Leitlinie zur Informationssicherheit am Klinikum rechts der Isar der Technischen Universität München (MRI) [1]

Das MRI erbringt Spitzenleistungen zum Wohl der Patienten. Dazu ist eine moderne und innovative Informationsverarbeitung essentielle Grundlage. Um diese Leistungen jederzeit verlässlich und auf höchstem Niveau erbringen zu können, ist es notwendig, die jederzeitige Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der verarbeiteten Informationen und der dazu notwendigen Systeme sicherzustellen. Darüber hinaus müssen die am MRI verarbeiteten Forschungs- und Patientendaten bestmöglich vor Missbrauch und unautorisierter Nutzung geschützt werden.

Um diesen Gegebenheiten Rechnung zu tragen und eine Informationssicherheit auf höchstem Niveau sicherzustellen, verabschiedet der Vorstand des MRI als Bestandteil der Managementstrategie des MRI diese Leitlinie.

1. Grundsätze und Geltungsbereich

Die Leitlinie zur Informationssicherheit bildet die Grundlage für einen kontinuierlichen Verbesserungsprozess. In ihr werden die Rahmenbedingungen für das Informationssicherheitsmanagement definiert. Sie bildet die Basis der Informationssicherheitsstrategie und wird durch Informationssicherheitsrichtlinien für einzelne Bereiche konkretisiert. Die Informationssicherheit ist damit integraler Bestandteil der Organisation des MRI und aller Geschäftsprozesse.

Die Leitlinie gilt für alle Mitarbeiter des MRI sowie für alle am MRI eingesetzten Verfahren. Alle anderen Personen, die für das MRI Leistungen erbringen oder dort Tätigkeiten ausüben, ohne direkt am MRI beschäftigt zu sein, externe Dienstleister und Auftragnehmer sind über das Regelwerk zur Informationssicherheit zu informieren und auf die Einhaltung desselben zu verpflichten.

2. Ziele

Die Informationssicherheit umfasst alle organisatorischen, technischen und personellen Maßnahmen, die geeignet sind, das Risiko der Verletzung der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Informationen zu minimieren. Informationen können dabei sowohl auf Papier, in digitaler Form oder auch in den Köpfen der Mitarbeiter vorliegen.

Die zum Schutz dieser Informationen getroffenen Maßnahmen dienen der Erfüllung der gesetzlichen, vertraglichen und betriebliche Vorgaben unter Berücksichtigung des Stands der Technik bei gleichzeitiger Wahrung der wirtschaftlichen Angemessenheit.

3. Verantwortlichkeiten

Allen am MRI tätigen Personen muss die Bedeutung der Informationssicherheit bewusst sein. Sie haben die Vorgaben und Regelungen des MRI zur Informationssicherheit zu beachten und ihr Handeln in der täglichen Arbeit entsprechend daran auszurichten. Vorfälle, die die Vertraulichkeit, Integrität, Verfügbarkeit oder Authentizität von Informationen beeinträchtigen oder verletzen, sind an den Informationssicherheitsbeauftragten (ISB, siehe unter Ziffer 5.1) zu melden.

[1] *Aus Gründen der leichteren Lesbarkeit wird auf eine geschlechtsspezifische Differenzierung verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung für alle Geschlechter.*

Beispiele für derartige Vorfälle sind:

- Vorfälle, bei denen aufgrund des Ausfalls von IT-Systemen der Betrieb des MRI eingeschränkt werden muss.
- Die unberechtigte Kenntnisnahme und Veränderung von Informationen.
- Der Verlust oder Diebstahl von elektronischen Geräten, auf denen schützenswerte Daten gespeichert sind.
- Einbruch bzw. Einbruchsversuche in IT-Systeme des MRI.
- Die Infektion von IT-Systemen des MRI mit Schadcode (Computerviren).
- Das Ausspähen, die Weitergabe und die unberechtigte Nutzung von Zugangsdaten für IT-Systeme des MRI.

Die Gesamtverantwortung für die Belange der Informationssicherheit trägt der Vorstand des MRI. Er legt das für das MRI notwendige Sicherheitsniveau fest und verabschiedet die Informationssicherheitsrichtlinien sowie das Informationssicherheitskonzept.

