# Uso del cloud nel settore ospedaliero e sanitario: cosa sapere e considerare

## Una panoramica pratica sull'utilizzo del cloud da parte delle strutture sanitarie

Versione 1.1, agosto 2026

Autori (in ordine alfabetico): Erik Dinkel, Stefan Hunziker, Stefan Juon, Philipp Stoll, Werner Ulmer

## Contenuto

## Introduzione

Il presente documento fornisce alle strutture sanitarie una base oggettiva e indipendente per la gestione delle soluzioni cloud. Non vengono volutamente trattati singoli fornitori o prodotti, né viene assunta una posizione sull'utilizzo del cloud.

L'obiettivo è fornire alle strutture sanitarie una base per affrontare il tema dell'utilizzo del cloud in modo autonomo e responsabile. A tal fine, il documento offre una panoramica dei principali aspetti e delle considerazioni che devono essere presi in conto. La prima parte si rivolge a tutte le persone che si occupano della tematica cloud. La seconda parte tratta casi d'uso concreti e aspetti tecnici ed è rivolta principalmente a specialisti.

## Management summary

Le strutture sanitarie hanno un mandato di prestazione per la cura dei pazienti. Tale mandato deve essere garantito in modo efficace, appropriato, economico e competitivo. Inoltre, le strutture sanitarie fanno parte delle infrastrutture critiche della Svizzera e devono, in quanto tali, assicurare la sicurezza dell'approvvigionamento. A tal fine, sistemi ICT resilienti sono un presupposto indispensabile. L'utilizzo dei servizi cloud svolge un ruolo centrale ed è semplicemente necessario. In una società sempre più digitale e interconnessa, in cui molte applicazioni e servizi possono essere utilizzati esclusivamente online, l'uso del cloud è ormai una realtà. La medicina moderna e sistemi resilienti non sono più possibili senza l'utilizzo del cloud.

Gli hyperscaler (ovvero grandi aziende attive a livello globale che offrono servizi cloud) sono attori centrali e non sostituibili. Solo loro dispongono della necessaria scalabilità, della capacità innovativa, del personale specializzato e di prodotti interoperabili nella quantità e dimensione richieste. La questione non è quindi se utilizzare o meno i servizi degli hyperscaler, bensì quali servizi si possono utilizzare e in che modo. Occorre considerare per i diversi casi d'uso i requisiti legali e identificare, valutare e ridurre a un livello accettabile i rischi connessi all'utilizzo. Ogni organizzazione, e quindi ogni struttura sanitaria, deve decidere autonomamente se determinati servizi debbano essere mantenuti localmente o gestiti tramite soluzioni cloud.

Oltre ai rischi specifici delle applicazioni e dell'organizzazione, esistono due rischi centrali di cui è necessario essere pienamente consapevoli: il vendor lock-in e il fallimento del sistema. Se l'infrastruttura ICT di un'organizzazione si basa interamente o in larga misura sui servizi cloud di un singolo fornitore e quest'ultimo non è di fatto sostituibile, un eventuale cambio di fornitore comporta un enorme dispendio di risorse finanziarie, umane e di tempo. Un'interruzione di tale fornitore, ad esempio a seguito di un attacco informatico o di un altro evento, avrebbe conseguenze gravi per tutte le organizzazioni che utilizzano i suoi servizi.

Se, ad esempio, i servizi di videoconferenza, telefonia ed e-mail di tutte le strutture sanitarie si basassero sull'infrastruttura di un unico fornitore e quest'ultimo dovesse subire un'interruzione, tutte le strutture sanitarie in Svizzera non sarebbero più raggiungibili tramite questi canali. L'utilizzo dei servizi cloud aumenta quindi non solo la resilienza dei sistemi ICT, ma può anche metterla a rischio nei casi descritti. È pertanto indispensabile predisporre ridondanze e piani di emergenza.

Rinunciare ai servizi cloud, in generale e anche nel settore medico, non è né sensato né possibile, dato che le strutture sanitarie, in quanto parte delle infrastrutture critiche, devono continuare a garantire il proprio mandato di prestazione a beneficio dei pazienti e la sicurezza dell'assistenza sanitaria in Svizzera. Il presente documento costituisce una guida di orientamento per le strutture sanitarie nell'affrontare e utilizzare i servizi cloud in modo adeguato al rischio.

# Parte generale – Situazione attuale e condizioni quadro

## 1 Introduzione all'utilizzo del cloud

L'utilizzo dei servizi cloud è ormai una realtà in un mondo sempre più digitale. La digitalizzazione si sta affermando progressivamente nel settore sanitario, che già oggi — o quantomeno nel prossimo futuro — non è più concepibile senza soluzioni digitali. Da ciò derivano nuove potenzialità e opportunità di cui beneficeranno sia la società nel suo insieme sia le persone singole. Le soluzioni cloud rappresentano un elemento centrale di questo mondo digitale, con le opportunità e i rischi ad esse connessi.

### Fra approvvigionamento e trasformazione digitale

Nel quadro del proprio mandato e delle relative convenzioni di prestazione, le strutture sanitarie garantiscono l'assistenza ai pazienti, che deve essere efficace, appropriata, economica e competitiva nella regione assegnata. Un elemento centrale è la crescente interconnessione con i fornitori di servizi nelle diverse fasi del processo, con l'obiettivo di garantire un'assistenza quanto più integrata possibile. Secondo il Consiglio federale, le strutture sanitarie fanno parte delle infrastrutture critiche. Per poter adempiere al proprio mandato anche in situazioni di crisi, sono necessari sistemi ICT resilienti — ambito in cui i servizi cloud risultano particolarmente adeguati. A ciò si aggiunge l'evoluzione del mercato: molte applicazioni e servizi non sono più offerti per la propria infrastruttura locale «on premise».

L'analisi del tema dell'utilizzo del cloud è quindi imprescindibile per le strutture sanitarie. Il presente documento intende fungere da guida e consentire un'analisi strutturata e differenziata della tematica.

### Struttura del documento

La prima parte del documento si rivolge ai decisori delle strutture sanitarie, nonché a tutte le persone interessate all'utilizzo delle soluzioni cloud. Essa tratta i seguenti temi:

- Le diverse forme di soluzioni cloud
- Il ruolo degli hyperscaler e il mito dello «Swiss Cloud»
- L'evoluzione delle soluzioni cloud
- Le considerazioni giuridiche relative al cloud
- Il caso particolare dell'US Cloud Act
- Le considerazioni economiche relative al cloud

La seconda parte del documento si rivolge alle persone che si occupano dell'implementazione concreta delle soluzioni cloud. Essa tratta i seguenti temi:

- L'importanza del cloud per backup e recovery
- Cloud only vs. utilizzo ibrido
- Casi d'uso
- Misure tecniche e organizzative
- Crittografia e gestione delle chiavi

## 2 Diverse forme di soluzioni cloud

I servizi cloud o il cloud computing si riferiscono alla fornitura di risorse IT — quali potenza di calcolo, spazio di archiviazione, software applicativi e database — tramite Internet. A differenza dei modelli IT tradizionali, nei quali le organizzazioni devono gestire i propri server e infrastrutture, i servizi cloud consentono di affidare tali compiti a fornitori terzi.

