DEUTSCHE KRANKENHAUS GESELLSCHAFT

Bundesverband der Krankenhausträger in der Bundesrepublik Deutschland

# Umsetzungshinweise nach § 75c SGB V

# Informationssicherheit in Krankenhäusern

## Stand: 07.12.2021

Kategorie: öffentlich

Status: Freigegeben

Version: 0.98

Kürzel: GF-Info-75c

Postfach 12 05 55
10595 Berlin
Wegelystraße 3
10623 Berlin

c/o HOPE
Avenue Marnix 30
1000 Brüssel
Telefon +32 2 540 25 50

Commerzbank AG
IBAN DE63 1004 0000 0788 4141 00
BIC COBADEFFXXX
UST-IdNr. DE119355528

www.dkgev.de

## Inhaltsverzeichnis

**1 Zusammenfassung ..... 3**
**2 Einleitung ..... 4**
**3 Verstehen, worum geht es ..... 5**
**4 Gefährdungen: Wodurch ist die Informationssicherheit in Krankenhäusern bedroht? ..... 7**
**5 Grundlegendes zum Starter-Paket und seiner Anwendung ..... 8**
**6 Gesetzliche Grundlagen ..... 10**
**7 Gap-Analyse ..... 12**
**8 Notfall- und Business-Continuity-Management ..... 13**
**9 Ausblick ..... 14**

## Dokumentenhistorie

| Version | Stand | Kap,/ Seite | Beschreibung der Änderung | Bearbeitung |
|---|---|---|---|---|
| **0.9** | 29.11.2021 | alle | Anlage des Dokuments | AG 75c SGB V |
| **0.91** | 06.12.2021 | alle | Kommentierung | AG 75c SGB V |
| **0.98** | 07.12.2021 | alle | Freigegeben | |



Danksagung: Besonderer Dank geht an dieser Stelle an die Mitglieder der Arbeitsgruppe „§ 75c SGB V“ der Deutschen Krankenhausgesellschaft, die maßgeblich zur Entstehung der Umsetzungshinweise, Empfehlungen und Vorlagen beigetragen hat.

# 1 Zusammenfassung

Ab dem 01.01.2022 sind alle Krankenhäuser verpflichtet, Maßnahmen zur Informationssicherheit nach dem Stand der Technik zu implementieren. Mit dem neuen § 75c SGB V wird die bereits seit 2017 bestehende Verpflichtung für KRITIS-Krankenhäuser (§ 8a BSI-Gesetz) jetzt auch für Nicht-KRITIS-Häuser eingeführt.

Auf den ersten Blick erscheint Informationssicherheit vielleicht als technische Aufgabe. In Wirklichkeit ist es aber in erster Linie eine Managementaufgabe. Eine Arbeitsgruppe der Deutschen Krankenhausgesellschaft (DKG) hat deshalb diese Umsetzungshinweise für die Geschäftsführung (kurz: GF-Info) zusammengestellt, die eine Übersicht zu den Zielen und Aufgaben gibt. Ergänzt wird dieses Dokument durch eine Checkliste für die initialen Aufgaben, fünf Arbeitshilfen und sechs Vorlagen. Zusammen bilden sie ein Starter-Paket zum neuen § 75c SGB V.

Zu den ersten Schritten gehört, seitens der Geschäftsführung ein interdisziplinäres Team mit der Vorbereitung zu beauftragen, einen - internen oder externen - Informationssicherheitsbeauftragten zu benennen, das Informationssicherheitsmanagement organisatorisch zu verankern und im Unternehmen zu kommunizieren.

Um einem Missverständnis vorzubeugen: Auch Nicht-KRITIS-Krankenhäuser haben in den vergangenen Jahren bereits zahlreiche Maßnahmen zur Informationssicherheit implementiert, um sich vor den stetig wachsenden Gefährdungen zu schützen. Anlässlich des jetzt wirksam werdenden § 75c SGB V sollte jedes Krankenhaus zunächst prüfen,

- ob die organisatorische Einbindung angemessen ist, das heißt, ein oder eine Informationssicherheitsbeauftragter (ISB) bestellt, eine Informationssicherheitsleitlinie verabschiedet und ein Informationssicherheitsmanagementsystem (ISMS) eingerichtet ist,

- inwieweit die bereits implementierten Maßnahmen dem Stand der Technik genügen und

- ob eine Einbindung in das Notfall- und Business-Continuity-Management sichergestellt ist.

Der oder die Informationssicherheitsbeauftragte sollte als Teil des betrieblichen Risikomanagements unabhängig von der Informations-, Medizin- und Haustechnik agieren können und direkt der Geschäftsführung berichten. Es bietet sich an, erfahrene Mitarbeitende aus dem Qualitäts- und Risikomanagement sowie Informations-, Medizin- und Haustechnik in die Umsetzung einzubeziehen. Letztlich ist Informationssicherheit eine Aufgabe, an der alle Mitarbeitenden mitwirken müssen. Die Aufmerksamkeit dafür kann über entsprechende Trainings geschaffen werden.

