UKS
Universitätsklinikum
des Saarlandes

Leitlinie zur Informationssicherheit des Universitätsklinikums des Saarlandes

Die klinische Versorgung unserer Patienten erfordert zunehmend die Verwendung von Verfahren und Abläufen, die sich auf Möglichkeiten der Informationstechnik (IT) stützen. Daher kommt der Sicherheit dieser Infrastruktur eine grundsätzliche und strategische Bedeutung zu. Auf Grund der sich schnell weiter entwickelnden technischen Möglichkeiten und der Heterogenität der IT-Landschaft, die zunehmend vernetzte Medizingeräte integriert, muss ein kontinuierlicher IT-Sicherheitsprozess realisiert werden, der die Verfügbarkeit der IT-Infrastruktur sicherstellt.

Als Krankenhaus verarbeiten wir besonders schützenswerte Daten unserer Patienten. Nicht erst durch das Inkrafttreten der DSGVO sind wir daher gefordert, technische und organisatorische Maßnahmen zu ergreifen, um diese Informationen zu schützen und zu verhindern, dass Unbefugte Einsicht erlangen oder Daten manipulieren. Die Vertraulichkeit, Integrität und Authentizität der im Klinikum verarbeiteten Informationen sind ein hohes, schützenswertes Gut.

In dieser Leitlinie zur Informationssicherheit (Informationssicherheitsleitlinie, ISL) werden für alle Einrichtungen des UKS, insbesondere für die für die schnelle und effiziente Krankenversorgung notwendigen Bereiche, die grundlegenden Ziele der Informationssicherheit festgelegt.

Stellenwert der Informationssicherheit

Sowohl für interne Prozesse der Verwaltung als auch für die sichere Versorgung unserer Patienten ist es unumgänglich, dass die für die Prozesse benötigten Informationen vollständig, korrekt und schnell an dem Ort zur Verfügung stehen, an dem sie benötigt werden. Dies ist heutzutage ohne eine moderne Informationstechnik (IT) nicht möglich. Da im UKS sehr sensible Daten unserer Patienten verarbeitet werden, müssen diese ausreichend geschützt werden und nur für die im direkten Behandlungs- bzw. Abrechnungsprozess involvierten Mitarbeiter zugänglich sein.

Informationssicherheit hat als Ziel den Schutz von Informationen jeglicher Art und Herkunft. Dabei können Informationen sowohl auf Papier, in Rechnersystemen oder auch in den Köpfen der Nutzer gespeichert sein[1]. Für das UKS ist daher die Informationssicherheit ein unverzichtbarer Grundwert, für den der Vorstand die Verantwortung übernimmt.

Geltungsbereich

Diese Leitlinie gilt für alle Einrichtungen des Universitätsklinikums des Saarlandes inkl. den Tochterunternehmen sowie die vom UKS betreute IT-Infrastruktur der medizinischen Fakultät auf dem Campus in Homburg.

Sicherheitsstrategie

Durch die aktuelle Gesetzgebung wie die Datenschutz-Grundverordnung (DSGVO), das IT-Sicherheitsgesetz und die KRITIS-Verordnungen leisten EU und Bundesregierung ihren Beitrag dazu, die personenbezogenen Daten und digitalen Infrastrukturen zu sichern. Da das UKS zu den kritischen Infrastrukturen im Gesundheitswesen gehört muss es auch diese gesetzlichen Vorschriften einhalten. Hierfür wurde ein umfangreiches Informationssicherheitsmanagementsystem (ISMS) etabliert.

Bei dem ISMS handelt es sich um einen kontinuierlichen Prozess, um mit wirtschaftlichem Ressourceneinsatz ein Höchstmaß an Sicherheit zu erreichen und verbleibende Restrisiken zu minimieren. Das ISMS orientiert sich an dem Branchenspezifischen Sicherheitsstandard (B3S) für das Gesundheitswesen, der ISO-Norm 27001 sowie dem IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

[1] Quelle: BSI-Standard 200-1

Sicherheitsziele

Primäre Aufgabe eines Krankenhauses ist es, durch ärztliche und pflegerische Hilfeleistungen Krankheiten, Leiden oder körperliche Schäden festzustellen und durch eine Behandlung zu heilen oder zumindest zu lindern. Die Informationssicherheit im UKS soll helfen, folgende Ziele umzusetzen:

- gesetzliche Vorschriften einzuhalten
- die Patientensicherheit und Behandlungseffektivität zu gewährleisten
- Dienstleistungen sicher, zuverlässig und vertrauenswürdig zu erbringen
- die Auswirkungen eines Schadensfalls auf ein vertretbares Maß zu reduzieren
- Ansehens- und Vertrauensverlust zu vermeiden.

