Leitlinie

zur

Informationssicherheit

im Bereich Krankenhäuser

Art.-Nr. 1006958/12.11/11718

Dokumenteneigenschaften

Verantwortung	ISBr
Klassifizierung	Intern
Gültigkeitszeit	Unbegrenzt
Überarbeitungsintervall	Jährlich
Nächste Überarbeitung	Oktober 2022
Dateiname	A.0.1_Leitlinie_zur_Informationssicherheit

Dokumentenstatus und Freigabe

Status	Version	Datum	Name und Abteilung/Firma
Erstellt	1.0	23.12.2021	

Dokumentenhistorie

Version	Änderung	Datum	Autor
1.0		23.12.2021	

Inhalt

1. Kontext

1.1 Einleitung

Die Caritas Trägergesellschaft mbH (cts), im Folgenden „cts“, etabliert für folgende Einrichtungen und Gesellschaften ein Managementsystem für Informationssicherheit (ISMS):

- Caritas Klinikum Saarbrücken, in Trägerschaft der Caritas Trägergesellschaft Saarbrücken mbH (cts),
- Vinzentius Krankenhaus Landau GmbH,
- St. Rochus Kliniken in Trägerschaft der cts Reha GmbH für den Bereich Krankenhaus (Neurologie Phase B)

Zentraler Bestandteil eines ISMS ist u. a die Leitlinie zur Informationssicherheit. Das vorliegende Dokument ist die Leitlinie zur Informationssicherheit der cts.

1.2 Geltungsbereich

Der Geltungsbereich dieser Leitlinie ist der Geltungsbereich des ISMS.

Die Richtlinie gilt für alle Mitarbeiterinnen und Mitarbeiter, im folgenden „Mitarbeitende“ im Geltungsbereich.

1.3 Ansprechpartner

Ansprechpartner/in zu allen Fragen dieser Richtlinien ist die/der ISB (ISB).

1.4 Verantwortlichkeiten

Diese Leitlinie hat die Geschäftsführung der cts freigegeben.

2. Stellenwert der Informationstechnologie und Informationssicherheit

Informationssicherheit stellt für die cts ein äußerst wichtiges Qualitätsmerkmal der Datenverarbeitung dar, da alle wesentlichen strategischen und operativen Geschäftsprozesse im Unternehmen durch Informationstechnologie (IT) maßgeblich unterstützt werden.

Ziel der cts ist es, die Daten und IT-Systeme in allen technikabhängigen medizinischen und kaufmännischen Bereichen in ihrer Verfügbarkeit so zu sichern, dass die zu erwartenden Stillstandzeiten und der maximale Datenverlust toleriert werden können. Es gilt die Integrität und Vertraulichkeit von sensiblen Unternehmensdaten und personenbezogenen Daten in ausreichender Weise zu garantieren; hierzu gehören Gesundheitsdaten von Patientinnen und Patienten, Beschäftigtendaten, Kundendaten, Daten von Lieferanten ebenso wie technische Unterlagen. Schadensfälle mit hohen finanziellen Auswirkungen und immaterielle Folgen in Form von Imageschäden für die cts müssen verhindert werden.

Beeinträchtigungen hinsichtlich der Verfügbarkeit der unternehmenseigenen Applikationen können ebenso gravierende Auswirkungen nach sich ziehen wie Unregelmäßigkeiten in Bezug auf die Integrität und Vertraulichkeit der verarbeiteten bzw. benutzten Informationen. Die Verfügbarkeit, Anwendungen und IT-Systeme werden nicht nur durch Externe bedroht, sondern können auch durch interne Schwachstellen gefährdet werden.

3. Unternehmensziele

Die Geschäftsführung der cts hat entschieden, zum Schutz der sensiblen Patientendaten höchstmögliche Sicherheitsmechanismen einzusetzen. Ein unbefugter Zugriff auf diese Daten hätte neben den rechtlichen Konsequenzen einen erheblichen Image- und Vertrauensverlust zur Folge. Dennoch kann es zweckgebunden erforderlich sein, diese Daten nach Maßgabe entsprechender Regularien anderen zugänglich zu machen oder zu übertragen.

