UNIVERSITÄTSKLINIKUM AUGSBURG

Informationssicherheitsleitlinie

des Universitätsklinikum Augsburg

Informationssicherheitsleitlinie	
Betrifft: Alle Mitarbeiter	
Erst-Erstellung am: 26.08.2019	Erstellt von: Stabsstelle Recht, Datenschutz, Informationssicherheit Informationssicherheitsbeauftragter
Änderung am: 28.11.2024	Änderung / Geprüft von: Informationssicherheitsbeauftragter gez. D. Smolinski gez. H. Jegust
Freigabe ab: siehe Seite 5	Freigabe durch: Gesamtvorstand

Inhaltsverzeichnis

Hinweis: In diesem Dokument wird ausschließlich das generische Maskulinum verwendet, es gilt gleichermaßen für alle Geschlechter.

1. Zweck und Stellenwert der Informationssicherheit

Der Einsatz moderner Informations-, Medizin- und Kommunikationstechnik ist essentielle Voraussetzung für die Aufgabenerfüllung des Universitätsklinikums Augsburg (UKA). Als Universitätsklinikum werden die Prozesse in allen klinischen und administrativen Bereichen, sowie Forschung und Lehre maßgeblich durch die IT-Technologie getragen.

Das UKA ist vom Bundesamt für Sicherheit in der Informationstechnik als sogenannte kritische Infrastruktur klassifiziert. (KRITIS V) Kritischen Infrastrukturen kommt besondere Bedeutung beim Aufrechterhalten der Zivilgesellschaft zu und unterliegt speziellen gesetzlichen und regulatorischen Anforderungen. Dementsprechend gilt es, die Informationstechnologie des UKA vor dem Hintergrund der Vereinbarkeit von Gesundheitsversorgung sowie Forschung und Lehre weiter zu entwickeln und unter dem Gesichtspunkt der kritischen Infrastruktur abzusichern. Hierzu sind Mindeststandards im Informationssicherheitsmanagement etabliert, die u.a. den Regelbetrieb von IT-Infrastruktur gesichert gewährleisten. Das UKA orientiert sich an der international gültigen Norm ISO27001:2022 und dem branchenspezifischen Sicherheitsstandard (B3S) für das Gesundheitswesen in seiner jeweils gültigen Version.

In Abgrenzung zu IT-Sicherheit umfasst Informationssicherheit neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht elektronisch verarbeiteten Informationen. Die allgemeinen Schutzziele Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität der Informationssicherheit beinhalten den Datenschutz. Eine enge Verzahnung von Informationssicherheit und Datenschutz ist daher unabdingbar.

In der Patientenversorgung des Universitätsklinikums Augsburg müssen schutzbedürftige sensible Gesundheitsdaten der Patienten verarbeitet werden. Deswegen kommt den Aspekten Patientensicherheit und Behandlungseffektivität neben den allgemeinen Schutzzielen ebenso eine hohe Bedeutung zu. Auch im Rahmen der übrigen Geschäftsprozesse ist die Verarbeitung von vertraulichen Daten, wie zum Beispiel Personaldaten oder Geschäftsgeheimnissen erforderlich. Die Vertraulichkeit von schutzbedürftigen Daten und die Aufrechterhaltung der Patientenversorgung und wichtiger Geschäftsprozesse sind durch wirksame und angemessene technische und organisatorische Maßnahmen am UKA sichergestellt.

Hierzu ist beim UKA ein Informationssicherheitsmanagementsystem (ISMS) implementiert, das kontinuierlich weiterentwickelt wird. Das ISMS trägt entscheidend dazu bei, dass die wesentlichen Informationen, Geschäftsprozesse sowie die für die Aufgabenerfüllung notwendige Informationstechnik geschützt ist und die Einhaltung der gesetzlichen, regulatorischen und vertraglichen Anforderungen gewährleistet wird. Der Fokus liegt dabei auf dem Schutz von personenbezogenen Daten und insbesondere von Gesundheits-, Forschungs- und Personaldaten.

