 | 36,0 | 18,0 | **66,0** |
| e-Rezept (ab 07/2022) | 0,0 | 36,0 | 36,0 | **72,0** |
| e-Arztbrief | 16,0 | 36,0 | 36,0 | **88,0** |
| ePA (elektronische Patientenakte) (ab 2022) | 24,0 | 72,0 | 144,0 | **240,0** |
| Forschungsprojekte | 8,0 | 24,0 | 12,0 | **44,0** |
| Gesundheits-Apps | 8,0 | 24,0 | 24,0 | **56,0** |
| **Zwischensumme IT-Sicherheit** | **96,0** | **336,0** | **378,0** | **810,0** |
| Anwendungen für Datenschutz nach DSGVO | 0,0 | 36,0 | 18,0 | **54,0** |
| Anwendungen für QM (z.B. QEP neu) | 8,0 | 36,0 | 36,0 | **80,0** |
| Anwendungen Patientensicherheit (IFSG/BG) | 12,0 | 24,0 | 18,0 | **54,0** |
| **Zwischensumme Datenschutz** | **20,0** | **96,0** | **72,0** | **188,0** |
| **GESAMT** | **116,0** | **432,0** | **450,0** | **998,0** |
| Einsparungen durch MC-PRAXIS 75b | **-48,0** | **-210,0** | **-150,0** | **-408,0** |
| Kalkulatorische Stundensätze | **84,00 €** | **26,55€** | **15,75 €** | |
| **Einsparungen in EURO gesamt** | **-4.032,00 €** | **-5.575,50 €** | **-2.362,50 €** | **-11.970,00 €** |

Durch ein cloudbasiertes Self Coaching System (cSCS) können über 40% der zeitlichen Aufwendungen gespart werden (nach ISO 9001 Norm)

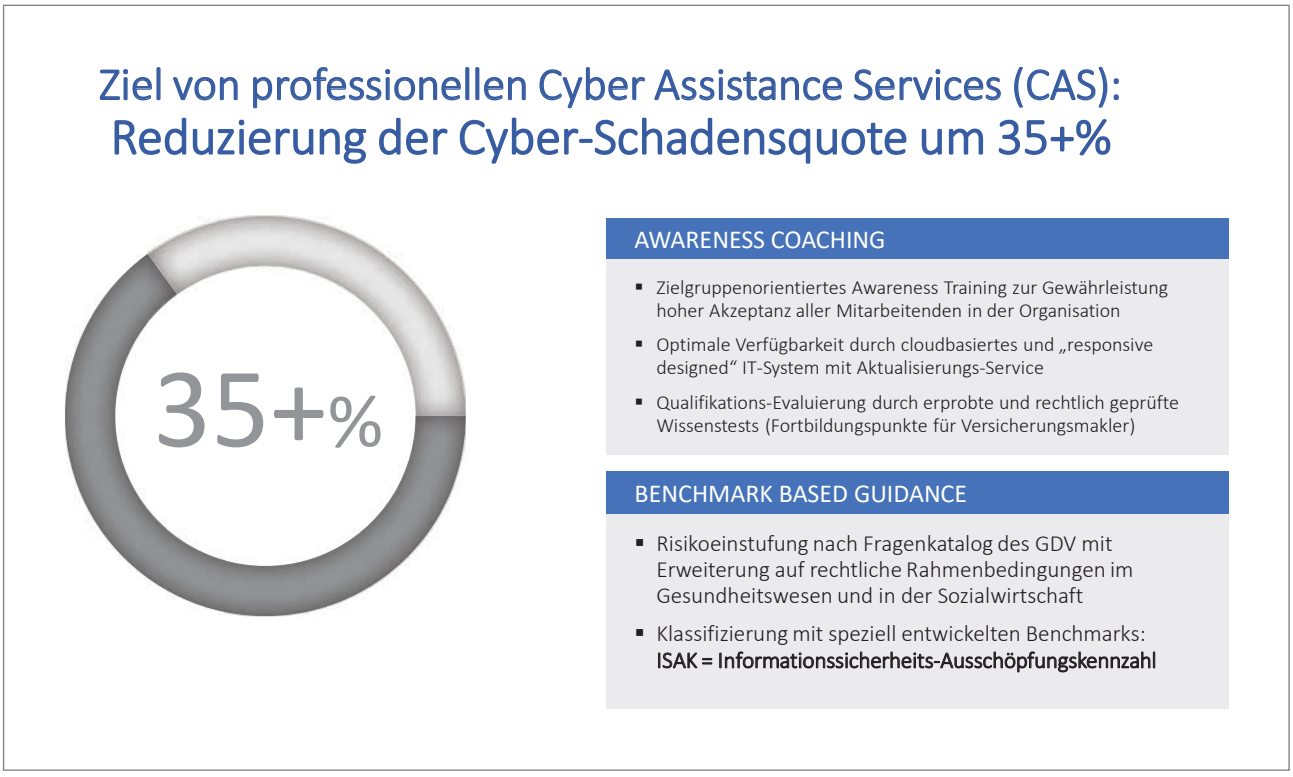
### 5.2.3 Ermittlung Art des Umfangs, der Umstände und Zwecke der Verarbeitung

Die medizinischen Versorger verarbeiten Personendaten je nach Fachrichtung und Praxisgröße sehr unterschiedlich. Das wird insbesondere durch die digitale Infrastruktur und die Funktionen der Anwendung abgebildet. Eine kleine Kinderarztpraxis hat andere Anforderungen an IT-Sicherheit als eine große radiologische Praxis. Deshalb ist eine kompakte Bestandsaufnahme für die Risikobewertung elementar.

