DIE SPITÄLER DER SCHWEIZ
LES HÔPITAUX DE SUISSE
GLI OSPEDALI SVIZZERI

Sicurezza delle informazioni e protezione dei dati

Esigenze sulla sicurezza ICT dei sistemi esterni

Versione 1.2

H+: Schweizer Spitäler, Kliniken und Pflegeinstitutionen
H+: Hôpitaux, cliniques et institutions de soins suisses
H+: Gli Ospedali, le cliniche e gli istituti di cura svizzeri

Geschäftsstelle · Lorrainestrasse 4A · 3013 Bern
T 031 335 11 11 · F 031 335 11 70
geschaeftsstelle@hplus.ch · www.hplus.ch

Contenuto

1 Introduzione 3
1.1 Oggetto e scopo 3
1.2 Campo di applicazione e responsabilità 3
2 Catalogo dei requisiti 4
2.1 Documentazione 4
2.2 Configurazione di base 5
2.3 Protezione contro i malware 7
2.4 Accesso alla rete 7
2.5 Regole d’accesso 8
2.6 Logging e tracciabilità 9
2.7 Sicurezza dei dati 9
2.8 Manutenzione e supporto 10
2.9 Integrazione 10
2.10 Conformità 10

Allegato A Gestione del catalogo dei requisiti 12

1 Introduzione

Oltre ai sistemi gestiti ed acquistati dall'ICT interna, composte da piattaforme (hardware e sistemi operativi) ed applicazioni, l'ecosistema ICT di un ospedale comprende una moltitudine di sistemi che vengono acquistati altrove e integrati o gestiti in tutto o in parte da terzi. Tali sistemi sono sommariamente indicati come sistemi esterni.

Tipicamente questi sistemi esterni si occupano di tecnologia medica o di gestione degli stabili.

Lo scopo di questo documento è quello di garantire, mediante misure adeguate, la sicurezza operativa dei sistemi esterni e di conseguenza la sicurezza del paziente, di proteggere la privacy del paziente e dei dipendenti, nonché di proteggere adeguatamente i sistemi esterni contro i rischi ICT, dagli attacchi informatici così come pure la non compromissione di altri sistemi della rete ospedaliera da parte dei sistemi esterni.

1.1 Oggetto e scopo

Questo documento descrive i requisiti minimi di sicurezza ICT di sistemi esterni durante le fasi di acquisto, l'integrazione e funzionamento. In particolare, si occuperà dei sistemi medicali. I requisiti presenti nel capitolo 2 devono essere presi in considerazione quando si acquistano sistemi di terzi nell'ambito di progetti o investimenti grandi e piccoli, nonché durante la messa in servizio e l'utilizzo di questi sistemi.

Il presente documento regola esplicitamente solo la parte ICT di un sistema terzo e non la parte tecnica che non ha rilevanza ICT.

1.2 Campo di applicazione e responsabilità

Le presenti esigenze sono vincolanti per tutti i sistemi esterni e, in particolare, tutti i sistemi medicali incluse le loro applicazioni, che vengono integrati nelle infrastrutture di rete locale dell'ospedale.

La discriminante per cui un sistema deve sottostare al presente documento è l'esistenza di una connettività di rete.

Il campo di applicazione comprende le fasi d'acquisto, integrazione e funzionamento. La gestione dei requisiti è spiegata nell' allegato A.

Il presente documento è indirizzato a:

- I fornitori di servizi (ad esempio fornitori / produttori, integratori) come parte dell'acquisto di sistemi esterni;
- I dipendenti interni che sono responsabili nel contesto degli appalti, l'integrazione e la gestione di sistemi esterni, autorizzati a prendere decisioni o comunque coinvolti, compresi i responsabili per gli investimenti e i responsabili di progetto.

Gli allegati da B a H citati nel presente catalogo sono forniti dalle istituzioni nell'ambito del processo di acquisizione di sistemi di terzi. Il loro contenuto è specifico per ogni istituzione.

