

SANITÀ DIGITALE:

RISCHI CALCOLATI E SFIDE NASCOSTE



NOTA INTRODUTTIVA

L'assistenza sanitaria si trova di fronte a una svolta digitale. Le innovazioni in materia di IA, telemedicina, tecnologia mobile e automazione stanno aprendo nuove possibilità per un'assistenza più intelligente e più connessa. Nonostante questi progressi, molte organizzazioni sanitarie devono ancora fare i conti con i sistemi legacy e le inefficienze operative.

Per i leader IT, la sfida è chiara. È fondamentale che le organizzazioni accelerino l'implementazione di tecnologie avanzate per migliorare gli esiti clinici, valorizzare le risorse umane e garantire percorsi assistenziali integrati che rispondano alle aspettative dei pazienti.

I sistemi legacy causano ritardi nell'accesso alle informazioni critiche, il che in ultima analisi riduce la qualità dell'assistenza. Nel frattempo, l'IA può migliorare la diagnostica, razionalizzare i flussi di lavoro e prevedere le esigenze del paziente, ma solo se supportata da un'infrastruttura moderna.

La misura in cui la nuova tecnologia viene integrata e la capacità di massimizzare i vantaggi di tutti i dispositivi e di tutte le applicazioni hanno un effetto preponderante



Stephanie Lopinski, VP, Global Marketing

sui risultati dei pazienti e sulla qualità dell'assistenza fornita. Le organizzazioni devono dare priorità a integrare i sistemi, accedere ai dati in tempo reale e abbandonare la tecnologia obsoleta per sbloccare i vantaggi della trasformazione digitale.

La nostra ultima ricerca esamina lo stato attuale delle organizzazioni sanitarie, le sfide che devono affrontare e le strategie di miglioramento.

Il rapporto 2025 di SOTI mette in evidenza tre temi chiave:

Intelligenza artificiale

L'adozione dell'IA nell'assistenza sanitaria sta crescendo rapidamente, con l'**81%** delle organizzazioni globali che la utilizzano per l'assistenza ai pazienti, in aumento rispetto al **61%** del 2024. Le sue applicazioni includono l'elaborazione di dati medici, l'aggiornamento delle cartelle cliniche, la personalizzazione dei trattamenti e la diagnosi di patologie.

Nonostante l'aumento dell'adozione dell'IA, solo il **36%** delle organizzazioni dispone di misure di sicurezza specifiche per l'IA, sollevando preoccupazioni sulla privacy dei pazienti. Pertanto, modernizzare i sistemi è fondamentale per garantire la privacy dei pazienti.

Il rapporto del 2025 dipinge un quadro chiaro: l'assistenza sanitaria sta progredendo dal punto di vista tecnologico, ma in modo disomogeneo. Il settore continuerà a faticare nel trasformare la semplice adozione dell'IA in una reale integrazione, fintanto che non saranno risolti i sistemi legacy, rafforzata la sicurezza dei dati e liberate le risorse IT dalla gestione continua dei problemi.

Sistemi legacy

Le organizzazioni sanitarie lottano per integrare sistemi interconnessi e soluzioni di telemedicina, principalmente a causa di sistemi legacy obsoleti difficili da gestire da remoto.

Questi sistemi presentano rischi significativi per la sicurezza, con l'**83%** delle organizzazioni che segnalano violazioni o fughe di dati o attacchi ransomware dal 2023. Inoltre, complicano l'integrazione di cartelle cliniche elettroniche, con un impatto sul **79%** delle organizzazioni.

Di conseguenza, quando le organizzazioni tentano di adottare nuove tecnologie, si trovano spesso di fronte a battute d'arresto che ostacolano l'innovazione e influenzano

negativamente l'esperienza del paziente. In definitiva, le limitazioni imposte da questi sistemi obsoleti influenzano direttamente i risultati dell'assistenza ai pazienti, rendendo fondamentale per le organizzazioni investire in tecnologie moderne e sistemi interconnessi per migliorare l'efficienza, la sicurezza e la qualità generale dell'assistenza.

Gestione dei dispositivi mobili + Gestione della mobilità aziendale

Le organizzazioni sanitarie si affidano sempre più a una gamma di dispositivi mobili, tra cui laptop, smartphone, tablet e apparecchiature specializzate come lettori RFID. La gestione di questi dispositivi presenta sfide significative nella sicurezza e nella risoluzione dei problemi remoti quando si basano su soluzioni di gestione dei dispositivi mobili (MDM) obsolete.

Tuttavia, l'attuale panorama richiede un'evoluzione al di là della tradizionale MDM per includere un approccio globale di gestione della mobilità aziendale (EMM).