Il cloud offre numerosi vantaggi, tra cui scalabilità, flessibilità, affidabilità e riduzione dei costi. Le organizzazioni possono adattare rapidamente e facilmente le risorse necessarie senza dover effettuare investimenti in capitale o personale. Inoltre, il cloud computing consente di accedere a una gamma più ampia di applicazioni e di distribuirle più rapidamente. Nel complesso, rappresenta una soluzione innovativa per

le organizzazioni che desiderano modernizzare e utilizzare in modo più efficace la propria infrastruttura ICT.

Il cloud computing è un approccio per fornire e utilizzare servizi IT in modo dinamico e in funzione delle esigenze tramite una rete. Le risorse offerte sono raggruppate in un pool e possono essere richieste e gestite rapidamente con un impegno minimo e una ridotta interazione con il fornitore. La fatturazione avviene sulla base dell'utilizzo effettivo.

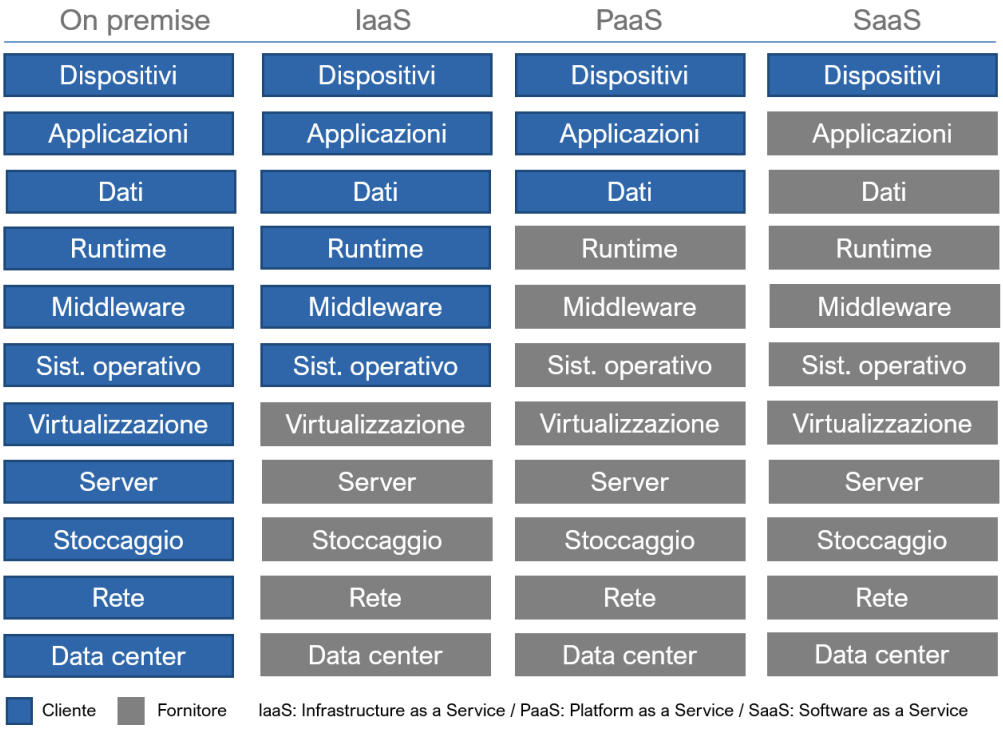
### Modelli cloud: IaaS, PaaS e SaaS

A seconda dei servizi forniti e delle responsabilità assunte, i servizi cloud possono essere suddivisi in tre modelli:

- Infrastructure as a Service (IaaS): in questo modello vengono fornite componenti di infrastruttura IT di base, quali potenza di calcolo, spazio di archiviazione e risorse di rete, tramite Internet. I clienti possono eseguire le proprie applicazioni e sistemi operativi su tali infrastrutture.
- Platform as a Service (PaaS): questo modello offre agli sviluppatori una piattaforma per creare, eseguire e gestire applicazioni senza doversi occupare dell'infrastruttura sottostante.
- Software as a Service (SaaS): questi servizi consentono agli utenti di accedere a applicazioni software tramite Internet. Le applicazioni sono ospitate e mantenute da fornitori terzi, mentre i clienti le utilizzano online.

Questi modelli si distinguono, tra l'altro, per una diversa ripartizione delle responsabilità tra fornitore cloud e cliente.

Panoramica dei diversi tipi di servizi cloud a confronto con i sistemi locali («on-premise»):




## 3 Il ruolo degli hyperscaler e il mito dello «Swiss Cloud»

Gli hyperscaler sono grandi aziende attive a livello globale che offrono servizi di cloud computing su larga scala. Tra gli hyperscaler più noti figurano Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud e Alibaba Cloud. Queste aziende gestiscono enormi data center in tutto il mondo per fornire infrastrutture IT e servizi cloud.

### Gli hyperscaler: il motore del mercato del cloud computing

Il ruolo degli hyperscaler nel mercato del cloud computing è diventato sempre più rilevante negli ultimi anni. Le organizzazioni che dipendono dai servizi cloud cercano soluzioni rapide, scalabili e affidabili. Gli hyperscaler sono in grado di soddisfare queste esigenze grazie alla gestione di grandi data center che permettono di offrire un'ampia gamma di servizi di infrastruttura IT e cloud.

Utilizzando i servizi cloud degli hyperscaler, le organizzazioni possono anche ottenere risparmi sui costi, evitando investimenti elevati nella propria infrastruttura IT. Gli hyperscaler offrono inoltre una vasta gamma di servizi, tra cui Infrastructure as a Service (IaaS), Platform as a Service (PaaS) e Software as a Service (SaaS), che possono essere utilizzati in base alle necessità.

Inoltre, gli hyperscaler dispongono di un elevato livello di competenze e tecnologie per supportare i clienti nello sviluppo, nell'implementazione e nella gestione dei servizi di cloud computing. Ciò li rende un'opzione fondamentale per le organizzazioni che vogliono rimanere competitive nell'attuale contesto economico.

Nel complesso, gli hyperscaler sono diventati indispensabili nel mondo odierno del cloud computing. Senza di essi, sarebbe più difficile per le organizzazioni reagire in modo rapido e flessibile alle esigenze del mercato.

### «Swissness» nel contesto cloud

I termini «Swiss Cloud» e «Swissness» si riferiscono a servizi cloud offerti da aziende svizzere e ospitati in Svizzera. Esiste la percezione che tali servizi offrano standard più elevati in termini di protezione dei dati, sicurezza e riservatezza rispetto ai servizi di altri fornitori.

È importante notare che «Swissness» non è una certificazione o un marchio ufficialmente riconosciuto. Tuttavia, vi sono alcune ragioni per cui i servizi cloud svizzeri sono spesso considerati particolarmente sicuri e affidabili. La Svizzera dispone di leggi rigorose in materia di protezione dei dati e di standard elevati per quanto riguarda la privacy e la sicurezza delle informazioni. Inoltre, il Paese è politicamente stabile, ha un elevato livello di certezza giuridica ed è neutrale, il che contribuisce a rafforzare la fiducia.