2 Catalogo dei requisiti

2.1 Documentazione

No.	requisito	categoria
SEC 1.1	**Documentazione tecnica d'architettura** Il fornitore documenta l'architettura del sistema, rispettivamente. della soluzione complessiva. La documentazione dell'architettura deve includere almeno i seguenti punti: ■ Panoramica di tutti i sistemi della soluzione, applicazioni e componenti; ■ Interfacce (sotto forma di origine, destinazione, protocollo(i), e lo scopo) tra gli attuali sistemi interni (ospedale) e sistemi esterni; ■ Altre comunicazioni di dati tra sistemi esistenti interni (ospedale) e sistemi esterni (come la trasmissione dei dati d'utilizzo, accesso remoto, monitoraggio). Il fornitore è tenuto a comunicare spontaneamente all'ospedale durante tutto il ciclo di vita del sistema rispettivamente della soluzione, tutti i cambiamenti concernenti la documentazione dell'architettura.	☑ obbligatorio ☐ richiesto
SEC 1.2	**Documentazione tecnica di funzionamento** Il fornitore documenta i sistemi e la loro configurazione in forma di: nome del sistema, il sistema operativo utilizzato, le applicazioni installate con il numero di versione, i servizi e gli account (in particolare quelli con accesso privilegiato), i numeri di serie di hardware e indirizzi MAC. Il fornitore mantiene aggiornata la documentazione tecnica di funzionamento durante l'intero ciclo di vita del sistema, in collaborazione con l'ospedale o ne passa la responsabilità alla struttura ospedaliera. La documentazione tecnica di funzionamento comprende almeno i seguenti punti: ■ Panoramica di tutti i sistemi della soluzione (per esempio, sistema operativo, applicazioni COTS[1]/ SOUP[2]) e qualsiasi altro componente essenziale, che sono necessari per il funzionamento sicuro; ■ L'installazione, la configurazione, il funzionamento e la manutenzione (a livello locale e/o in remoto), descrizione di tutti i sistemi associati alla soluzione, applicazioni e componenti, compreso il loro editore, licenza del prodotto e il numero di versione; ■ Matrice delle porte di comunicazione nel seguente formato: origine, destinazione, protocollo di rete, porta e scopo. La documentazione tecnica di funzionamento è parte del collaudo.	☑ obbligatorio ☐ richiesto
SEC 1.3	**Documentazione operativa di funzionamento** Il sistema è documentato dal fornitore in collaborazione con lo specialista competente del relativo servizio dell'ospedale. Questa documentazione operativa comprende almeno i seguenti punti: ■ Le responsabilità all'interno dell'ospedale e dei fornitori con i loro contatti, nonché le procedure di manutenzione, di supporto e le modalità amministrative; ■ La documentazione per l'utente della soluzione (Manuale). Il fornitore mantiene aggiornata la documentazione tecnica di funzionamento durante l'intero ciclo di vita del sistema presso l'ospedale. La documentazione operativa del funzionamento è parte del collaudo.	☑ obbligatorio ☐ richiesto
SEC 1.4	**Documentazione relativa alla sicurezza** La documentazione relativa alla sicurezza comprende almeno i seguenti punti: ■ Politica aziendale di sicurezza e protezione dei dati; ■ ISO 27'001 certificato, se applicabile; ■ IEC 62'304 certificato, se applicabile; ■ Ulteriori certificazioni in materia di sicurezza e protezione dei dati;	☑ obbligatorio ☐ richiesto

[1] COTS: Commercial off-the-shelf (software commerciale acquistato)

[2] SOUP: Software of unknown provenance (software di provenienza ignota)

No.	requisito	categoria
	▪ Il documento „Manufacturer Disclosure for Medical Device Security“ (https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx) è compilato e allegato; ▪ Certificato CE della soluzione; ▪ Attuazione delle raccomandazioni e le migliori pratiche per la sicurezza e la privacy (p.es: ISO 27 018). Il fornitore mantiene aggiornata la documentazione di sicurezza durante l'intero ciclo di vita del sistema presso l'ospedale.	
SEC 1.5	**Manufacturer Disclosure for Medical Device Security** Il documento „Manufacturer Disclosure for Medical Device Security“ (http://www.himss.org/resourcelibrary/MDS2) è compilato e allegato.	☑ obbligatorio ☐ richiesto
	Eccezioni: Il criterio SEC 1.5 è rilevante solo per i sistemi medicali.	
SEC 1.6	**Collaudo e messa in servizio** Un sistema esterno può essere messo in servizio produttivamente solo dopo l'accettazione da parte del servizio interessato, il servizio di assistenza (ad esempio, ospedale, medico) e l'ICT. Il collaudo deve essere protocollato in forma scritta.	☑ obbligatorio ☐ richiesto