Con l'evolversi della tecnologia sanitaria, bisogna spostare l'attenzione verso una piattaforma integrata che includa diagnostica avanzata, analisi dei dati e intelligenza operativa. Questo approccio consente alle organizzazioni di affrontare i problemi in modo proattivo, sfruttando gli approfondimenti per prendere decisioni informate e ottimizzare i flussi di lavoro. Digitalizzando i processi e automatizzando i compiti amministrativi, i fornitori di assistenza sanitaria possono migliorare l'efficienza operativa e offrire una migliore assistenza ai pazienti.

Soluzioni di gestione dei dispositivi mobili efficaci richiedono anche che la gestione completa del ciclo di vita promuova la sostenibilità. Le organizzazioni dovrebbero mirare a massimizzare la durata di vita dei loro dispositivi, utilizzando informazioni sullo stato della batteria e modelli di utilizzo per sviluppare strategie di sostituzione sostenibili. Questa gestione proattiva non solo aiuta a mantenere i dispositivi più a lungo, ma riduce anche le vulnerabilità e protegge i dati dei pazienti.

IL PANORAMA DELL'ASSISTENZA SANITARIA STA CAMBIANDO:

PROGRESSI E INNOVAZIONI DAL 2020

2020 - 2021

- Sicurezza: l'**81%** mostra preoccupazioni riguardo alla sicurezza delle cartelle cliniche dei pazienti
- Problemi relativi alla tecnologia: il **63%** riporta guasti relativi al dispositivo o al sistema su base settimanale
- Impatto tecnologico sull'assistenza al paziente: l'**81%** ha problemi con i sistemi e la tecnologia durante l'assistenza ai pazienti

475 fornitori di assistenza a domicilio, infermieri e altri operatori sanitari in sette Paesi nel mondo

2022

- Sicurezza: il **73%** delle organizzazioni ha sperimentato una violazione o una fuga di dati dal 2020
- IoT/Telemedicina: il **98%** ha implementato funzionalità di IoT/dispositivi di telemedicina
- L'impatto dei tempi di inattività dei dispositivi mostra che il **53%** degli operatori segnala interruzioni regolari che causano ritardi nell'assistenza ai pazienti, con una perdita media di 3,4 ore settimanali per dipendente dovuta a questi fermi operativi

1.300 professionisti IT che lavorano in organizzazioni sanitarie in otto Paesi nel mondo

2023

- Protezione dei dati sanitari: il **97%** degli intervistati esprime preoccupazioni relative alla protezione delle cartelle cliniche
- Sicurezza della rete: il **55%** ha subito una fuga di dati accidentale o pianificata da fonti interne; il **53%** non è in grado di rilevare nuovi dispositivi che si connettono al sistema a causa di sistemi obsoleti, con conseguente vulnerabilità
- Sistemi legacy: il **52%** sostiene che i sistemi legacy non siano in grado di risolvere i problemi in modo tempestivo. Il **37%** ritiene che i sistemi obsoleti rendano più vulnerabili alle violazioni della sicurezza
- Tempo di inattività: 3,4 ore perse in una comune settimana a causa di difficoltà tecniche o di sistema

1.450 professionisti IT che lavorano in organizzazioni sanitarie in nove Paesi nel mondo

2024

- IA: l'**85%** ritiene che l'IA possa contribuire a semplificare i compiti, ma attualmente solo il 23% la sta utilizzando in modo diffuso
- Sicurezza: il **71%** trasferisce i dati su dischi rigidi esterni/backup durante lo smaltimento di vecchi dispositivi. Il **23%** indica la sicurezza dei dati come principale preoccupazione in ambito IT
- IoT/Telemedicina: il **67%** riscontra problemi ricorrenti con i dispositivi IoT/di telemedicina che causano ritardi nell'assistenza ai pazienti
- Sistemi legacy: il **63%** afferma di utilizzare tecnologie obsolete, e il **45%** ha subito una violazione dei dati o una fuga di dati accidentale nell'ultimo anno
- Tempo di inattività: si perdono 3,9 ore a settimana per ogni dipendente a causa delle interruzioni

1.450 professionisti IT/decision maker che lavorano in strutture sanitarie di nove Paesi nel mondo

2025

- IA: l'**81%** sta utilizzando l'IA per l'assistenza ai pazienti, in aumento rispetto al 61% del 2024
- Sicurezza: l'**83%** ha riportato una fuga di dati accidentale, violazione di dati esterna o attacco ransomware DDoS negli ultimi 12 mesi. Il **30%** menziona la sicurezza dei dati come principale preoccupazione in ambito IT
- IoT/Telemedicina: il **96%** riscontra difficoltà nell'implementazione di dispositivi medici IoT/di telemedicina
- Sistemi legacy: il **45%** sostiene che l'IT ereditato renda le reti vulnerabili ad attacchi
- Gestione dei dispositivi mobili: il **47%** sostiene che le soluzioni di gestione dei dispositivi mobili siano fondamentali per la risoluzione remota dei problemi