In aggiunta, le aziende svizzere godono spesso di un'elevata reputazione in termini di qualità e affidabilità, il che può contribuire a rafforzare la fiducia nei loro servizi cloud.

Tuttavia, ciò non significa necessariamente che tutti i servizi cloud svizzeri siano automaticamente più sicuri o affidabili rispetto a quelli di altri fornitori. È fondamentale analizzare attentamente le caratteristiche specifiche dei singoli servizi cloud per individuare la soluzione più adatta alle esigenze di un'organizzazione.

## 4 Evoluzione futura delle soluzioni cloud

Esistono numerose previsioni sull'evoluzione dei servizi cloud. Tra le principali tendenze e sviluppi si annoverano:

Strategie multi-cloud: le organizzazioni adottano sempre più una combinazione di servizi cloud di diversi fornitori per aumentare la flessibilità e l'affidabilità della propria infrastruttura IT.

Edge computing: l'elaborazione dei dati e delle applicazioni non avviene più esclusivamente in data center centralizzati, ma anche alla periferia della rete (edge), ossia vicino agli utenti finali o alle fonti dei dati. Ciò consente tempi di risposta più rapidi e migliori prestazioni.

Intelligenza artificiale e apprendimento automatico: i servizi cloud rappresentano una piattaforma ideale per l'elaborazione di grandi volumi di dati e l'esecuzione di algoritmi di machine learning. Questo consente alle organizzazioni di ottenere informazioni preziose e sviluppare applicazioni innovative.

Tecnologie a container: i container IT impacchettano e trasportano software in modo standardizzato (analogamente a come i container navali trasportano merci), permettendo alle organizzazioni di gestire e scalare le applicazioni in modo più efficiente e flessibile, contribuendo a rendere il cloud ancora più accessibile.

Cloud only / cloud ibrido: le organizzazioni adottano sempre più modelli ibridi che combinano cloud pubblico e cloud privato. Ciò consente di sfruttare i vantaggi del cloud senza dover trasferire completamente l'infrastruttura IT.

Cloud ibrido / on-premise: una parte delle applicazioni e dell'infrastruttura è gestita nel cloud, mentre un'altra parte rimane in esercizio a livello locale. Una possibile variante consiste, ad esempio, nel gestire nel cloud le applicazioni di comunicazione e collaborazione, mantenendo invece localmente le applicazioni critiche per il core business, in particolare quelle con dati strutturati e sensibili. La decisione se gestire un'applicazione nel cloud o localmente viene presa caso per caso, sulla base di una valutazione di opportunità, rischi, costi e requisiti legali.

Nel complesso, il futuro dei servizi cloud sarà caratterizzato da innovazioni e nuove tecnologie che consentiranno alle organizzazioni di utilizzare la propria infrastruttura IT in modo più efficace ed efficiente. Le organizzazioni che utilizzano il cloud saranno in grado di reagire più rapidamente e con maggiore flessibilità alle mutevoli esigenze del contesto attuale, rafforzando così la propria competitività.

# 5 Considerazioni giuridiche relative al cloud

Il cloud computing comporta sempre un'esternalizzazione e quindi un trattamento dei dati da parte di terzi. Tale trattamento è affidato contrattualmente a un fornitore che elabora i dati per conto della struttura sanitaria mandante. Non si tratta di una pubblicazione dei dati. Questa distinzione è importante, poiché il trattamento su incarico è soggetto a requisiti diversi rispetto alla pubblicazione. La responsabilità dei dati rimane comunque sempre in capo alla struttura sanitaria mandante.

### Tipi di dati ed esigenze di protezione

Per un utilizzo conforme al diritto del cloud, la prima questione riguarda i dati da trattare: di che tipo di dati si tratta e quanto sono sensibili? A seconda del tipo di dati, si applicano requisiti giuridici e di sicurezza delle informazioni differenti. È utile distinguere tra le seguenti categorie:

- Dati pubblici
- Dati interni all'organizzazione
- Dati aziendali riservati
- Dati personali (che possono essere pubblici, interni o riservati)
- Dati personali sensibili, come ad esempio i dati dei pazienti

### Stato dei dati

Una volta chiarito il tipo di dati, occorre valutare il loro stato: sono identificabili, pseudonimizzati o anonimizzati? A seconda di ciò, continuano o meno a essere considerati dati personali.

I dati sono considerati pseudonimizzati (o sufficientemente pseudonimizzati) quando possono essere attribuiti a una persona determinata solo con uno sforzo sproporzionato. La reidentificazione rimane possibile tramite una chiave di identificazione. Se tale chiave è detenuta esclusivamente dal mandante, i dati possono essere considerati anonimizzati dal punto di vista del fornitore.

A differenza della pseudonimizzazione, l'anonimizzazione è irreversibile: non è più possibile risalire alla persona. Una volta anonimizzati, i dati non sono più considerati dati personali.

### Paese di archiviazione e trattamento

Un ulteriore aspetto riguarda il luogo di archiviazione e trattamento dei dati: avviene in Svizzera o all'estero?

Se il trattamento avviene in Svizzera, si applica il diritto svizzero, inclusi il segreto professionale e d'ufficio. Secondo la prassi corrente, il fornitore può essere vincolato contrattualmente a un livello di protezione equivalente e le violazioni possono essere perseguite. Secondo un'interpretazione giuridica più restrittiva, sostenuta anche da alcune autorità di vigilanza, il segreto professionale potrebbe opporsi in linea di principio all'esternalizzazione nel cloud. Un'interpretazione così rigida renderebbe di fatto impossibile l'utilizzo

del cloud per il trattamento dei dati dei pazienti. In una società sempre più digitale, si pone quindi la questione se le strutture sanitarie possano ancora adempiere al proprio mandato senza ricorrere al cloud.

Se i dati sono trattati all'estero, si applica il diritto del Paese interessato e non quello svizzero, con possibilità limitate di controllo e di esecuzione.

#### Esigenze legali per il trattamento di dati sensibili

Qualora si intendano trattare dati personali sensibili (ad es. dati dei pazienti) nel cloud, è necessaria una base contrattuale ai sensi della normativa sulla protezione dei dati. Devono essere rispettati i principi di finalità e proporzionalità: i dati possono essere trattati solo per lo scopo per cui sono stati affidati e devono essere limitati a quanto strettamente necessario.

Ogni nuovo trattamento o modifica sostanziale riguardante dati personali sensibili richiede una valutazione d'impatto sulla protezione dei dati. A seconda della base giuridica applicabile (diritto federale o cantonale), può essere necessaria una consultazione preventiva dell'autorità di vigilanza.

