Requisiti di sicurezza di base per i sistemi informatici

Sicurezza delle informazioni e protezione dei dati

Versione 2.7 maggio 2025

Indice

1 Introduzione

1.1 Oggetto e finalità

I sistemi di una struttura sanitaria comprendono, oltre ai sistemi acquisiti e gestiti dall'ICT interna (di cui fanno parte piattaforma, ovvero hardware e sistema operativo, e applicazioni), anche una vasta gamma di sistemi acquisiti tramite altri canali e integrati, in tutto o in parte, da terzi.

La presente direttiva definisce i requisiti minimi tecnici e organizzativi in materia di sicurezza delle informazioni e protezione dei dati applicabili ai sistemi della struttura sanitaria. L'obiettivo del documento è garantire la sicurezza operativa dei sistemi e, di conseguenza, la sicurezza dei pazienti, assicurare la tutela della privacy di pazienti e collaboratori, nonché proteggere adeguatamente i sistemi dalle minacce informatiche.

Per garantire un'ampia accettazione di tali requisiti, è fondamentale il coordinamento con i principali attori del settore. L'H-CSC coordina pertanto questi requisiti di sicurezza di base con l'associazione ospedaliera H+ e con la rete per la tecnologia ospedaliera IHS «Infrastructure Hôpital Suisse / Infrastruktur Hospital Schweiz».

Sono inoltre coinvolti i principali fornitori, affinché i requisiti risultino per loro comprensibili e tracciabili e i processi di approvvigionamento congiunti possano essere supportati in modo ottimale.

1.2 Delimitazione

Il presente documento definisce i requisiti di sicurezza di base relativi alla sicurezza delle informazioni e alla protezione dei dati di un sistema. Requisiti di altra natura, quali ad esempio tempi di servizio, usabilità o requisiti funzionali di un sistema, non sono oggetto del presente documento.

L'esternalizzazione dell'esercizio di un sistema a un fornitore di servizi comporta requisiti aggiuntivi. Tali requisiti non fanno parte del presente documento. Ciò vale anche per l'utilizzo di Software-as-a-Service (SaaS).

1.3 Ambito di applicazione

Il presente documento si applica a tutti i sistemi, in particolare a tutti i sistemi di tecnologia medica (comprese le relative applicazioni), che sono integrati nell'infrastruttura di rete locale della struttura sanitaria e/o tramite i quali vengono trattati dati della struttura sanitaria (dati delle e dei pazienti, dati del personale nonché dati aziendali medici e non medici).

Per i sistemi medicali connessi alla rete, il presente documento si applica anche nel caso in cui il sistema non sia collegato alla rete IT della struttura sanitaria (cfr. art. 74, ODmed[1]).

Il documento copre le fasi di approvvigionamento, messa in servizio, esercizio e dismissione.

I principali destinatari sono i seguenti gruppi:

- prestatori di servizi e fornitori
- collaboratrici e collaboratori interni delle strutture sanitarie che, nell'ambito dell'approvvigionamento, dell'integrazione, dell'esercizio e della dismissione dei sistemi, sono responsabili e autorizzati a prendere decisioni o altrimenti coinvolti, in particolare responsabili degli investimenti e dei progetti.

  Nota: Per le strutture membri dell'H-CSC sono disponibili ulteriori documenti sulla piattaforma H-CSC, che supportano l'implementazione interna di queste direttive. Tra questi figurano, ad esempio, presentazioni per sensibilizzare la direzione o gli uffici acquisti, nonché una guida per l'applicazione dei requisiti di sicurezza di base nei processi di approvvigionamento o nelle gare pubbliche (bandi).

1.4 Basi di riferimento

Il presente documento si basa sulle leggi e disposizioni vigenti emanate dalle autorità di regolamentazione svizzere e cantonali, nonché su standard tecnici e organizzativi riconosciuti.

1.5 Carattere vincolante e flessibilità

I presenti requisiti di sicurezza di base diventano vincolanti nel momento in cui vengono richiesti dalla rispettiva struttura sanitaria nei confronti dei fornitori (ad es. tramite richieste di offerta, documentazione di gara, condizioni di acquisto, ecc.).

I requisiti di sicurezza di base si evolvono in funzione dello stato della tecnica, ma dovrebbero rimanere il più possibile stabili sia per le strutture sanitarie sia per i fornitori. Né le strutture sanitarie né i fornitori dovrebbero doversi confrontare ripetutamente con requisiti formulati in modo diverso e strutturati in maniera differente per gli stessi sistemi.

Tuttavia, i requisiti devono poter essere adattati alle capacità di una struttura sanitaria o a una specifica acquisizione di un sistema. Per questo motivo sono previste due diverse modalità di applicazione di tali requisiti.

