IT-Grundschutzanforderungen an Systeme

Informationssicherheit und Datenschutz

Version 2.7 von Mai 2025

Inhalt

1 Einleitung

1.1 Gegenstand und Zweck

Die Systemumgebung einer Gesundheitseinrichtung umfasst nebst den von der internen ICT beschafften und verwalteten Systemen, bestehend aus Plattform (Hardware und Betriebssystem) und Applikationen, eine Vielzahl von Systemen, welche anderweitig beschafft und ganz oder teilweise durch Dritte integriert werden.

Mit der vorliegenden Vorgabe werden die minimalen technischen und organisatorischen Informationssicherheits- und Datenschutzanforderungen der Gesundheitseinrichtung an Systeme festgelegt. Ziel des Dokumentes ist es, die Betriebssicherheit der Systeme und daraus folgend die Patientensicherheit sicherzustellen, den Schutz der Privatsphäre von Patientinnen und Patienten und Mitarbeitenden zu gewährleisten sowie die Systeme angemessen gegen Cyberbedrohungen zu schützen.

Zur breiten Akzeptanz solcher Vorgaben ist die Abstimmung mit den wichtigsten Akteuren im Markt entscheidend. Das H-CSC stimmt deshalb diese Grundschutzanforderungen mit dem Spitalverband H+ und dem Netzwerk für Spitaltechnik IHS «Infrastruktur Hospital Schweiz» ab.

Ebenso werden die wichtigsten Lieferanten involviert, damit auch für sie die Vorgaben verständlich und nachvollziehbar sind und die gemeinsamen Beschaffungsprozesse optimal unterstützt werden können.

1.2 Abgrenzung

Das vorliegende Dokument stellt IT-Grundschutzanforderungen an die Informationssicherheit und den Datenschutz eines Systems. Anders gelagerte Anforderungen wie z.B. Servicezeiten, Usability, oder fachliche Anforderungen an ein System werden nicht behandelt.

Durch die Auslagerung des Betriebs eines Systems an einen Dienstleister entstehen zusätzliche Anforderungen. Diese sind nicht Bestandteil dieses Dokuments. Dies gilt auch für den Einsatz von Software-as-a-Service (SaaS).

1.3 Geltungsbereich

Das vorliegende Dokument gilt für alle Systeme, insbesondere für alle medizintechnischen Systeme inkl. deren Anwendungen, welche in die lokale Netzwerkinfrastruktur der Gesundheitseinrichtung integriert und/oder mit denen Daten der Gesundheitseinrichtung (Daten der Patientinnen und Patienten, Daten der Mitarbeitenden sowie medizinische und nicht medizinische Geschäftsdaten) bearbeiten werden.

Für netzwerkfähige medizinische Systeme gilt das vorliegende Dokument auch dann, wenn das System nicht mit dem IT-Netzwerk der Gesundheitseinrichtung verbunden ist (vgl. Art. 74, MepV[1]).

Das Dokument umfasst die Phasen Beschaffung, Inbetriebnahme, Betrieb und Ausserdienststellung.

Angesprochen sind primär folgende Kreise:

- Dienstleister und Lieferanten
- Interne Mitarbeitende der Gesundheitseinrichtungen, welche im Rahmen der Beschaffung, Integration, Betrieb und Ausserdienststellung von Systemen verantwortlich, entscheidungsbefugt oder anderweitig involviert sind, namentlich Investitions- und Projektleitende.

  Hinweis: Für Gesundheitseinrichtungen, die Mitglied des H-CSC sind, stehen weitere Dokumente auf der H-CSC-Plattform zur Verfügung, welche bei der internen Implementierung dieser Vorgaben unterstützen. Beispielsweise Präsentationen zur Überzeugung des Managements oder des Einkaufs, ein Leitfaden zur Anwendung der IT-Grundschutzanforderungen im Beschaffungsprozess oder in öffentlichen Ausschreibungen (Submissionen).

1.4 Grundlagen

Die Grundlage für dieses Dokument bilden die geltenden Gesetze und Vorgaben von schweizerischen und kantonalen Regulierungsbehörden sowie anerkannte technische und organisatorische Standards.

1.5 Verbindlichkeit und Flexibilität

Die vorliegenden IT-Grundschutzanforderungen erlangen Verbindlichkeit, in dem sie von der jeweiligen Gesundheitseinrichtung gegenüber den Lieferanten eingefordert werden (z.B. über Offertanfragen, Ausschreibungsunterlagen, Einkaufsbedingungen etc.).

Die Grundschutzanforderungen entwickeln sich entlang dem Stand der Technik weiter, sollen sich aber sowohl für Gesundheitseinrichtungen als auch Lieferanten möglichst statisch verhalten. Weder Gesundheitseinrichtungen noch Lieferanten sollen sich immer wieder aufs Neue, mit abweichend formulierten und unterschiedlich gegliederten Anforderungen für die gleichen Systeme befassen müssen.

Trotzdem müssen Anforderungen auf die Fähigkeiten einer Gesundheitseinrichtung bzw. eine spezifische Beschaffung eines Systems angepasst werden können. Aus diesem Grund werden zwei unterschiedliche Anwendungen dieser Anforderungen unterstützt.