2.2 Configurazione di base

No.	requisito	categoria
SEC 2.1	**Piattaforme e sistemi operativi** Il fornitore deve indicare se l'ospedale deve assumersi la responsabilità per la gestione e il funzionamento della soluzione in parte o in totale (vedi anche SEC 1-3). In caso contrario, la soluzione è completamente basata su piattaforme e sistemi operativi supportati dall'ospedale di cui all'allegato B.	☑ obbligatorio ☐ richiesto
SEC 2.2	**Sistema operativo obsoleto** L'uso di sistemi operativi non più supportati dai produttori non è permesso. Il fornitore è tenuto a specificare se il sistema operativo utilizzato nella soluzione offerta è supportato dal produttore, indicando la data di "End-of-Support". Se l' "End-of-Support" cade durante la vita prevista della soluzione, il fornitore presenta un piano d'aggiornamento, comprensivo dei costi in dettaglio.	☑ obbligatorio ☐ richiesto
SEC 2.3	**Ciclo di vita dei prodotti software integrati** Il fornitore si impegna per tutti i prodotti software integrati (ad esempio, sistema operativo, database, COTS/SOUP): ▪ Di applicare gli aggiornamenti software pubblicati dai fornitori e mantenere aggiornate le versioni in modo tempestivo; ▪ Informare immediatamente l'ICT se il software integrato non è più mantenuto da parte del fornitore, e questo a prescindere dalla durata dell'apparecchio. Le ragioni di questo devono essere menzionate; ▪ Per i prodotti Microsoft Windows di supportare: l'attuale "Current Branch for Business" (Current Branch [Semi Annual Channel] with Deferred Updates e "Long Term Servicing Channel"; mentre per office di supportare la versione "on premises" oppure la versione cloud Office 365.	☐ obbligatorio ☑ richiesto
SEC 2.4	**Minimizzazione dell'esposizione del sistema** Per ridurre al minimo l'esposizione del sistema, i seguenti requisiti devono essere applicati: ▪ L'accesso a Internet è bloccato. In caso contrario, le richieste di accesso a internet devono essere descritte; ▪ Installazione unicamente di pacchetti software necessari e servizi del sistema operativo; ▪ Disinstallare rispettivamente disabilitare tutti i software e servizi di rete inutili; ▪ Installazione di un firewall locale, che consente solo l'accesso alle porte di rete predefinite.	☑ obbligatorio ☐ richiesto