Specificazione: per i processi di approvvigionamento reattivi delle strutture sanitarie

Le strutture sanitarie possono rinforzare o indebolire singoli requisiti di sicurezza di base nel loro insieme. Tali scostamenti e la ponderazione dei requisiti sono definiti dalla struttura sanitaria in un documento separato denominato «Requisiti di sicurezza di base per i sistemi informatici – **Specificazione**» e trasmessi direttamente ai fornitori. Grazie alla specificazione, gli scostamenti risultano facilmente identificabili per i fornitori. Il contenuto dei requisiti non viene tuttavia modificato (baseline).

Autodichiarazione: per i processi di approvvigionamento proattivi dei fornitori

L'autodichiarazione consente a un fornitore di verificare e documentare una sola volta i propri prodotti rispetto ai requisiti di sicurezza di base. Tale autodichiarazione può essere utilizzata dal fornitore nei propri processi di approvvigionamento proattivi per tutte le strutture sanitarie. A tal fine, sul sito web dell'H-CSC è disponibile un modello.

[1] Ordinanza relativa ai dispositivi medici del 1° luglio 2020; RS 812.213

1.6 Definizioni dei termini

Termine	Definizione
Struttura sanitaria	Le strutture sanitarie sono organizzazioni il cui scopo principale consiste nella cura o nel trattamento delle pazienti e dei pazienti oppure nella promozione della salute pubblica. Rientrano in questa categoria tra l'altro ospedali, cliniche e istituti di cura.
Sistema	Per sistema si intende hardware o software fornito, integrato e/o gestito, in tutto o in parte, da terzi. Un sistema comprende tutti i componenti messi a disposizione da un fornitore o da un prestatore di servizi. Ciò include hardware, firmware, sistema operativo, driver, middleware, applicazioni ausiliarie e principali, nonché tutti i componenti utilizzati dal fornitore o dal prestatore di servizi tramite subfornitori. Rientrano, ad esempio, applicazioni aggiuntive (*add-ons / plug-ins*), codice sorgente integrato, librerie collegate, ecc.
Dispositivo mobile	Un dispositivo mobile è un dispositivo che, per dimensioni e peso, può essere trasportato senza particolare sforzo fisico, utilizzato in modo mobile e/o rimosso senza essere notato dall'ambito di responsabilità della struttura sanitaria. Esempi sono notebook, tablet, smartphone o piccoli dispositivi di tecnologia medica. I dispositivi mobili possono essere parte integrante di un sistema.
Trattamento dei dati	Per trattamento dei dati si intende qualsiasi operazione sui dati, quali l'acquisizione, la conservazione, l'archiviazione, l'utilizzo, la consultazione, la rielaborazione, la modifica, la comunicazione o la distruzione dei dati, ecc.

1.7 Struttura del documento

A supporto dei fornitori di dispositivi medici, ove opportuno, sono indicati riferimenti al *Manufacturer Disclosure Statement for Medical Device Security* [R02].

Tutti i requisiti e i modelli di clausole contrattuali sono contrassegnati da un ID di riferimento, univoco all'interno del presente documento.

2 Requisiti

2.1 Principi e linee guida

ID	Requisito
01.01	Comprensione della sicurezza: deve essere garantito in ogni momento e in ogni ambito che l'esercizio del sistema non arrechi alcun danno né alle persone né alla struttura sanitaria. Le vulnerabilità vengono prese sul serio e risolte tempestivamente.
01.02	Conoscenza del sistema e compatibilità: il fornitore di un sistema deve conoscere tutti i componenti che lo costituiscono. Deve garantire che tali componenti siano in ogni momento compatibili tra loro all'interno del sistema.
01.03	Defense-in-depth: un sistema deve essere protetto mediante diverse misure di sicurezza complementari e reciprocamente integrate, al fine di ottenere ridondanza nel soddisfacimento dei requisiti di sicurezza. Nel loro insieme, le misure di sicurezza devono avere un effetto preventivo, di detezione e reattivo.
01.04	Least privilege e need-to-know: l'assegnazione dei diritti di accesso e dei privilegi deve avvenire in modo minimo. Ciò vale per le utenti e gli utenti di un sistema, per i servizi attivati e le funzionalità aggiuntive, nonché per le relazioni di comunicazione consentite.
01.05	Security by default: i sistemi devono essere progettati, configurati e gestiti in modo tale che tutte le misure di sicurezza ragionevoli in uno specifico contesto siano attivate di default e possano esplicare la loro efficacia senza che le utenti e gli utenti debbano occuparsene.

ID	Requisito
	I componenti di sistema che applicano decisioni di accesso devono essere progettati in modo tale che, in caso di malfunzionamento, non siano possibili accessi non autorizzati.
01.06	Privacy by design e privacy by default: le misure di protezione dei dati sono integrate in modo sistematico nei processi di sviluppo del sistema. I sistemi sono progettati affinché impostazioni di protezione dei dati sicure siano definite come standard fin dall'inizio.