Spezifikation: Für reaktive Beschaffungsprozesse der Gesundheitseinrichtungen

Gesundheitseinrichtungen sollen einzelne Grundschutzanforderungen als Ganzes schwächen oder stärken können. Solche Abweichungen und die Gewichtungen der Anforderungen werden in einem separaten Dokument «IT-Grundschutzanforderungen an Systeme - **Spezifikation**» durch die Gesundheitseinrichtung definiert und direkt an die Lieferanten abgegeben. Durch die Spezifikation sind Abweichungen für die Anbieter leicht erkennbar. Der Inhalt der Anforderungen wird dadurch nicht verändert (Baseline).

Selbstdeklaration: Für proaktive Beschaffungsprozesse der Lieferanten

[1] Medizinprodukteverordnung vom 1. Juli 2020; RS 812.213

Die Selbstdeklaration ermöglicht einem Lieferanten seine Produkte einmalig gegenüber den IT-Grundschutzanforderungen zu prüfen und zu dokumentieren. Diese Selbstdeklaration kann der Lieferant in seinen proaktiven Beschaffungsprozessen für alle Gesundheitseinrichtungen einsetzen. Ihnen steht dafür auf der Webseite des H-CSC eine Vorlage zur Verfügung.

1.6 Begriffsdefinitionen

Begriff	Definition
Gesundheits-einrichtung	Gesundheitseinrichtungen sind Organisationen, deren Hauptzweck in der Versorgung oder Behandlung von Patienten und Patientinnen oder der Förderung der öffentlichen Gesundheit besteht. Darunter fallen unter anderem Spitäler, Kliniken und Pflegeinstitutionen.
System	Bei einem System handelt es sich um Hard- oder Software, die ganz oder teilweise durch Dritte geliefert, integriert und/oder betrieben wird. Ein System umfasst alle Komponenten, die von einem Lieferanten oder Dienstleister bereitgestellt werden. Dies beinhaltet Hardware, Firmware, Betriebssystem, Treiber, Middleware, Hilfs- und Hauptapplikationen sowie sämtliche Komponenten, die der Lieferant oder Dienstleister von Unterlieferanten einsetzt. Beispielsweise Zusatzapplikationen, integrierten Source Code, verlinkte Libraries etc.
Mobiles Gerät	Ein mobiles Gerät ist ein Gerät, welches aufgrund seiner Grösse und Gewichts ohne grössere körperliche Anstrengung transportierbar, mobil einsetzbar und/oder unbemerkt aus dem Verantwortungsbereich der Gesundheitseinrichtung entnommen werden kann. Beispiele hierfür sind: Notebook, Tablet, Smartphone, oder kleine medizintechnische Geräte. Mobile Geräte können Bestandteil eines Systems sein.
Datenbearbeitung	Unter Datenbearbeitung versteht sich jeglicher Umgang mit Daten wie das Beschaffen, Aufbewahren, Speichern, Verwenden, Einsehen, Umarbeiten, Verändern, Bekanntgeben oder Vernichten von Daten etc.

1.7 Dokumentaufbau

Zur Unterstützung von Lieferanten von Medizinprodukten sind dort wo sinnvoll, Referenzen zum Manufacturer Disclosure Statement for Medical Device Security [R02] angegeben.

Alle Anforderungen und Mustervertragsklauseln sind mit einer Referenz-ID versehen, welche innerhalb dieses Dokumentes eindeutig ist.

2 Anforderungen

2.1 Grundsätze und Prinzipien

ID	Anforderung
01.01	Sicherheitsverständnis: Es muss jederzeit und in jedem Bereich sichergestellt sein, dass durch den Betrieb des Systems weder Personen noch der Gesundheitseinrichtung irgendwelchen Schaden zugeführt wird. Schwachstellen werden ernstgenommen und zeitnah behoben.
01.02	Systemkenntnis und Kompatibilität: Ein Lieferant eines Systems muss sämtliche Komponenten kennen, aus denen sein System besteht. Er muss sicherstellen, dass diese Komponenten jederzeit innerhalb des Systems miteinander kompatibel sind.
01.03	Defense-in-Depth: Ein System muss mit verschiedenen, sich gegenseitig ergänzenden, komplementären Sicherheitsmassnahmen geschützt werden, um in Bezug auf die Erfüllung

ID	Anforderung
	der Sicherheitsanforderungen Redundanz zu erwirken. Die Sicherheitsmassnahmen müssen insgesamt eine präventive, detektive und reaktive Wirkung haben.
01.04	Least Privilege und Need-to-Know: Die Vergabe von Zugriffsrechten und Privilegien muss minimal erfolgen. Dies gilt für die Benutzerinnen und Benutzer eines Systems, die aktivierten Dienste und Zusatzfunktionalitäten sowie die zulässigen Kommunikationsbeziehungen.
01.05	Security by Default: Systeme müssen so entwickelt, konfiguriert und betrieben werden, dass alle in einem spezifischen Umfeld sinnvollen Sicherheitsmassnahmen standardmässig aktiviert sind und ihre Wirkung entfalten können, ohne dass sich die Benutzerinnen und Benutzer darum kümmern müssen. Systemkomponenten, welche Zugriffsentscheidungen durchsetzen, müssen so ausgelegt werden, dass bei einer Fehlfunktion keine unerlaubten Zugriffe möglich sind.
01.06	Privacy by Design und Privacy by Default: Datenschutzmassnahmen werden durchgängig in die Systementwicklungsprozesse eingebunden. Systeme werden so entwickelt, dass sichere Datenschutzeinstellungen von Anfang an als Standard festgelegt sind.