Se i dati sono trattati all'estero, ciò è consentito solo se il livello di protezione dei dati nel Paese destinatario è almeno equivalente a quello svizzero. Anche se è possibile vincolare contrattualmente il fornitore a un livello di protezione equivalente, le possibilità di applicazione sono più limitate e si applica il diritto locale. A causa del rischio più elevato, sono necessarie trasparenza, nonché un consenso esplicito e verificabile delle persone interessate. Restano inoltre applicabili tutti gli obblighi giuridici e il dovere di diligenza.

Infine, i dati devono essere protetti in ogni momento conformemente allo stato dell'arte della sicurezza delle informazioni, ad esempio mediante cifratura e controlli di accesso basati sui ruoli, sia durante la trasmissione sia durante l'archiviazione.

## 6 Caso particolare dell'US Cloud Act

L'utilizzo del cloud computing per il trattamento di dati per conto terzi che coinvolge dati personali sensibili, in particolare dati dei pazienti, è generalmente possibile secondo la prassi giuridica corrente, a condizione che esista una base contrattuale adeguata e che siano adottate le necessarie misure di sicurezza delle informazioni. Ciò vale in particolare quando l'infrastruttura cloud si trova in Svizzera. Tuttavia, un caso particolare è rappresentato dall'applicazione extraterritoriale dell'US Cloud Act.

Secondo tale normativa, le autorità statunitensi possono, nell'ambito di un procedimento penale in corso contro una persona, richiedere l'accesso ai dati di tale persona presso aziende con un legame con gli Stati Uniti. Pertanto, se un'organizzazione — inclusa una struttura sanitaria — tratta dati nel cloud tramite un fornitore con un legame con gli Stati Uniti, le autorità statunitensi possono potenzialmente accedere a tali dati, anche se l'infrastruttura cloud utilizzata è situata in Svizzera.

Il trattamento dei dati dei pazienti presso un fornitore cloud con legami con gli Stati Uniti è quindi problematico dal punto di vista della protezione dei dati e deve essere esaminato caso per caso in modo approfondito. In generale, e in particolare per i fornitori cloud con legami con gli Stati Uniti, è fondamentale definire e specificare preventivamente i casi d'uso concreti. Su questa base, occorre valutare rischi, opportunità e costi, nonché verificare i requisiti legali.

Oltre alla riservatezza, devono essere considerati anche l'integrità e la disponibilità dei dati. Quest'ultimo aspetto è determinante per garantire il funzionamento di una struttura sanitaria e quindi la sicurezza dell'approvvigionamento di un'infrastruttura critica. Sulla base di tale analisi, devono essere definite e attuate tempestivamente misure atte a eliminare i rischi o a ridurli a un livello accettabile.

### 6.1 Nota sul Privacy Shield 2.0 e sul Swiss-U.S. Data Privacy Framework

Il 10 luglio 2023 la Commissione europea ha adottato la decisione di adeguatezza relativa all'EU-U.S. Data Privacy Framework, talvolta denominato anche «Privacy Shield 2.0». La decisione stabilisce che gli Stati Uniti garantiscono un livello di protezione adeguato per i dati personali trasferiti dall'UE a imprese statunitensi certificate ai sensi dell'EU-U.S. Data Privacy Framework e incluse nell'apposito elenco del U.S.

Department of Commerce. In linea di principio, i dati personali possono essere trasferiti a tali imprese senza ulteriori garanzie in materia di protezione dei dati.

Per i trasferimenti di dati dalla Svizzera, dal 15 settembre 2024 esiste una normativa svizzera corrispondente sotto forma dello Swiss-U.S. Data Privacy Framework. Il Consiglio federale ha inserito gli Stati Uniti, per quanto riguarda i dati personali trasferiti a imprese statunitensi certificate nell'ambito di tale quadro, nell'elenco degli Stati o dei settori specifici che garantiscono un livello adeguato di protezione dei dati. Ai sensi dell'articolo 16 capoverso 1 LPD, tali trasferimenti di dati possono pertanto avvenire, in linea di principio, senza garanzie supplementari. Per i trasferimenti a imprese statunitensi non certificate continuano invece a essere necessarie garanzie adeguate ai sensi dell'articolo 16 capoverso 2 LPD.

La stabilità giuridica e istituzionale di questi quadri di protezione dei dati deve tuttavia essere rivalutata alla luce della decisione della Corte Suprema degli Stati Uniti del 29 giugno 2026 nella causa Trump v. Slaughter. La Corte Suprema ha dichiarato incompatibile con il principio costituzionale della separazione dei poteri la normativa secondo cui i membri della Federal Trade Commission potevano essere rimossi dall'incarico soltanto per determinati motivi importanti, in particolare per negligenza nell'adempimento dei propri doveri, incapacità o abuso d'ufficio. I Commissioners della FTC possono quindi, in linea di principio, essere rimossi dal Presidente senza che debba essere dimostrata la sussistenza di uno di tali motivi.

Questa decisione è rilevante per lo Swiss-U.S. Data Privacy Framework, poiché la FTC è responsabile dell'applicazione dei principi in materia di protezione dei dati nei confronti della maggior parte delle imprese statunitensi partecipanti. La valutazione svizzera dell'adeguatezza del 2024 si basava espressamente sul presupposto che i Commissioners della FTC potessero essere rimossi durante il loro mandato di sette anni soltanto per un motivo importante e, su tale base, qualificava la FTC, insieme al U.S. Department of Transportation, come autorità di controllo indipendente. La soppressione di questa protezione contro la rimozione costituisce pertanto una modifica successiva sostanziale di un presupposto sul quale si fondava la valutazione svizzera dell'adeguatezza. Essa può far sorgere dubbi in merito all'indipendenza istituzionale e all'assenza di influenze politiche sull'applicazione dello Swiss-U.S. Data Privacy Framework.

La decisione della Corte Suprema non abroga direttamente lo Swiss-U.S. Data Privacy Framework. Il riconoscimento svizzero dell'adeguatezza rimane formalmente applicabile finché il Consiglio federale non modifica la relativa disciplina nell'ordinanza sulla protezione dei dati o finché un'autorità competente o un tribunale non giunga a una conclusione diversa. Alla luce delle mutate condizioni istituzionali, è tuttavia prevedibile un nuovo esame del Framework. Le imprese che, per i trasferimenti di dati, si basano esclusivamente sullo Swiss-U.S. Data Privacy Framework dovrebbero monitorare gli ulteriori sviluppi e, in particolare in caso di dati personali degni di particolare protezione o di grandi quantità di dati personali, predisporre garanzie supplementari o alternative.

Rimane controverso se l'introduzione dell'EU-U.S. Data Privacy Framework e dello Swiss-U.S. Data Privacy Framework incida sul caso particolare del U.S. CLOUD Act. I due quadri di protezione dei dati non eliminano i poteri conferiti dalla legge alle autorità statunitensi di richiedere, alle condizioni previste dal CLOUD Act, la consegna di dati da parte di fornitori statunitensi.

Alla luce della situazione attuale, nel presente documento si parte dal presupposto che il caso particolare del U.S. CLOUD Act debba continuare a essere considerato separatamente. La decisione della Corte Suprema rafforza, piuttosto, la necessità di valutare regolarmente, oltre alla certificazione formale di un destinatario statunitense, anche i rischi effettivi relativi all'accesso ai dati, alla vigilanza e alla tutela giuridica.