2.2 Organizzazione

ID	Requisito
02.01	Responsabilità: i compiti, le competenze e le responsabilità relative al sistema devono essere concordati tra la struttura sanitaria e il fornitore prima della stipula del contratto. In particolare, devono essere disciplinate le responsabilità per i singoli componenti di un sistema, nonché le responsabilità per il corretto funzionamento congiunto del sistema con componenti messi a disposizione dalla struttura sanitaria.
02.02	Responsabilità per il sistema: il fornitore è responsabile del corretto funzionamento di tutti i componenti del sistema inclusi nell'ambito di fornitura. Ciò comprende anche il corretto funzionamento congiunto con componenti messi a disposizione dalla struttura sanitaria e conformi alle specifiche concordate per iscritto.
02.03	Obbligo di segnalare gli incidenti di sicurezza: gli incidenti di sicurezza (attacchi informatici) che coinvolgono i fornitori e i loro subfornitori (incluse le violazioni della protezione dei dati) devono essere segnalati nel rispetto dei termini di legge (Legge sulla sicurezza delle informazioni, LSIn). La struttura sanitaria deve essere informata entro 24 ore dalla rilevazione tramite l'unità competente della struttura sanitaria e successivamente aggiornata in modo continuativo [R03].
02.04	Gestione attiva del ciclo di vita: il fornitore garantisce il rispetto dei cicli di vita definiti dai produttori per tutti i componenti dei propri sistemi (incluse applicazioni, sistemi operativi, ecc.). I componenti per i quali non sono più disponibili aggiornamenti di sicurezza devono essere sostituiti. Rif. MDS2: DOC-8
02.05	Gestione attiva delle vulnerabilità: il fornitore mantiene un sistema di gestione delle vulnerabilità (*vulnerability management*) per tutti i componenti del sistema. Egli verifica regolarmente i componenti del sistema alla ricerca di vulnerabilità e monitora le segnalazioni di vulnerabilità dei rispettivi produttori dei componenti. Il fornitore informa la struttura sanitaria in modo attivo e trasparente in merito a nuove vulnerabilità non appena vengono individuate, indipendentemente dal fatto che sia già disponibile una contromisura. L'ICT della struttura sanitaria designa un punto di contatto per tali segnalazioni [R03]. Rif. MDS2: CSUP-11 Rif. MDS2: RDMP-4
02.06	Punto di contatto per le vulnerabilità: il fornitore designa un punto di contatto all'interno della propria organizzazione al quale la struttura sanitaria può segnalare le vulnerabilità individuate. Il fornitore garantisce che tali segnalazioni siano trattate tempestivamente da specialisti e che la struttura sanitaria venga informata sui risultati.
02.07	Risoluzione delle vulnerabilità: il fornitore mette a disposizione tutti i mezzi necessari per la risoluzione delle vulnerabilità. Le patch di sicurezza devono essere installate tempestivamente, oppure rese disponibili alla struttura sanitaria per l'installazione, a partire dal momento della loro disponibilità e in funzione del grado di gravità della vulnerabilità, classificata secondo l'ultima versione del Common Vulnerability Scoring System (CVSS).

ID	Requisito
02.08	Tempistiche per la risoluzione delle vulnerabilità: le tempistiche per la risoluzione delle vulnerabilità si basano sul Common Vulnerability Scoring System (CVSS). Si applica quanto segue: ▪ Critico (CVSS = 9.0 – 10.0): il più rapidamente possibile[1] ▪ Alto (CVSS = 7.0 – 8.9): 2 settimane ▪ Medio (CVSS = 4.0 – 6.9): 1 mese ▪ Basso (CVSS = 0.1 – 3.9): 2 mesi [1] La durata dipende dai rischi di disponibilità associati all'installazione. Qualora componenti del sistema siano messi a disposizione dalla struttura sanitaria in accordo con il fornitore, la struttura sanitaria è responsabile dell'aggiornamento di tali componenti. La responsabilità complessiva per il corretto funzionamento del sistema rimane comunque in capo al fornitore. Il fornitore definisce nei confronti della struttura sanitaria i componenti da utilizzare per l'aggiornamento e garantisce la compatibilità del componente aggiornato con il sistema complessivo.
02.09	Autorizzazione alla messa in esercizio: il sistema viene messo in esercizio produttivo solo dopo l'accettazione da parte dei settori specialistici coinvolti (ad es. tecnica degli edifici, informatica medica, tecnologia medica) e dell'ICT della struttura sanitaria [R03]. L'accettazione viene documentata per iscritto.
02.10	Presa in consegna o trasporto di sistemi fisici: i sistemi e tutti i loro componenti possono lasciare la struttura sanitaria esclusivamente previa autorizzazione del personale ICT competente della struttura sanitaria [R03]. Prima della presa in consegna o del trasporto di sistemi o componenti, indipendentemente dal motivo, i dati della struttura sanitaria devono essere cancellati in modo irreversibile [05.05] oppure distrutti in modo sicuro [05.06]. Ciò deve essere confermato per iscritto al personale ICT competente della struttura sanitaria prima della presa in consegna o del trasporto.