Nach einer Einleitung (Kapitel 2) wird dargestellt, worum es bei der Implementierung eines systematischen Informationssicherheitsmanagements geht (Kapitel 3). Kapitel 4 beschreibt die aktuellen spezifischen Sicherheits-Gefährdungen in Krankenhäusern. Inhalte und grundlegende Anwendungshinweise zum aktuellen Dokumenten Paket beschreibt Kapitel 5. Kapitel 6 gibt einen kurzen Überblick über einschlägige gesetzliche Grundlagen und Fördermöglichkeiten. Kapitel 7 be-

schreibt, wie mit einer initialen Gap-Analyse eine Bestandsaufnahme der Prozesse, Anlagen und Gegenstände sowie der bereits implementierten Informationssicherheitsmaßnahmen erfolgen kann. Kapitel 8 erläutert, warum und wie Informationssicherheit in das Notfall- und Business-Continuity-Management integriert werden sollte. Der Ausblick stellt weitere Arbeitshilfen und Vorlagen in Aussicht und erläutert das weitere Vorgehen (Kapitel 9).

# 2 Einleitung

Mit dem im Oktober 2020 erlassenen Patientendatenschutzgesetz (PDSG) und dem neu eingeführten § 75c SGB V sind ab Januar 2022 alle Krankenhäuser verpflichtet, Vorkehrungen zur Vermeidung von Störungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind.

Alle Krankenhäuser sind daher verpflichtet, ihre IT-Systeme nach dem Stand der Technik durch angemessene Vorkehrungen zu schützen. Diese Verpflichtungen können Krankenhausbetreiber insbesondere erfüllen, indem sie den branchenspezifischen Sicherheitsstandard (B3S) für Krankenhäuser umsetzen. Ein solcher Maßstab beschreibt informationssicherheitstechnische Prozesse und Maßnahmen, anhand derer ein angemessenes Schutzniveau bei gleichzeitiger Wahrung des üblichen Versorgungsniveaus der Patientenversorgung und der Verhältnismäßigkeit der umzusetzenden Maßnahmen erreicht werden kann. § 75c Absatz 2 SGB V regelt, dass mit Einhaltung des für KRITIS-Krankenhäuser erstellten B3S Krankenhäuser auch die Anforderungen aus Absatz 1 erfüllt sind. Neben dem B3S können auch andere Maßstäbe angewendet werden, wenn damit die Schutzziele in Absatz 1 erfüllt werden. Eine Nachweispflicht gegenüber dem BSI ergibt sich für Nicht-KRITIS-Krankenhäuser nicht. Sie haben jedoch alle zwei Jahre ihre Informationssicherheitsmaßnahmen an den aktuellen Stand der Technik anzupassen.

Aus § 75c SGB V sind keine direkten Sanktionen für den Fall einer Nichterfüllung ableitbar. Dennoch ist eine kurzfristige Umsetzung angemessener Vorkehrungen zur Informationssicherheit für Krankenhäuser essenziell, da im Fall eines Cyberangriffes etwaige Schadensersatzansprüche gegen den Träger geltend gemacht werden könnten. Ein Nachweis darüber, angemessene Vorkehrungen zum Schutz der IT-Systeme getroffen zu haben, könnte dann entlastend wirken. Wenn es im Zuge eines Sicherheitsvorfalls jedoch zu einem Verstoß gegen den Datenschutz kommt, kann dies eine Strafe von 2 bis 4 % des Umsatzes[1] nach sich ziehen.

Das vorliegende Dokument beschreibt, worin die Herausforderungen des § 75c SGB V („IT-Sicherheit in Krankenhäusern“) bestehen und gibt Empfehlungen, wie diese bewältigt werden können.

Diese Unterlage richtet sich an die Geschäftsführung von Krankenhäusern, für die die Umsetzung des § 75c SGB V zum 01.01.2022 verpflichtend wird. Es handelt sich um alle nach § 108 SGB V zugelassenen Krankenhäuser, die nicht bereits zu den KRITIS-Krankenhäusern gehörten, also weniger als 30.000 vollstationäre Fälle pro Jahr behandeln.

[1] Art. 83 DSGVO

Empfehlungen zur Informationssicherheit in KRITIS-Krankenhäusern können dem Branchenspezifischen Sicherheitsstandard B3S Krankenhaus entnommen werden.

# 3 Verstehen, worum geht es

Cybersicherheit und Hackerangriffe sind in aller Munde. Die Auswirkungen mit tagelangen Ausfällen in Wertschöpfungsprozessen, erpresserischen Lösegeldforderungen und hohen Kosten für die Wiederherstellung des Vertrauens haben bereits seit einigen Jahren ihren Einzug in die Tagespresse und Nachrichtensendungen erhalten. Das Thema fristet kein Nischendasein mehr und dies nicht zuletzt auf Grund der Brisanz und Spürbarkeit im täglichen privaten sowie geschäftlichen Umfeld.