## 7 Considerazioni economiche relative al cloud

Con l'introduzione delle soluzioni cloud e il passaggio da modelli «on-premise» a licenze in modalità di abbonamento, si è affermato un nuovo approccio finanziario all'utilizzo del software nelle organizzazioni. In passato hardware e software venivano acquistati direttamente, mentre oggi il software viene sempre più spesso acquisito «as a Service» su base di noleggio. Non si tratta quindi più di investimenti, bensì di costi operativi che vengono contabilizzati direttamente nei costi di esercizio (passaggio da CapEx a

OpEx). Ciò comporta una riduzione del rischio finanziario, in quanto non è più necessario pianificare e sostenere investimenti con immobilizzazione del capitale e ammortamenti (di norma su quattro anni).

Questo modello (OpEx) offre una flessibilità nettamente maggiore. Le soluzioni possono essere adattate più rapidamente alle esigenze effettive e si riduce anche la pressione legata al finanziamento della manutenzione. A seconda del modello di abbonamento scelto, è inoltre possibile implementare adeguamenti tecnici in modo più rapido rispetto al modello di acquisto (CapEx). L'adozione di nuove tecnologie risulta quindi significativamente più veloce.

Il principale vantaggio economico del cloud computing risiede nella flessibilità che esso offre. Consente alle organizzazioni di adattare rapidamente l'ambiente IT ai requisiti e alle esigenze in continua evoluzione. Alla luce della crescente e sempre più rapida digitalizzazione della società, questa capacità assume un'importanza sempre maggiore. Ciò vale in particolare per il settore sanitario, anch'esso interessato da una trasformazione digitale accelerata.

Sarebbe tuttavia errato affermare che una soluzione basata sul cloud sia sempre più economica rispetto a una soluzione locale «on-premise». Gli impatti finanziari devono essere valutati caso per caso, in funzione delle applicazioni concrete e degli sforzi necessari per garantire un utilizzo conforme al diritto e sicuro. Occorre inoltre considerare che i fornitori cloud possono modificare i prezzi nel tempo — generalmente al rialzo — e che un eventuale cambio di fornitore può comportare costi elevati.

## 8 Aspetti geopolitici

Alla luce dei recenti sviluppi, oltre agli aspetti sopra menzionati, è necessario considerare anche il contesto geopolitico e il comportamento talvolta imprevedibile di alcuni attori.

A causa della nuova realtà con cui ci confrontiamo, non si può escludere completamente che, ad esempio, aumenti arbitrari dei dazi o restrizioni normative possano avere un impatto sugli operatori o sugli utenti dei servizi cloud, che connessioni o servizi vengano limitati o interrotti per esercitare pressione, oppure che un data center di un fornitore venga fisicamente distrutto a seguito di un conflitto armato — come avvenuto all'inizio di marzo 2026 durante un attacco missilistico contro un data center di Amazon Web Services negli Emirati Arabi Uniti.

Questi rischi sono amplificati dall'elevata dipendenza da un numero limitato di fornitori globali. Ne deriva un profilo di rischio complesso che comprende non solo aspetti tecnici, ma anche dimensioni strategiche e di politica di sicurezza, che possono influenzare direttamente la sicurezza dell'approvvigionamento nel settore sanitario. Tali aspetti devono essere presi in considerazione nelle valutazioni e nelle decisioni, ponderando rischi, opportunità e alternative e adottando misure adeguate.

# Parte specifica – Dettagli per l'implementazione concreta

## 9 L'importanza del cloud per backup e recovery

Le analisi di impatto sul business (Business Impact Analysis), unite ai requisiti elevati in termini di Recovery Time Objective (RTO) e Transaction Processing Objective (RPO) nelle strutture sanitarie, evidenziano l'importanza di un'elevata disponibilità dei sistemi ICT. Gli eventi di interruzione mostrano che, nel peggiore dei casi, una struttura sanitaria può provvisoriamente continuare a operare senza un supporto IT essenziale — ma al prezzo di una forte riduzione della produttività e di un notevole impegno per mantenere e ricostruire i flussi informativi rilevanti. Nell'ambito del Business Continuity Management a più livelli, le soluzioni cloud offrono approcci efficaci e scalabili per garantire o ripristinare la continuità.

Un ulteriore vantaggio delle soluzioni cloud è che le competenze, i servizi e il supporto sono generalmente forniti dal fornitore, che assicura anche l'aggiornamento dei sistemi e del software. Di norma, i sistemi vengono quindi aggiornati tempestivamente e le vulnerabilità di sicurezza corrette. I livelli di servizio devono essere disciplinati contrattualmente e, a seconda del tipo di servizio cloud, la responsabilità del cliente varia.

Un'ulteriore sfida riguarda l'integrazione dei dati provenienti da sistemi medici. Diversi produttori di dispositivi, come pacemaker o glucometri, raccolgono questi dati in soluzioni cloud proprietarie. Per garantire un trattamento ottimale, tali dati dovrebbero poter essere aggregati e resi disponibili nei sistemi del team di cura interprofessionale.

Nota: nell'utilizzo di dispositivi medici devono essere rispettate le direttive dell'associazione professionale dei medici svizzeri FMH

# 10 Cloud only vs. utilizzo ibrido

La transizione dall'attuale modello predominante «on-premise» al cloud è un processo di lunga durata, che dipende da diversi fattori:

- Disponibilità delle offerte e disimpiego graduale delle applicazioni o dei servizi locali
- Riduzione dei sistemi legacy non compatibili con il cloud
- Requisiti legali e normative in materia di protezione dei dati
- Coesistenza di servizi cloud privati e pubblici
- Nuovi servizi disponibili esclusivamente in ambiente cloud (ad es. telemedicina, monitoraggio remoto dei pazienti, utilizzo di dispositivi wearable)

### Gestione dei bisogni del business e della tecnologia nelle organizzazioni IT interne

La competenza chiave (Unique Selling Proposition, USP) di un reparto ICT all'interno di una struttura sanitaria risiede nella capacità di fungere da interfaccia tra la tecnologia e i processi principali di diagnosi e trattamento dei pazienti. Senza una comprensione approfondita di entrambi gli ambiti, non è possibile fornire consulenza e supporto proattivi orientati alla creazione di valore. Le tecnologie di base e le infrastrutture tendono a diventare commodity; la sfida per i reparti ICT interni consiste quindi nell'orchestrare i diversi elementi e fornitori e nel gestire in modo ottimale la complessità.

### Sfide ICT: carenza di personale qualificato e trasformazione digitale

La trasformazione digitale nel settore sanitario è in ritardo di circa dieci anni rispetto ad altri settori (banche, assicurazioni, telecomunicazioni). Questo ritardo si osserva anche, in misura analoga, rispetto ad alcuni Paesi esteri (Estonia, Singapore, Stati Uniti).