2.2 Organisation

ID	Anforderung
02.01	Verantwortlichkeiten: Die Aufgaben, Kompetenzen und Verantwortlichkeiten für das System sind vor Vertragsabschluss zwischen der Gesundheitseinrichtung und dem Lieferanten vereinbart. Insbesondere sind die Verantwortlichkeiten für die einzelnen Komponenten eines Systems sowie die Verantwortlichkeiten für das korrekte Zusammenspiel eines Systems mit Komponenten, die von der Gesundheitseinrichtung zur Verfügung gestellt werden, geregelt.
02.02	Verantwortung für das System: Der Lieferant ist für das korrekte Verhalten sämtlicher Systemkomponenten verantwortlich, die zum Lieferumfang des Systems gehören. Dies umfasst auch das korrekte Zusammenspiel mit Komponenten, die von der Gesundheitseinrichtung zur Verfügung gestellt werden und seinen schriftlich vereinbarten Spezifikationen entsprechen.
02.03	Meldepflicht von Sicherheitsvorfällen: Sicherheitsvorfälle (Cyberangriffe) bei Lieferanten und deren Unterlieferanten (darunter fallen auch Datenschutzverletzungen) werden gemäss den gesetzlichen Fristen gemeldet (Informationssicherheitsgesetz). Die Gesundheitseinrichtung ist innert 24 Stunden nach der Detektion über die zuständige Stelle der Gesundheitseinrichtung zu informieren und anschliessend aktiv auf dem Laufenden zu halten [R03].
02.04	Aktives Lifecycle-Management: Der Lieferant stellt sicher, dass er für sämtliche Komponenten (inkl. Applikationen, Betriebssysteme etc.) seiner Systeme die von den Herstellern vorgegebenen Lebenszyklen einhält. Komponenten, für die keine Sicherheitsupdates mehr erhältlich sind, sind zu ersetzen. MDS2 Referenz: DOC-8
02.05	Aktives Schwachstellen-Management: Der Lieferant unterhält ein Schwachstellen-Management (Vulnerability-Management) für sämtliche Komponenten des Systems. Er überprüft die Komponenten des Systems regelmässig auf Schwachstellen und verfolgt die Schwachstellenmeldungen der jeweiligen Hersteller der Komponenten. Der Lieferant informiert die Gesundheitseinrichtung aktiv und transparent über neue Schwachstellen, sobald er sie entdeckt. Dies unabhängig davon, ob bereits eine Gegenmassnahme verfügbar ist. Die ICT der Gesundheitseinrichtung benennt dem Lieferanten eine Ansprechstelle für solche Meldungen [R03]. MDS2 Referenz: CSUP-11 MDS2 Referenz: RDMP-4

ID	Anforderung
02.06	Ansprechstelle für Schwachstellen: Der Lieferant benennt eine Ansprechstelle in seinem Unternehmen, an die die Gesundheitseinrichtung erkannte Schwachstellen melden kann. Er stellt sicher, dass diese Meldungen von Fachleuten in seinem Unternehmen zeitnah bearbeitet und die Gesundheitseinrichtung über die Ergebnisse informiert wird.
02.07	Behebung von Schwachstellen: Der Lieferant stellt sämtliche zur Behebung von Schwachstellen erforderlichen Mittel zur Verfügung. Security Patches werden ab dem Zeitpunkt ihrer Verfügbarkeit, in Abhängigkeit des nach der jüngsten Version des Common Vulnerability Scoring Systems (CVSS) eingeordneten Schweregrades der Schwachstelle, zeitnah installiert oder gegenüber der Gesundheitseinrichtung für die Installation freigegeben.
02.08	Zeitliche Vorgaben zur Behebung von Schwachstellen: Die zeitlichen Vorgaben für die Behebung von Schwachstellen richten sich nach dem Common Vulnerability Scoring Systems (CVSS). Dabei gilt: ▪ Kritisch (CVSS = 9.0 - 10.0): so schnell wie möglich[1] ▪ Hoch (CVSS = 7.0 - 8.9): 2 Wochen ▪ Mittel (CVSS = 4.0 - 6.9): 1 Monat ▪ Niedrig (CVSS = 0.1 - 3.9): 2 Monate [1] die Zeitdauer richtet sich nach den mit der Installation verbundenen Verfügbarkeitsrisiken. Werden Komponenten des Systems gemäss Absprache mit dem Lieferanten durch die Gesundheitseinrichtung bereitgestellt, ist die Gesundheitseinrichtung für die Aktualisierung dieser Komponenten zuständig. Die Gesamtverantwortung für die korrekte Funktionalität des Systems, bleibt weiterhin beim Lieferanten. Der Lieferant definiert gegenüber der Gesundheitseinrichtung die zur Aktualisierung einzusetzenden Komponenten. Er stellt seinerseits sicher, dass die Kompatibilität der aktualisierten Komponente mit dem Gesamtsystem sichergestellt ist.
02.09	Freigabe zur Inbetriebnahme: Das System wird erst nach der Abnahme durch die involvierten Fachbereiche (z.B. Gebäudetechnik, Medizininformatik, Medizintechnik) und die ICT der Gesundheitseinrichtung [R03] produktiv in Betrieb genommen. Die Abnahme wird schriftlich protokolliert.
02.10	Übernahme bzw. Mitnahme von physischen Systemen: Systeme und alle dessen Komponenten dürfen nur mit Bewilligung der zuständigen ICT-Mitarbeitenden [R03] der Gesundheitseinrichtung verlassen. Vor der Übernahme oder Mitnahme von Systemen oder Komponenten, unabhängig des Grundes, sind die Daten der Gesundheitseinrichtung irreversibel zu löschen [05.05] oder sicher zu vernichten [05.06]. Dies ist gegenüber den zuständigen ICT-Mitarbeitenden der Gesundheitseinrichtung, vor der Übernahme oder Mitnahme schriftlich zu bestätigen.