Die folgenden Fragen sind für die Art des Umfangs, die Umstände und die Zwecke der Verarbeitung relevant:

- Umfang der elektronischen Dokumentation (nur Diagnosen und Leistungsziffern oder auch Befunde, Therapien und Behandlungspläne
- Integrierte Medizintechnik mit digitaler Verarbeitung von Patientendaten und Schnittstellen (z.B. GDT, HL 7, DICOM)
- Einsatz von innovativen digitalen Anwendungen (Video-Sprechstunden, Gesundheits-Apps, internet-basiertes Terminmanagement etc.)
- Teilnahme an wissenschaftlichen Forschungsprojekten, Qualitätssicherungsmaßnahmen etc. mit elektronischer Datenverarbeitung etc.

Die Bandbreite der Digitalisierung in der medizinischen Versorgung ist relativ groß. Entsprechend komplex ist auch die Evaluierung der Risiken für Cyberschutz und Informationssicherheit. Gemessen werden können die unterschiedlichen Voraussetzungen nur mit objektiven Benchmarks (z.B. Informationssicherheits-Ausschöpfungskennzahlen wie **ISAK** der **MCSS AG**).




Die Erhöhung des Bewusstseins für Informationssicherheit (Awareness Coaching) und die Objektivierung der Rechtskonformität für IT-Sicherheit und Datenschutz sind integrale Bestandteile der Assistance Services (Benchmark based Guidance).

### 5.2.4 Eintrittswahrscheinlichkeit und Schwere des Risikos

Die Einschätzung der Eintrittswahrscheinlichkeit eines Risikos der Informations- und Cyber-Sicherheit ist für den einzelnen Arzt/ die einzelne Ärztin sehr schwierig. Umfragen zeigen allerdings, dass die Risiken meist unterschätzt werden.

In diesem Kontext werden Versicherungen und Dienstleister empfohlen. In der Präambel der IT-Sicherheitsrichtlinie nach § 75b SGB V heißt es dazu: „Bei der Umsetzung (der IT-Richtlinie) können Risiken auch an Dritte, wie IT-Dienstleister oder Versicherer, übertragen werden."

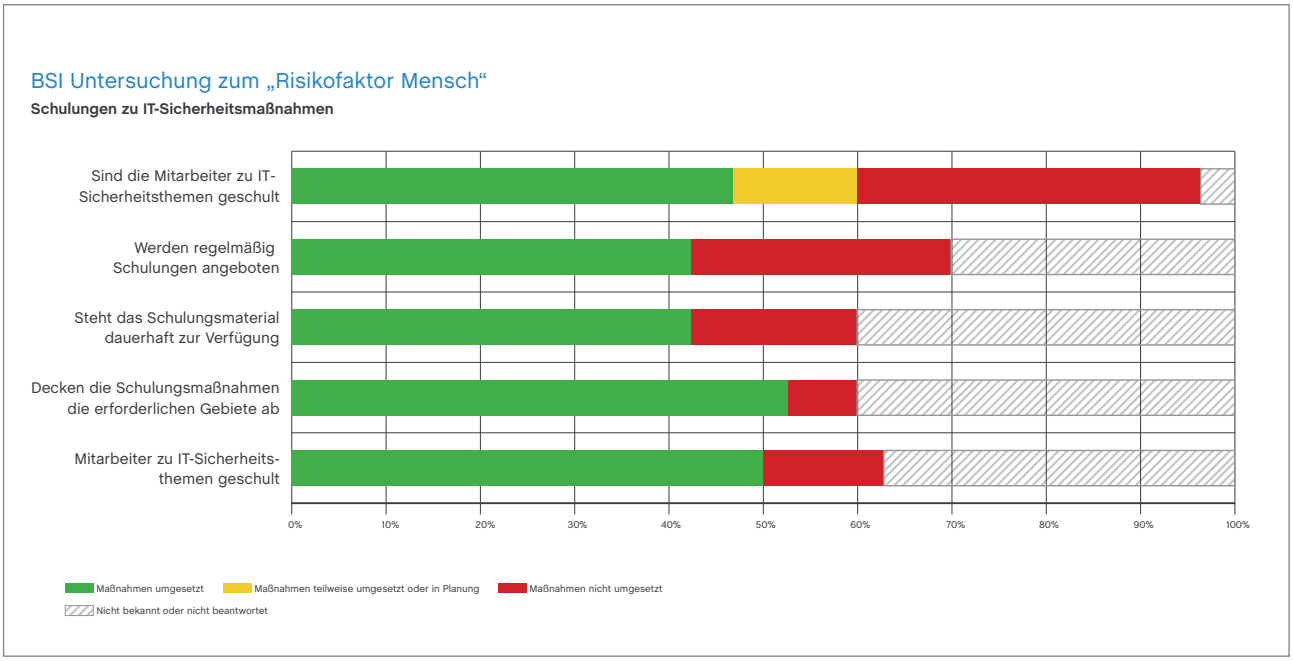
Bei der Übertragung der Risiken an Externe ist auf die Qualifikation der Dienstleister zu achten. Diese sollten spezielle Erkenntnisse und Erfahrungen im Bereich der medizinischen Versorgung haben und nachweisen können (BSI relevante Ausbildungen und Qualifikationen als Datenschutzbeauftragte).