Di conseguenza, sono ancora ampiamente diffuse applicazioni locali, spesso basate su architetture client/server, nelle quali manca una chiara separazione tra i diversi livelli (dati, logica di business e presentazione). I fornitori sono spesso piccole e medie imprese, la cui capacità di esecuzione nel lungo periodo, in particolare per quanto riguarda il supporto operativo e lo sviluppo, può risultare limitata.

La carenza di specialisti ICT è particolarmente evidente in due ambiti: da un lato, la formazione ICT è poco attrattiva per chi entra nel settore sanitario; dall'altro, le strutture sanitarie non sono competitive dal punto di vista salariale per attrarre profili altamente specializzati (ad es. ingegneri M365, architetti di sicurezza IT, ecc.). Inoltre, indipendentemente dall'utilizzo del cloud, le strutture sanitarie devono gestire un gran numero di dispositivi medicali connessi alla rete, creando un ambito specifico che richiede personale IT altamente qualificato.

# 11 Casi d'uso

## 11.1 Videotelefonia

La videotelefonia trasmette dati audio e video in tempo reale. Di norma si tratta unicamente di una trasmissione senza memorizzazione dei dati. Un'eccezione si verifica quando le comunicazioni vengono registrate a fini di tracciabilità o di garanzia della qualità.

### Principali domande da porsi:

- La videotelefonia può essere tecnicamente limitata alla sola trasmissione di dati audio e video?

- È noto quali dati accessori (metadati) vengono memorizzati dal fornitore per scopi di segnalazione e se tale memorizzazione e il successivo trattamento sono conformi ai requisiti legali? Il fornitore applica il principio di minimizzazione dei dati, secondo cui vengono raccolti e trattati solo i dati strettamente necessari?
- La videotelefonia o i dati audio e video trasmessi fanno riferimento a persone? Se non sono rilevanti solo i dati degli utenti trasmessi, ma anche le immagini dei partecipanti, essi possono richiedere una protezione della sfera privata.
- Si raccomanda l'utilizzo di uno sfondo virtuale, come previsto dalla maggior parte delle applicazioni. Tuttavia, questa funzione è spesso disponibile solo tramite applicazioni installate e non tramite browser. In tal caso, si consiglia di informare i partecipanti che è possibile disattivare la videocamera per proteggere la propria privacy. Questa informazione dovrebbe essere comunicata preferibilmente già nell'invito o al più tardi all'inizio della riunione.
- I dati degli utenti possono essere almeno cifrati? La cifratura è end-to-end oppure avviene solo durante la trasmissione (data-in-transit) o la memorizzazione (data-at-rest)?

In caso di registrazione, i dati audio e video vengono memorizzati. Si pongono quindi ulteriori domande:

- Qual è lo scopo della registrazione? Per quanto tempo vengono conservati i dati? È possibile ridurre la durata della conservazione? È garantito che i dati non vengano utilizzati per altri scopi e che vengano cancellati entro un termine adeguato al raggiungimento dello scopo?
- Esiste una base giuridica, un interesse legittimo o il consenso dei partecipanti per tale trattamento? Ciò vale anche per i dati degli utenti trasmessi durante la comunicazione?

#### Rischi per la comunicazione basata sul cloud

Un utilizzo esteso o generalizzato di servizi di comunicazione basati su cloud crea una forte dipendenza dal servizio in termini di disponibilità. Un guasto del fornitore o una limitazione dell'accesso (connettività) può avere un impatto significativo sul funzionamento della struttura sanitaria, in particolare per le comunicazioni critiche interne ed esterne. È pertanto consigliabile predisporre soluzioni di backup (ridondanze) e testarle regolarmente con scenari realistici.

La crescente integrazione di algoritmi per il rilevamento di contenuti non appropriati (ad es. tramite intelligenza artificiale) comporta il rischio che immagini mediche trasmesse vengano erroneamente classificate come contenuti inappropriati e bloccate. Ciò può avere un impatto significativo su specifici casi d'uso, come la telemedicina. Tali funzionalità vengono spesso introdotte dai fornitori senza preavviso o con breve preavviso, rendendo difficile per le strutture sanitarie reagire. È quindi fondamentale chiarire tempestivamente con il fornitore le possibilità di configurazione e di disattivazione di tali algoritmi.

In sintesi, l'utilizzo della videotelefonia nelle strutture sanitarie offre importanti vantaggi e può generare valore aggiunto in numerosi casi d'uso. Tuttavia, è essenziale non lasciarsi guidare esclusivamente da tali vantaggi e valutare con attenzione un utilizzo esteso o generalizzato. Si sono dimostrati efficaci modelli operativi scalabili e ibridi, in cui le comunicazioni critiche vengono gestite tramite soluzioni locali tradizionali.

### 11.2 Collaborazione

La collaborazione comprende, nel senso generale, l'interazione tramite videotelefonia e in più la modifica simultanea di dati archiviati centralmente da parte di partecipanti interni ed esterni. Il caso d'uso descritto al punto 11.1 viene quindi esteso includendo la memorizzazione e il trattamento dei dati, tipicamente nell'ambiente cloud di un fornitore di servizi.

#### Principali domande da porsi:

- È possibile garantire che i dati archiviati centralmente siano adeguatamente protetti contro accessi non autorizzati (obiettivo: riservatezza) e modifiche indebite (obiettivo: integrità)?
- I dati possono essere ripristinati in caso di perdita nell'ambiente cloud del fornitore (obiettivo: disponibilità)?
- È possibile tracciare gli accessi e le modifiche ai dati?

- L'assegnazione dei diritti di accesso spetta esclusivamente al proprietario dell'area di lavoro condivisa o a persone da lui esplicitamente autorizzate (amministrazione delegata)? Oppure ogni partecipante può condividere dati con terzi?

### 11.3 Messaggistica istantanea

La messaggistica istantanea (chat) è generalmente intesa come l'invio di brevi messaggi a una persona o a un gruppo. Il contenuto può includere, oltre al testo, immagini o documenti allegati. I messaggi vengono memorizzati in modo da poter essere consultati anche in un secondo momento. La trasmissione avviene di norma all'interno di uno spazio di indirizzamento protetto, per cui i messaggi possono essere inviati solo a partecipanti appartenenti a tale spazio.

Principali domande da porsi:

- Il mittente può sempre identificare chi ha accesso ai contenuti?
- È possibile garantire che i dati trasmessi non vengano utilizzati dal fornitore per altri scopi (cfr. WhatsApp)?
- È noto quali metadati vengono raccolti e memorizzati durante la trasmissione, per quali scopi e da chi vengono trattati? Il fornitore applica il principio di minimizzazione dei dati?

### 11.4 E-mail

Per e-mail si intende la trasmissione di testi e dati tramite un'applicazione dedicata, spesso un client di posta elettronica. Tale applicazione non viene utilizzata solo per la trasmissione di informazioni, ma anche per la loro archiviazione, ad esempio in una struttura di cartelle all'interno del client.