2.3 Dokumentation

ID	Anforderung
03.01	Architekturdokumentation: Die Architektur des Systems resp. der Gesamtlösung wird vollständig dokumentiert. Die Architekturdokumentation umfasst dabei mindestens folgende Punkte: 1. Grafische Gesamtübersicht aller der Lösung zugehörigen Systeme, Applikationen und Komponenten. 2. Nachweis über alle Komponenten der eingesetzten Softwareprodukte und ihre Beziehungen innerhalb der Softwarelieferkette (Software Bill of Materials).

ID	Anforderung
	3. Schnittstellen zu bereits vorhandenen internen und externen Systemen mit mindestens folgenden Angaben: Quelle, Ziel, Protokoll(e), Verschlüsselung, Authentisierung, übermittelte Datenobjekte mit Klassifikation der Vertraulichkeit und Angabe des Zwecks, 4. Datenkommunikationen zu bereits bestehenden internen und externen Systemen (z.B. Übermittlung von Verbrauchsdaten, Fernzugriffe, Monitoring). 5. Datenflüsse in der Form: Zweck, Dateninhalt, Schutz der Vertraulichkeit bei Datenübertragung und Datenspeicherung. Zur Klassifizierung der Vertraulichkeitsstufen der Datenobjekte gilt die entsprechende Vorgabe der Gesundheitseinrichtung [R03]. MDS2 Referenz: DOC-10
03.02	Technische Betriebsdokumentation: Für das System wird eine technische Betriebsdokumentation geliefert, die mindestens folgende Punkte umfasst: 1. Gesamtübersicht aller der Lösung zugehörigen Systeme (z.B. Betriebssystem, Applikationen, COTS[2]/SOUP[3]) und jede andere wesentliche Komponente, welche für einen stabilen und sicheren Betrieb notwendig sind. 2. Installation, Konfiguration, Betrieb und Wartung (vor Ort und/oder aus der Ferne), Beschreibung aller der Lösung zugehörigen Systeme, Applikationen und Komponenten, inklusive deren Herausgeber, Produktlizenz und Versionsnummer. 3. Systeme und deren Konfiguration in der folgenden Form: Systembezeichnung, eingesetztes Betriebssystem, installierte Applikationen mit Angabe der Versionsnummer, Dienste und Accounts (insbesondere jene mit privilegierter Berechtigung), 4. Auflistung sämtlicher elektronischer Datenträger im System, auf denen Daten der Gesundheitseinrichtung gespeichert werden könnten. Anzugeben sind der Speichertyp (z.B. SSD, HDD etc.) und der physische Ort im Gerät, um die Medien zu finden, 5. Deklaration aller temporärer und permanenter Datenspeicherorte mit Deklaration, welche Daten der Gesundheitseinrichtung dort gespeichert werden, 6. Kennzeichnung der für den einwandfreien Betrieb zu überwachende Kontrollpunkte mit den Parametern, die zum einwandfreien Betrieb gehören, 7. Kommunikationsmatrix im folgenden Format: Quelle, Ziel, Netzwerkprotokoll, Port sowie Zweck. MDS2 Referenz: DOC-10 MDS2 Referenz: SBOM-1
03.03	Operative Betriebsdokumentation: Für das System wird eine operative Betriebsdokumentation erstellt, welche mit der zuständigen Fachstelle der Gesundheitseinrichtung [R03] abgestimmt wird. Diese operative Betriebsdokumentation umfasst mindestens: 1. die internen (Gesundheitseinrichtung) und externen (Anbieter) Verantwortlichkeiten und Kontakte sowie die zugehörigen Wartungs-, Support- und Administrationsprozesse, insbesondere: a) Deklaration der Betriebsverantwortung der Systemkomponenten b) Anleitung für den 1st Level Support, wie bei welchen bekannten Fehlern zu verfahren ist c) Anleitung für den 2nd Level Support, wie Fehler zu analysieren sind und wann an den 3rd Level Support (Hersteller) eskaliert werden soll