2.3 Documentazione

ID	Requisito
03.01	Documentazione dell'architettura: l'architettura del sistema e/o della soluzione complessiva deve essere documentata in modo completo. La documentazione dell'architettura comprende almeno i seguenti punti: 1. rappresentazione grafica d'insieme di tutti i sistemi, le applicazioni e i componenti che fanno parte della soluzione; 2. evidenza di tutti i componenti dei prodotti software utilizzati e delle loro relazioni all'interno della catena di fornitura del software (Software Bill of Materials); 3. interfacce verso sistemi interni ed esterni già esistenti, con almeno le seguenti informazioni: sorgente, destinazione, protocollo/i, cifratura, autenticazione, oggetti dati trasmessi con classificazione del livello di riservatezza e indicazione dello scopo; 4. comunicazioni di dati verso sistemi interni ed esterni già esistenti (ad es. trasmissione di dati di consumo, accessi remoti, monitoraggio); 5. flussi di dati nella forma: scopo, contenuto dei dati, protezione della riservatezza durante la trasmissione e l'archiviazione dei dati. Per la classificazione dei livelli di riservatezza degli oggetti dati si applica la relativa direttiva della struttura sanitaria [R03].

ID	Requisito
	Rif. MDS2: DOC-10
03.02	Documentazione tecnica di esercizio: per il sistema viene fornita una documentazione tecnica di esercizio che comprende almeno i seguenti punti: 1. panoramica generale di tutti i sistemi che fanno parte della soluzione (ad es. sistema operativo, applicazioni, COTS[2]/SOUP[3]) e di ogni altro componente essenziale necessario per un esercizio stabile e sicuro; 2. installazione, configurazione, esercizio e manutenzione (in loco e/o da remoto), descrizione di tutti i sistemi, le applicazioni e i componenti della soluzione, inclusi editore, licenza del prodotto e numero di versione; 3. sistemi e relative configurazioni nella seguente forma: denominazione del sistema, sistema operativo utilizzato, applicazioni installate con indicazione del numero di versione, servizi e account (in particolare quelli con privilegi elevati); 4. elenco di tutti i supporti di memorizzazione elettronici presenti nel sistema sui quali potrebbero essere archiviati dati della struttura sanitaria. Devono essere indicati il tipo di supporto (ad es. SSD, HDD, ecc.) e la posizione fisica nel dispositivo per poter individuare i supporti; 5. dichiarazione di tutti i luoghi di memorizzazione temporanei e permanenti, con indicazione dei dati della struttura sanitaria ivi archiviati; 6. identificazione dei punti di controllo da monitorare per il corretto funzionamento, con indicazione dei parametri rilevanti per un esercizio regolare; 7. matrice di comunicazione nel seguente formato: sorgente, destinazione, protocollo di rete, porta e scopo. Rif. MDS2: DOC-10 Rif. MDS2: SBOM-1
03.03	Documentazione operativa di esercizio: per il sistema viene redatta una documentazione operativa di esercizio, concordata con l'unità competente della struttura sanitaria [R03]. Tale documentazione comprende almeno: 1. le responsabilità e i contatti interni (struttura sanitaria) ed esterni (fornitore), nonché i relativi processi di manutenzione, supporto e amministrazione, in particolare: a) dichiarazione della responsabilità operativa dei componenti del sistema; b) istruzioni per il supporto di 1° livello su come procedere in caso di errori noti; c) istruzioni per il supporto di 2° livello su come analizzare gli errori e quando effettuare l'escalation al supporto di 3° livello (produttore); d) istruzioni su come arrestare correttamente i componenti del sistema; e) istruzioni su come avviare correttamente i componenti del sistema; 2. la documentazione utente della soluzione (manuale utente).
03.04	Documentazione di sicurezza: il fornitore mette a disposizione la seguente documentazione di sicurezza relativa al prodotto offerto e/o alla propria organizzazione: 1. *Information Security Policy*; 2. certificato ISO 27001, se disponibile; 3. attuazione di raccomandazioni e best practice in ambito di sicurezza e protezione dei dati (ad es. ISO 27018);