Die vorliegende Leitlinie definiert die Ziele der Organisation im Bereich der Informationssicherheit unter Berücksichtigung der gesetzlichen Anforderungen. Sie ist mit der Geschäfts- und Unternehmensstrategie abgestimmt und wird bei der Weiterentwicklung der Strategie berücksichtigt. Die Leitlinie wird regelmäßig überprüft ggf. angepasst.

Die zur Gewährleistung der Informationssicherheit und zur Umsetzung der gesetzlichen Anforderungen im Bereich des Datenschutzes erforderlichen Aufgaben und Pflichten gegenüber Patienten, Kunden, Vertragspartnern, Dienstleistern, Behörden und sonstigen Dritten werden in dieser Leitlinie festgelegt. Diese Aufgaben und Pflichten können in Dienstvereinbarungen, Richtlinien und Arbeitsanweisungen weiter konkretisiert werden.

2. Geltungsbereich

Mit dieser Leitlinie werden die elementar gültigen Informationssicherheitsvorgaben für das UKA festgelegt. Diese Vorgaben gelten ebenfalls, wenn das UKA von Dritten Leistungen in Anspruch nimmt oder für Dritte Leistungen erbringt.

Die Aufgaben, Rechte und Pflichten, die der Datenschutzbeauftragte (DSB) gemäß den datenschutzrechtlichen Bestimmungen wahrnimmt, bleiben unberührt.

Verstöße gegen die Vorgaben dieser Leitlinie oder die begleitenden Regelwerke zur Informationssicherheit können eine Schadensersatzpflicht auslösen und darüber hinaus arbeitsrechtliche Konsequenzen bis hin zur Kündigung haben.

3. Ziele der Informationssicherheit

Das wesentliche Ziel aller innerhalb des UKA ergriffenen Informationssicherheitsmaßnahmen ist die Sicherstellung der Verfügbarkeit der kritischen Dienstleistungen der Einrichtung. Die Sicherstellung der qualitativ angemessenen Patientenversorgung nimmt dabei eine herausgehobene Stellung durch Betrachtung der Patientensicherheit und des Behandlungserfolges ein.

1. Daraus ergeben sich die folgenden primären Ziele für das UKA:

- Verhinderung der Gefährdung für Menschenleben in der Patientenversorgung (Schutz der Sicherheit der Patienten),
- die wirksame Behandlung des Patienten unter Benutzung von Informationen und wirksamen Therapiemaßnahmen, ggf. auf Basis eines Informationsaustausches zwischen unterschiedlichen verantwortlichen Organisationseinheiten (Schutz der Effektivität der Behandlung),
- wirtschaftliche und rechtliche Existenzsicherung der Einrichtung (Schutz der Einrichtung).

2. Neben diesen Zielen werden gleichwertig auch die vier elementaren Schutzziele der Informationssicherheit verfolgt. Damit sichergestellt, dass

- die medizinischen Versorgungskapazitäten in angemessener Qualität und Quantität aufrechterhalten werden (Verfügbarkeit),
- keine Daten verfälscht werden, deren Richtigkeit für die Versorgung unbedingt erforderlich ist (Integrität),
- durchgehend die notwendige Information erhalten bleibt, von wem die Daten erfasst wurden (Authentizität),
- keine Daten, deren Bekanntwerden sekundär die Verfügbarkeit und Integrität der IT-Infrastruktur beeinträchtigen oder die Sicherheit eines Patienten gefährden können, unberechtigten Dritten zugänglich werden (Vertraulichkeit).

Das UKA strebt ein angemessenes Informationssicherheitsniveau an. Dies bedeutet einerseits, dass die Kosten der eingesetzten Informationssicherheitsmaßnahmen verhältnismäßig in Bezug auf die Informationen oder IT-Systeme sein müssen.