4. Bezug zu Gesetzen

Aufgrund seiner Bedeutung in der Patientenversorgung ist das MRI als Kritische Infrastruktur im Bereich Gesundheitswesen eingestuft und unterliegt den Vorgaben des IT-Sicherheitsgesetzes. Weitere gesetzliche Vorgaben für den Bereich der Informationssicherheit ergeben sich unter anderem aus der EU-Datenschutzgrundverordnung, der Medizinprodukte-Betreiberverordnung sowie dem Bayerischen Krankenhausgesetz.

5. Organisation

5.1. Informationssicherheitsbeauftragter

Der Vorstand des MRI ernennt einen Informationssicherheitsbeauftragten (ISB/CISO), der der Stabsstelle Datenschutz der Kaufmännischen Direktion zugeordnet ist. Dieser ist Ansprechpartner für alle Fragen und Belange der Informationssicherheit und erreichbar unter informationssicherheit@mri.tum.de.

Der ISB berichtet direkt an den Vorstand des MRI. Neben seiner Beratungsfunktion koordiniert und steuert der ISB den Aufbau und Betrieb der Informationssicherheitsorganisation und des dazugehörigen Informationssicherheitsmanagementsystems (ISMS). Meldungen zu Sicherheitsvorfällen sind an ihn zu richten.

5.2. Informationssicherheits-Managementteam

Das Informationssicherheits-Managementteam (ISMT) entwickelt gemeinsam mit dem ISB und DSB des MRI das Informationssicherheitskonzept und unterstützt und berät den ISB bei der Umsetzung und Steuerung des Informationssicherheitsprozesses und dem Aufbau und Betrieb des ISMS.

Mitglieder des ISMT sind:

- Der ISB und DSB
- Der Leiter GB Informationstechnologie
- Der Leiter Stabsstelle Datenschutzmanagement
- Der Medizintechnik-IT-Risikomanager
- Der Leiter der Stabsstelle Qualitäts- und Risikomanagement

Bei Bedarf können zur Unterstützung des ISMT weitere Sachverständige zu den Sitzungen als Berater eingeladen werden.

5.3. Stellvertretungen

Für alle unter 5.1 bis 5.2 genannten verantwortlichen Funktionen sind Vertretungen einzurichten.

6. Zusammenarbeit

Die Arbeitsbereiche der Informationssicherheit und des Datenschutzes weisen hinsichtlich der unter Nr. 2 genannten Ziele Überlappungen auf. Der vom Vorstand des MRI benannte DSB und ISB, sowie das Datenschutzmanagementteam arbeiten daher vertrauensvoll zusammen und tauschen sich regelmäßig aus. Das zu erstellende Sicherheitskonzept wird gemeinsam erarbeitet und die daraus resultierenden Maßnahmen miteinander abgestimmt.

Redundanzen innerhalb der verschiedenen Managementsysteme am MRI sollen vermieden werden. Synergien, die sich aus dem einheitlichen Aufbau der am MRI eingesetzten ISO-Normen ISO 9001 (Qualitätsmanagement) und ISO 31000 (Risikomanagement) ergeben, sollen genutzt werden. Daher erfolgt der Aufbau des ISMS nach ISO 27001 in enger Abstimmung und Zusammenarbeit mit der Stabsstelle Qualität- und Risikomanagement.

7. Ressourcen

Für die sich aus dieser Leitlinie ergebenden Aufgaben werden dem ISB und dem ISMT die notwendigen personellen und finanziellen Ressourcen durch den Vorstand des MRI zur Verfügung gestellt. Den beteiligten Personen der unter Punkt 5 genannten Informationssicherheitsorganisation werden entsprechende Qualifizierungen und Fortbildungen, die zur Erfüllung ihrer Aufgaben im Bereich Informationssicherheit notwendig sind, auf Kosten des MRI ermöglicht.

8. Kontinuierliche Verbesserung

Um der kontinuierlich erfolgenden Veränderung der Informationssicherheitsorganisation im MRI Rechnung zu tragen, werden alle Regelungen dieser Leitlinie und der ihr untergeordneten Regelungen einem kontinuierlichen Verbesserungsprozess unterworfen und in regelmäßigen Abständen, mindestens einmal jährlich, überprüft und bei Bedarf angepasst.

9. Inkrafttreten

Die vorstehende Leitlinie tritt zum 01.05.2024 in Kraft.

Dr. Martin Siess
Ärztlicher Direktor
Vorstandsvorsitzender

Marie le Claire
Kaufmännische Direktorin

Silke Großmann
Pflegedirektorin

Univ.-Prof. Dr. Stephanie E. Combs
Dekanin der TUM School of Medicine and Health