1. STELLENWERT DER INFORMATIONSSICHERHEIT

Für die KKRN Katholisches Klinikum Ruhrgebiet Nord GmbH (KKRN GmbH) als Arbeitgeber im Gesundheitswesen mit ca. 3.000 Mitarbeitenden im nördlichen Ruhrgebiet spielt die Informationstechnologie (IT) eine tragende Rolle und wirkt unterstützend bei allen Prozessen der Patientenversorgung, egal ob im ambulanten, stationären, elektiven oder Notfallbereich. Administrative Aufgaben, wie zum Beispiel das Finanzmanagement, Personalverwaltung, Einkauf und Controlling sind ohne IT nicht effizient zu gestalten.

Für die KKRN GmbH als sogenannte kritische Infrastruktur dürfen Ausfälle in der Verfügbarkeit von IT-Systemen nicht die Versorgungssicherheit und das Patientenwohl gefährden. Ausfälle sind nicht tolerierbar und müssen jederzeit durch Ersatzverfahren kompensiert werden können. Negative Auswirkungen auf den Behandlungsprozess müssen vermieden werden. Auch in Teilbereichen dürfen die klinischen und verwaltungstechnischen Prozesse nicht vollständig zum Erliegen kommen.

Nicht nur die Verfügbarkeit, sondern auch die Integrität der Daten (Korrektheit, Vollständigkeit und Konsistenz von Daten) zur Krankenversorgung ist von existentieller Bedeutung, um den Behandlungserfolg und die Patientensicherheit sicherzustellen.
Weiterhin muss gewährleistet sein, dass die besonderen sensiblen Daten unserer Patienten und Mitarbeitenden nicht an Unberechtigte gelangen (Vertraulichkeit).

Die Geschäftsführung unterstützt alle notwendigen Maßnahmen zur Informationssicherheit und hat die vorliegende Leitlinie zur Informationssicherheit beschlossen, um durch eine sichere IT-Nutzung und einen sicheren IT-Betrieb bei der KKRN GmbH sowohl Patientenversorgung als auch Lehre kontinuierlich auf höchstem Niveau betreiben zu können und die Prozesse in der Verwaltung zu unterstützen.

Geltungsbereich und übergeordnete Ziele
Die Leitlinie zur Informationssicherheit richtet sich an alle Mitarbeitende aller Organisationseinheiten, sowohl in der KKRN GmbH als auch bei den Tochtergesellschaften der KKRN GmbH.

Die in dieser Leitlinie beschriebenen Grundprinzipien werden auf alle Beziehungen zu Dritten angewendet, welche z. B. über Lieferanten-, Dienstleistungs- oder Kooperationsbeziehungen Zugang zu Informationen des Klinikverbundes erlangen.

Die Realisierung von angemessener Verfügbarkeit, Vertraulichkeit und Integrität aller verarbeiteten Informationen, sowie die Gewährleistung des Datenschutzes und damit die Sicherstellung der Behandlungseffektivität und der Schutz des Patientenwohls bei informationsverarbeitenden Prozessen, sind neben der Einhaltung aller gesetzlichen und rechtsrelevanten Regelungen die grundlegenden Ziele der Informationssicherheit innerhalb der KKRN GmbH.

Dabei bezeichnet:

- Verfügbarkeit, dass die relevanten Informationen, Anwendungen und IT-Systeme für Berechtigte im vorgesehenen Umfang mit vertretbaren Antwortzeiten der Systeme nutzbar sind.
- Vertraulichkeit, dass die Informationen ausschließlich von denen genutzt werden können, die diese zur Aufgabenerfüllung benötigen. Der Schutz vor Informationsdiebstahl von außen sowie geeignete Berechtigungskonzepte für den Zugriff auf Informationen innerhalb der KKRN GmbH werden durch Informationssicherheit umgesetzt.

- 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 nachvollziehbar sein.

Für IT-Systeme, Daten und Informationen im direkten Behandlungskontext von Patienten gelten maximale Anforderungen.

Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der zu schützenden Informationen und IT-Systeme stehen.

Ziel ist es, durch geeignete Maßnahmen das Patientenwohl und den Behandlungserfolg zu jeder Zeit sicherzustellen.

Informationssicherheitsvorfälle mit hohen finanziellen und datenschutzrechtlichen Auswirkungen sowie Schäden in Bezug auf die Reputation der KKRN GmbH sollen verhindert werden.

Ein Informationssicherheitsmanagementsystem (ISMS) ist aufgebaut und wird fortgeschrieben. Das ISMS soll die kontinuierliche Überwachung und Verbesserung der Informationssicherheit innerhalb der KKRN GmbH gewährleisten. Damit kommt die KKRN GmbH den gesetzlichen Anforderungen aus dem IT-Sicherheitsgesetz (IT-SiG), der Verordnung für kritische Infrastrukturen (KRITIS V) und dem Sozialgesetzbuch V nach.

2. LEITSÄTZE

Die nachfolgenden Leitsätze bestimmen die Gestaltung der Informationssicherheit in der KKRN GmbH:

- Die Kriterien für angemessene Sicherheitsmaßnahmen sind deren Wirksamkeit in Verbindung mit einem tragbaren Restrisiko. Dabei werden insbesondere die wirtschaftliche Angemessenheit, die technische und die organisatorische Umsetzbarkeit berücksichtigt.

- Gesetzliche und vertragliche Anforderungen sowie Selbstverpflichtungen gegenüber Dritten werden erfüllt.

- Die Verfügbarkeit der IT-Systeme, die für die ordnungsgemäße Durchführung insbesondere der ambulanten und stationären Patientenversorgung und der IT-gestützten Verwaltungsprozesse erforderlich ist, wird gewährleistet. Neben technischen Absicherungsmaßnahmen sind organisatorische Maßnahmen etabliert.

- Jegliche Informationsverarbeitung entspricht von der Erhebung bis zur Löschung den Anforderungen der Informationssicherheit des kirchlichen Datenschutzgesetzes, der DSVGO und dem BDSG. Sämtliche IT-Systeme werden in angemessener sicherer Weise und Umgebung betrieben.

- Es gibt eine geordnete Vorgehensweise für die Inbetriebnahme und die Änderung von IT- Systemen und Verfahren der Informationsverarbeitung. Hierbei wird die Informationssicherheit stets in angemessenem Umfang berücksichtigt.

- Anwenderinnen und Anwender haben ein Grundverständnis für die Belange der Informationssicherheit und werden regelmäßig für diese sensibilisiert. IT-Systeme werden ausschließlich durch hochqualifiziertes Personal mit der erforderlichen Fachkunde betreut.