Andererseits muss die Sicherheit der Patienten stets gewährleistet sein. Die Grundlage der Verhältnismäßigkeitsprüfung bilden die durchgeführten Schutzbedarfsanalysen der einzelnen Anwendungen bzw. der darin verarbeiteten Informationen, die Teil des integrierten Risikomanagements am UKA sind.

Die umzusetzenden Maßnahmen sind einem Spannungsfeld ausgesetzt zwischen

- äußeren und inneren Bedrohungen,
- rechtlichen Rahmenbedingungen,
- wirtschaftlichen Betrachtungen,
- Unternehmenszielen,
- Anforderungen aus Forschung und Lehre,
- Nutzeranforderungen,
- Patientenanforderungen und
- Anforderungen externer Partner.

Als grundlegend wird festgehalten, dass alle Beschäftigten des UKA auf die Einhaltung der einschlägigen Gesetze und vertraglichen Regelungen verpflichtet sind. Negative finanzielle oder immaterielle Folgen für das UKA sind zu vermeiden. Schadensfälle der Informationstechnik mit existenzbedrohenden finanziellen Auswirkungen oder Personenschäden müssen verhindert werden. Alle Beschäftigte – egal in welchem Unternehmensbereich und welcher hierarchischen Funktion – haben sich ihrer Verantwortung beim Umgang mit Informationen und IT Systemen bewusst zu sein und die Strategie zur Informationssicherheit nach besten Kräften zu unterstützen.

4. Grundlagen und Grundsätze des Informationssicherheitsmanagements

Die Aufgaben der Informationssicherheit sind fest in der Organisationsstruktur des UKA verankert. Die Informationssicherheit ist ein übergeordnetes Unternehmensziel, ohne dies können die anderen Ziele des UKA nicht erreicht werden. Der Stand der Informationssicherheit wird mithilfe des PDCA Zyklus (Plan – Do – Check – Act) innerhalb des ISMS kontinuierlich verbessert.

Es ist ein Informationssicherheitsbeauftragter (ISB) bestellt, der die zentrale Anlaufstelle für alle internen und externen Informationssicherheitsthemen bildet und in seiner Funktion direkt an den Vorstand des UKA berichtet.

Der Informationssicherheitsbeauftragte ist disziplinarisch der Stabsstellenleitung Stabsstelle Recht, Datenschutz und Informationssicherheit unterstellt.

Der Vorstand wird zudem in einem jährlichen Bericht des Informationssicherheitsbeauftragten über den Stand der Umsetzung der Informationssicherheitsziele, besonderer Vorkommnisse und weiterer erforderlicher Maßnahmen informiert.

Die Mitarbeiter werden regelmäßig zur aktiven Umsetzung und Notwendigkeit der Informationssicherheit sensibilisiert und geschult. Diese Maßnahmen werden durch den ISB und DSB gesteuert.

5. Verantwortungsbereich

Die Gesamtverantwortung für die Informationssicherheit und den Datenschutz obliegt dem Gesamtvorstand. Die Führungskräfte sind verpflichtet, die Vorgaben zur Informationssicherheit umzusetzen und zu überwachen. Alle Mitarbeiter sind zur Einhaltung der Vorgaben verpflichtet.

Sowohl der ISB als auch der DSB werden von allen Führungskräften bei der Erfüllung ihrer Aufgaben ausreichend unterstützt.

6. In-Kraft-Treten

Diese Leitlinie tritt mit sofortiger Wirkung in Kraft.

Augsburg, den 01.12.2024

gez. i.V. Dr. M. Wehler	gez. i.V. Dr. R. Linné	gez.	gez.
Prof. Dr. Klaus Markstaller	Michael Bungarten	Susanne Arnold	Prof. Dr. Martina Kadmon
Ärztlicher Direktor und Vorstandsvorsitzender	Kaufmännischer Direktor	Pflegedirektorin	Dekanin