[2] Commercial of the shelf software
[3] Software of unknown pedigree

ID	Anforderung
	d) Anleitung, wie die Systemkomponenten ordnungsgemäss heruntergefahren werden e) Anleitung, wie die Systemkomponenten ordnungsgemäss hochgefahren werden 2. die Benutzerdokumentation der Lösung (Benutzerhandbuch).
03.04	Sicherheitsdokumentation: Der Lieferant stellt folgende Sicherheitsdokumentation zum angebotenen Produkt bzw. zu seiner Organisation bereit: 1. *Information Security Policy* 2. ISO 27'001 Zertifikat falls vorhanden 3. Umsetzung von Empfehlungen und best-Practices im Bereich Sicherheit und Datenschutz (z.B. ISO 27018), 4. Weitere Zertifizierungen im Bereich Sicherheit und Datenschutz falls vorhanden 5. Anleitung, wie ein abgestürztes System gestartet wird und welche Prüfungen zur Datenintegrität vorgenommen werden müssen, 6. Anleitung, wie ein eingeschränkter Betrieb (Notbetrieb) wieder in den einwandfreien Betrieb gebracht wird. MDS2 Referenz: SGUD-1
03.05	Sicherheitsdokumentation für medizintechnische Systeme: Für medizintechnische Systeme liegen folgende Nachweise vor: 1. IEC 62'304 Zertifikat 2. CE-Zertifikat 3. *Manufacturer Disclosure Statement for Medical Device Security* (MDS2) MDS2 Referenz: RDMP-1
03.06	Dokumentation für die Abnahme: Bei der Abnahme des Systems durch die Gesundheitseinrichtung liegt folgende Dokumentation vor: ▪ Architekturdokumentation ▪ Technische Betriebsdokumentation ▪ Operative Betriebsdokumentation ▪ Sicherheitsdokumentation ▪ Sicherheitsdokumentation für medizintechnische Systeme, falls zutreffend.
03.07	Form der Dokumentation: Die Dokumentation erfolgt in elektronischer Form und in einem gängigen Format (z.B. PDF).
03.08	Prüfung: Sämtliche Dokumentation muss der Gesundheitseinrichtung zur Abnahme vorgelegt werden. Eine Inbetriebnahme des Systems erfolgt erst nach erfolgreicher Abnahme der Dokumentation. Sämtliche Änderungen der Dokumentation, ausgenommen Bagatelländerungen, werden der Gesundheitseinrichtung während der gesamten Betriebsphase des Systems aktiv zur Kenntnis gebracht und sofern erforderlich im Voraus abgestimmt.

2.4 Grundkonfiguration

ID	Anforderung
04.01	Minimierung der Systemexposition: Zur Minimierung der System-Exposition werden folgende Massnahmen umgesetzt:

ID	Anforderung
	1. Sperren des Internetzugangs, sofern dieser nicht für die Funktion oder Sicherstellung des Betriebs erforderlich ist. 2. Deinstallation resp. Deaktivierung aller nicht notwendiger Software-Pakete und Netzwerkdienste. Es dürfen ausschliesslich Software-Pakete und Dienste installiert werden, welche für den Betrieb des Systems absolut erforderlich sind. Werden temporär Hilfskomponenten installiert (z.B. während einer Wartung), sind diese nach Abschluss der Arbeiten zu deinstallieren. 3. Installation einer lokalen Firewall, welche nur die Erreichbarkeit von vordefinierten Netzwerk-Ports erlaubt. 4. Deaktivierung der USB-Ports, Bluetooth-Schnittstellen etc. sowie anderweitiger Anschlussmöglichkeiten, sofern diese nicht im Betrieb benötigt werden. 5. Deaktivierung der Funktionen «AutoRun/AutoPlay». MDS2 Referenz: SAHD-1
04.02	Einsatz von risikobehafteten Technologien: Es werden keine Technologien mit bekannten Sicherheitsrisiken, z.B. Protokolle wie SMBv1, FTP oder Telnet, eingesetzt. MDS2 Referenz: TXCF-5
04.03	Einschränkung von Schnittstellen: Kommunikationsverbindungen werden ausschliesslich über die mit der Gesundheitseinrichtung vereinbarten und dokumentierten Schnittstellen aufgebaut. Nicht genutzte Schnittstellen werden deaktiviert, so dass darüber keine Kommunikation möglich ist.
04.04	Endpoint Protection: Das System wird mittels einer Endpoint Protection Lösung vor Schadsoftware und Missbrauch von Systemkomponenten geschützt. Falls der Betrieb einer Endpoint Protection Lösung die Konformität (CE, MDR etc.) des Systems verletzt, wird dies durch den Lieferanten ausgewiesen. MDS2 Referenz: MLDP-2
04.05	Aktualisierung der Endpoint Protection: Security Intelligence Updates für die Endpoint Protection Lösung werden regelmässig, mindestens aber täglich, installiert. Neue Versionen der Endpoint Protection Lösung werden zeitnah installiert. Zu diesem Zweck darf das System Verbindung zum Internet aufbauen [04.01]

2.5 Datensicherheit

ID	Anforderung
05.01	Verschlüsselte Datenspeicherung: Daten werden gemäss der Klassifizierungsrichtlinie der Gesundheitseinrichtung [R03] behandelt. Sensitive Daten und Personendaten werden mindestens «at Rest» mit einem sicheren kryptographischen Verfahren verschlüsselt; dies gilt insbesondere für die Datenhaltung auf mobilen Geräten. MDS2 Referenz: STCF-1
05.02	Sichere kryptographische Verfahren: Zur Verschlüsselung werden ausschliesslich als sicher eingestufte kryptographische Verfahren und Schlüssellängen eingesetzt. Die Gesundheitseinrichtung orientiert sich hierbei an der technischen Richtlinie TR-02102 des des Bundesamtes für Sicherheit Deutschland BSI [R01].
05.03	Datenübermittlung und -speicherung: Der Lieferant speichert keine Daten der Gesundheitseinrichtung auf seiner IT-Infrastruktur oder seinen Speichermedien (USB-Sticks, Disks etc.). Dasselbe gilt für die Datenübermittlung.