No.	requisito	categoria
	▪ Disattivazione delle porte USB e altri dispositivi removibili; ▪ Disattivazione delle funzioni "AutoRun / AutoPlay".	
	Eccezioni: Fatta eccezione per il punto sull'accesso Internet, il criterio SEC 2.4 non è rilevante per soluzioni applicative pure. E 'consentito l'uso dell'interfaccia USB per i dongle per scopi di licenza e di autenticazione; in questo caso, viene eliminata la richiesta di disattivare le porte USB.	
SEC 2.5	**Tecnologie ad alto rischio Informatico** L'ospedale ha lo scopo di eliminare le tecnologie ad alto rischio informatico. Il fornitore deve chiarire se una delle tecnologie classificate a rischio per l'ospedale è parte della soluzione. L'elenco delle tecnologie a rischio sono elencati nell'allegato C. Il fornitore deve suggerire una tecnologia alternativa. Se non ci sono alternative possibili, i seguenti punti devono essere chiariti: ▪ Caso d'uso della soluzione che richiede queste tecnologie; ▪ Spiegazione del perché nessuna alternativa viene presa in considerazione; ▪ Piano e scadenza per la sostituzione di queste tecnologie nella linea di soluzione del prodotto interessato.	☐ obbligatorio ☑ richiesto
SEC 2.6	**Release Management** Al momento della consegna del sistema, per ogni applicazione, la versione più recente approvata dal costruttore deve essere installata.	☐ obbligatorio ☑ richiesto
	Nota: Se non v'è alcuna possibilità di installare l'ultima versione rilasciata, l'ICT può decidere di isolare la soluzione dalla rete. Questa circostanza è da includere nel calcolo del TCO, con un impatto sulla valutazione dell'offerta.	
SEC 2.7	**Gestione della sicurezza** Il processo per la gestione di aggiornamenti relativi alla sicurezza (patch di sicurezza, aggiornamenti e Fixes) si basa sui bollettini sulla sicurezza dei rispettivi produttori. Questo vale sia per il sistema operativo che per le applicazioni. Il fornitore comunica le vulnerabilità, difetti o malfunzionamenti di sicurezza entro 30 di calendario giorni e garantisce che gli aggiornamenti forniti dal produttore (inclusi produttori di terze parti come Microsoft) siano installati entro e non oltre 60 di calendario giorni dalla pubblicazione del bollettino sulla sicurezza del produttore, rispettivamente viene rilasciato per l'installazione da parte dell'ospedale. In caso di situazioni ad alto rischio, questo termine dovrà essere ridotto secondo le esigenze dell'ospedale (p.es: Wannacry).	☐ obbligatorio ☑ richiesto
	Nota: Per soluzioni applicative il criterio SEC-2.7 riguarda solo l'applicazione stessa.	
	Nota: Se non v'è alcuna possibilità di installare l'ultima versione rilasciata, l'ICT può decidere di isolare la soluzione dalla rete. Questa circostanza è da includere nel calcolo del TCO, con un impatto sulla valutazione dell'offerta.	
SEC 2.8	**Affidabilità della soluzione** Il fornitore garantisce in ogni momento l'affidabilità della soluzione durante il suo ciclo di vita in ospedale. Se non è possibile per il fornitore: ▪ Di seguire il ciclo di aggiornamenti del software (vedi SEC 2.3) e/o; ▪ Di convalidare e installare entro 60 giorni di calendario le ultime patch di sicurezza e/o aggiornamenti software (vedi SEC 2.7). gli viene chiesto di documentare gli scenari di rischio conseguenti. Il fornitore documenta i possibili scenari di rischio, e ne sottolinea il potenziale impatto sull'ospedale nei seguenti punti: ▪ Sicurezza delle cure mediche; ▪ Sicurezza dei dati dei pazienti e/o dipendenti; ▪ La sicurezza fisica dei pazienti/personale; ▪ Conformità legale.	☐ obbligatorio ☑ richiesto
SEC 2.9	**Meccanismi di crittografia** I meccanismi di crittografia e la scelta delle proprietà (p.es lunghezza della chiave) sono realizzati come richiesto dai siti di riferimento pertinenti (es BSI, NIST).	☑ obbligatorio ☐ richiesto

2.3 Protezione contro i malware

No.	requisito	categoria
SEC 3.1	**Anti-malware** Una soluzione anti-malware è installata su tutti i sistemi core, sistemi periferici e sistemi client della soluzione. Un meccanismo di tipo "whitelisting applicazione" che blocca l'esecuzione di software non autorizzati è anche considerato accettabile. Esclusioni dell'attività dell'anti-malware sono autorizzate ma devono essere definite per ogni sistema e documentate. Se il fornitore non suggerisce uno dei meccanismi sopra descritti, deve motivarne le ragioni e chiarire gli scenari di rischio connessi. Se l'uso di un programma antivirus viola la conformità "CE", questo deve essere comprovato.	☑ obbligatorio ☐ richiesto
SEC 3.2	**Regolarità dei controlli anti-malware** Il controllo effettuato dalla soluzione anti-malware avviene regolarmente. Un controllo completo deve essere fatto almeno settimanalmente. I risultati dei test sono forniti all'ospedale su richiesta. Ogni malware scoperto deve essere segnalato all'ospedale.	☑ obbligatorio ☐ richiesto
SEC 3.3	**Aggiornamento del software anti-malware e delle firme ("signatures")** La soluzione anti-malware installata deve essere aggiornata regolarmente, almeno quotidianamente con le firme e le versioni.	☑ obbligatorio ☐ richiesto
SEC 3.4	**Anti-malware standard della società** Se lo standard dell'ospedale secondo la descrizione nell'allegato D viene adottato, l'aggiornamento delle firme e delle versioni avviene dai sistemi centrali dell'ospedale.	☐ obbligatorio ☑ richiesto
Eccezioni: i criteri SEC da 3.1 a 3.4 SEC non sono rilevanti per soluzioni applicative pure.		