Es soll ein angemessenes Sicherheitsniveau für die erforderlichen Schutzbedarfe angestrebt werden. Grundlage für diese Entscheidung war eine Gefährdungsabschätzung über die Werte der zu schützenden Güter sowie des vertretbaren Aufwands an Personal- und Finanzmitteln für Informationssicherheit. Dies bedeutet im Einzelnen:

Bewusstsein für Informationssicherheit:

Um Informationssicherheit gewährleisten zu können, sind angemessene technische und organisatorische Maßnahmen erforderlich. Diese können nur dann hinreichen wirksam sein, wenn alle Beschäftigten die möglichen Gefährdungen für die Informationssicherheit kennen und in ihren Aufgabenbereichen entsprechend verantwortlich handeln. Regelmäßige Fortbildungen zur Informationssicherheit können hierbei unterstützen.

Einhaltung von Gesetzen oder Vorschriften:

Die Maßnahmen für Informationssicherheit sollen auch dazu beitragen, dass die für die cts relevanten Gesetze, Vorschriften und vertraglichen Verpflichtungen eingehalten werden.

Als wichtigste zu beachtende Rahmenbedingungen gelten dabei:

- Patientendatenschutzgesetz (PDSG)
- Kirchliches Datenschutzgesetz (KDG)
- §§ 238 - 239, 257 - 261 Handelsgesetzbuch (HGB)
- § 41 Abs. 1 GmbH-Gesetz (GmbHG)

Informationssicherheit unterstützt damit auch die Einhaltung von Gesetzen und Vorschriften.

Mit dem Patientendatenschutzgesetz hat der Deutsche Bundestag am 3. Juli 2020 auch Änderungen in Bezug auf die Informationssicherheit in Krankenhäusern beschlossen. Der neue §75c Absatz 1 SGB V verpflichtet alle Krankenhäuser in Deutschland, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind. Als kritische Infrastrukturen im Hinblick auf die Versorgung

der Bevölkerung gelten auch Krankenhäuser und hier insbesondere die Dienstleistungen in den Bereichen Aufnahme, Diagnose, Therapie, Unterbringung/Pflege und Entlassung.

Funktionale Aufgabenerledigung:

Die Informationstechnik muss so betrieben werden, dass Geschäftsinformationen hinreichend schnell verfügbar sind. Ausfälle, die zu unangemessenen Terminüberschreitungen führen, sind nicht tolerierbar.

Informationssicherheit unterstützt damit auch eine funktionale Aufgabenerledigung.

Vermeidung materieller Schäden:

Unmittelbare oder mittelbare finanzielle Schäden können durch den Verlust der Vertraulichkeit schutzbedürftiger Daten, die Veränderung von Daten oder den Ausfall einer IT-Anwendung oder eines Systems entstehen.

Informationssicherheit wirkt damit auch materiellen Schäden entgegen.

Wahrung von Persönlichkeitsrechten und Geschäftsgeheimnissen:

Vertraulichkeit und Integrität der für die cts wichtigen Informationen sind zu schützen, unabhängig davon, in welcher Form sie vorliegen. Auch im Umgang mit elektronischen Dokumenten und Informationen ist daher Geheimhaltungsanweisungen strikt Folge zu leisten.

Vermeidung von Ansehensverlust bzw. Imageschaden:

Finanzielle Schäden und ein negatives Image für die cts müssen verhindert werden. Informationssicherheit vermeidet damit Ansehensverlust und Imageschaden der cts.

Kontinuierliche Verbesserung

Ferner strebt die cts die kontinuierliche Verbesserung ihrer Prozesse rund um die Informationssicherheit an.

4. Organisation des Managementsystems für Informationssicherheit

Grundsätzlich sind folgende Verantwortlichkeiten innerhalb des ISMS definiert:

4.1 Geschäftsführung

Die Geschäftsführung der cts ist das oberste Entscheidungsgremium. Sie verabschiedet auf Vorschlag des ISBn diese Informationssicherheitsleitlinie.