1.750 professionisti informatici e decision maker operanti nel settore sanitario in nove Paesi nel mondo

Dal 2020 SOTI svolge attività di ricerca in campo sanitario. Con l'evoluzione dello studio, è cresciuto progressivamente sia il numero di Paesi coinvolti che quello dei partecipanti. Le tendenze degli ultimi cinque anni includono le seguenti informazioni rilevanti:

CONTENUTI

Metodologia

Panoramica globale

Risultati principali

**La svolta: l'intelligenza artificiale
è sempre più utilizzata
nell'assistenza ai pazienti**

**La sfida: i sistemi legacy limitano il
valore della tecnologia emergente**

**L'evoluzione necessaria: dal
gestione dei dispositivi mobili and
gestione della mobilità aziendale**

Conclusione

METODOLOGIA

Quest'anno la ricerca di SOTI ha ampliato il suo raggio d'azione includendo **1.750 intervistati in 11 Paesi**: Stati Uniti (200), Canada (150), Messico (150), Regno Unito (200), Germania (150), Francia (150), Svezia (150), Paesi Bassi (150), Italia* (150), Spagna* (150) e Australia (150). Il questionario è stato completato tra gennaio e marzo 2025 da professionisti nel campo IT per le organizzazioni sanitarie.

*Nuove aree geografiche incluse nel rapporto sull'assistenza sanitaria del 2025.



PANORAMA GLOBALE

Per questo rapporto, organizzazione sanitaria:



Un ospedale che fornisce assistenza ai pazienti in prima linea.



Una struttura sanitaria primaria polispecialistica, comprendente ad esempio: ambulatori di medicina generale, studi medici di famiglia e ambulatori multispecialistici.



Una struttura ambulatoriale che eroga servizi sanitari di primo livello in una o più specialità, ad esempio: salute mentale, neurologia, fisioterapia, ecc.



Un operatore sanitario che fornisce servizi di telemedicina o assistenza remota direttamente al paziente.

Le organizzazioni sanitarie variavano da 50 a oltre 5.000 dipendenti. Sebbene tutti gli intervistati fossero coinvolti nei processi decisionali IT per un'organizzazione sanitaria, i loro ruoli variavano da professionisti IT a dirigenti di alto livello e C-suite.



RISULTATI GLOBALI

|| **96%**

rivela che le organizzazioni incontrano difficoltà nell'implementazione di dispositivi medici IoT/telemedicina, dove l'integrazione dei sistemi rappresenta la sfida maggiore.

L' **83%**

mostra come gli incidenti di sicurezza rimangono elevati: fughe accidentali di dati, violazioni esterne e attacchi ransomware DDoS non mostrano segni di diminuzione.

|| **47%**

evidenzia che i decision maker IT a livello globale considerano fondamentali le soluzioni Mobile Device Management per la risoluzione remota dei problemi.

|| **45%**

indica che i sistemi IT obsoleti sono la causa principale della vulnerabilità delle reti agli attacchi informatici.

L' **81%**

fa emergere preoccupazioni a livello mondiale sulla protezione delle informazioni cliniche in fase di dismissione dei device mobili.

L' **81%**

rivela che le strutture sanitarie utilizzano ormai l'IA in qualche forma per migliorare l'efficienza e l'efficacia delle cure, un aumento significativo dal 61% del 2024.

|| **40%**

mostra che le organizzazioni sostituiscono i dispositivi obsoleti quando diventano disponibili nuove versioni.

|| **30%**

identifica la data security come priorità assoluta in ambito informatico, con una crescita significativa rispetto al 23% del 2024.



LA SVOLTA: L' INTELLIGENZA ARTIFICIALE NELL'ASSISTENZA AI PAZIENTI

Gli ultimi anni hanno visto il mondo della sanità compiere avanzamenti significativi, grazie all'applicazione sempre più diffusa della tecnologia a beneficio dei pazienti. L'ascesa dell'IA sta rimodellando il modo in cui i fornitori di assistenza sanitaria offrono servizi e interagiscono con i pazienti.

Sfruttare l'IA per migliorare la diagnostica, personalizzare i piani di trattamento e semplificare le operazioni ha catturato l'attenzione delle organizzazioni sanitarie in tutto il mondo. Quest'anno, la nostra indagine ha rilevato che l'IA viene utilizzata per l'assistenza ai pazienti nell'**81%** delle organizzazioni sanitarie, un terzo in più rispetto al 2024 (**61%**).

La maggior parte delle organizzazioni che non utilizzano ancora l'IA per l'assistenza ai pazienti almeno la stanno valutando (**16%** a livello globale), mentre solo il **3%** dei responsabili IT afferma che la propria organizzazione non ha piani per adottarla.