### 5.2.5 Technische und Organisatorische Maßnahmen (TOM)

Die „technischen und organisatorischen Maßnahmen" (TOM) werden rechtlich nicht weiter spezifiziert. Für die vertragsärztliche Versorgung ergeben sich Leitlinien aus der IT-Sicherheitsrichtlinie nach § 75b SGB V und der QM-Richtlinie § 4 (GBA) nach §§ 135ff. SGB V (siehe 2.3 Qualitätsmanagement).

Die wichtigsten TOM sind zentrale Elemente des QM-Systems und auch der Versicherungsbedingungen, den sogenannten Obliegenheiten, der Cyber-Versicherungen (auch relevant für Haftpflicht und Betriebsunterbrechungsversicherungen). Sie werden in Prozessbeschreibungen (Verfahrensanweisungen nach ISO 9001 und Internen Regelungen nach QEP) festgeschrieben.

Um auch eine konkrete Anwendung zu gewährleisten, müssen die TOM-Anweisungen ständig allen Mitarbeitenden zur Verfügung stehen.




Die BSI Analyse macht deutlich, dass technische und besonders organisatorische Maßnahmen gezielt im Bereich der Mitarbeiter-Schulung eingesetzt werden müssen. Es fehlen vor allem regelmäßige Schulungen und das notwendige Coaching-Material.

Nach dem „Stand der Technik“ ist dies z.B. durch die Verwendung von cloudbasierten Systemen möglich, die auch auf allen mobilen Endgeräten (wie Smartphones, Tabletcomputern und Laptops) genutzt werden können.

Die Umsetzung von TOM kann aus den Anlagen 1-5 der IT-Sicherheitsrichtlinie abgeleitet werden. Danach sind Prozessbeschreibungen sinnvoll für die folgenden Arbeitsbereichen:

- Regelmäßige Datensicherungen (Modul 14 Anlage 1)
- Gewährleistung der Netzwerksicherheit (Modul 32-34 Anlage 1)
- Nutzung der IT-Arbeitsplätze (Endgeräte) (Modul 12-15 Anlage 1)
- Anwendung des Betriebssystems WINDOWS (Anlage 16-18 Anlage 1)
- Einsatz von Office-Produkten wie WORD, EXCEL etc. (Anlage 5-6 Anlage 1)
- Nutzung von Virenschutzprogrammen (Modul 15 Anlage 1)
- Einsatz von Wechseldatenträgern/Speichermedien (Modul 28-31 Anlage 1)
- Verwendung von Mobil-/Smartphones und Tablets (Modul 20-27 Anlage 1)
- APP-Nutzung (Mobile Anwendungen) (Modul 1-4 Anlage 1)
- Internet-Anwendungen (Modul 7-11 Anlage 1)
- Anwendung von digitaler Medizintechnik (Module 1-6 Anlage 4)
- Nutzung der Telematikinfrastruktur (Modul 1-7 Anlage 5)

Die Prozessbeschreibungen können frei definiert oder nach Normen wie QEP (QM System der KBV) ISO 9001 erstellt werden. Aus Kostengründen empfiehlt sich die Nutzung vorstrukturierter Dokumentensammlungen. Diese werden auch in cloudbasierten Systemen, speziell für medizinische und pflegende Versorgungseinrichtungen angeboten (z.B. **MC-PRAXIS 75b**, **MC-KLINIK**, **MC-CURA** der **MCSS AG, Köln**).

### 5.2.6 Zusammenfassung der Normen nach Art. 32 DSGVO

Die Rechtsnormen der Informationssicherheit (und des Datenschutzes) ergeben sich für alle Einrichtungen/Unternehmen, die Personendaten verarbeiten, aus Art. 32 DSGVO. Für die ärztliche Versorgung (Vertragsarzt) ergeben sich die rechtlichen Rahmenbedingungen zusätzlich aus dem Digitale-Versorgungs-Gesetz (DVG) Richtlinien nach § 75b und § 75c SGB V.

Bei Nichteinhaltung der Normen ergeben sich umfangreiche Risiken und Rechtsfolgen (siehe 5.1 – 5.5). Diese können allerdings durch Versicherungen und Dienstleister relativiert werden.

## 5.3 Übertragung der Risikoumsetzung an Dienstleister und Versicherer

### 5.3.1 Umsetzung der Rechtsnorm mit Dienstleistern

Die Risiken aus den Verpflichtungen für Informationssicherheit, Datenschutz (und QM) können unter bestimmten Voraussetzungen an qualifizierte Dienstleister übertragen werden. Allerdings verbleibt die Gesamtverordnung bei dem Arzt/der Ärztin und/oder dem Management von Krankenhäusern und Kliniken.