Die Geschäftsführung der in 1.1 genannten Gesellschaften und im Falle des Caritas Klinikums Saarbrücken die Kaufmännische und Ärztliche Direktion haben sicherzustellen, dass das ISMS entsprechend dieser Leitlinie umgesetzt und aktualisiert wird und dass die notwendigen Ressourcen verfügbar sind. Der IT-Leitung und der/dem ISBn werden von den Geschäftsführungen ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden, zu informieren und die festgelegten Sicherheitsziele zu erreichen.

Sie haben das ISMS mindestens einmal jährlich zu überprüfen (bzw. immer im Falle von erheblichen Änderungen) und freizugeben. Zweck dieser Überprüfung ist der Nachweis der Angemessenheit, Eignung und Wirksamkeit des ISMS.

Die Gesamtverantwortung für die ordnungsgemäße und sichere Aufgabenerfüllung (und damit die Informationssicherheit) obliegt der Geschäftsführung der in 1.1 genannten Gesellschaften und im Falle des Caritas Klinikums Saarbrücken der Kaufmännischen und Ärztlichen Direktion.

4.2 IT-Leitung

Für die operative IT-Sicherheit des von der cts betriebenen Rechenzentrums ist die Leitung der „Abteilung IT/Rechenzentrum" der cts verantwortlich. Für die operative IT-Sicherheit der in Ziffer 1.1 dieser Leitlinie genannten Einrichtungen und Gesellschaften sind deren IT-Leitungen verantwortlich. Sie sind für den sicheren Betrieb der IT und die Umsetzung geeigneter Sicherheitsmechanismen verantwortlich. In Zusammenarbeit mit der/dem ISBn bringt sie die für die Informationssicherheit spezifischen Aspekte und Anliegen ein und ist für die Umsetzung geeigneter Sicherheitsmaßnahmen zuständig.

Die IT-Leitung stellt sicher, dass die/der ISB frühzeitig in alle IT-Projekte eingebunden wird.

4.3 Informationssicherheitsbeauftragte/r (ISB)

Die/Der ISB ist für die Koordination des Betriebs des ISMS verantwortlich sowie für die Berichterstattung über dessen Leistungsfähigkeit. Sie/Er ist des Weiteren für die Koordination bzw. Umsetzung von Informationssicherheitstrainings und –programmen zur Bewusstseinsbildung (Awareness) für Mitarbeitende verantwortlich. Die/Der ISB definiert, welche sich auf Informationssicherheit beziehende Informationen durch wen und wann kommuniziert werden. Dies gilt sowohl für interne als auch externe Parteien.

Er ist für die Aufstellung und Implementierung des Plans für Training und Awareness verantwortlich, dem alle Personen unterliegen, die eine Rolle im ISMS innehaben.

Die Einführung neuer Anwendungen, Verfahren, Prozesse und Infrastrukturkomponenten bedarf einer Freigabe durch die/den Informationssicherheitsbeauftrage/n. Dabei muss besonderes Augenmerk darauf gerichtet werden, dass durch den Einsatz der neuen Komponenten und Verfahren die Risiken hinsichtlich Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) nicht erhöht werden.

Die/Der ISB berät die Geschäftsführung und die Fachbereiche in Fragen der Informationssicherheit und arbeitet mit der IT-Leitung zusammen. Sie/Er beobachtet laufend die technischen und organisatorischen Fortentwicklungen im Bereich der Informationssicherheit und schlägt in Abstimmung mit der IT-Leitung die notwendigen Maßnahmen vor. Des Weiteren ist sie/er frühzeitig in

alle Projekte einzubinden, um schon in der Planungsphase alle sicherheitsrelevanten Aspekte berücksichtigen zu können.

4.4 IS-Management-Team (ISMS-Team)

Das ISMS-Team setzt sich aus der/dem ISBn, sowie fachkundigen Mitarbeitern für die Administration und für den Betrieb zusammen. Das ISMS-Team hält regelmäßige Treffen ab. Die Protokolle der Sitzungen werden den Geschäftsführungen bzw. den Einrichtungsverantwortlichen der in Ziffer 1.1 genannten Gesellschaften und Einrichtungen zur Kenntnisnahme überlassen.