L'IA è più diffusa nel Regno Unito, dove il **94%** dei responsabili IT ha dichiarato che la propria organizzazione la utilizza per l'assistenza ai pazienti, in aumento rispetto al **47%** del 2024. In Australia, il **93%** ha affermato di utilizzare l'IA, in aumento dal **70%**.

Utilizzo dell'Intelligenza Artificiale nell'assistenza sanitaria: confronto percentuale tra 2024 e 2025

	2025	2024		2025	2024
	81%	61%		81%	45%
	80%	72%		71%	53%
	87%	72%		70%	43%
	82%	80%		74%	-
	94%	47%		83%	-
	77%	71%		93%	70%

INTELLIGENZA ARTIFICIALE PER ALLEGGERIRE IL CARICO AMMINISTRATIVO

Sebbene il numero di organizzazioni che utilizzano l'IA sia aumentato, il modo in cui stanno applicando la tecnologia rimane in gran parte invariato rispetto allo scorso anno. Nel 2025, l'utilizzo più comune dell'IA riguarda l'elaborazione e/o l'analisi dei dati medici (**60%** dei responsabili IT ha dichiarato che la propria organizzazione la utilizza per questo scopo), seguito dall'aggiornamento delle cartelle cliniche (**59%**). Poco meno della metà (**46%**) usa l'IA per pianificare il miglior corso di trattamento, mentre il **45%** la usa per personalizzare i trattamenti e il **40%** per diagnosticare patologie.

In quali di queste attività legate all'assistenza pazienti viene impiegata l'IA nella tua struttura? (Rivolto a chi utilizza l'IA nell'assistenza ai pazienti)

Risultati globali	2025	2024
Per elaborare e/o analizzare dati medici	60%	60%
Per aggiornare le cartelle cliniche dei pazienti	59%	56%
Per pianificare il miglior percorso terapeutico	46%	47%
Per personalizzare i trattamenti	45%	44%
Per altre finalità amministrative	45%	20%
Per diagnosticare patologie	40%	38%
NET: Per l'aggiornamento delle anamnesi e altre procedure amministrative	79%	63%

Un cambiamento significativo quest'anno è l'aumento dell'IA utilizzata per altri scopi amministrativi. Nel 2024, il **20%** dei responsabili IT ha segnalato l'utilizzo dell'IA in questo ambito, mentre nel 2025 questa percentuale è aumentata al **45%**.

Delegando compiti noiosi all'IA, il personale sanitario può concentrarsi su aspetti importanti dell'assistenza ai pazienti. Se consideriamo anche le organizzazioni che utilizzano l'IA per l'aggiornamento delle cartelle cliniche, osserviamo che un netto **79%** impiega l'IA per almeno una finalità amministrativa.





Il Regno Unito e gli Stati Uniti sono i principali utilizzatori di IA per la personalizzazione delle terapie (**57%** e **55%**, rispettivamente), mentre il Regno Unito guida la classifica nella diagnosi di patologie con l'IA (**52%**). Svezia (**53%**) e Canada (**52%**) hanno segnalato l'uso maggiore dell'IA per altri scopi amministrativi.

Nella ricerca dello scorso anno, abbiamo scoperto che oltre la metà (**57%**) dei professionisti IT aveva alcune riserve sull'uso dell'IA nell'assistenza ai pazienti, preoccupati che questa rappresentasse una minaccia per la loro privacy. Quest'anno abbiamo scoperto che tutte le organizzazioni hanno attuato almeno alcune misure di sicurezza per i dispositivi mobili, ma solo il **36%** dispone di misure di sicurezza specifiche per l'IA. Considerando il notevole aumento nell'utilizzo dell'IA nell'ultimo anno, questa sembra essere un'area che più organizzazioni sanitarie dovrebbero esplorare.

A quali misure di sicurezza per i dispositivi mobili dai la priorità?

Aggiornamenti periodici	51%
Formare ed educare i dipendenti sulle minacce specifiche e sulle migliori pratiche in materia di sicurezza	45%
Garantire il rispetto delle leggi sulla regolamentazione e sulla protezione dei dati (ad esempio RGPD, EHDS)	45%
Limitare l'accesso ai dati sensibili a determinati ruoli e responsabilità	45%
Autenticazione a più fattori	44%
Crittografia	42%
Controlli di sicurezza periodici	42%
Misure di sicurezza specifiche per l'IA	36%
Implementare l'anonimizzazione dei dati	34%
Avere in atto un piano di risposta agli incidenti	33%
Cancellazione remota	23%

L'anno scorso, più di otto professionisti IT su dieci (**83%**) hanno affermato che l'IA rappresenta una strategia essenziale per il risparmio dei costi nelle organizzazioni sanitarie. Quest'anno, l'uso dell'IA nell'assistenza ai pazienti è aumentato. Considerati i problemi che i sistemi legacy pongono all'adozione di tecnologie emergenti e le persistenti criticità nella sicurezza dei dati del settore, la gestione dei dispositivi che le utilizzano richiede un monitoraggio rigoroso per garantirne un impiego sicuro e ottimale.