Nach den üblichen Sorgfaltspflichten obliegt den Verantwortlichen bei Beauftragung von Dienstleistern insbesondere:

- Die Prüfung der Qualifikation des Dienstleisters. Dies bezieht sich auf die globale Sachkenntnis für Informationssicherheit (beispielsweise BSI Grundschutz-Ausbildung) und Datenschutz (z.B. Ausbildung zum Datenschutzbeauftragten)
- Die Feststellung der Fachkenntnis des Dienstleisters im medizinischen Umfeld (Nachweis der Betreuung von Arztpraxen und Kliniken) in vergleichbaren Projekten (z.B. Einführung von Qualitätsmanagement und Datenschutz in der Gesundheitsversorgung)
- Die Dienstleister sollten alle relevanten Vorlagen für Dokumente und Checklisten im Rahmen einer Auftragserteilung nachweisen und zur Verfügung stellen können
- Der Dienstleistungsvertrag sollte dem Standard für Dienstleistungsverträge im Gesundheitswesen (z.B. berufliche Schweigepflicht) berücksichtigen und insbesondere die Normen nach § 75b (bzw. § 75c) SGB V referenzieren (Mitgeltung der Rechtsnormen)
- Die Prüfung der o.g. Bedingungen wird in einem Dokument nach QM-Richtlinien aufgenommen (z.B. „Lieferanten-Audit“ nach ISO 9001)

### 5.3.2 Umsetzung der Rechtsnorm mit Versicherungen (Cyber-, Haftpflicht- und BU-Versicherer)

Durch die zunehmende Komplexität der Digitalisierung im Gesundheitswesen und in der Sozialwirtschaft lassen sich Risiken niemals gänzlich ausschließen. Dadurch werden Absicherungen durch maßgeschneiderte Versicherungsprodukte unverzichtbar.

Der Fall der Universitätsklinik Düsseldorf hat gezeigt, welche Dimensionen mit einer relativ unstrukturierten Cyber-Attacke verbunden sein können. Der Todesfall einer Patientin und der Aufnahmestopp neuer Patienten über Wochen hat Schadenssummen von wahrscheinlich 7 bis 8-stelligen Eurobeträgen verursacht.

Sowohl für die Versicherer wie auch die Versicherten werden Cyber-Versicherungen in der medizinischen Versorgung zukünftig eine deutlich größere Bedeutung bekommen. Existentielle Bedrohungen für Versicherte lassen sich nur über einen professionellen Versicherungsschutz ausschließen.

Die Cyber-Versicherer müssen ihre Produkte dem schnellen Wandel der IT-Nutzung und der damit verbundenen Risiken anpassen. Das gilt für die folgenden Konditionsparametern:

- Die Preise werden an die steigenden Risiken anzupassen sein
- Die Obliegenheiten sind auf die tatsächlichen Risiken der Zielgruppen auszurichten
- „Assistance-Dienstleistungen“ werden zum Standard im Gesundheitsbereich (Monitoring nach Benchmarks und Awareness Coaching)
- Regelmäßiges Reporting (z.B. Jahresberichte nach § 75b Kapitel IV, Ziffer 5.: jährliche Evaluationspflichten und Umsetzung kontinuierlicher Verbesserungsprozesse) wird verpflichtend

Der GDV (Gesamtverband der deutschen Versicherer) hat einen “unverbindlichen Muster-Fragebogen zur Risikoerfassung im Rahmen von Cyber-Versicherungen für kleine und mittelständische Unternehmen“ herausgegeben. Diese Sammlung von Fragestellungen kann als allgemeine Leitlinie herangezogen werden.

Allerdings ist die Liste nicht zielgruppenspezifisch auf Heilberufe ausgerichtet. Insofern müssen die Fragenkomplexe nach den Anforderungen nach § 75b SGB V um folgende Module ergänzt werden:

- Anwendungen der Telematikinfrastruktur allgemein mit ePA, e-Rezept, TIM und Notfalldaten-Management
- Nutzung von Video-bzw. Online-Sprechstunden
- Integrierte Internet-Anwendungen wie z.B. webbasierte Terminkalender
- Einsatz von digitaler Medizintechnik
- Elektronische Datenkommunikation im Rahmen wissenschaftlicher Forschungen
- Anwendungen von IoT (Internet of Things) z.B. bei Überwachung von Körperfunktionen (Diabetes-Monitoring, Beobachtung kardiologischer Parameter etc.)
- Therapeutische Einbeziehung von Gesundheits-Apps (z.B. digitale Schmerz-Tagebücher)

## 5.4 Arzt- und Zahnarztpraxen, MVZ, Pflege- und Reha-Einrichtungen

Die IT-Sicherheitsrichtlinie nach § 75b SGB V unterscheidet für Arzt- und Zahnarztpraxen und MVZ nach der Größe der medizinischen Versorgungseinrichtung. Dabei wird nach 3 Kategorien unterschieden:

- Einzelpraxen (bis 5 Mitarbeitende)
- Gemeinschaftspraxen (bis 20 Mitarbeitenden)
- Großpraxen (über 20 Mitarbeitende) inkl. Pflege und Reha-Einrichtungen

### 5.4.1 Einzelpraxen

Die Einzelpraxis hat die geringsten Anforderungen zu erfüllen. Der/die Vertragsarzt/-ärztin hat primär seinen Versorgungsauftrag zu erfüllen: Bestehen Kapazitäts- und Qualifikationseinschränkungen muss der Arzt/die Ärztin lediglich die Minimalanforderungen erfüllen.