2.4 Accesso alla rete

No.	requisito	categoria
SEC 4.1	**Protocolli di connessione sicura nell'intranet** Qualsiasi comunicazione dei protocolli di collegamento nella rete intranet deve essere cifrata (SSH, SFTP, TLS, ecc). Le eccezioni sono da documentare.	☐ obbligatorio ☑ richiesto
SEC 4.2	**Protocolli di connessione sicura verso Internet** I protocolli di connessione sicura e cifrata (SSH, SFTP, TLS, etc.) devono essere utilizzati per eventuali comunicazioni verso Internet.	☑ obbligatorio ☐ richiesto
SEC 4.3	**Funzionalità di routing** Il sistema non deve fornire bridging, routing o altra funzione di inoltro per altri segmenti di rete; funzioni corrispondenti devono essere disattivate.	☑ obbligatorio ☐ richiesto
SEC 4.4	**Indirizzamento di rete** Gli indirizzi di rete sono specificati dall'ospedale o definiti in accordo con l'ospedale.	☑ obbligatorio ☐ richiesto
SEC 4.5	**Collegamenti di comunicazione cablati** Per i collegamenti di comunicazione cablate, saranno utilizzati esclusivamente i componenti di rete dell'ospedale in conformità all'allegato E.	☑ obbligatorio ☐ richiesto
SEC 4.6	**Collegamenti di comunicazione wireless (WLAN)** Per i collegamenti di comunicazione senza fili, saranno utilizzati esclusivamente componenti di rete dell'ospedale in conformità all'allegato E. Per l'autenticazione è richiesto l'accesso alla rete tramite WPA2 Enterprise / EAP-TLS. I certificati necessari vengono emessi in ospedale.	☑ obbligatorio ☐ richiesto
SEC 4.7	**Le connessioni in uscita verso Internet** Le connessioni in uscita su Internet possono avvenire soltanto verso gli indirizzi IP definiti del fornitore di servizi. Un accesso diretto dei sistemi interni su Internet non è consentita ai sistemi, ed è fornito necessariamente tramite un sistema DMZ.	☐ obbligatorio ☑ richiesto

No.	requisito	categoria
SEC 4.8	**Autenticazione di rete (Network Access Control)** La soluzione supporta i metodi per l'autenticazione di rete IEEE 802.1x. Se necessario, il provider offre un meccanismo alternativo per l'autenticazione di rete ad un livello comparabile di sicurezza.	☐ obbligatorio ☑ richiesto
SEC 4.9	**La sincronizzazione dell'orario del sistema** La soluzione deve supportare la sincronizzazione dell'orario di sistema basato sul protocollo di rete NTP.	☑ obbligatorio ☐ richiesto
Eccezioni: i criteri SEC 4.3 a 4.6 SEC e SEC 4.8 a 4.9 SEC non sono rilevanti per soluzioni applicative pure.		

2.5 Regole d'accesso

No.	requisito	categoria
SEC 5.1	**Regole password** Gli account utente locale e utente generico, in particolare l'account utente di amministrazione, così come quelli con i quali è possibile l'accesso alle informazioni sensibili, inclusi i dati personali del paziente, devono essere protetti da password. Le regole della password dell'ospedale sono riportati nell'allegato F.	☑ obbligatorio ☐ richiesto
SEC 5.2	**Modifica della password** Le password locali standard/di default devono essere modificate prima dell'inizio produttivo. Le password utilizzate non possono essere utilizzate da altri clienti. Se esiste la possibilità che terzi non autorizzati possano venire a conoscenza di tali password, questo evento deve essere segnalato all'ospedale e le password devono essere modificate immediatamente	☑ obbligatorio ☐ richiesto
	Nota: il criterio SEC-5.2 non richiede alcuna implementazione tecnica, ma può anche essere realizzato a livello organizzativo.	
SEC 5.3	**Salvaguardia della password con un solo ruolo** Se il dispositivo consente solo un solo account per ruolo, la password associata deve essere memorizzata in ospedale.	☑ obbligatorio ☐ richiesto
SEC 5.4	**Blocco account utente dopo inserimento credenziali errate** Un account utente deve essere bloccato dopo tre immissioni errate. Uno sblocco automatico avviene dopo un periodo di tempo configurabile, conformemente alla definizione indicata nell'allegato F.	☐ obbligatorio ☑ richiesto
SEC 5.5	**Blocco della sessione utente in caso di inattività** Dopo un tempo di inattività definito nell'allegato F, la sessione utente è bloccata ed è necessaria una riautenticazione.	☐ obbligatorio ☑ richiesto
SEC 5.6	**Separazione degli account tecnici e di servizio** Account per tecnici, servizi e applicazioni devono essere separati. A questi account devono essere forniti dei diritti minimi.	☑ obbligatorio ☐ richiesto
SEC 5.7	**Utilizzo di account di amministratore locale** Gli account di amministratore locale possono essere utilizzati solo per la manutenzione e la configurazione. L'uso operativo deve avvenire tramite ID utente personali.	☑ obbligatorio ☐ richiesto
SEC 5.8	**Autorizzazione basata sui ruoli** L'autorizzazione è basata sui ruoli. I ruoli sono, almeno parzialmente, liberamente configurabili.	☐ obbligatorio ☑ richiesto
SEC 5.9	**Gestione centralizzata tramite Active Directory** Le soluzioni basate su sistema operativo Windows saranno integrati nella Active Directory della società. I seguenti criteri sono automaticamente soddisfatti: ■ Blocco dell'account utente dopo inserimento credenziali non corrette (SEC-5.4); ■ Blocco della sessione utente a causa di inattività (SEC-5.5); ■ Utilizzo di account amministratore locale (SEC 5.7).	☐ obbligatorio ☑ richiesto