Im aktuellen Bericht vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Lage der IT-Sicherheit in Deutschland wird eine Verschärfung der Gefährdungslage für das Gesundheitswesen und besonders auch für Krankenhäuser deutlich. Es gilt, die wichtigsten Handlungsfelder zur Abwehr der Gefahren zu identifizieren und sich kontinuierlich zu verbessern.


***Abbildung 1: Auszug aus dem aktuellen Bericht zur Lage der IT-Sicherheit in Deutschland***

Auf die oberste Leitung eines Unternehmens, hier eines Krankenhauses kommt dabei eine bedeutende Aufgabe zu. Sie trägt die Gesamtverantwortung dafür, dass

Risiken adäquat begegnet wird und muss entscheidende Weichenstellungen vorantreiben, um die damit verbundenen Prozessveränderungen im Haus umzusetzen und ggf. liebgewonnene Freiheiten zu überdenken, wenn nicht sogar zu beschneiden.

| |
|---|
| Informationssicherheit ist dabei kein Produkt oder eine einmalige Sache, sondern ist selbst ein Prozess, der kontinuierliche Aufmerksamkeit auf allen Ebenen erfordert. |

Hierbei ist nicht nur die Benennung eines Informationssicherheitsbeauftragten erforderlich, sondern ein deutliches Commitment auf Führungsebene und eine interdisziplinäre Zusammenarbeit von mehreren Experten aus dem Haus sowie mit externen Lieferanten und Dienstleistern von hoher Bedeutung, um folgende Verbesserungen herbeizuführen:

- Berücksichtigung von Informationssicherheitsaspekten bereits bei der Ausschreibung und Beschaffung von Informationstechnologien, Medizintechnik, Telekommunikationstechnik oder sonstiger mit dem Krankenhausnetzwerk verbundenen Technologien.

- Kontinuierliche Überprüfung von Systemen auf Schwachstellen und deren Behandlung.

- Schaffung von Verantwortlichkeiten und Zuständigkeiten für die Informationssicherheit von Systemen und Anwendungen/Programmen über den gesamten Lebenszyklus hinweg.

- Definition von klaren Zuständigkeiten für Zugangs- und Zugriffsberechtigungen, besonders für den Entzug dessen, auch über die Erstinbetriebnahme hinaus.

- Schaffung von jederzeit aktueller und zugänglicher Transparenz über die System- und Anwendungslandschaft und deren Relevanz in den Prozessen des Krankenhauses.

- Schaffung von Kapazitäten im Haus, um das Zusammenspiel von Tätigkeiten durch Lieferanten und Dienstleistern mit den internen und individuellen Sicherheitsrichtlinien und -maßnahmen zu überwachen und ggf. Nachbesserung einzufordern.

- Etablierung einer Kultur der Übung bei Vorfällen und Ausfällen und des Lernens daraus. Fehler machen ist dabei erlaubt und fördert das Lernen.

- Schulung und Sensibilisierung des Personals zielgerichtet nach den erforderlichen Skills in allen Bereichen.

- Auffinden von Nebenwegen, welche die Sicherheit umgehen und klare Positionierung, dass diese zukünftig verhindert werden müssen.

Diese Liste macht deutlich, dass Informationssicherheit auf allen Ebenen des Unternehmens gelebt werden muss, von der Verwaltung bis zum operativen Personal, vom Mitarbeiter bis zur obersten Führungskraft. Der Erfolg bei der Einführung

eines sog. Informationssicherheitsmanagementsystems (ISMS) ist direkt verbunden mit dem nachhaltigen Einfordern der Umsetzung von Sicherheitsmaßnahmen durch die oberste Leitung.

Da ein ISMS einer ähnlichen Struktur wie dem Qualitätsmanagementsystem oder anderen bekannten Managementsystemen folgt, ergeben sich in dem Zusammenspiel zu bereits dort etablierten Verfahren große Synergieeffekte und Analogien besonders in

- der Lenkung von Dokumenten,
- der Vorbereitung und Durchführung von internen und externen Audits,
- dem Risikomanagement und
- dem Projektmanagement.

# 4 Gefährdungen: Wodurch ist die Informationssicherheit in Krankenhäusern bedroht?

Die Daten und Fakten aus den Sicherheitsreports von Dienstleistern, aber auch aus dem aktuellen Jahresbericht "Die Lage der IT-Sicherheit in Deutschland 2021" des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sind alarmierend. Umfang und Qualität der Angriffe auf Unternehmen haben dramatisch zugenommen und werden mittlerweile weltweit als größtes Unternehmensrisiko eingeschätzt.

> „Der Bericht zur Lage der IT-Sicherheit in Deutschland 2021 zeigt, dass die Gefahren im Cyberraum weiter zunehmen und selbst Bereiche betreffen, die für unsere Gesellschaft elementar sind, wie etwa die Stromversorgung oder die medizinische Versorgung."
>
> Horst Seehofer, Bundesminister Inneres, Bau und Heimat, BSI-Lagebericht 2021

***Abbildung 2: Aus dem BSI-Lagebericht zur IT-Sicherheit in Deutschland 2021***

Auch im Gesundheitsbereich lässt sich eine stetige Zunahme an relevanten Vorfällen beobachten.