Das ISMS-Team plant die notwendigen Tätigkeiten zur Aufrechterhaltung und Verbesserung der Informationssicherheit. Weiterhin werden im ISMS-Team Audits geplant und Sicherheitsvorfälle besprochen. Im ISMS-Team werden auch die Dokumente des ISMS laufend überprüft und überarbeitet. Planungen und Änderungen im Anwendungsbereich sind stets im ISMS-Team abzustimmen

4.5 Mitarbeitende

Mitarbeitende sollen sich stets der Bedeutung der Informationssicherheit bewusst sein und aktiv an der Abwehr und Bekämpfung von materiellen und ideellen Schäden mitwirken. Sie sollen verantwortungsbewusst mit den Informationssystemen und den darauf gespeicherten und dort verarbeiteten Daten umgehen und auf die Wahrung von Betriebs- und Geschäftsgeheimnissen achten.

Der Schutz der Integrität, Verfügbarkeit und Vertraulichkeit von Werten unterliegt der Verantwortung der Eigentümer der jeweiligen Werte.

Bei Unregelmäßigkeiten müssen Mitarbeitende unverzüglich die/den Informationssicherheits-beauftragte/n und ihre Vorgesetzten informieren. Es wird erwartet, dass jeder Nutzer von IT-Systemen die vorliegende Informationssicherheitsleitlinie kennt und beachtet.

4.6 Weitere Verantwortlichkeiten

Für alle Informationen, Geschäftsprozesse sowie die unterstützenden informationstechnischen Systeme und Infrastruktureinrichtungen werden Verantwortliche (Informations-, Prozess- und Systemeigentümer, Eigentümer von Zielobjekten) benannt. Diese sind dafür zuständig, die geschäftliche Bedeutung von Informationen und Technik einzuschätzen und darauf zu achten, dass Mitarbeitende dieser Bedeutung entsprechend handeln. Sie verwalten Zugriffsrechte und Autorisierungen in ihrem Zuständigkeitsbereich. Sie sind auch dafür verantwortlich, externen Dienstleistern und Kooperationspartnern die Vorgaben der cts zur Informationssicherheit zur Kenntnis zu geben und deren Einhaltung zu überwachen.

5. Folgen von Zuwiderhandlungen

Beabsichtigte oder grob fahrlässige Handlungen, die Sicherheitsvorgaben verletzen, können finanzielle Verluste bedeuten, Patientinnen und Patienten, Mitarbeitende und Geschäftspartner schädigen und den Ruf der cts gefährden. Bewusste Verstöße gegen verpflichtende Sicherheitsregeln können arbeitsrechtliche und unter Umständen auch strafrechtliche Konsequenzen haben und zu Regressforderungen führen.

6. Weitere Maßnahmen

Ausgehend vom „Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung in Krankenhäusern“ der Deutschen Krankenhausgesellschaft zur Einführung und Aufrechterhaltung eines Managementsystems für Informationssicherheit werden diverse weiterführende Regelungen geschaffen, die dieses ISMS konkretisieren und gleichfalls gültig sind.

Von zentraler Bedeutung dieser weiterführenden Regelungen wird im Rahmen der Einführung eines Managementsystems für Informationssicherheit ein Risikomanagementsystem aufgebaut. Dieses dient dazu Risiken der Informationssicherheit im Geltungsbereich zu identifizieren, unter Berücksichtigung der Informationssicherheitsschutzziele Verfügbarkeit, Integrität und Vertraulichkeit sowie den Risikofaktoren der Patientensicherheit und Behandlungseffektivität zu bewerten und mit angemessenem Aufwand durch geeignete und wirksame Maßnahmen zu reduzieren.

7. Inkrafttreten

Die Richtlinie tritt zum 01.07.2022 in Kraft

Freigegeben durch: Geschäftsführung

Saarbrücken, 13.6.2022

Rafael Lunkenheimer

Heinz Palzer