ID	Anforderung
	Ausgenommen von dieser Anforderung sind Systemdaten, welche für die Sicherstellung des Betriebs zwingend erforderlich sind. Daten werden nicht ohne schriftliche Einwilligung der Verantwortlichen [R03] aus der Gesundheitseinrichtung entfernt. Werden Cloud-Systeme zur Bearbeitung oder Speicherung von Daten eingesetzt, sind diese zu dokumentieren und deren Einsatz durch die Gesundheitseinrichtung explizit zu bewilligen.
05.04	Lebenszyklus der Daten: Der Lebenszyklus (Erhebung, Bearbeitung, Archivierung und Löschung) der Daten ist dokumentiert und berücksichtigt interne und externe Compliance-Vorgaben bezüglich der Aufbewahrungspflicht der Gesundheitseinrichtung [R03]. Das System löscht Daten nur dann autonom, wenn diese Löschung gemäss den für die Gesundheitseinrichtung geltenden Gesetzen und internen Richtlinien erlaubt ist. Das System stellt eine Schnittstelle zur Verfügung, über welche die für die Gesundheitseinrichtung relevanten Daten dem Archiv-System der Gesundheitseinrichtung rechtskonform zugeführt werden können (z.B. Behandlungsdaten). Die Datensicherung erfolgt nach den Standardmethoden und Prozessen der Gesundheitseinrichtung [R03].
05.05	Sichere Löschfunktion: Das System unterstützt sichere Löschfunktionen, die für das irreversible Löschen sämtlicher Daten der Gesundheitseinrichtung von lokalen Datenträgern verwendet werden können. Namentlich sämtliche Daten zu Patientinnen und Patienten, Zugangsdaten wie Passworte und Schlüssel, Nutzungsstatistiken, Messresultate etc. Diese Löschfunktionen entsprechen dem Standard VSIT des BSI oder dem Standard DoD-5220.22-M (E) und sind vom Lieferanten ausführlich in der Dokumentation beschrieben. Nach Anwendung der Löschfunktionen verbleiben auf dem Gerät lediglich Informationen, die der initialen Grundkonfiguration des Systems und dem Werkszustand entsprechen.
05.06	Datenvernichtung: Beim Austausch von Speichermedien werden alle darauf gespeicherten Daten vorgängig sicher gelöscht [05.05]. Alternativ kann der Lieferant die Datenträger sicher vernichten und umweltkonform entsorgen oder der Gesundheitseinrichtung zur Vernichtung übergeben. Dies belegt er der Gesundheitseinrichtung schriftlich. Speichermedien werden nicht ohne schriftliche Einwilligung der Verantwortlichen der Gesundheitseinrichtung aus der Gesundheitseinrichtung entfernt. Die physische Datenträgervernichtung erfolgt nach Norm DIN 66399 (Schutzklasse 2) [R04]. MDS2 Referenz: SGUD-2

2.6 Datenschutz

ID	Anforderung
06.01	Zentrales Management: Der Zugriff auf sensitive Personendaten auf Systemen innerhalb der Gesundheitseinrichtung erfolgt ausschliesslich über persönliche Benutzerkonten, welche zentral durch die Gesundheitseinrichtung verwaltet werden. Lokale Benutzer für solche Zugriffe werden nicht eingesetzt. MDS2 Referenz: AUTH-1.1
06.02	Datenbearbeitung: Die Bearbeitung von personenbezogenen und anderweitig schützenswerten Daten erfolgt ausschliesslich in der Schweiz oder in einem Land mit einem angemessenen Datenschutzniveau. Relevant ist das Gesetz in der jeweils aktuellen Fassung, das für die jeweilige Gesundheitseinrichtung gilt (Nationales oder Kantonales Recht). Als Stichdatum gilt das Datum des Angebots resp. des Kaufs.

ID	Anforderung
06.03	Auflistung der Personendaten: Der Lieferant zeigt auf, welche personenbezogenen Daten vom System bearbeitet und gespeichert werden: 1. Aufstellung der Daten mit der entsprechenden Begründung in Bezug auf die Verhältnismässigkeit und Zweckbindung. 2. Aufbewahrungsdauer von dauerhaft gespeicherten Daten. 3. Nennung der Länder, in welche diese Daten potenziell exportiert werden könnten (Speicherung, Sicherung, Zugriff). MDS2 Referenz: MPII-1 MDS2 Referenz: MPII-2 MDS2 Referenz: MPII-3