## 4.1 Ein typisches Szenario und Beispiele aus dem Krankenhausbereich

Ein Krankenhaus wird Opfer eines Hackerangriffs mit einem Verschlüsselungstrojaner. Kein Zugriff mehr auf Patientenakten, alle digitalen Kommunikationsmittel sind gestört, Operationen müssen verschoben werden, Abmeldung von der Notfallversorgung, Laboranforderungen können nicht mehr gestellt werden, das Krankenhaus und mittlerweile auch Patienten werden erpresst aufgrund zuvor entwendeter Daten.

Eine Situation, die leider gar nicht so abwegig ist. Zumindest zeigen das die zahlreichen Vorfälle aus den letzten Monaten aus Unikliniken und Krankenhäusern.

Alle Vorfälle zogen nicht nur hohe finanzielle Aufwände nach sich, sondern auch enorme personelle Anstrengungen für alle Klinik- und Geschäftsbereiche, nicht nur die IT-Abteilung, zur Bewältigung der Folgen der Angriffe.

### 4.2 Ransomware: die derzeit größte Bedrohung

Die Kombination verschiedener Angriffspunkte, z. B. dem nachfolgend beschriebenen Social Engineering und dem Ausnutzen von Schwachstellen, erlaubt es den Angreifern, oft unbemerkt in die sensiblen IT-Infrastrukturen zu gelangen. In der Regel werden dann in aller Ruhe die Möglichkeiten sondiert und Daten entwendet. Die Angriffe werden vielfach erst dann detektiert, wenn die Daten bereits abgeflossen oder verschlüsselt sind und kein Zugriff mehr möglich ist.

Unzählige, nahezu täglich neu hinzukommende Opfer aus allen Branchen (z. B. öffentliche Verwaltungen, Unternehmen) zeigen, dass es scheinbar ein sehr lukratives Geschäft für Angreifer ist und betont die Bedeutung und Wichtigkeit, Informationssicherheit auszubauen und kontinuierlich weiterzuentwickeln.

### 4.3 Social Engineering: Zunahme von Angriffen

Sicherheitsexperten verzeichnen zudem eine hohe Zunahme an Angriffen aus dem Bereich des Social Engineering. Angreifer erhoffen sich damit schnelle Erfolge bei den unter hohen Zeitdruck arbeitenden MitarbeiterInnen. Schad- oder Phishing-E-Mails mit angeblichen Gehaltssteigerungen oder einer dringenden Aufforderung zu einer Prüfung der Anmeldedaten sind dabei tagtäglich zu beobachten und sind von ungeschulten und wenig sensibilisierten MitarbeiterInnen kaum zu erkennen.

### 4.4 Informationssicherheit: Voraussetzung für erfolgreiche Digitalisierungsstrategie

Die Digitalisierung der Krankenhäuser hat enorm an Fahrt aufgenommen. Jedoch erhöht die zunehmende Digitalisierung auch die Abhängigkeit und vor allem die Komplexität der eingesetzten Informationssysteme. Gleichzeitig ist der Stellenwert der IT innerhalb der Krankenhäuser nicht überall im gleichen Maße gestiegen.

So wird neben gut sensibilisierten Mitarbeiterinnen und Mitarbeitern zunehmend auch das Schwachstellenmanagement im Krankenhaus immer relevanter, da Angreifer meist nicht warten, bis die Gelegenheit besteht, ein notwendiges Sicherheitsupdate einer kritischen Anwendung einzuspielen.

Durch die zunehmende interne und externe Vernetzung der ehemals sehr geschlossenen IT-Infrastruktur eines Krankenhauses, erhöhen sich die Angriffsflächen um ein Vielfaches. Nicht geschlossene Sicherheitslücken, wie beispielsweise im Produkt Microsoft Exchange Mailserver, aber auch bei vielen anderen Anwendungen, inklusive der Medizintechnik, erhöhen das Potential eines erfolgreichen Angriffes. Viele dieser Angriffe hätten mit einem zeitnahen Update verhindert werden können.

## 5 Grundlegendes zum Starter-Paket und seiner Anwendung

Die gesetzliche Vorgabe des § 75c SGB V stellt Krankenhäuser vor enorme Herausforderungen, da Informationssicherheit seitens der Geschäftsführung innerhalb der Organisation u. U. neu bewertet und kurzfristig erste Maßnahmen initiiert werden müssen. Aufgrund der Komplexität und hohen querschnittlichen Durchdringung von Informationssicherheit durch alle Ebenen und Prozesse sollte die Umsetzung dabei anhand eines gestuften und projektierten Vorgehens erfolgen.

