Leitlinie Informationssicherheit

FB_5_5002

Stellenwert der Informationsverarbeitung

Für das Klinikum der Universität München (KUM) als leistungsstarkes Universitätsklinikum spielt die Informationsverarbeitung eine wesentliche Rolle, und unterstützt nahezu alle Prozesse maßgeblich, wie etwa medizinische Versorgung, Forschung und Lehre, administrative Aufgaben, Finanzmanagement und Personalverwaltung.

Ein Ausfall von IT- und Kommunikationssystemen muss kurzfristig behoben bzw. kompensiert werden können, auch in Teilbereichen dürfen die klinischen und verwaltungstechnischen Prozesse nicht zusammenbrechen. Nicht nur die Verfügbarkeit, sondern auch die Integrität der Daten aus Forschung und Krankenversorgung ist von existentieller Bedeutung. Schließlich muss darüber hinaus sichergestellt werden, dass diese Daten nicht an Unberechtigte gelangen.

Der Vorstand unterstützt alle notwendigen Maßnahmen zur Informationssicherheit und hat die vorliegende Leitlinie zur Informationssicherheit beschlossen, um durch eine sichere IT-Nutzung und sicheren IT-Betrieb am KUM sowohl Patientenversorgung als auch Forschung und Lehre kontinuierlich auf höchstem Niveau betreiben zu können und gleichzeitig die Verwaltung optimal zu unterstützen.

Geltungsbereich und übergreifende Ziele

Die vorliegende Leitlinie bestimmt die Prinzipien zur Ausgestaltung der Informationssicherheit am KUM. Sie ist unmittelbar an alle Organisationseinheiten, Mitarbeiterinnen und Mitarbeiter des KUM gerichtet.

Die in dieser Leitlinie beschriebenen Grundprinzipien sind ebenfalls konsequent auf alle Beziehungen zu juristisch Dritten anzuwenden, die z.B. über Lieferanten-, Dienstleistungs- oder Kooperationsbeziehungen Zugang zu Informationen des Klinikums erlangen.

Die Realisierung von angemessener Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität aller verarbeiteten Informationen sowie Patientensicherheit und Behandlungseffektivität sind, ebenso wie die Gewährleistung des Datenschutzes und die Einhaltung aller gesetzlichen und rechtsrelevanten Regelungen, grundlegende Ziele der Informationssicherheit.

Dabei bezeichnet

- **Verfügbarkeit**, dass die relevanten Informationen, Anwendungen und IT-Systeme für Berechtigte im vorgesehenen Umfang und in angemessener Zeit nutzbar sind.
- **Vertraulichkeit**, dass die Informationen ausschließlich von denen genutzt werden, die sie auch wirklich benötigen. Neben der Sicherung gegen Informationsdiebstahl von außen beinhaltet dieses Ziel auch geeignete Berechtigungskonzepte für den korrekten Zugriff auf Informationen innerhalb des KUM.

Erstellung:

Hülle, Frank

Prüfung:

26.05.2020 Kruber, Kurt Dr.

Freigabe:26.05.2020 Huppertz, Marcus
04.06.2020 Zendler, Markus
05.06.2020 Jauch, Karl-Walter Prof. Dr.

Leitlinie Informationssicherheit
FB_5_5002

- **Integrität**, dass Veränderungen an sensiblen Informationen durch absichtliches Handeln genauso wie durch inkorrekte Verarbeitungsprozesse verhindert werden. Die Unverfälschtheit und Vollständigkeit von Informationen, Anwendungen und IT-Systemen muss sichergestellt und überprüfbar sein.
- **Authentizität**, dass sichergestellt ist, von wem die jeweilige Information stammt.
- **Patientensicherheit**, die Freiheit von unvermeidbaren Risiken einer physischen Verletzung oder eines Schadens an der Gesundheit von Menschen. Dies schließt auch die Vermeidung einer nachhaltigen psychischen Belastung ein.
- **Behandlungseffektivität**, dass die wirksame Behandlung des Patienten unter Benutzung von Informationen und wirksamen Therapiemaßnahmen, ggf. auf Basis eines Informationsaustausches zwischen unterschiedlichen verantwortlichen Organisationseinheiten sichergestellt ist.