2.7 Protokollierung und Nachvollziehbarkeit

ID	Anforderung
07.01	Protokollierung: Alle Aktionen auf dem System, namentlich: ▪ An- und Abmeldevorgänge, ▪ Fehlersituationen, ▪ Privilegierte und administrative Funktionsausführungen, ▪ Änderungen von Zugriffsrechten und Benutzerrollen, ▪ Änderungen der Systemkonfigurationen, werden nachvollziehbar protokolliert. MDS2 Referenz: AUDT-1 MDS2 Referenz: AUDT-1.1 MDS2 Referenz: AUDT-1.2 MDS2 Referenz: AUDT-2.1 MDS2 Referenz: AUDT-2.2
07.02	Audit-Trail: Die Protokollierung zeichnet jegliche Bearbeitung von relevanten technischen, personenbezogenen oder besonders schützenswerten Daten im Sinne eines Audit-Trails auf. MDS2 Referenz: AUDT-2 MDS2 Referenz: AUDT-2.1 MDS2 Referenz: AUDT-2.2 MDS2 Referenz: AUDT-2.3 MDS2 Referenz: AUDT-2.4 MDS2 Referenz: AUDT-2.5 MDS2 Referenz: AUDT-2.6 MDS2 Referenz: AUDT-2.7 MDS2 Referenz: AUDT-2.8 MDS2 Referenz: AUDT-2.8.1 MDS2 Referenz: AUDT-2.8.2 MDS2 Referenz: AUDT-2.9 MDS2 Referenz: AUDT-2.10 MDS2 Referenz: AUDT-2.11
07.03	Manipulationsschutz von Protokolldaten: Auf dem System zwischenzeitlich oder dauerhaft gespeicherte Protokolldaten werden vor Manipulation und unberechtigtem Zugriff geschützt. MDS2 Referenz: AUDT-7
07.04	Weiterleitung von Protokolldaten: Das System ist in der Lage, Protokolldaten über eine standardisierte Schnittstelle und ein standardisiertes Format (z.B. Syslog) an einen zentralen Logserver der Gesundheitseinrichtung weiterzuleiten.

ID	Anforderung
	MDS2 Referenz: AUDT-5 MDS2 Referenz: AUDT-5.1 MDS2 Referenz: AUDT-5.2 MDS2 Referenz: AUDT-5.3

2.8 Kommunikation und Netzwerkzugang

ID	Anforderung
08.01	Sichere Kommunikationsprotokolle: Das System setzt ausschliesslich Kommunikationsprotokolle mit als sicher eingestuften kryptographischen Verfahren und Schlüssellängen ein. Die Gesundheitseinrichtung orientiert sich hierbei an der technischen Richtlinie TR-02102 des BSI [R01].
08.02	Überwachung von Übertragungsfehlern: Bei einer Datenübertragung auf ein zentrales System der Gesundheitseinrichtung (z.B. PACS), werden Übertragungsfehler detektiert. Die Benutzenden oder die zuständige ICT-Stelle der Gesundheitseinrichtung [R03] werden über den Übertragungsfehler unverzüglich informiert.
08.03	Verschlüsselung: Alle internen und externen Kommunikationsverbindungen vom und zum System werden mittels sicherer Kommunikationsprotokolle verschlüsselt.
08.04	Routingfunktionalitäten: Das System ermöglicht keine Bridging-, Routing- oder anderweitige Forward-Funktionalitäten für andere Netzwerksegmente. Entsprechende Funktionen werden deaktiviert.
08.05	Netzwerkadressierungen: Das System unterstützt eine konfigurierbare Netzwerkadressierung, so dass diese von der Gesundheitseinrichtung vorgegeben werden kann.
08.06	Drahtgebundene Kommunikationsverbindungen: Drahtgebundene Kommunikationsverbindungen werden ausschliesslich über die Netzwerkinfrastruktur der Gesundheitseinrichtung aufgebaut. Ein System, welches an das Netzwerk angeschlossen wird, unterstützt eine portbasierte Authentifizierung nach dem Standard 802.1x mittels EAP-TLS oder gleichwertige Alternativen, welche seitens ICT der Gesundheitseinrichtung [R03] freigegeben sind.
08.07	Drahtlose Kommunikationsverbindungen (WLAN): Für drahtlose Kommunikationsverbindungen werden ausschliesslich die Netzwerkkomponenten der Gesundheitseinrichtung genutzt. Der eingesetzte Verschlüsselungsstandard entspricht mindestens WPA2 Enterprise. Als Authentifizierungsprotokoll wird EAP-TLS eingesetzt. Gleichwertige alternative Lösungen sind zulässig, wenn sie seitens ICT der Gesundheitseinrichtung [R03] freigegeben sind.
08.08	Bluetooth-Verbindungen: Wenn Bluetooth-Verbindungen notwendig sind, sollen diese bei Bluetooth Classic mindestens Security Mode 4 Level 4 entsprechen und bei Bluetooth LE Security Mode 1 Level 4.
08.09	Ausgehende Web-Verbindungen ins Internet: Wenn Internet-Verbindungen erforderlich sind, werden diese zwingend über den Web Proxy der Gesundheitseinrichtung geführt. Das System verfügt hierfür über eine Proxy Fähigkeit.
08.10	Synchronisierung der Systemzeiten: Das System unterstützt zur Synchronisierung der Systemzeit das Netzwerkprotokoll NTP. MDS2 Referenz: AUDT-4.1.1