Krankenhäuer können die Vorgaben des § 75c SGB V erfüllen, indem sie den branchenspezifischen Sicherheitsstandard (B3S) in der jeweils gültigen Fassung umsetzen. Zur Unterstützung wurden die Anforderungen und Risikoelemente des B3S mit Blick auf die Umsetzbarkeit in Krankenhäusern bewertet und in einen Stufenplan[2] überführt. Ziel ist es, eine einfache Einstiegsmöglichkeit in die Umsetzung von Informationssicherheit aufzeigen. Die einzelnen Stufen bauen dabei aufeinander auf. Wesentlicher Schwerpunkt dieser Dokumentenfassung (Starter-Paket) ist die Umsetzung der Anforderungen der Stufe 1, wobei auf die weiteren Stufen, wo immer notwendig, abgestellt wird. Mit Umsetzung aller Stufen ist die Einhaltung des branchenspezifischen Sicherheitsstandards B3S gegeben.

Eine weitere Alternative zum Einstieg kann für Krankenhäuser auch die LSI-Orientierungshilfe "IT-Sicherheit in Kliniken" und der Maßnahmenkatalog der Arbeitsgruppe "Smart Hospitals" der "Universität der Bundeswehr" sein. Die LSI-Orientierungshilfe kann per E-Mail beim Landesamt für Sicherheit in der Informationstechnik (LSI) Bayern angefragt werden. Der Maßnahmenkatalog steht unter https://www.unibw.de/code/smart-hospitals zum Download bereit.

Weiterhin sollte die Umsetzung durch ein interdisziplinäres Team des Krankenhauses erfolgen, welche alle Bereiche des Krankenhauses einbindet. Daher wird ein projektiertes Vorgehen[3] empfohlen. Als Einstieg können die *Arbeitshilfe „Priorisierung_Anforderungen_§75c.xlsx* sowie die *ChecklisteProjekt_ISMS_v09.xlsx*, in denen auf weitere Unterstützungsdokumente verwiesen wird, dienen.

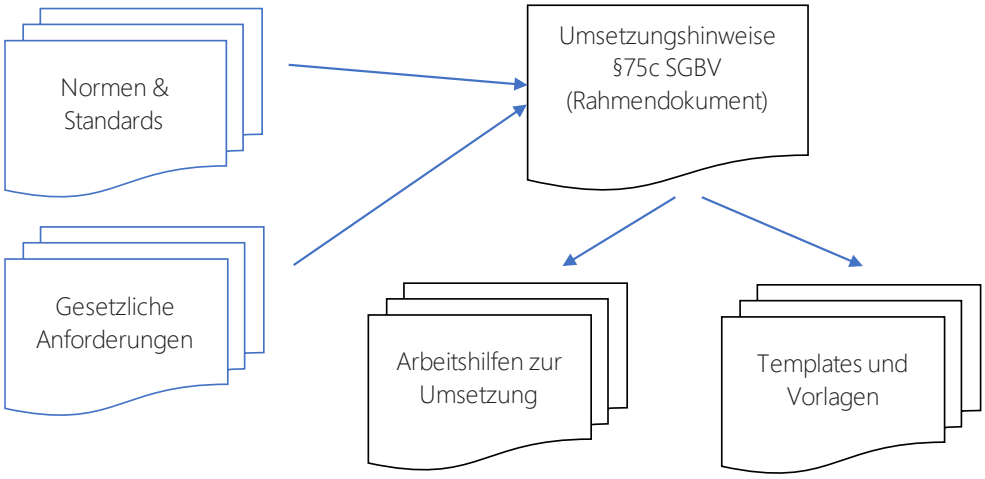


***Abbildung 3: Dokumentenstruktur (Starter-Paket)***

| **Bestandteile „Starter-Paket“** | |
|---|---|
| Umsetzungshinweise/Information | • Dokument „GF-Info-75c-SGB-V“ (dieses Dokument)<br>• ChecklisteProjekt_ISMS |

[2] Arbeitshilfe „Priorisierung_Anforderungen_§75c.xlsx“
[3] ChecklisteProjekt_ISMS_v09.xlsx

| | |
|---|---|
| Arbeitshilfen | • Priorisierung_Anforderungen_§75c<br>• Scope-Definition<br>• Awareness<br>• GAP-Analyse<br>• Notfallmanagement |
| Templates und Vorlagen | • ISB_Bestellung_Intern/Extern<br>• Leitlinie_Informationssicherheit<br>• Risiken_und_Massnahmen<br>• Übersicht_Risiken<br>• Ereigniss_Erfassung |

# 6 Gesetzliche Grundlagen

Seit Verkündung der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) gilt eine Verpflichtung für Krankenhäuser mit einer Fallzahl ab 30.000 vollstationären Fällen pro Jahr, die Umsetzung des Stands der Technik gemäß § 8a BSI-Gesetzes nachzuweisen. Diese sogenannten KRITIS-Krankenhäuser fallen unter die Definition der kritischen Infrastrukturen und müssen besondere Maßnahmen zur Informationssicherheit ergreifen.