L'ADOZIONE DI IOT E TELEMEDICINA È UNIVERSALE, MA PERMANGONO CRITICITÀ

L'integrazione di tecnologie interconnesse sta ridefinendo il panorama sanitario, in particolare attraverso la telemedicina, che collega dispositivi e sistemi sia all'interno delle strutture sanitarie che da remoto. Quest'anno, quasi tutti i responsabili IT (**99%**) hanno indicato che le loro organizzazioni utilizzano qualche forma di dispositivi connessi o soluzioni di telemedicina.

Nonostante questo elevato livello di adozione, l'efficienza operativa di questi sistemi è inferiore alle aspettative.

LA SFIDA:

**I SISTEMI LEGACY
LIMITANO IL VALORE
DELLA TECNOLOGIA
EMERGENTE**

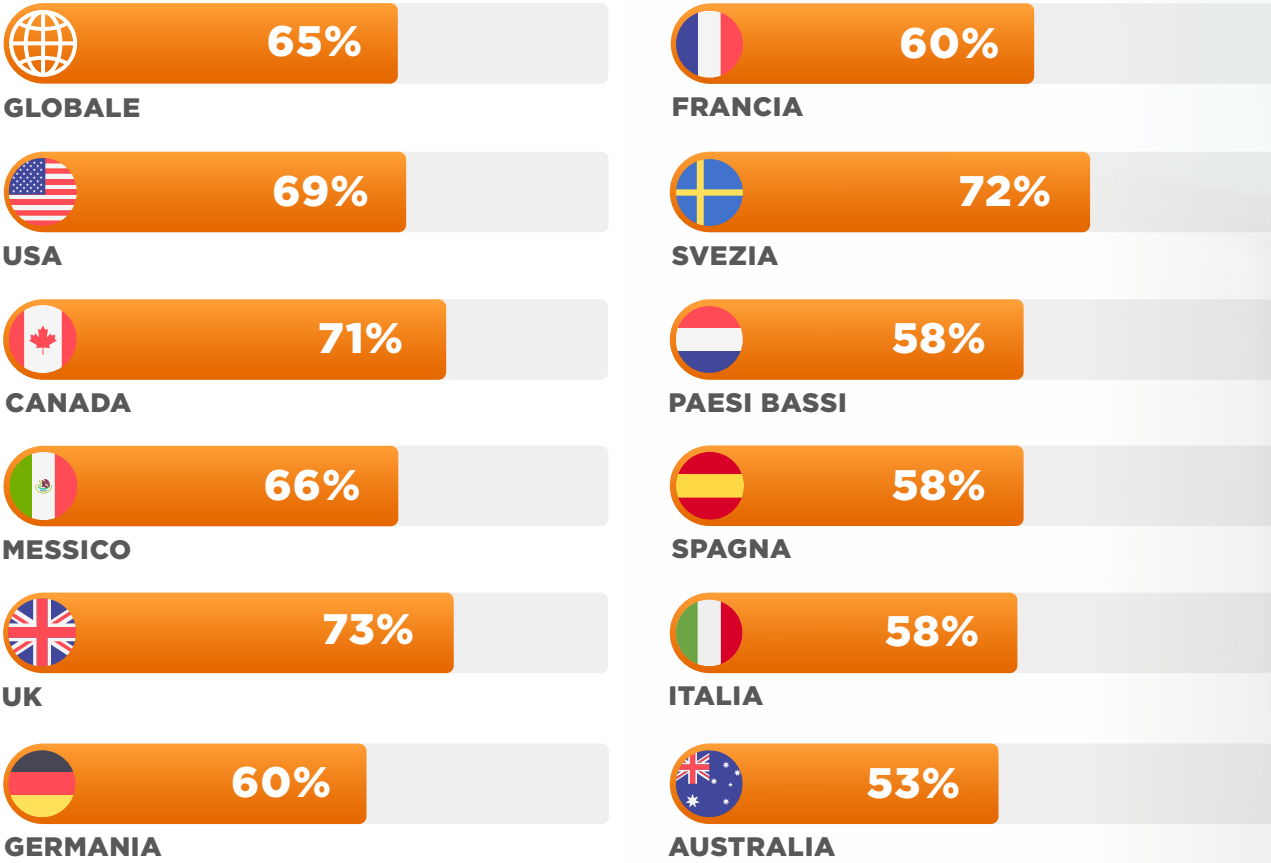
Un significativo

96%

dei leader IT ha riportato
di avere difficoltà con
queste tecnologie.