Hierfür müssen – bei gleichzeitiger Sicherstellung der Vertraulichkeit und Integrität der verarbeiteten Informationen – alle für den Behandlungsprozess benötigten Infrastrukturen verfügbar sein.

Vertraulichkeit

Personenbezogene Daten sind ein hohes Gut, welches ausreichend geschützt werden muss. Hierzu gehören neben den Informationen zu unseren Patienten auch die Daten unserer Mitarbeiter. Die Patienten sollen sich vertrauensvoll ans UKS zum Zweck einer Untersuchung und Behandlung wenden können, ohne befürchten zu müssen, dass die Informationen, die sie zum Zweck der Behandlung offenlegen, zu ihrem Schaden oder Nachteil genutzt werden. Daher setzt sich das UKS das Ziel, die Vertraulichkeit der ihr anvertrauten Daten zu schützen.

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.[2]

Integrität

Der Behandlungsprozess in einem Krankenhaus basiert auf der Zuverlässigkeit der zuvor bei Diagnosen erhobenen Daten. Wenn Daten verfälscht werden kann es zu schweren Schädigungen, z.B. einer falschen Medikamentengabe, führen. Daher gehört die Sicherstellung der Integrität der Daten zu einem weiteren Sicherheitsziel.

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.[2]

Verfügbarkeit

Für eine effiziente Behandlung der Patienten werden klinische Systeme, Anwendungen und Daten zeitnah benötigt. Die Verfügbarkeit dieser Infrastruktur für alle Berechtigten muss im benötigten Umfang sichergestellt werden.

Die *Verfügbarkeit* von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.[2]

Authentizität

Der Zugriff auf Patientendaten darf nur durch berechtigte Mitarbeiter entsprechend dem Rollen- und Berechtigungskonzept erfolgen. Weiterhin muss sichergestellt werden, dass sich z.B. ein Notebook per WLAN nur dann an das interne UKS-Netz anmelden kann, wenn es als UKS-eigenes Gerät erkannt wurde. Daher muss sowohl bei Personen als auch Geräten die Authentizität geprüft werden.

Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen.[2]

[2] Quelle: BSI IT-Grundschutz Glossar

Sicherheitsorganisation

Am UKS wurde ein Infromationssicherheitsmanagementsystem (ISMS) etabliert und die entsprechenden organisatorischen Voraussetzungen geschaffen. Der Vorstand übernimmt die Gesamtverantwortung für den Sicherheitsprozess. Ein Informationssicherheitsbeauftragter wurde bestellt, der sehr eng mit dem Risikomanagementbeauftragten (RMB), dem Datenschutzbeauftragten (DSB) und dem Zentralen Qualitätsmanagement zusammenarbeitet. Gremien für die schnelle Herbeiführung von Entscheidungen bei Sicherheitsvorfällen und zur schnellen Reaktion (CERT) wurden geschaffen.

Die Informationssicherheit betrifft ohne Ausnahme alle Mitarbeiter. Jeder Einzelne kann durch ein verantwortungs- und qualitätsbewusstes Handeln Schäden vermeiden und zum Erfolg beitragen. Eine Sensibilisierung für Informationssicherheit und entsprechende Schulungen der Mitarbeiter sowie aller Führungskräfte sind daher eine Grundvoraussetzung für die Aufrechterhaltung der Informationssicherheit.

Vorstand

Der Vorstand des UKS ist für das zielgerichtete und ordnungsgemäße Funktionieren der Institution verantwortlich und damit auch für die Gewährleistung der Informationssicherheit nach innen und außen.