Mit Verkündung des Patienten-Daten-Schutz-Gesetzes (PDSG), das am 19.10.2020 in Kraft getreten ist, gilt auch für Krankenhäuser, die nicht zur kritischen Infrastruktur zählen, eine Verpflichtung zum besonderen Schutz ihrer IT-Sicherheit.

**§ 75c IT-Sicherheit in Krankenhäusern**

(1) [1]Ab dem 1. Januar 2022 sind Krankenhäuser verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind. [2]Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung des Krankenhauses oder der Sicherheit der verarbeiteten Patienteninformationen steht. [3]Die informationstechnischen Systeme sind spätestens alle zwei Jahre an den aktuellen Stand der Technik anzupassen.

(2) [1]Die Krankenhäuser können die Verpflichtungen nach Absatz 1 insbesondere erfüllen, indem sie einen branchenspezifischen Sicherheitsstandard für die informationstechnische Sicherheit der Gesundheitsversorgung im Krankenhaus in der jeweils gültigen Fassung anwenden, dessen Eignung vom Bundesamt für Sicherheit in der Informationstechnik nach § 8a Absatz 2 des BSI-Gesetzes festgestellt wurde.

(3) [1]Die Verpflichtung nach Absatz 1 gilt für alle Krankenhäuser, soweit sie nicht ohnehin als Betreiber Kritischer Infrastrukturen gemäß § 8a des BSI-Gesetzes angemessene technische Vorkehrungen zu treffen haben.

## 6.1 § 75c SGB V IT-Sicherheit in Krankenhäusern

Ab dem 01.01.2022 sind nun alle nach § 108 zugelassenen Krankenhäuser verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zu treffen, um den im Gesetz definierten Schutzziele zu erreichen.

**Schutzziele:** Die Schutzziele werden gem. § 75c SGB V wie folgt definiert

- Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit
- weitere Sicherheitsziele für die informationstechnischen Systeme, Komponenten oder Prozesse des Krankenhauses

Diese Schutzziele sind darauf gerichtet, die medizinische Versorgung sowohl im Sinne der Patientensicherheit als auch der Behandlungseffektivität jederzeit mit hoher Kontinuität und unter Berücksichtigung der Sensitivität der Daten zu gewährleisten.

**Verhältnismäßigkeit der Maßnahmen:** Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung des Krankenhauses oder der Sicherheit der verarbeiteten Patienteninformationen steht.

**Frequenz der Anpassung:** Die informationstechnischen Systeme sind spätestens alle zwei Jahre an den aktuellen Stand der Technik anzupassen.

**Prüfmaßstab:** Als einen möglichen Prüfmaßstab für die Erfüllung der Anforderungen des Gesetzes wird der B3S Krankenhaus genannt: „Die Krankenhäuser können die Verpflichtungen nach Absatz 1 insbesondere erfüllen, indem sie einen branchenspezifischen Sicherheitsstandard für die informationstechnische Sicherheit der Gesundheitsversorgung im Krankenhaus in der jeweils gültigen Fassung anwenden, dessen Eignung vom Bundesamt für Sicherheit in der Informationstechnik nach § 8a Absatz 2 des BSI-Gesetzes festgestellt wurde."

## 6.2 Weitere gesetzliche Grundlagen

Weitere gesetzliche Grundlagen, aus der sich Anforderungen zur Informationssicherheit ableiten lassen sind das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTRaG) und die Aktien- und GmbH-Gesetze.

**Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTRaG):** Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich sieht seit seinem Inkrafttreten im Jahr 1998 eine Verpflichtung zur Reduktion von unternehmenskritischen Risiken vor. Zu diesen Risiken fallen auch Risiken, die die Informationssicherheit von Unternehmen gefährden.

**Aktien- und GmbH-Gesetze:** § 93 des Aktien-Gesetzes und § 43 GmbH-Gesetzes definieren, was unter „Sorgfalt des ordentlichen und gewissenhaften Geschäftsleiters" zu verstehen ist. Zu diesen Sorgfaltspflichten lässt sich eine Verpflichtung zur Reduktion von Risiken, die die Informationssicherheit gefährden, ableiten.

### 6.3 Förderung

**Krankenhauszukunftsfonds (Nicht-KRITIS-Krankenhäuser):** Am 29.10.2020 trat das Krankenhauszukunftsgesetz in Kraft. Darin enthalten ist eine Regelung für einen Krankenhauszukunftsfonds. Dazu wurde ein Paragraph in das Krankenhausfinanzierungsgesetzt eingefügt (§ 14a KHG) und die Krankenhausstrukturfondsverordnung mit § 19 Abs. 1 KHSFV um eine Liste von 11 Fördertatbeständen ergänzt. Maßnahmen zur Informationssicherheit sind integraler Bestandteil der Fördertatbestände (FTB) 1 bis 9. Zudem fördert FTB 10 übergreifende Maßnahmen zur Informationssicherheit. Ausgeschlossen sind Maßnahmen, die nach § 12a Absatz 1 Satz 4 Nr. 3 KHG in Verbindung mit § 11 Absatz 1 Nr. 4 lit. a KHSFV förderfähig sind.