Uno dei problemi principali è la mancanza di integrazione tra i sistemi utilizzati per i dispositivi connessi e le applicazioni di telemedicina. Il fenomeno trova riscontro nei seguenti dati statistici raccolti nelle varie aree geografiche.

I sistemi utilizzati per i dispositivi medici IoT/telemedicina non sono integrati:



La sfida più significativa affrontata quest'anno dal **65%** delle organizzazioni è la mancanza di integrazione tra questi sistemi. Ciò riguarda le sfide dell'interoperabilità, come l'incapacità di accedere alle informazioni complete sulla salute del paziente in un unico luogo (segnalata dal **43%** dei partecipanti) e la mancanza di aggiornamenti automatici in tutti i sistemi (**40%**). Inoltre, il **65%** dei decision maker IT ha espresso frustrazione per le difficoltà delle proprie organizzazioni nel fornire i dati rilevanti alle persone giuste al momento più opportuno.

Queste criticità sono evidenti a livello globale, ma risultano particolarmente marcate in Australia (**77%**), Regno Unito (**73%**) e Canada (**71%**). Problemi di integrazione sono comuni anche tra le organizzazioni sanitarie che operano in ambiti multidisciplinari. Chi vive queste problematiche include per il **69%** ambulatori e studi medici generici, e per il **67%** cliniche specializzate in una o più aree. Rispetto ad altri contesti, il **62%** dei responsabili IT di strutture ospedaliere di primo intervento e di enti specializzati in servizi di telemedicina ha segnalato analoghe difficoltà di integrazione sistemica (**60%**).

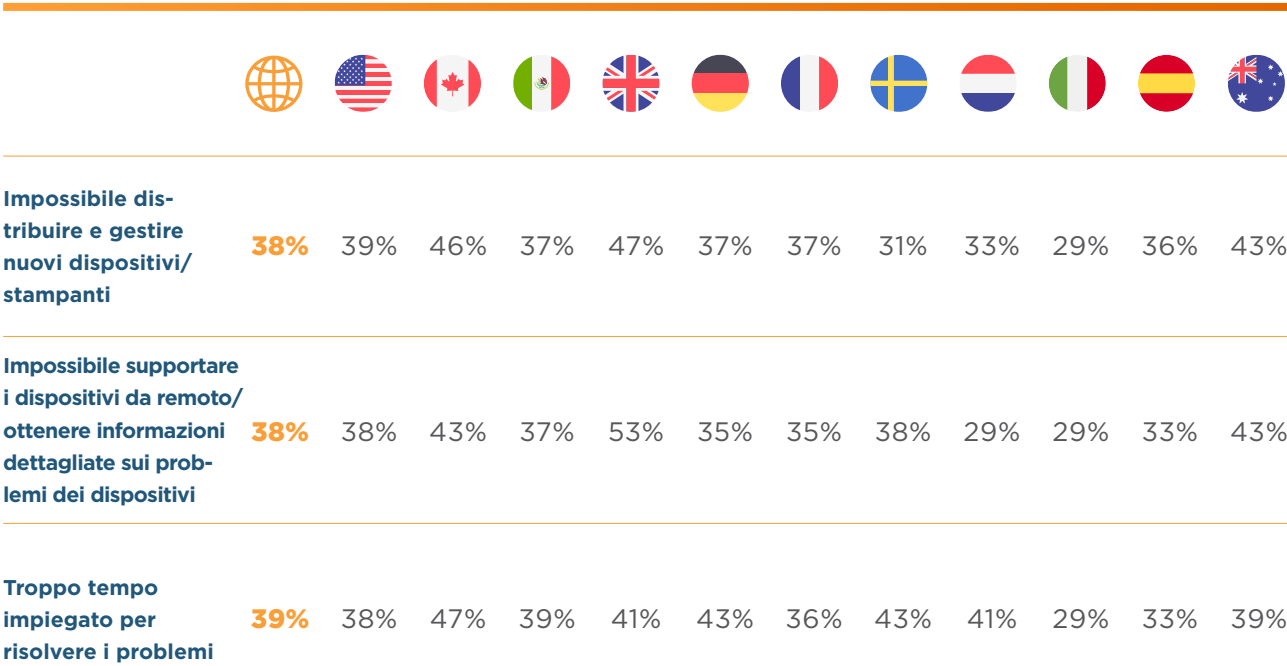


I SISTEMI LEGACY CREANO PROBLEMI DI INTEGRAZIONE E INTEROPERABILITÀ

La percentuale di decision maker IT le cui organizzazioni utilizzano tecnologie obsolete è scesa dal **63%** nel 2024 al **55%** quest'anno. Tuttavia, secondo il **97%** dei responsabili IT, le rispettive aziende dispongono ancora di infrastrutture legacy. Circa la metà di coloro che utilizzano tecnologie legacy non le considera obsolete, tuttavia queste stesse tecnologie stanno influenzando la capacità delle organizzazioni di adattarsi a nuovi modi di lavorare.