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

ID	Requisito
	4. ulteriori certificazioni in ambito di sicurezza e protezione dei dati, se disponibili; 5. istruzioni su come riavviare un sistema andato in crash e quali verifiche devono essere effettuate per garantire l'integrità dei dati; 6. istruzioni su come riportare un esercizio limitato (modalità di emergenza) a un funzionamento regolare. Rif. MDS2: SGUD-1
03.05	Documentazione di sicurezza per sistemi di tecnologia medica: per i sistemi di tecnologia medica sono disponibili le seguenti attestazioni: 1. certificato IEC 62304; 2. certificato CE; 3. *Manufacturer Disclosure Statement for Medical Device Security* (MDS2). Rif. MDS2: RDMP-1
03.06	Documentazione per l'accettazione: al momento dell'accettazione del sistema da parte della struttura sanitaria è disponibile la seguente documentazione: ▪ documentazione dell'architettura; ▪ documentazione tecnica di esercizio; ▪ documentazione operativa di esercizio; ▪ documentazione di sicurezza; ▪ documentazione di sicurezza per sistemi di tecnologia medica, se applicabile.
03.07	Forma della documentazione: la documentazione viene fornita in formato elettronico e in un formato comunemente utilizzato (ad es. PDF).
03.08	Verifica: tutta la documentazione deve essere presentata alla struttura sanitaria per l'accettazione. La messa in esercizio del sistema avviene solo dopo l'avvenuta accettazione della documentazione. Tutte le modifiche alla documentazione, ad eccezione di modifiche di lieve entità, devono essere comunicate attivamente alla struttura sanitaria durante l'intera fase di esercizio del sistema e, se necessario, concordate preventivamente.

2.4 Configurazione di base

ID	Requisito
04.01	Riduzione dell'esposizione del sistema: per ridurre l'esposizione del sistema vengono adottate le seguenti misure: 1. blocco dell'accesso a Internet, qualora non sia necessario per il funzionamento o per garantire l'esercizio del sistema; 2. disinstallazione o disattivazione di tutti i pacchetti software e servizi di rete non necessari. Devono essere installati esclusivamente i pacchetti software e i servizi strettamente necessari per l'esercizio del sistema. Qualora vengano installati temporaneamente componenti ausiliari (ad es. durante un'attività di manutenzione), questi devono essere disinstallati al termine dei lavori; 3. installazione di un firewall locale che consenta l'accesso solo a porte di rete predefinite; 4. disattivazione delle porte USB, delle interfacce Bluetooth e di altre possibilità di connessione, qualora non siano necessarie per l'esercizio; 5. disattivazione delle funzioni «AutoRun/AutoPlay».

ID	Requisito
	Rif. MDS2: SAHD-1
04.02	Utilizzo di tecnologie a rischio: non vengono utilizzate tecnologie con rischi di sicurezza noti, ad esempio protocolli quali SMBv1, FTP o Telnet. Rif. MDS2: TXCF-5
04.03	Limitazione delle interfacce: le connessioni di comunicazione vengono stabilite esclusivamente tramite le interfacce concordate e documentate con la struttura sanitaria. Le interfacce non utilizzate vengono disattivate in modo da impedire qualsiasi comunicazione tramite esse.
04.04	Protezione degli endpoint: il sistema è protetto da malware e dall'uso improprio dei componenti di sistema mediante una soluzione di endpoint protection. Qualora l'utilizzo di una soluzione di endpoint protection comprometta la conformità del sistema (CE, MDR, ecc.), ciò deve essere dichiarato dal fornitore. Rif. MDS2: MLDP-2
04.05	Aggiornamento della endpoint protection: gli aggiornamenti di Security Intelligence per la soluzione di endpoint protection vengono installati regolarmente, almeno su base giornaliera. Le nuove versioni della soluzione di endpoint protection vengono installate tempestivamente. A tal fine, il sistema può stabilire una connessione a Internet [04.01].

2.5 Sicurezza dei dati

ID	Requisito
05.01	Archiviazione dei dati cifrata: i dati sono trattati conformemente alla direttiva di classificazione della struttura sanitaria [R03]. I dati sensibili e i dati personali devono essere cifrati almeno «at rest» mediante un procedimento crittografico sicuro; ciò vale in particolare per l'archiviazione dei dati su dispositivi mobili. Rif. MDS2: STCF-1
05.02	Procedimenti crittografici sicuri: per la cifratura vengono utilizzati esclusivamente procedimenti crittografici e lunghezze delle chiavi considerati sicuri. La struttura sanitaria si orienta in tal senso alla direttiva tecnica TR-02102 dell'Ufficio federale tedesco per la sicurezza informatica (BSI) [R01].
05.03	Trasmissione e memorizzazione dei dati: il fornitore non memorizza dati della struttura sanitaria sulla propria infrastruttura IT o sui propri supporti di memorizzazione (chiavette USB, dischi, ecc.). Lo stesso vale per la trasmissione dei dati. Sono esclusi da tale requisito i dati di sistema strettamente necessari a garantire l'esercizio. I dati non possono essere rimossi dalla struttura sanitaria senza il consenso scritto delle persone responsabili [R03]. Qualora vengano utilizzati sistemi cloud per il trattamento o la memorizzazione dei dati, questi devono essere documentati e il loro utilizzo deve essere espressamente autorizzato dalla struttura sanitaria.
05.04	Ciclo di vita dei dati: il ciclo di vita dei dati (raccolta, trattamento, archiviazione e cancellazione) è documentato e tiene conto dei requisiti di conformità (*compliance*) interni ed esterni relativi agli obblighi di conservazione della struttura sanitaria [R03]. Il sistema cancella i dati in modo autonomo solo qualora tale cancellazione sia consentita dalle leggi e dalle direttive interne applicabili alla struttura sanitaria.