Dazu gehören:

- Orientierung der Mitarbeitenden zur Informationssicherheit und zum Datenschutz
- Festlegung der Zuständigkeiten für IS und DS im Team (beispielsweise Erstkraft)
- Berücksichtigung von IS und DS im Schulungsplan der Praxis (nach Berufsrecht)
- Delegierung von IS- und DS- Maßnahmen an externe Dienstleister (z.B. Lizenzvertrag für ein einfaches ISMS/DSMS)

### 5.4.2 Gemeinschaftspraxen (6-20 Mitarbeitende mit IT-Zugriff)

Größere Praxen (ab 2 tätigen Ärzten/-innen in der Patientenversorgung) haben im Regelfall höhere Anforderungen zur Umsetzung der Rechtsnormen zu erfüllen. Diese sind in Anlage 2 zur IT-Sicherheitsrichtlinie nach § 75b SGB V dokumentiert. Mindestens sind die Anforderungen an eine Einzelpraxis zu erfüllen (6.4.2). Je nach Komplexität der elektronischen Datenverarbeitung wird ein DSB nach DSGVO vorgeschrieben.

### 5.4.3 Großpraxen, Reha- und Pflegeinrichtungen mit vertragsärztlicher Versorgung

Größere medizinische Versorgungseinrichtungen müssen nach den Regelungen der DSGVO ab 20 Mitarbeitenden einen DSB einsetzen. Dieser muss nach Art. 32 der DSGVO auch Anforderungen an Informationssicherheit erfüllen können.

Im Regelfall wird die Umsetzung eines ISMS/DSMS z.B. nach VdS 10000 und 10010 (Systeme der Schadensverhütungs-GmbH des GDV) oder ISO 27001 erwartet.

Für diese Zielgruppen sind externe Dienstleister zu empfehlen. Diese sind im Regelfall deutlich wirtschaftlicher als der Aufbau und die Vorhaltung eigener interner Kapazitäten.

## 5.5 Krankenhäuser und Kliniken nach § 75b und § 75c SGB V

Für Krankenhäuser, die nicht in die KRITIS Kategorie fallen, gilt für die stationäre Behandlung § 75c SGB V und für die ambulante Behandlung (angeschlossene Ambulanzabteilungen) § 75b SGB V analog zu Arztpraxen.

Im Einzelfall kommt es bei der Anwendung der Rechtsnormen auf die tatsächlichen Versorgungsverträge an.

Für die Regelungen nach § 75c SGB V wird ein gesondertes White Paper zur Verfügung gestellt.

## 5.6 Krankenhäuser nach KRITIS

Krankenhäuser mit mehr als 30.000 Abrechnungsfällen pro Jahr fallen unter die sogenannten KRITIS Regelung. Nach Angaben des statistischen Bundesamtes stehen in Deutschland ca. 1.900 Krankenhäuser mit knapp 500.000 Betten zur Verfügung. Die Zahl großer Kliniken mit 600 und mehr Betten belief sich im Jahr 2017 auf 175. Pro Jahr werden etwa 19,5 Mio. Fälle behandelt. Rund 29 % der Krankenhäuser befinden sich in öffentlicher Trägerschaft, 34 % werden von Kirchengemeinden, Stiftungen oder Vereinen unterhalten (sogenannte freigemeinnützige Trägerschaft), 37 % privat betrieben.

Die Rechtsnormen sind entsprechend der Größenordnung (KRITIS) und den Trägerschaften (öffentliche Träger, Kirchen, Stiftungen oder Vereine) zu beurteilen. Das gilt sowohl für die Regelungen für Informationssicherheit als auch für den Datenschutz (die Kirchen folgen eigenen Datenschutz-Regelungen).

Siehe White Paper zu Rechtsnormen zur Informationssicherheit/Cyberschutz für Krankenhäuser.

# 6 Handlungsempfehlungen

Die aktuellen Rahmenbedingungen für Arztpraxen ändern sich in einem Rekordtempo.
Die eingeleitete Digitalisierung und die steigenden Belastungen in der medizinischen Versorgung machen zusätzliche technische und organisatorische Maßnahmen erforderlich:

1. Bevor die Maßnahmen konkret geplant werden können, ist eine bereichsübergreifende Bestandsaufnahme zu erstellen. Diese Ist-Aufnahme ist zu differenzieren nach Informationssicherheit und Cyberschutz nach der IT-Sicherheitsrichtlinie gemäß § 75b SGB V, Datenschutz nach DSGVO und Qualitätsmanagement nach § 137 SGB V.
2. Die bestehenden Zuständigkeiten und Rollen im Team (Sicherheits-Beauftragte, QM-Beauftragte etc.) sind zu überprüfen und wenn notwendig neu zu definieren.
3. Alle Mitarbeitende sind in den Optimierungsprozess (Change-Management) einzubeziehen. Dazu eignet sich ein Team-Meeting, in dem alle Mitarbeitende informiert und aufgeklärt werden.
4. In einem Schulungsplan mit Definition von Inhalten und Zielen (Curriculum) wird festgelegt, in welchem Zeitrahmen (12-36 Monate) eine rechtskonforme Struktur erreicht werden kann.
5. Viele Aufgaben lassen sich delegieren. Deshalb ist zu prüfen, welche Partner welche Aufgaben übernehmen können und wie diese wirtschaftlich und rechtssicher (Übernahme von Garantien) einbezogen werden können.
6. Um gegen größere Schäden geschützt zu sein, empfiehlt sich unbedingt der Abschluss einer Cyber-Versicherung, die auf medizinische Versorgungseinrichtungen ausgerichtet ist (Abdeckung aller relevanten Risiken).
7. Unabhängig von der Versicherung ist ein pragmatischer Notfallplan für alle möglichen Störfälle zu entwickeln und jederzeit verfügbar zu machen (z.B. auf Smart Phones und Tablets).
8. Um eine langfristige Nachhaltigkeit zu gewährleisten, ist der Einsatz eines digitalen Managementsystems zu prüfen, das die Aufgaben und Lösungen transparent und für alle Mitarbeitenden verfügbar macht. Dazu sollte ein cloudbasiertes System unabhängig von dem Praxis-Netzwerk aus Sicherheitsgründen gewählt werden.
9. Um eine dauerhafte Qualitäts- und Rechtskonformität zu etablieren, ist ein Monitoringsystem (beispielsweise mit Kennzahlen) einzuführen, das der verantwortlichen Leitung eine ständig aktuelle Transparenz gewährleistet und mögliche Lücken und Risiken aufzeigt.