Der Vorstand

- übernimmt die Gesamtverantwortung für Informationssicherheit
- initiiert, steuert und kontrolliert den Sicherheitsprozess
- legt die Zuständigkeiten für Informationssicherheit fest und
- stellt notwendige organisatorische, personelle und finanzielle Ressourcen bereit.

Krisenstab für IT-Sicherheitsvorfälle

Bei einem massiven Sicherheitsvorfall wie einem umfangreichen Virenbefall wird der Krisenstab für IT-Sicherheitsvorfälle zusammengerufen. Der Krisenstab entscheidet

- ob eine Meldung an den Landesdatenschutzbeauftragten und/oder dem BSI erfolgt
- ob der Vorfall zur Anzeige gebracht wird
- ob eine Unterstützung des Versicherers gewünscht wird
- ob eine Abmeldung von der Notfallversorgung erfolgt und
- wie die Öffentlichkeit informiert wird.

Informationssicherheitsbeauftragter (ISB)

Der Informationssicherheitsbeauftragte (ISB) ist für alle Fragen rund um die Informationssicherheit zuständig. Er ist direkt dem Vorstand unterstellt und berichtet an diesen. Er trägt maßgeblich dazu bei, die Vertraulichkeit, Integrität und Verfügbarkeit schützenswerter Informationen am UKS auf Dauer zu gewährleisten. Der ISB ist frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen. Er ist zentraler Ansprechpartner für Mitarbeiter und Dritte bei Fragen zur Informationssicherheit.

Zu den Aufgaben des ISB gehört es,

- den Sicherheitsprozess zu steuern und zu koordinieren,
- ein Managementsystem zur Informationssicherheit (ISMS – Information Security Management System) zu etablieren,
- Sensibilisierungen und Schulungen zur Informationssicherheit zu initiieren und zu koordinieren,
- sicherheitsrelevante Vorfälle zu untersuchen und ggfs. an das BSI zu melden,
- den Vorstand und andere Sicherheitsverantwortliche über den Status der Informationssicherheit zu berichten,
- regelmäßig die Leitlinie auf Aktualität und Angemessenheit zu überprüfen.

Zentrum für Informations- und Kommunikationstechnik (ZIK)

Das Zentrum für Informations- und Kommunikationstechnik (ZIK) ist die zentrale Dienstleistungseinrichtung für die Konzeption, die Organisation und den Betrieb der IT-Systeme und der Netzwerke im Klinikum. Im Bereich der passiven und aktiven Netzwerkinfrastruktur ist das ZIK für den gesamten Campus Homburg inkl. der Gebäude der Universität des Saarlandes (UdS) zuständig. Ein Arbeitsschwerpunkt des ZIK ist die Einführung und laufende Betreuung von klinischen IT-Systemen und deren Verknüpfung zu einem umfassenden Gesamtsystem.

CERT

Das Computer Emergency Response Team (CERT) des ZIK ist zuständig für die sofortige Bearbeitung von sicherheitsrelevanten Vorfällen im Zusammenhang mit der Nutzung der vom ZIK betreuten IT-Infrastruktur. Hierzu gehört u.a. das Computernetzwerk, Server und Speicher, PCs, Drucker, Anwendungen und Kennungen.

Die Aufgaben des CERT sind:

- schnelle und effiziente Hilfe bei einem Sicherheitsvorfall
- Sperrung von Rechnern bzw. Kennungen bei akuten Vorfällen
- Dokumentation und Aufbereitung von Vorfällen
- Meldung von Vorfällen an den ISB
- Nutzung von IT-Sicherheitssystemen

Aktualisierung der Informationssicherheitsleitlinie

Im Rahmen des Informationssicherheitsprozesses überprüft der ISB diese Leitlinie nach spätestens 3 Jahren auf ihre Aktualität und initiiert ggfs. eine Anpassung.

Inkrafttreten und Veröffentlichung

Die vorliegende Informationssicherheitsleitlinie tritt mit Wirkung zum 01.12.2022 in Kraft.

Homburg, den 17.11.2022

Prof. Dr. J. Diedler Ärztlicher Direktorin	U. Kerle Kaufmännischer Direktor	S. Sari Pflegedirektor	Prof. Dr. M. D. Menger Dekan der Medizinischen Fakultät