ID	Requisito
	Il sistema mette a disposizione un'interfaccia tramite la quale i dati rilevanti per la struttura sanitaria possono essere trasferiti in modo conforme alla legge al sistema di archiviazione della struttura sanitaria (ad es. dati di trattamento). Il backup dei dati avviene secondo i metodi e i processi standard della struttura sanitaria [R03].
05.05	Funzione di cancellazione sicura: il sistema supporta funzioni di cancellazione sicura che consentono la cancellazione irreversibile di tutti i dati della struttura sanitaria dai supporti di memorizzazione locali, in particolare di tutti i dati delle pazienti e dei pazienti, delle credenziali di accesso quali password e chiavi, delle statistiche di utilizzo, dei risultati di misurazione, ecc. Tali funzioni di cancellazione sono conformi allo standard VSIT del BSI oppure allo standard DoD-5220.22-M (E) e sono descritte in modo dettagliato dal fornitore nella documentazione. Dopo l'applicazione delle funzioni di cancellazione, sul dispositivo rimangono esclusivamente le informazioni corrispondenti alla configurazione di base iniziale del sistema e allo stato di fabbrica.
05.06	Distruzione dei dati: in caso di sostituzione dei supporti di memorizzazione, tutti i dati ivi memorizzati devono essere preventivamente cancellati in modo sicuro [05.05]. In alternativa, il fornitore può distruggere i supporti di memorizzazione in modo sicuro e smaltirli in modo ecocompatibile oppure consegnarli alla struttura sanitaria per la distruzione. Tale operazione deve essere comprovata per iscritto alla struttura sanitaria. I supporti di memorizzazione non possono essere rimossi dalla struttura sanitaria senza il consenso scritto delle persone responsabili. La distruzione fisica dei supporti di memorizzazione avviene secondo la norma DIN 66399 (classe di protezione 2) [R04]. Rif. MDS2: SGUD-2

2.6 Protezione dei dati

ID	Requisito
06.01	Gestione centralizzata: l'accesso ai dati personali sensibili sui sistemi all'interno della struttura sanitaria avviene esclusivamente tramite account utente personali, gestiti centralmente dalla struttura sanitaria. Non vengono utilizzati account locali per tali accessi. Rif. MDS2: AUTH-1.1
06.02	Trattamento dei dati: il trattamento dei dati personali e di altri dati meritevoli di protezione avviene esclusivamente in Svizzera o in un Paese con un livello di protezione dei dati adeguato. Fa fede la normativa vigente applicabile alla rispettiva struttura sanitaria (diritto nazionale o cantonale). Come data di riferimento vale la data dell'offerta o dell'acquisto.
06.03	Elenco dei dati personali: il fornitore indica quali dati personali vengono trattati e memorizzati dal sistema: 1. elenco dei dati con la relativa motivazione in relazione al principio di proporzionalità e alla limitazione delle finalità; 2. durata di conservazione dei dati memorizzati in modo permanente; 3. indicazione dei Paesi verso i quali tali dati potrebbero potenzialmente essere esportati (memorizzazione, backup, accesso). Rif. MDS2: MPII-1 Rif. MDS2: MPII-2 Rif. MDS2: MPII-3