Principali domande da porsi:

- La cifratura dei dati durante la trasmissione è garantita senza interruzioni?
- È possibile utilizzare una firma per verificare l'autenticità del mittente mediante procedure crittografiche?
- Esiste una modalità separata per la trasmissione cifrata delle e-mail che non si limiti alla sola cifratura del trasporto?

### 11.5 Sistemi clinici e amministrativi

Nel contesto dei sistemi clinici e amministrativi si intendono quelli utilizzati per il trattamento dei dati dei pazienti — quindi dati personali particolarmente sensibili — nonché dei dati dei collaboratori, che possono anch'essi includere dati sensibili. Ciò comprende in linea di principio tutti i sistemi informativi e applicativi, nonché i sistemi ausiliari e i servizi di supporto correlati.

Principali domande da porsi:

- È possibile determinare in modo trasparente in quale Paese (giurisdizione) e, idealmente, in quale data center del fornitore sono archiviati i dati?
- È possibile escludere che servizi accessori (ad es. per analisi) comportino il trasferimento dei dati verso Paesi con un livello di protezione dei dati non adeguato?
- È possibile verificare che i dati siano cifrati almeno durante la trasmissione (data-in-transit) e la memorizzazione (data-at-rest), e idealmente anche durante l'elaborazione (data-in-processing)?
- È garantito che la gestione delle chiavi sia effettuata dal cliente o da un soggetto da lui incaricato, e non dal fornitore?
- È possibile garantire, idealmente, che i dati siano cifrati già prima della trasmissione all'ambiente cloud del fornitore tramite un servizio terzo?
- Il cliente è a conoscenza dei potenziali punti di accesso del fornitore ai dati in chiaro (ad es. tramite memory dump a fini di supporto)?
- Il cliente sa da quale Paese il fornitore eroga i servizi di supporto? Può garantire che, per tali attività, non vengano trasferiti dati sensibili verso Paesi con un livello di protezione inadeguato?

- Il fornitore è disposto e in grado di rendere trasparenti i propri rapporti di subfornitura? Esiste un obbligo di informazione e un diritto di veto per il cliente in caso di nuovi subfornitori?
- Il cliente può garantire un'uscita completa dall'ambiente cloud entro un termine ragionevole (di norma tre-sei mesi) senza subire un'interruzione significativa del servizio? Ciò è garantito anche in caso di cambiamento di proprietà del fornitore?
- Il cliente è in grado di ripristinare completamente i dati in caso di perdita, rispettando tutti i requisiti di sicurezza?
- Il cliente è in grado di mantenere un livello di servizio adeguato in caso di perturbazioni dell'ambiente cloud del fornitore (continuità del servizio)?
- Il fornitore concede al cliente diritti di audit sufficienti (test di penetrazione, audit)? Fornisce rapporti di audit esterni?
- Il cliente può contare su una connettività adeguata verso l'ambiente cloud del fornitore?
- Il cliente ha effettuato un'analisi dei rischi conforme ai requisiti normativi e ne garantisce la gestione per tutta la durata del servizio?

# 12 Misure tecniche e organizzative

## 12.1 Determinazione dei rischi per caso d'uso

Nella sezione precedente sono stati descritti i diversi casi d'uso e le principali domande di verifica. Le risposte a tali domande consentono di identificare i rischi esistenti. A tal fine è utile anche l'impiego di un catalogo dei rischi per stabilire se un determinato rischio si applica o meno. Un catalogo di questo tipo può includere, ad esempio, i seguenti rischi (basati sull'ENISA Cloud Computing Risk Assesment):

### Rischi organizzativi

R.1 Lock-in del fornitore

R.2 Perdita di controllo dei processi

R.3 Sfide in materia di conformità

R.4 Danni reputazionali

R.5 Interruzione o degradazione del servizio cloud

R.6 Acquisizione del fornitore cloud

R.7 Fallimento della catena di approvvigionamento

### Rischi tecnici

R.8 Sovra o sotto allocazione delle risorse

R.9 Isolamento insufficiente rispetto ad altri clienti

R.10 Rischi interni presso il fornitore

R.11 Compromissione delle interfacce applicative con il cloud

R.12 Intercettazione dei dati durante la trasmissione

R.13 Furto di dati durante upload o download

R.14 Cancellazione insufficiente dei dati

R.15 Attacchi Distributed Denial of Service (DDoS)

R.16 Economic Denial of Service (EDoS)

R.17 Perdita delle chiavi di cifratura

R.18 Scansioni Internet malevole

R.19 Compromissione dell'infrastruttura cloud

R.20 Conflitti tra backup locali e cloud

### Rischi giuridici

R.21 Accesso ai dati imposto per legge

R.22 Cambiamenti del quadro normativo

R.23 Rischi in materia di protezione dei dati

R.24 Rischi legati alle licenze / violazioni di licenza

Una volta identificati i rischi, è necessario valutarne l'impatto, stimando la probabilità di occorrenza e l'entità del danno. In alternativa, è possibile stimare i valori minimi e massimi del danno.

### Valutazione dei potenziali danni

L'analisi dell'impatto può essere strutturata secondo le dimensioni di riservatezza, disponibilità, integrità e tracciabilità. Occorre valutare le conseguenze per la struttura sanitaria, ad esempio in caso di indisponibilità di servizi critici.

In concreto, si tratta di stimare i danni potenziali nel caso in cui videotelefonia, piattaforme di collaborazione, servizi di messaggistica, e-mail o sistemi clinici e amministrativi non siano più disponibili, oppure se i dati vengano rubati, manipolati, cancellati o distrutti, o ancora se venga meno l'integrità o la tracciabilità delle informazioni.

È fondamentale considerare il tipo e il volume dei dati trattati, nonché la criticità dei processi coinvolti. Occorre inoltre valutare la perdita di controllo sui dati, la dipendenza dal fornitore (vendor lock-in) e il rischio di attacchi informatici attraverso sistemi esposti nel cloud.

### Misure per minimizzare i rischi

Una volta identificati i rischi e i relativi impatti, è necessario valutare le misure esistenti e il rischio residuo. Se quest'ultimo è ritenuto troppo elevato, devono essere adottate misure aggiuntive fino a ridurlo a un livello accettabile.

Gli obiettivi di protezione riservatezza, disponibilità, integrità e tracciabilità devono essere adeguatamente garantiti. A tal fine, è necessario definire le misure adottate e i rischi residui.

Devono essere previste soluzioni e responsabilità per i seguenti ambiti:

- Autenticazione
- Autorizzazione
- Logging e auditing
- Backup dei dati
- Aggiornamenti software / patching
- Protezione perimetrale (phishing, sicurezza e-mail, allegati)
- Protezione delle informazioni (in base alla classificazione dei dati)
- Data Leakage Prevention (DLP)
- Security Information & Event Management (SIEM), threat intelligence
- Sicurezza degli endpoint connessi al cloud

Infine, occorre valutare se tali requisiti possano essere soddisfatti dalle soluzioni offerte dal fornitore cloud o se sia opportuno adottare una strategia multi-vendor. La decisione dipende dalle soluzioni già in uso, dal livello di soddisfazione e dai vantaggi potenziali in termini di efficacia e costi, nonché dalla possibilità di integrazione con i sistemi esistenti.