# 7 Zusammenfassung

Der Gesetzgeber hat mit verschiedenen Rechtsnormen, auf die sich aus der zunehmenden Digitalisierung im HealthCare Bereich ergebenden Risiken für die IT-Sicherheit und den Datenschutz reagiert und Anforderungen an die Berufsträger zum Schutz von Patientendaten erlassen.

Diese technischen und organisatorischen Anforderungen verpflichten die Berufsträger, sich strukturiert und nachhaltig mit dem Schutz von Patientendaten in Form eines umfassenden Managementsystems für IT-Sicherheit zu beschäftigen und hierfür geeignete Nachweise zu erbringen.

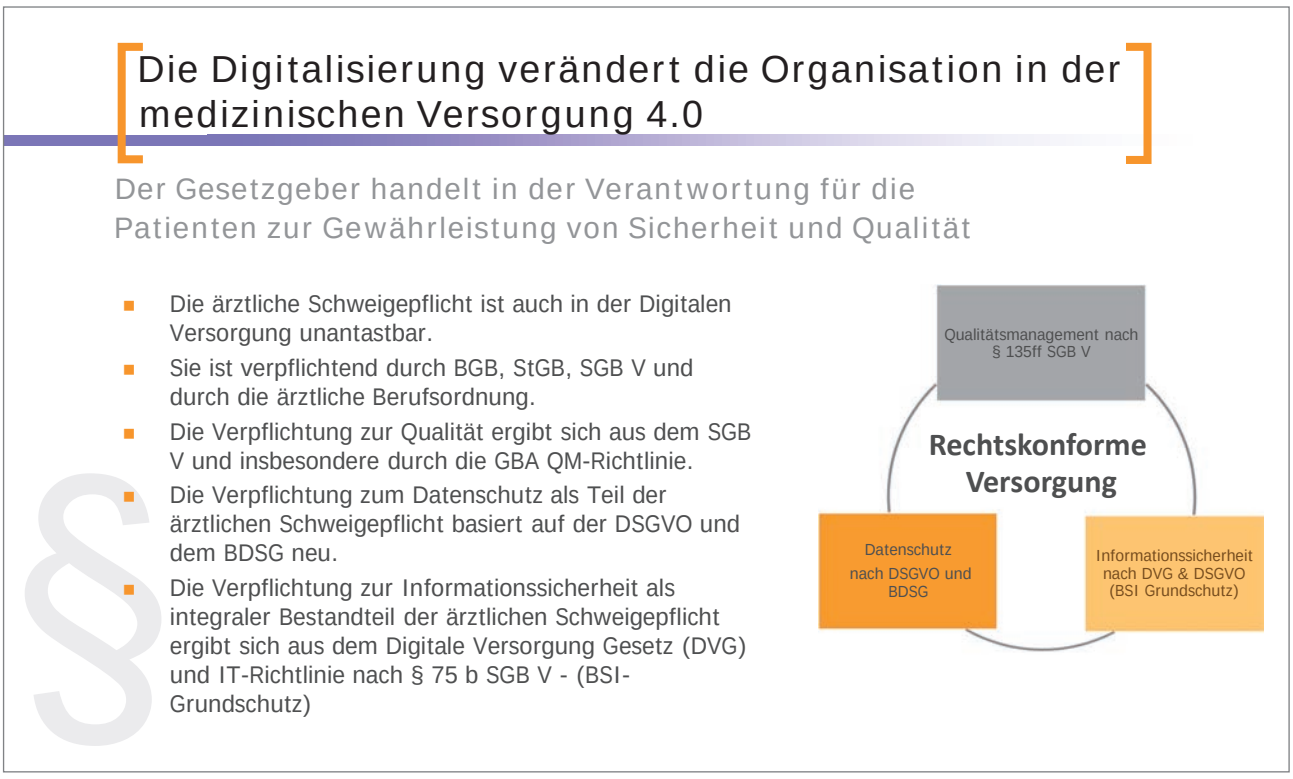
Eine Nichtbeachtung dieser Anforderungen kann grundsätzlich und speziell im Schadenfall empfindliche Konsequenzen nach sich ziehen.

Die Bandbreite reicht hier von Geldbußen bis hin zu berufsrechtlichen Restriktionen.

Um es den Betroffenen einfacher zu machen, diese Maßnahmen einzuführen, umzusetzen und zu dokumentieren, besteht die Möglichkeit, sich der Hilfe von externen Dritten in Form von unterschiedlichen Dienstleistungen zu bedienen.