2.9 Zugriffssteuerung

ID	Anforderung
09.01	Separierung von Konten für Systemdienste: Dienstkonten (Konten für Systemdienste) werden von Benutzerkonten separiert. Sie verfügen ausschliesslich über Berechtigungen, die zum Betrieb der vorgesehenen Systemdienste erforderlich sind (Minimalprinzip). MDS2 Referenz: AUTH-2
09.02	Nutzung von lokalen Administratorenkonten: Lokale Administratorenkonten werden ausschliesslich für die Wartung und Konfiguration verwendet. Die betriebliche Nutzung erfolgt über persönliche Benutzerkonten.
09.03	Authentisierte Zugriffe: Zugriffe auf das System erfolgen ausschliesslich authentisiert. Alle Benutzerkonten werden mittels geeigneten Authentifizierungsmechanismen geschützt. MDS2 Referenz: AUTH-1
09.04	Authentisierung bei Schnittstellen: Die Datenübertragung mittels Schnittstellen erfolgt ausschliesslich authentisiert. Dabei werden mindestens das Sender- vom Empfängersystem authentifiziert. Authentisierungsinformationen (Passwörter, Schlüsselmaterial etc.) werden vor unbefugten Zugriffen geschützt abgelegt.
09.05	Passwortregelung: Standardpasswörter werden nach den Vorgaben der Gesundheitseinrichtung [R03] vor produktiver Inbetriebnahme geändert. Es ist sichergestellt, dass die eingesetzten Passwörter spezifisch pro Gesundheitseinrichtung erzeugt sind und bei anderen Kunden nicht zum Einsatz kommen. Besteht die Möglichkeit, dass unberechtigte Dritte Kenntnis über solche Passwörter erlangen, wird dies vom Lieferanten der Gesundheitseinrichtung umgehend angezeigt und die Passwörter werden in den betroffenen Systemen geändert. MDS2 Referenz: PAUT-6
09.06	Umgang mit Zugangsinformationen: Zugangsinformationen (z.B. Passworte, digitale oder physische Schlüssel etc.) werden als geheim klassifiziert und vom Lieferanten und dessen Systemen als solche behandelt bzw. geschützt. Zugangsinformationen werden regelmässig, in zu definierenden Intervallen, geändert [R03].
09.07	Autorisierung: Das System verfügt über eine rollenbasierte oder vergleichbare Autorisierung. MDS2 Referenz: AUTH-2
09.08	Provisionierung von Berechtigungen: Das System unterstützt die Anbindung des IAM-Systems der Gesundheitseinrichtung über eine standardisierte Schnittstelle zur Provisionierung von Berechtigungen. MDS2 Referenz: PAUT-2
09.09	Sperrung der Benutzersession bei Inaktivität: Das System verfügt über die Fähigkeit, Sessions durch den Benutzer manuell zu sperren (z.B. beim Verlassen des Systems). Eine Benutzersession wird, nach einer durch die Gesundheitseinrichtung bestimmbaren Zeitdauer, nach Inaktivität automatisch gesperrt [R03]. MDS2 Referenz: ALOF-1
09.10	Federated Identity: Die Authentifizierung von Benutzern und die Übermittlung von Informationen, welche für den Zugriff auf Ressourcen erforderlich sind, erfolgt über ein Trust-Verhältnis zwischen dem System und der dafür vorgesehenen Infrastruktur der Gesundheitseinrichtung (Federated Identity).

ID	Anforderung
	MDS2 Referenz: PAUT-2

2.10 Wartung und Support

ID	Anforderung
10.01	Fernzugriffe: Lieferanten, welche Fernzugriff auf das System der Gesundheitseinrichtung benötigen, erfüllen die dafür erforderlichen Sicherheitsvorgaben und nutzen ausschliesslich die Fernzugriffssysteme der Gesundheitseinrichtung [R03]. Der Fernzugriff muss über persönliche Benutzerkonten erfolgen. Lieferantenspezifische Fernzugriffssysteme werden von der Gesundheitseinrichtung nicht unterstützt. MDS2 Referenz: RMOT-1 MDS2 Referenz: RMOT-2 MDS2 Referenz: RMOT-3
10.02	Vorankündigung von Wartungsarbeiten: Wartungsarbeiten durch den Lieferanten, ungeachtet dessen ob diese vor Ort, oder per Fernzugriff erfolgen, sind der Fachabteilung und der ICT der Gesundheitseinrichtung [R03] voranzumelden. Sollten besondere Umstände sofortige Wartungsarbeiten erfordern, so werden diese im Nachhinein innert 24h der Fachabteilung und der ICT inkl. einer nachvollziehbaren Begründung der Dringlichkeit nachgemeldet.
10.03	Wartungsarbeiten mittels Wechseldatenträgern: Der Anschluss von Wechseldatenträgern an Systeme der Gesundheitseinrichtung (inkl. der vom Lieferanten gelieferten Systeme) sind nicht zulässig. Wechseldatenträger für den Transfer oder zur Sicherung von Daten werden von der Gesundheitseinrichtung bereitgestellt. Der Lieferant stellt Software, die zur Durchführung einer Wartung erforderlich ist, mindestens zwei Wochen vor der Durchführung der Wartungsarbeiten den zuständigen ICT-Mitarbeitenden der Gesundheitseinrichtung zur Verfügung. Diese prüfen die Software und stellen sie dem Lieferanten auf einem geeigneten Medium der Gesundheitseinrichtung für die Wartung bereit.

3 Referenzen

#	Bezeichnung	Referenz
R01	BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen (auf Deutsch und auf Englisch)	Link
R02	Manufacturer Disclosure Statement for Medical Device Security (Version 2019, auf Englisch)	Link
R03	Eingesetzte Standards und IT-Strategie sowie Kontaktstellen der Gesundheitseinrichtung. Dieses Dokument wird von der Gesundheitseinrichtung direkt an die Lieferanten abgegeben.	Beilage der GE
R04	DIN 66399-1 Büro- und Datentechnik - Vernichten von Datenträgern (auf Deutsch und auf Englisch)	Link

Die Referenzen wurden letztmals am 02.02.2026 geprüft.