Quattro decisori IT su dieci (**38%**) sostengono che l'IT legacy impedisca loro di implementare e gestire nuovi dispositivi/stampanti; secondo la stessa percentuale, ciò significa che non possono supportare i dispositivi da remoto o ottenere informazioni dettagliate sui problemi dei dispositivi.

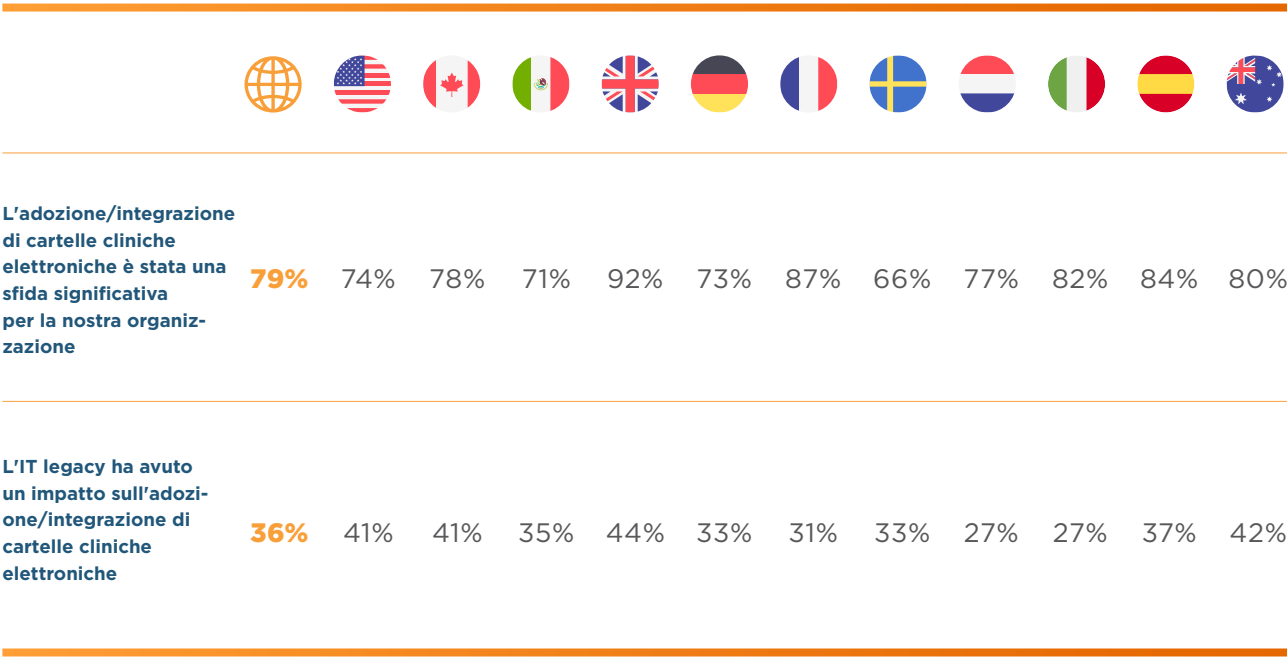
Che impatto ha la tecnologia legacy sulle tue operazioni quotidiane?



Con l'aumento di cartelle cliniche elettroniche (EMR) per consentire la condivisione ottimizzata dei dati dei pazienti all'interno delle organizzazioni sanitarie e l'uso crescente di dispositivi di telemedicina, l'integrazione e l'interoperabilità sono più critiche che mai. Tuttavia, i risultati di quest'anno rivelano che i problemi di integrazione del sistema causati dai sistemi legacy rimangono un ostacolo.

Più del 75% (**79%**) dei responsabili informatici ha evidenziato come l'implementazione degli EMR rappresenti una criticità rilevante, con **36%** che identifica nei sistemi obsoleti la causa primaria. L'impatto delle tecnologie obsolete sull'adozione/integrazione dei sistemi EMR è particolarmente critico nel Regno Unito (**44%**), negli Australia (**42%**) negli Stati Uniti e in Canada (ognuno **41%**).

L'adozione e l'integrazione dei sistemi EMR ha incontrato ostacoli significativi a causa dell'infrastruttura IT legacy



I dati indicano che l'adattamento umano è essenziale per utilizzare efficacemente le nuove tecnologie. Il **30%** dei partecipanti crede che i sistemi vengano cambiati troppo spesso e che l'organizzazione non riesca a stare al passo. Un ulteriore **33%** ha dichiarato che la formazione degli utenti sui nuovi sistemi rallenta i processi e influisce sull'assistenza ai pazienti. Tuttavia, la sfida più grande nel funzionamento ottimale dei dispositivi medici IoT e di telemedicina deriva da sistemi obsoleti nel settore sanitario:

Il **90%**

delle organizzazioni richiede maggiori investimenti in tecnologie nuove o migliori per migliorare l'assistenza ai pazienti, e

L' **89%**

per più dispositivi interconnessi.