Dazu gehören qualifizierte Anbieter von Management Systemen genauso wie Versicherungen und deren Assistance Leistungen.

Es soll so sichergestellt werden, dass der Schutz von Patientendaten beachtet, mit einem angemessenen Aufwand sichergestellt und eventuelle Schadenfälle in Ihrem Ausmaß reduziert werden.




Auszug aus einem Vortrag von Arno Zurstraßen, Anwalt für Medizinrecht, Köln: Qualitätsmanagement, Datenschutz und IT-Sicherheit können und sollten in einem rechtlichen Kontext verstanden werden.

Eine entsprechende Dokumentation in Form eines Managementsystems für die Bereiche IT-Sicherheit, Datenschutz und Qualitätsanforderungen dient dabei nicht nur der Kontrolle von Maßnahmen und des Reifegrades der Umsetzung, sondern ist auch im Schadenfall die geeignete Grundlage, um auf eventuelle rechtliche Konsequenzen zur Enthaftung vorbereitet zu sein.

Hierbei ist auch die Darstellung eines persönlichen Risiko Scores hilfreich, wenn es um die Bewertung innerhalb einer Zielgruppe und die Gespräche mit Versicherungen bezüglich der möglichen Restrisiken geht.

Im Idealfall lassen sich so mit geringen finanziellen Mittel geeignete Systeme und Mechanismen etablieren, die vor weitergehenden finanziellen Risiken und schlimmstenfalls Reputationsschäden schützen.

Die finanziellen und zeitlichen Einsparpotentiale kommen dabei der Praxisorganisation und dem Wohl der Patienten/-innen Zugute.

Die Komplexität bei der Umsetzung von Informationssicherheit, Cyberschutz und Datenschutz in der medizinischen Versorgung wurde deutlich anspruchsvoller.

### Damit verbunden sind neue Verpflichtungen, aber auch zusätzliche Freiräume

1. Die IT-Sicherheitsrichtlinie nach § 75b/75c SGB V in Kombination mit Art. 32 DSGVO definiert umfassende gesetzliche Verpflichtungen für IT-Sicherheit und Datenschutz in Arztpraxen und Krankenhäusern.

2. Bei Nichteinhaltung der gesetzlichen Regelungen können berufsrechtliche, datenschutzrechtliche und versicherungsrechtliche Folgen mit entsprechenden finanziellen Konsequenzen drohen.

3. Der Gesetzgeber sieht allerdings vor, dass zur Minimierung der Risiken spezialisierte Dienstleister und Versicherungen (z.B. Cyber-Versicherer) vertraglich verpflichtet werden können.

4. Bei der Auswahl der Partner ist auf die Spezialisierung der Dienstleister zu achten, da mehr als 70% der Risiken branchenspezifisch begründet sind. Im Gesundheitsbereich begründet dies die gesetzlich definierte Digitalisierung mit dem DVG.

5. Wesentliche Leistungen im Kontext von Cyber-Versicherungen werden durch sogenannte „Assistance Dienstleistungen“ definiert. Dazu gehören innovative Coaching- und Awareness Dienstleistungen vor allem innovative Coaching- und Awareness Dienstleistungen für alle Mitarbeitende, da bis zu 80% der Sicherheitsstörfälle auf den „Faktor Mensch“ zurückzuführen sind. Besonders ist auf die fachspezifischen Anforderungen der Zielgruppen im Bereich Gesundheit und Soziales zu achten.

6. Mit „Silent Cyber“ Risiken wird IT-Sicherheit und Cyberschutz auch für bestehende klassische Versicherungen im Haftpflicht- und BU-Bereich relevant. Insofern sind spezielle Assistance Dienstleistungen auch für größere Versicherungssegmente wirtschaftlich bedeutsam.

7. Der „Stand der Technik“ (nach § 75 SGB V und Art. 32 DSGVO) wird durch innovative digitale Lösungen wie wirtschaftliche Cloud-Anwendungen, „Software as a Service“ (SaaS), E-Learning, Machine Learning und Künstliche Intelligenz (KI) repräsentiert.

8. Die Reife und Wirksamkeit der IT-Sicherheit und des Cyberschutzes wird zukünftig mit Anwendung standardisierter Benchmarks (vergleiche **ISAK**, Informationssicherheits-Kennzahl der MCSS AG, **Köln** objektivierbar sein.

9. Ab 2021 wird die Bundesanstalt für Finanzdienstleistungsaufsicht (kurz BaFin) Cyber-Policen zu einem Aufsichtsschwerpunkt machen.

10. Rechtskonformität und Wirtschaftlichkeit in der medizinischen Versorgung wird insbesondere durch die Kombination von Informationssicherheit (nach § 75 SGB V), Datenschutz (nach DSGVO) und Qualitätsmanagement (nach §§ 135ff SGB V und §4 GBA-QM RL) erreicht. Ein konsolidiertes und dynamisches Prozessmanagement (ISMS-DSMS-QMS) in der medizinischen Versorgung kann bis zu 45% an Zeitkapazitäten und Finanzressourcen sparen.

11. Cyberversicherungen werden im Jahr 2025 ein jährliches Prämienvolumen von voraussichtlich 1,25 Milliarden Euro erreichen. Die Branchen „Gesundheit und Soziales“ werden ein Volumen von ca. 250 Millionen Euro ausmachen und damit ein großes weitgehend homogenes Segment repräsentieren.