**Krankenhausstrukturfonds (KRITIS-Krankenhäuser):** Die Krankenhausstrukturfonds-Verordnung sieht in § 12a Abs. 1 Nr. 4 lit. a) KHSFV eine Förderung von Informationssicherheit vor. Tatsächlich sind nur wenige Krankenhäuser diesbezüglich gefördert worden. So hat das Land NRW eine Förderung von IT-Sicherheit zunächst ausgeschlossen und im Jahr 2021 auf maximal 5 % des für NRW verfügbaren KHSFV-Fördervolumens begrenzt.

## 7 Gap-Analyse

Eine Gap-Analyse (Bestandsaufnahme) erfasst das aktuelle Sicherheitsniveau des Krankenhauses, gemessen an einem anerkannten Maßnahmenkatalog oder Sicherheitsstandard. Die Herausforderung dabei ist, die schützenswerten sicherheitskritischen Gegenstände (Assets) für den Kernprozess der medizinischen Versorgung (Patientenversorgung) zu erfassen und zu bewerten.

Ausgangspunkt für die Erfassung des Anwendungsbereichs und der hier genutzten Assets sollte dabei eine Prozesslandkarte der medizinischen Versorgung im Krankenhaus sein. Die identifizierten Prozesse und Systeme werden anschließend hinsichtlich ihrer Risiken bewertet. Dabei wird insbesondere auf die Sicherstellung der medizinischen Versorgung im Krankenhaus abgestellt.

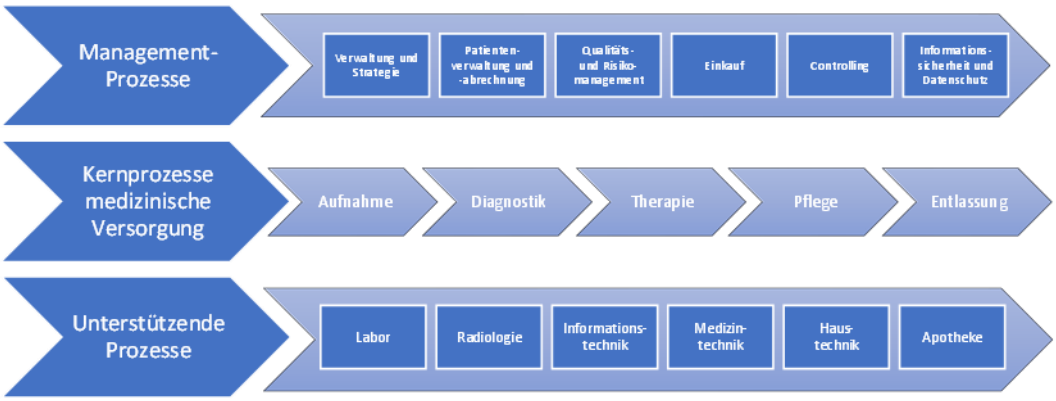


***Abbildung 4: Beispielhafte Prozesslandkarte „Medizinische Versorgung im Krankenhaus“***

Aus dieser Betrachtung lassen sich die schutzwürdigen Objekte (Assets) für die weiteren Schritte ableiten und dokumentieren.

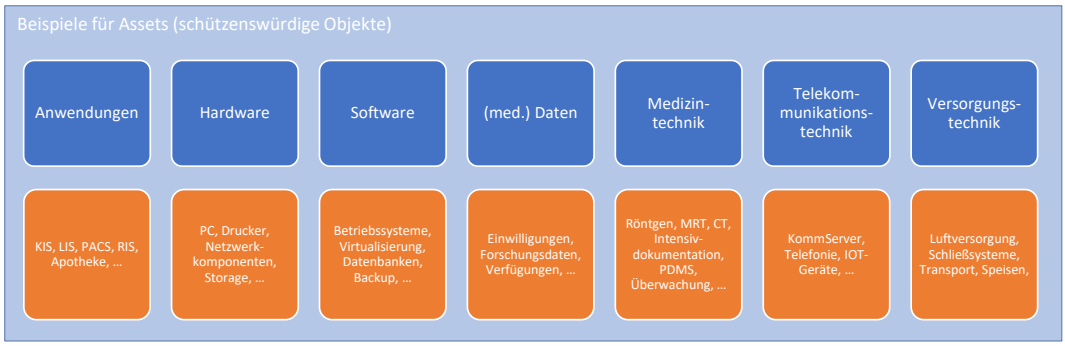


***Abbildung 5: Beispiele für schützenswerte Objekte (Assets) im Krankenhaus***

Die fünf wesentlichen Bestandteile der Gap-Analyse sind nachfolgend dargestellt.


***Abbildung 6: Beispielhafter Ablauf einer Gap-Analyse***

Für eine ausführliche Beschreibung und Beispiele sei auf die Arbeitshilfe „Gap-Analyse“[4] verwiesen.