2.6 Logging e tracciabilità

No.	requisito	categoria
SEC 6.1	**Logging** Tutte le azioni sui sistemi e applicazioni, tra cui l'accesso e gli eventi di disconnessione e le situazioni di errore devono venire registrate così da renderle tracciabili.	☑ obbligatorio ☐ richiesto
SEC 6.2	**Tracciabiltà (audit rail)** La registrazione tiene traccia di tutti gli accessi ai dati tecnici, personali o particolarmente sensibili, in ottica di un processo di audit.	☐ obbligatorio ☑ richiesto
SEC 6.3	**Protezione contro la manomissione dei dati di log** I dati di log memorizzati temporaneamente o permanentemente sui sistemi sono protetti contro la manipolazione e l'accesso non autorizzato.	☐ obbligatorio ☑ richiesto
SEC 6.4	**Inoltro dati del protocollo** I dati di log possono essere inoltrati a un server log centrale. Il fornitore descrive i modi per farlo (ad esempio tramite syslog)	☐ obbligatorio ☑ richiesto

2.7 Sicurezza dei dati

No.	requisito	categoria
SEC 7.1	**Elaborazione dei dati** Il fornitore indicherà quali dati personali e sensibili che necessitano di una protezione appropriata sono trattati e memorizzati dalla soluzione: ■ Elenco di dati con la giustificazione in termini di proporzionalità e di finalità; ■ Periodo di conservazione dei dati memorizzati in modo permanente; ■ Elenco dei paesi in cui potrebbero potenzialmente essere esportati tali dati.	☑ obbligatorio ☐ richiesto
SEC 7.2	**Archiviazione dati cifrati** L'archiviazione locale dei dati personali e sensibili che necessitano di una protezione appropriata è cifrata.	☐ obbligatorio ☑ richiesto
SEC 7.3	**Trasmissione dei dati** La trasmissione dei dati personali, sensibili o che necessitano di una protezione appropriata, a sistemi esterni al di fuori della società può avvenire esclusivamente alle seguenti condizioni: ■ I dati vengono trasmessi esclusivamente cifrati; ■ I dati personali/sensibili sono trasmessi esclusivamente in forma anonima o sotto pseudonimo.	☐ obbligatorio ☑ richiesto
SEC 7.4	**Ciclo di vita dei dati** Il ciclo di vita (raccolta, elaborazione, archiviazione e cancellazione) dei dati è documentato e tiene conto dei requisiti di conformità interni ed esterni per quanto riguarda l'obbligo di conservazione.	☐ obbligatorio ☑ richiesto
SEC 7.5	**Backup e ripristino** Il fornitore deve fornire una stima del volume di backup dei dati tecnici, personali e sensibili per una conservazione di 10 anni. La memorizzazione dei dati prodotti dalla soluzione deve essere conforme alle norme applicabili in Svizzera e agli standard dell'ospedale. Il backup di questi dati deve essere effettuata secondo metodi e processi standard dell'ospedale (vedi allegato G). In nessun caso possono essere utilizzati per questo dischi rigidi locali o supporti removibili (hard drive USB, per esempio).	☐ obbligatorio ☑ richiesto
SEC 7.6	**Distruzione dei dati** Per i supporti di memorizzazione che vengono sostituiti, i dati devono essere cancellati in anticipo. Il fornitore di servizi può eliminare il disco se dimostra all'ospedale per iscritto che la distruzione sicura viene effettuata secondo la norma DIN 66399 (classe 2). I dati subiscono una cancellazione sicura secondo la norma VSIT dell'ufficio federale germanico delle sicurezza (BSI) o secondo lo standard DoD 5220.22-M (E).	☑ obbligatorio ☐ richiesto