## 12.2 Cifratura e gestione delle chiavi

Per proteggere adeguatamente i dati, la cifratura rappresenta una misura fondamentale. Occorre distinguere tra: 1) cifratura durante la trasmissione (in transit), 2) cifratura dei dati memorizzati (at rest) e 3) cifratura durante l'elaborazione (in process). La cifratura dei dati durante la trasmissione verso il cloud è indispensabile e deve essere sempre garantita.

### Punti da osservare per la cifratura dei dati “at rest”

Per quanto riguarda la cifratura dei dati memorizzati nel cloud (at rest), i fornitori offrono diverse soluzioni di gestione delle chiavi che devono essere valutate. La gestione delle chiavi è una condizione necessaria per l’utilizzo del cloud: senza di essa, i servizi cloud non possono essere utilizzati. È quindi essenziale chiarire le modalità di accesso alle chiavi.

Una distinzione fondamentale riguarda il fatto che la gestione delle chiavi sia effettuata dal fornitore nel cloud (con una chiave dedicata per ciascun cliente) oppure localmente dalla struttura sanitaria. In quest’ultimo caso, la responsabilità ricade interamente sulla struttura sanitaria. Se la gestione delle chiavi è affidata al fornitore, quest’ultimo garantisce la funzionalità, ma sussiste il rischio che collaboratori con diritti di accesso possano accedere alle chiavi e quindi ai dati. Questo rischio non sussiste nel caso di gestione locale.

Una maggiore sicurezza può essere garantita da soluzioni che richiedono un’ulteriore autorizzazione per l’accesso alle chiavi da parte dei collaboratori del fornitore. Tale autorizzazione può essere fornita da personale del fornitore con specifiche funzioni di controllo oppure da collaboratori designati della struttura sanitaria.

È importante assicurarsi che le persone incaricate di autorizzare tali accessi siano disponibili in base ai livelli di servizio richiesti. Se è necessario fornire supporto anche al di fuori degli orari di ufficio, anche le persone responsabili delle autorizzazioni devono essere disponibili; in caso contrario, gli interventi non potranno essere effettuati tempestivamente.

### Punti da osservare per la cifratura dei dati “in process”

La cifratura dei dati durante l’elaborazione (in process) rappresenta una sfida particolare,iIn particolare quando l’esecuzione nelle soluzioni SaaS avviene direttamente nel cloud e non localmente o nel browser. Le soluzioni disponibili variano a seconda del fornitore e comportano generalmente una maggiore complessità, una maggiore probabilità di errore e limitazioni funzionali.

Questo tipo di cifratura richiede che le persone che trattano i dati utilizzino una chiave non detenuta dal fornitore. La gestione della crittografia deve quindi essere effettuata dalla struttura sanitaria. Ad esempio, in caso di elaborazione congiunta con partner esterni, questi ultimi devono accedere all’infrastruttura della struttura per ottenere un certificato (chiave), che consenta loro di decifrare e trattare i dati nel cloud.

Questa configurazione è complessa e comporta rischi per la disponibilità. Inoltre, la soluzione di cifratura deve essere compatibile con le applicazioni cloud utilizzate; in caso contrario, tali applicazioni non possono essere impiegate.

Occorre quindi verificare caso per caso se esistono soluzioni per la cifratura dei dati in elaborazione e quali limitazioni comportino. Attualmente non è nota alcuna soluzione che consenta una cifratura affidabile dei dati «in process» mantenendo tutte le funzionalità. In assenza di tale cifratura, le funzionalità restano complete, ma i dati possono essere potenzialmente accessibili ai collaboratori del fornitore con i relativi diritti di accesso durante l’elaborazione.

*Questo documento è disponibile in diverse versioni linguistiche. In caso di discrepanze o interpretazioni divergenti, fa fede esclusivamente la versione tedesca.*

## A proposito degli autori

### Erik Dinkel

Erik Dinkel è dal 2018 CISO e dal 2024 anche Chief Security Officer (CSO) dell'Universitätsspital Zürich (USZ). Prima di entrare all'USZ, ha lavorato nel Business Risk Management e come Head Access Governance presso Credit Suisse Svizzera. Ha conseguito un master presso l'Università di Zurigo (M.A. UZH) in scienze politiche e dispone di formazioni complementari nei settori della gestione aziendale, del risk management e della sicurezza delle informazioni (CAS UZH, CAS FHNW, BSI). Dal 2021 è docente di cybersicurezza e sicurezza delle informazioni presso la Hochschule Luzern e, da agosto 2025, è presidente del Healthcare Cyber Security Center.

### Stefan Hunziker

Medico promosso e specialista in informatica gestionale, Stefan Hunziker ha diretto dal 2002 l'informatica medica e dal 2012 al 2025 l'IT del gruppo LUKS Gruppe. Parallelamente, dal 2021 al 2025 ha rappresentato come CIO l'area IT nella direzione del gruppo. In questo periodo è stato responsabile dell'integrazione IT dell'ospedale di Nidvaldo nel LUKS Gruppe. Dal 2026 lavora per l'Universitätsspital Zürich come responsabile di progetto nella trasformazione digitale.

### Stefan Juon

Stefan Juon ha lavorato dal 2009 al 2022 presso il Kantonsspital Graubünden in diverse funzioni, da ultimo dal 2016 al 2022 come responsabile della sicurezza delle informazioni (CISO) e co-responsabile ICT. Possiede una formazione in ingegneria e in economia aziendale a livello terziario, nonché qualifiche avanzate in sicurezza delle informazioni, gestione dei rischi e architettura IT. È inoltre certificato ITIL, TOGAF e CISA.

### Philipp Stoll

Philipp Stoll è un ingegnere meccanico di formazione. Negli ultimi 20 anni fino al suo pensionamento, è stato membro della direzione dell'Universitäts-Kinderspital beider Basel (UKBB). Da allora lavora come consulente per aziende del settore sanitario. Le sue aree di competenza comprendono edilizia, logistica, approvvigionamento, manutenzione, tecnologia medica e sicurezza, con una particolare specializzazione nell'interfaccia tra utenti e progettisti. Dal 2011 è inoltre delegato di H+ presso l'Ufficio federale della protezione della popolazione (UFPP) e l'Ufficio federale per l'approvvigionamento economico del Paese (UFAE).

### Werner Ulmer

Werner Ulmer è dal 2024 CISO della Direzione dell'economia pubblica del Cantone di Zurigo. In precedenza è stato CISO del Kantonsspital St. Gallen (oggi HOCH Health Ostschweiz) e dei relativi gruppi ospedalieri, dove ha guidato lo sviluppo strategico e operativo della sicurezza delle informazioni fino all'ottenimento della certificazione ISO 27001. Grazie a solide formazioni — tra cui presso la Hochschule Luzern — e a una lunga esperienza, dispone di una comprovata competenza in cybersicurezza, sicurezza delle informazioni, gestione dei rischi e governance della sicurezza.