2.7 Protocollo e tracciabilità

ID	Requisito
07.01	Protocollo: tutte le azioni sul sistema, in particolare: ▪ operazioni di accesso e disconnessione; ▪ situazioni di errore; ▪ esecuzioni di funzioni privilegiate e amministrative; ▪ modifiche dei diritti di accesso e dei ruoli utente; ▪ modifiche delle configurazioni di sistema; vengono protocollate in modo tracciabile. Rif. MDS2: AUDT-1 Rif. MDS2: AUDT-1.1 Rif. MDS2: AUDT-1.2 Rif. MDS2: AUDT-2.1 Rif. MDS2: AUDT-2.2
07.02	Audit trail: la registrazione documenta qualsiasi trattamento di dati tecnici rilevanti, dati personali o dati particolarmente sensibili, costituendo un audit trail completo. Rif. MDS2: AUDT-2 Rif. MDS2: AUDT-2.1 Rif. MDS2: AUDT-2.2 Rif. MDS2: AUDT-2.3 Rif. MDS2: AUDT-2.4 Rif. MDS2: AUDT-2.5 Rif. MDS2: AUDT-2.6 Rif. MDS2: AUDT-2.7 Rif. MDS2: AUDT-2.8 Rif. MDS2: AUDT-2.8.1 Rif. MDS2: AUDT-2.8.2 Rif. MDS2: AUDT-2.9 Rif. MDS2: AUDT-2.10 Rif. MDS2: AUDT-2.11
07.03	Protezione contro la manipolazione dei dati di log: i dati di log memorizzati temporaneamente o permanentemente sul sistema sono protetti contro la manipolazione e l'accesso non autorizzato. Rif. MDS2: AUDT-7
07.04	Inoltro dei dati di log: il sistema è in grado di inoltrare i dati di log a un server centrale di log della struttura sanitaria tramite un'interfaccia standardizzata e un formato standardizzato (ad es. Syslog). Rif. MDS2: AUDT-5 Rif. MDS2: AUDT-5.1 Rif. MDS2: AUDT-5.2 Rif. MDS2: AUDT-5.3

2.8 Comunicazione e accesso alla rete

ID	Requisito
08.01	Protocolli di comunicazione sicuri: il sistema utilizza esclusivamente protocolli di comunicazione con procedimenti crittografici e lunghezze delle chiavi considerati sicuri. La struttura sanitaria si orienta in tal senso alla direttiva tecnica TR-02102 del BSI [R01].
08.02	Monitoraggio degli errori di trasmissione: in caso di trasmissione di dati verso un sistema centrale della struttura sanitaria (ad es. PACS), gli errori di trasmissione vengono rilevati. Le

ID	Requisito
	persone utilizzatrici o l'unità ICT competente della struttura sanitaria [R03] vengono informate immediatamente dell'errore di trasmissione.
08.03	Cifratura: tutte le connessioni di comunicazione interne ed esterne da e verso il sistema sono cifrate mediante protocolli di comunicazione sicuri.
08.04	Funzionalità di routing: il sistema non consente funzionalità di bridging, routing o altre funzionalità di inoltro verso altri segmenti di rete. Le relative funzioni vengono disattivate.
08.05	Indirizzamento di rete: il sistema supporta un indirizzamento di rete configurabile, in modo che possa essere definito dalla struttura sanitaria.
08.06	Connessioni di comunicazione cablate: le connessioni di comunicazione cablate vengono stabilite esclusivamente tramite l'infrastruttura di rete della struttura sanitaria. Un sistema collegato alla rete supporta un'autenticazione basata sulla porta secondo lo standard 802.1X mediante EAP-TLS o soluzioni alternative equivalenti approvate dall'ICT della struttura sanitaria [R03].
08.07	Connessioni di comunicazione wireless (WLAN): per le connessioni di comunicazione wireless vengono utilizzati esclusivamente i componenti di rete della struttura sanitaria. Lo standard di cifratura utilizzato è almeno WPA2 Enterprise. Come protocollo di autenticazione viene utilizzato EAP-TLS. Soluzioni alternative equivalenti sono ammesse se approvate dall'ICT della struttura sanitaria [R03].
08.08	Connessioni bluetooth: qualora siano necessarie connessioni Bluetooth, queste devono corrispondere almeno a Security Mode 4 Level 4 per Bluetooth Classic e a Security Mode 1 Level 4 per Bluetooth LE.
08.09	Connessioni web in uscita verso internet: qualora siano necessarie connessioni a Internet, queste devono obbligatoriamente essere instradate tramite il web proxy della struttura sanitaria. Il sistema dispone a tal fine di funzionalità proxy.
08.10	Sincronizzazione dell'orario di sistema: il sistema supporta il protocollo di rete NTP per la sincronizzazione dell'orario di sistema. Rif. MDS2: AUDT-4.1.1

2.9 Controllo degli accessi

ID	Requisito
09.01	Separazione degli account per i servizi di sistema: gli account di servizio (account per i servizi di sistema) sono separati dagli account utente. Essi dispongono esclusivamente delle autorizzazioni necessarie per l'esercizio dei servizi di sistema previsti (principio del minimo privilegio). Rif. MDS2: AUTH-2
09.02	Utilizzo di account amministrativi locali: gli account amministrativi locali vengono utilizzati esclusivamente per attività di manutenzione e configurazione. L'utilizzo operativo avviene tramite account utente personali.
09.03	Accessi autenticati: gli accessi al sistema avvengono esclusivamente previa autenticazione. Tutti gli account utente sono protetti mediante adeguati meccanismi di autenticazione. Rif. MDS2: AUTH-1
09.04	Autenticazione delle interfacce: la trasmissione dei dati tramite interfacce avviene esclusivamente in modalità autenticata. Viene autenticato almeno il sistema mittente rispetto a quello