2.8 Manutenzione e supporto

No.	requisito	categoria
SEC 8.1	**Processo standard di accesso remoto** L'accesso remoto viene fatto usando gli standard dell'ospedale secondo la descrizione nell'allegato H. Altre opzioni di connessione sono disattivate. Se lo standard della struttura ospedaliera per la soluzione non può essere attuato, il fornitore deve giustificare le ragioni e presentare una soluzione alternativa con un livello comparabile di sicurezza.	☐ obbligatorio ☑ richiesto
SEC 8.2	**Accesso remoto** Un accesso remoto ai sistemi della società è eseguito in conformità con i seguenti requisiti: ▪ Gli accessi sono cifrati; ▪ Gli accessi sono registrati in maniera non alterabile. Si tratta di ricostruire quale persona (chi) ha eseguito l'accesso in quel momento (quando) su quale sistema (dove); ▪ Gli accessi sono, almeno una volta, autenticati da un ID utente personale, preferibilmente su sistemi della società. Se questa autenticazione non viene eseguita sui sistemi della società, i registri di controllo sono forniti all'ospedale regolarmente, e senza l'assistenza della società, ma almeno su richiesta dell'ospedale.	☑ obbligatorio ☐ richiesto
SEC 8.3	**Preavviso per lavori di manutenzione** Tutti i lavori di manutenzione da parte del fornitore del servizio, indipendentemente dal fatto che si svolgano a livello locale o in remoto, vanno preavvisati allo specialista di settore e al supporto. Se le circostanze speciali richiedono manutenzione immediata queste devono essere comunicate entro 24 ore agli specialisti e al servizio di assistenza, indicando in modo comprensibile le ragioni dell'urgenza.	☑ obbligatorio ☐ richiesto

2.9 Integrazione

No.	requisito	categoria
SEC 9.1	**Monitoraggio degli errori di trasmissione** Il fornitore deve indicare se un trasferimento di dati della soluzione ad un sistema centralizzato dell'ospedale (ad es PACS) è previsto; se e in quale forma un errore di trasmissione sarà segnalato immediatamente all'utente e al servizio informatica. Che possibilità ci sono di individuare, per es., che un sistema d'immagini non fornisce più i dati al sistema di archiviazione delle immagini (protezione contro la perdita dei dati)?	☐ obbligatorio ☐ richiesto
SEC 9.2	**Scambio dei dati** Il fornitore deve specificare se la soluzione supporta funzionalità "Web Services", in questo caso fornisce la documentazione tecnica dei "Web Services" offerti. Se la soluzione non supporta questo tipo di scambio di dati, il fornitore deve indicare come la sua soluzione può essere integrata in un'architettura SOA (ad esempio tramite proxy). Se non esistono alternative, il fornitore deve specificare se lo sviluppo di "Web Services" è presente sulla sua roadmap e il periodo in cui prevede la loro disponibilità.	☐ obbligatorio ☐ richiesto

2.10 Conformità

No.	requisito	categoria
SEC 10.1	**Accordo contrattuale** L'uso di sistemi (ad esempio, sistema operativo) e applicazioni non più supportati non è consentito. Ciò include anche applicazioni o componenti di produttori di terze parti che sono rilevanti per il funzionamento della soluzione. L'accordo contrattuale tra l'ospedale e il fornitore stabilisce che quest'ultimo rispetti il ciclo di vita indicato dal produttore per i sistemi e le applicazioni utilizzate. Il fornitore informa l'ospedale non appena le applicazioni in uso non vengono più sviluppate.	☑ obbligatorio ☐ richiesto