# 8 Notfall- und Business-Continuity-Management

**Definition Notfall**

Ein Notfall ist ein andauender Ausfall von Prozessen oder Ressourcen mit hohem oder sehr hohem Schaden und verlangt eine besondere Notfallorganisation.

Nichtmedizinische unerwünschte Ereignisse lassen sich beispielsweise in Anlehnung an BSI 200-4 (Community Draft) [5]wie folgt abstufen: Störung, Notfall, Krise und Katastrophe.

Deshalb ist ein gut strukturiertes und getestetes Notfall-Management die Voraussetzung für die Aufrechterhaltung bzw. schnellstmögliche Wiederherstellung, der für die medizinische Patientenversorgung im Krankenhaus erforderlichen Ressourcen und Prozesse.

Auf Grund der kontinuierlichen Steigerung der Hackeraktivitäten sowie der steigenden Abhängigkeit von digital unterstützten Prozessen, auch im Sektor der Gesundheitsversorgung, ist es dringend erforderlich, die Einführung bzw. Verbesserung des Notfall-Management-Prozesse in der Projekt-Priorisierung hoch zu bewerten.

In Abbildung 7 werden die Bausteine des Notfall-Management-Prozesses dargestellt:

[4] Arbeitshilfe_GAP-Analyse
[5] Der BSI-Standard 200-4 wird derzeit erarbeitet. Bis zur Veröffentlichung der finalen Fassung bleibt der BSI-Standard 100-4 gültig. Anschließend erfolgt die Anpassung der Arbeitshilfe Notfallmanagement


***Abbildung 7: Beispielhafte Prozessdarstellung Notfallmanagement***

Durch die Unternehmensleitung muss ein Projekt zu Initiierung bzw. Überarbeitung des Notfallmanagement gestartet werden. Die Unternehmensleitung steht in der Gesamtverantwortung. In diesem Kontext sorgt die Unternehmensleitung für ausreichende Ressourcen, wie Personal, Zeit und Finanzmittel. Ergebnis dieser Phase ist die Leitlinie zum Notfallmanagement.

In der Konzeptphase erfolgen die Durchführung von Business-Impact-Analyse (BIA) und Risikoanalysen (RA) als Grundlage der Entwicklung einer geeigneten Notfallstrategie nebst Notfallvorsorgekonzept.

Die Notfallbewältigung spielt im Alltag der Kliniken eine herausragende Rolle, da sie im Falle eines Notfalls entscheidend für die Wiederherstellung der Ressourcen und der Prozesse ist. Das Notfallhandbuch ist hier das zentrale Dokument, das zu jeder Zeit für die Notfallorganisation im Zugriff sein muss.

Weiterhin sind Übungen und Tests ein wichtiger Bestandteil des Notfallmanagement-Prozesses, um die erarbeiteten Dokumente in der Praxis zu überprüfen und ggf. Anzupassen.

Instrumente der Aufrechterhaltung und kontinuierlichen Verbesserung des Notfallmanagements sind Standards, Selbstüberprüfungen sowie Schulung und Sensibilisierung aller Mitarbeiter.

Eine ausführliche Beschreibung der einzelnen Schritte sowie Beispiele sind der Arbeitshilfe “Notfallmanagement”[6] zu entnehmen.

# 9 Ausblick

Das vorliegende Starter-Paket stellt einen einfachen Zugang zum Thema Informationssicherheit dar und unterstützt Krankenhäuser bei der Bestandsaufnahme. Es zeigt die wichtigsten ersten Schritte zur Absicherung und zu einem systematischen Informationssicherheitsmanagement auf.

Wie bereits erwähnt, ist Informationssicherheit kein Produkt oder eine einmalige Sache, sondern ist selbst ein (Management-)Prozess, der kontinuierliche Aufmerksamkeit auf allen Ebenen erfordert und ständig überprüft und verbessert werden muss.

Insofern ist es folgerichtig, dass auch das Starter-Paket weiterentwickelt und um weitere Arbeitshilfen und Templates ergänzt wird.

Die Arbeitsgruppe “§ 75c SGB V” der DKG wird mit Beginn des Jahres 2022 Inhalte eines Starter-Paket-Plus festlegen und mit der Bereitstellung von weiteren Arbeitshilfen und Vorlagen fortfahren.

[6] Arbeitshilfe_Notfallmanagement

Weitere Schritte im Jahresverlauf könnten Maßnahmen zur Förderung der Kommunikation und zum Erfahrungsaustausch zwischen Krankenhäusern zur Verbesserung der Informationssicherheit sein.

Ein funktionierendes ISMS erhöht die Robustheit insbesondere bei Cyberangriffen und ermöglicht eine schnelle Wiederherstellung der medizinischen Versorgung im Krankenhaus nach einem Schadereignis.

Und nicht zuletzt werden damit auch die Patienteninnen und Patienten geschützt, die sich im berechtigten Vertrauen auf die beste medizinische Versorgung in die Obhut der Krankenhäuser begeben. Informationssicherheit ist auch Patientensicherheit.