ID	Requisito
	destinatario. Le informazioni di autenticazione (password, materiale crittografico, ecc.) sono archiviate in modo protetto contro accessi non autorizzati.
09.05	Regole sulle password: le password standard vengono modificate prima della messa in esercizio produttiva in conformità alle direttive della struttura sanitaria [R03]. È garantito che le password utilizzate siano generate in modo specifico per ciascuna struttura sanitaria e non vengano utilizzate presso altri clienti. Qualora sussista la possibilità che terzi non autorizzati vengano a conoscenza di tali password, il fornitore ne informa immediatamente la struttura sanitaria e le password vengono modificate nei sistemi interessati. Rif. MDS2: PAUT-6
09.06	Gestione delle informazioni di accesso: le informazioni di accesso (ad es. password, chiavi digitali o fisiche, ecc.) sono classificate come riservate e trattate e protette come tali dal fornitore e dai suoi sistemi. Le informazioni di accesso vengono modificate regolarmente, secondo intervalli da definire [R03].
09.07	Autorizzazione: il sistema dispone di un meccanismo di autorizzazione basato sui ruoli o di un meccanismo equivalente. Rif. MDS2: AUTH-2
09.08	Approvvigionamento delle autorizzazioni: il sistema supporta il collegamento al sistema IAM della struttura sanitaria tramite un'interfaccia standardizzata per il provisioning delle autorizzazioni. Rif. MDS2: PAUT-2
09.09	Blocco della sessione utente in caso di inattività: il sistema consente all'utente di bloccare manualmente la sessione (ad es. allontanandosi dal sistema). Inoltre, una sessione utente viene bloccata automaticamente dopo un periodo di inattività definito dalla struttura sanitaria [R03]. Rif. MDS2: ALOF-1
09.10	Identità federata: l'autenticazione degli utenti e la trasmissione delle informazioni necessarie per l'accesso alle risorse avvengono tramite un rapporto di fiducia (*trust*) tra il sistema e l'infrastruttura della struttura sanitaria predisposta a tal fine (*federated identity*). Rif. MDS2: PAUT-2

2.10 Manutenzione e supporto

ID	Requisito
10.01	Accessi remoti: i fornitori che necessitano di accesso remoto ai sistemi della struttura sanitaria rispettano i requisiti di sicurezza previsti a tal fine e utilizzano esclusivamente i sistemi di accesso remoto della struttura sanitaria [R03]. L'accesso remoto deve avvenire tramite account utente personali. I sistemi di accesso remoto specifici dei fornitori non sono supportati dalla struttura sanitaria. Rif. MDS2: RMOT-1 Rif. MDS2: RMOT-2 Rif. MDS2: RMOT-3
10.02	Preavviso delle attività di manutenzione: le attività di manutenzione svolte dal fornitore, indipendentemente dal fatto che avvengano in loco o tramite accesso remoto, devono essere preannunciate alla struttura specialistica e all'ICT della struttura sanitaria [R03]. Qualora circostanze particolari richiedano interventi di manutenzione immediati, questi devono essere

ID	Requisito
	comunicati successivamente entro 24 ore alla struttura specialistica e all'ICT, corredati da una motivazione comprensibile dell'urgenza.
10.03	Attività di manutenzione mediante supporti di memorizzazione rimovibili: il collegamento di supporti di memorizzazione rimovibili ai sistemi della struttura sanitaria (inclusi i sistemi forniti dal fornitore) non è consentito. I supporti di memorizzazione rimovibili per il trasferimento o il backup dei dati sono messi a disposizione dalla struttura sanitaria. Il fornitore mette a disposizione del personale ICT competente della struttura sanitaria il software necessario per l'esecuzione delle attività di manutenzione almeno due settimane prima dell'intervento. Tale software viene verificato e successivamente reso disponibile al fornitore su un supporto idoneo della struttura sanitaria per l'esecuzione della manutenzione.

3 Riferimenti

#	Denominazione	Riferimento
R01	BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen (in tedesco e inglese)	link
R02	Manufacturer Disclosure Statement for Medical Device Security (versione 2019, in inglese)	link
R03	Standard applicati e strategia IT nonché i punti di contatto della struttura sanitaria (IS). Questo documento viene fornito direttamente dall'IS ai fornitori.	Allegato della SS
R04	DIN 66399-1 Büro- und Datentechnik - Vernichten von Datenträgern (in tedesco e inglese)	link

Le referenze sono state verificate l'ultima volta il 2.2.2026.