12. Mit professionellen „Assistance Dienstleistungen“ lassen sich mehr als 35 % der Cyberschäden durch geführtes Awareness Coaching vermeiden. Marktuntersuchungen (GDV & BSI) zeigen, dass nur zwischen 40-50% der Mitarbeitenden auf Cyber-Risiken professionell vorbereitet sind.

# 8 Die Autoren

## Arno Zurstraßen

Arno Zurstraßen, M.A. ist als Fachanwalt für Medizinrecht und Sozialrecht, Mediator und Supervisor in Köln niedergelassen. Mit seiner Erfahrung von über 25 Jahren berät er Ärzte/-innen, Zahnärzte/-innen, Praxisnetze und ärztliche Berufsverbände
mit Schwerpunkt Rechtskonformität und Arzthaftungsrecht. Die Umsetzung der umfangreichen Rechtsvorschriften für Ärzte/-innen mit innovativen Konzepten und professionelle Technologien ist ein besonderes Credo für ihn.

Arno Zurstraßen berät Ärzte/-innen auch bei Praxisabgaben oder -verschmelzungen. Dabei stützt er sich auf ein strukturiertes Projektmanagement, das er speziell nach Qualitätsmanagement-Kriterien im Team mit IT-Fachleuten entwickelt hat.

Er ist Autor von vielen Publikationen in der Fachpresse und bekannter Referent auf ärztlichen Kongressen. Als Mitglied des Aufsichtsrats der **MCSS AG, Köln** gewährleistet er die rechtliche Kompatibilität innovativer digitaler Managementsysteme für die medizinische Versorgung.

## Christian Schottmüller

Christian Schottmüller studierte Betriebswirtschaftslehre und Jura an der Universität in Köln.

Seit dem Jahr 2008 ist er in verschiedenen Leitungsfunktionen für die Versicherungswirtschaft tätig und arbeitete dort seit 2014 unter anderem daran mit, Standards für die IT-Sicherheit im präventiven Bereich durch Informationssicherheits-Managementsysteme zu entwickeln. In seiner Laufbahn vermittelte er sein profundes Branchenwissen in zahlreichen Schulungen und Vorträgen.

Im Jahr 2021 übernahm Christian Schottmüller die Verantwortung für die Umsetzung von Cyberschutz und Informationssicherheit im Gesundheitswesen und in der Sozialwirtschaft als Direktor der **MCSS AG, Köln**.

## Rainer Waedlich

Rainer Waedlich ist Experte für Health-IT (E-Health), Cyberschutz und Qualitätsmanagement im Gesundheitsbereich. In seiner über 40-jährigen Berufslaufbahn im Gesundheitswesen hat er, national und international, software-basierte Produkte im Bereich der elektronischen Patientenakte (EPA), Qualitätssicherung und Qualitätsmanagement entwickelt und über 1.000 Arztpraxen und Kliniken weltweit in IT-Fragen beraten.

Im Bereich Big Data Analytics und Machine Learning hat Rainer Waedlich in internationalen Projektgruppen an Health-IT Anwendungen, u.a. mit IBM Watson Teams in den USA und Japan gearbeitet.

Als Aufsichtsratsvorsitzender deutscher und amerikanischer Health IT-Unternehmen war er 15 Jahre lang u.a. für die Rechtskonformität von wissensbasierten Projekten verantwortlich (Entwicklung von Algorithmen für Vorstufen von KI-Anwendungen, „Artificial Intelligence in Medicine“).

Sein Spezialgebiet, neben E-Health, sind Optimierungs-Strategien im organisatorischen und versorgungstechnischen Bereich, z.B. mit KAIZEN Konzepten (KAIZEN = das japanische Prinzip der ständigen Optimierung). Aktuell ist er Aufsichtsratsvorsitzender der **MCSS AG, Köln** und im Unternehmen verantwortlich für Rechtskonformität von IT-Anwendungen.

# 9 Referenzen


- Digitale-Versorgung-Gesetz (DVG) § 75b SGB V
- Richtlinie nach § 75b SGB V (KBV)
- Krankenhauszukunftsgesetz (KHZG)
- BSI Empfehlungen nach Anlage 6
  (Informatorische Quellen des BSI zu den Anforderungen der Richtlinie nach § 75b SGB V)
- Bundesdatenschutz Gesetz § 64 BDSG
- EU-Datenschutzverordnung Art. 32 DSGVO
- BSI-Standard 200-1 (bsi.bund.de)
- VdS Standard RL 10000 Informationssicherheit (ISMS) und VdS 10010 (DS)
- Aufsatz zu „IT-Sicherheit betrifft nicht nur Großkrankenhäuser – die Regulierung der IT-Sicherheit im ambulanten und stationären Bereich“
  Autoren: Tilmann Dittrich und Jan Ippach

# Anmerkung

Das digitale **MCSS Ökosystem** wurde vom Bundesministerium für Wirtschaft (BMWi) im Rahmen eines ZIM Forschungs- und Innovationsprojekts gefördert.

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

ZIM
Zentrales
Innovationsprogramm
Mittelstand

MCSS AG
MioCloud
Solution Systems

A Weinsbergstraße 190
50825 Köln
T 0221/47 44 77 44
F 0221/47 44 77 55
E info@mcss-ag.de
W mcss-ag.de