No.	requisito	categoria
SEC 10.2	**Accordo di Privacy (NDA)** Un accordo sulla protezione dei dati ai sensi del diritto svizzero è negoziato o è parte integrante dell'accordo contrattuale; è preferito il modello proposto dall'ospedale.	☑ obbligatorio ☐ richiesto
SEC 10.3	**Dichiarazione dei flussi di dati** Quando i dati vengono trasmessi a terzi (ad esempio per il rilevamento di errori o controlli di qualità), questi devono essere spiegati in dettaglio nella forma: scopo, contenuto dei dati, misure per proteggere la riservatezza in caso di trasmissione e archiviazione dei dati.	☑ obbligatorio ☐ richiesto
SEC 10.4	**La memorizzazione dei dati** La conservazione dei dati personali e sensibili viene effettuata esclusivamente in Svizzera o in un paese con un adeguato livello di protezione dei dati. Rilevante a questo proposito è la lista dei paesi della privacy federale e pubblico ufficiale IFPDT nella versione corrente. La data di riferimento è la data del l'offerta. In caso di memorizzazione di dati all'estero, la fornitura di memorizzazione dei dati in Svizzera è desiderabile come opzione. La decisione finale del percorso di archiviazione dei dati viene presa dall'ospedale durante la fase di valutazione.	☑ obbligatorio ☐ richiesto
SEC 10.05	**Accesso remoto** L'accesso remoto è realizzato dalla Svizzera o da un paese con un livello adeguato di protezione dei dati. Rilevante è l'elenco dei paesi pubblicato dal preposto federale alla protezione dei dati e alla trasparenza IFPDT nella versione corrente. La data di riferimento è la data del l'offerta.	☑ obbligatorio ☐ richiesto
SEC 10.06	**Licenza** Il fornitore è responsabile della corretta concessione di licenze di componenti da lui consegnati. Il fornitore garantisce i diritti d'uso illimitati e fornisce aggiornamenti di tutti i componenti, quando richiesto. Se necessario, il fornitore è tenuto a stipulare un contratto Escrow (deposito a garanzia).	☑ obbligatorio ☐ richiesto
SEC 10.07	**Penetration Testing** Il fornitore riconosce all'ospedale il diritto di eseguire controlli di sicurezza necessari (ad esempio, controllo della sicurezza, test di penetrazione) richiesti dalle autorità competenti e garantisce all'ente, rispettivamente al mandatario dell'Ospedale, un accesso senza restrizioni ai documenti necessari.	☑ obbligatorio ☐ richiesto
SEC 10.08	**Funzionamento in rete autonoma** Sistemi di alimentazione autonomi possono essere azionati in modalità di funzionamento (sotto carico), in modo indipendente per almeno otto ore.	☐ obbligatorio ☑ richiesto

Allegato A: Gestione del catalogo dei requisiti

Il fornitore deve commentare tutti i criteri secondo il catalogo nel Capitolo 2 completando il foglio in autodichiarazione.

A.1 Fase

- **Acquisto**
  I requisiti di cui al capitolo 2 devono essere considerati per l'acquisto di un sistema da parte del fornitore di servizi;
- **Integrazione**
  I requisiti di cui al capitolo 2 devono essere considerati per la messa in servizio di un sistema da parte del fornitore di servizi;
- **Funzionamento**
  I requisiti di cui al capitolo 2 devono essere considerati per il funzionamento di un sistema da parte del fornitore di servizi.

A.2 categoria

- **Obbligatorio**

  I requisiti obbligatori sono vincolanti. Il mancato rispetto di uno o più criteri di aggiudicazione obbligatoria comporterà l'esclusione dell'offerta.

  Oltre all'adempimento diretto di un criterio obbligatorio, è possibile anche un adempimento indiretto. L'adempimento indiretto è definito come realizzazione tenendo conto di misure e precauzioni aggiuntive. Questi devono essere spiegati in dettaglio nel foglio supplementare;
- **Richiesto**

  I requisiti desiderati sono utilizzati nella somma della qualifica del sistema, che viene presa in considerazione nel contesto delle offerte.

A.3 Conformità

- **sì**

  La richiesta è soddisfatta;
- **no**

  Il requisito non è soddisfatto;
- **non rilevante**

  La richiesta non è pertinente. Questo adempimento è consentito solo per i criteri per i quali sono definite eccezioni nel catalogo dei requisiti e se sono soddisfatte le condizioni descritte per un'eccezione. L'adempimento è in ogni caso da descrivere in modo dettagliato e comprensibile.