Insbesondere für IT-Systeme, Daten und Informationen im direkten Behandlungskontext von Patienten gelten maximale Anforderungen an die Verfügbarkeit, Integrität und Vertraulichkeit, Stillstandzeiten sind insbesondere im Kontext der Patientenbehandlung nur in einem sehr geringen Maße akzeptabel, da diese negative Auswirkungen auf den Behandlungsprozess haben. Der Vorstand ist sich jedoch bewusst, dass es keine 100% sicheren und verfügbaren IT- und Kommunikationssysteme gibt, so dass technische Absicherungsmaßnahmen durch organisatorische Prozessabsicherungsmaßnahmen begleitet werden.

Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der zu schützenden Informationen und IT-Systeme stehen. Ziel ist es, durch die grundlegenden Maßnahmen die Sicherheit der Patienten zu erhöhen bzw. Gefährdung der Patienten zu verhindern. Daneben sollen Schadensfälle mit hohen finanziellen und datenschutzrechtlichen Auswirkungen sowie Schäden in Bezug auf die öffentliche Wahrnehmung des Universitätsklinikums verhindert werden.

Ein Information Security Management System (ISMS) ist aufzubauen und fortzuschreiben. Das ISMS soll die kontinuierliche Überwachung und Verbesserung der Informationssicherheit am KUM gewährleisten.

Leitsätze

Die nachfolgenden Leitsätze bestimmen die Gestaltung der Informationssicherheit am KUM.

- Die vorrangigen Kriterien für geeignete Sicherheitsmaßnahmen sind deren Wirksamkeit in Verbindung mit einem tragbaren Restrisiko. Dabei werden insbesondere die wirtschaftliche Angemessenheit, die Ergonomie sowie die größtmögliche Handlungsfreiheit für Lehre und Forschung berücksichtigt.
- Gesetzliche und vertragliche Anforderungen sowie Selbstverpflichtungen, wie die zur guten wissenschaftlichen Praxis, werden erfüllt.
- Die Verfügbarkeit der IT, die für die ordnungsgemäße Durchführung insbesondere der Patientenversorgung, Forschung und der IT-gestützten Verwaltungsprozesse erforderlich ist, wird gewährleistet.
- Jeglicher Umgang mit Daten und Informationen entspricht von der Erhebung bis zur Löschung den Anforderungen der Informationssicherheit. Sämtliche IT-Systeme werden in angemessener Weise und Umgebung betrieben.

Leitlinie Informationssicherheit
FB_5_5002

- Es gibt eine geordnete Vorgehensweise für die Inbetriebnahme und die Änderung von IT-Verfahren. In diesem werden die Belange der Informationssicherheit in angemessenem Umfang berücksichtigt.
- Anwenderinnen und Anwender haben ein Grundverständnis für die Belange der Informationssicherheit. IT-Systeme werden durch Personal betreut, welches über die erforderliche Fachkunde verfügt.
- Das Angebot regelmäßiger und anlassbezogener Schulungen gehört zum Selbstverständnis eines geordneten Informationssicherheitsprozesses.
- Die Wirksamkeit und Angemessenheit der Sicherheitsmaßnahmen wird regelmäßig überprüft und dokumentiert. Dies schließt die vorliegende Leitlinie zur Informationssicherheit ein.
- Verletzungen der Informationssicherheit werden kommuniziert und dokumentiert, so dass schnell, angemessen und nachhaltig auf sie reagiert werden kann.

Zentrale Angebote unterstützen die Umsetzung der Leitsätze.

Organisationsstruktur

Es ist vom Betreiber (Vorstand) ein Informationssicherheitsbeauftragter zu benennen und eine geeignete Informationssicherheits-Organisationsstruktur zu schaffen.