I SISTEMI LEGACY CREANO RISCHI DI SICUREZZA



Più di otto decisori IT su dieci (83%)

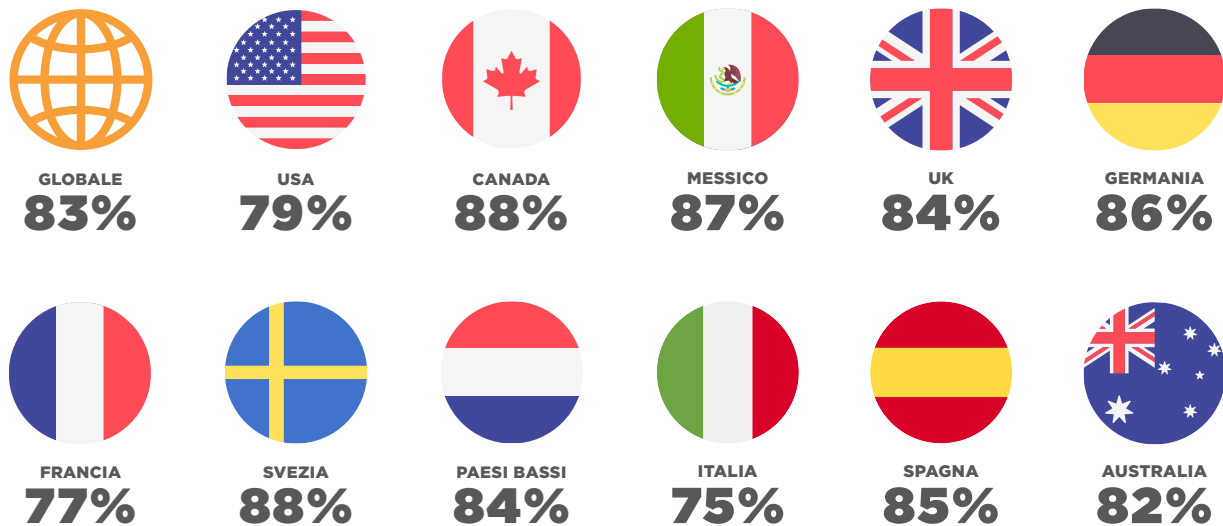
hanno affermato che la loro organizzazione ha dovuto affrontare almeno una **violazione/fuga di dati o un attacco ransomware** dal 2023.

Ciò è coerente con i dati del 2024 (85%), indicando che tali minacce continuano a prevalere e non vengono gestite in modo efficace.

La variazione nella percentuale annuale complessiva di organizzazioni in cui si verificano incidenti può essere minima, ma ora quasi la metà ha registrato una fuga accidentale di dati (48% rispetto al 2022, quando era del 33%); due terzi hanno sperimentato una violazione di dati da una fonte esterna o un attacco ransomware (65%, in linea con il 2024 ma in aumento rispetto al 48% del 2022 e al 52% del 2023).

L'unico tipo di incidente per cui si ha assistito a un cambiamento significativo quest'anno è la percentuale di decisori IT che segnala una fuga di dati prevista per i dipendenti, che è sceso dal 34% del 2024 al 24% del 2025.

Negli ultimi 12 mesi si sono verificati uno o più incidenti di sicurezza:



Con un calo previsto per quest'anno delle violazioni dei dati dei dipendenti, l'elemento umano della sicurezza dei dati può iniziare a essere sotto controllo, ma le fonti basate sulla tecnologia sono ben lungi dall'essere eliminate.

Quest'anno, quasi la metà dei decisori IT (45%) sostiene che l'IT ereditata abbia reso le reti vulnerabili agli attacchi di sicurezza, un aumento del 36% rispetto al 2024.

Si tratta di una questione che interessa le organizzazioni di tutto il mondo, ma che desta maggiore preoccupazione in alcuni Paesi: oltre la metà dei decisori IT in Svezia (55%), Francia (54%), Australia (53%) e Canada (51%) teme ancora che la propria rete sia suscettibile ad attacchi di sicurezza a causa dell'IT ereditato in atto.

La preoccupazione per l'IT ereditata sta crescendo ogni anno ed è aumentata in ogni paese oggetto dell'indagine. Senza affrontare problemi di sistema legacy, le organizzazioni devono affrontare una crescente esposizione alle minacce per la sicurezza, a inefficienze operative e a ostacoli all'assistenza ai pazienti.

"L'IT ereditata rende la nostra rete vulnerabile agli attacchi di sicurezza"

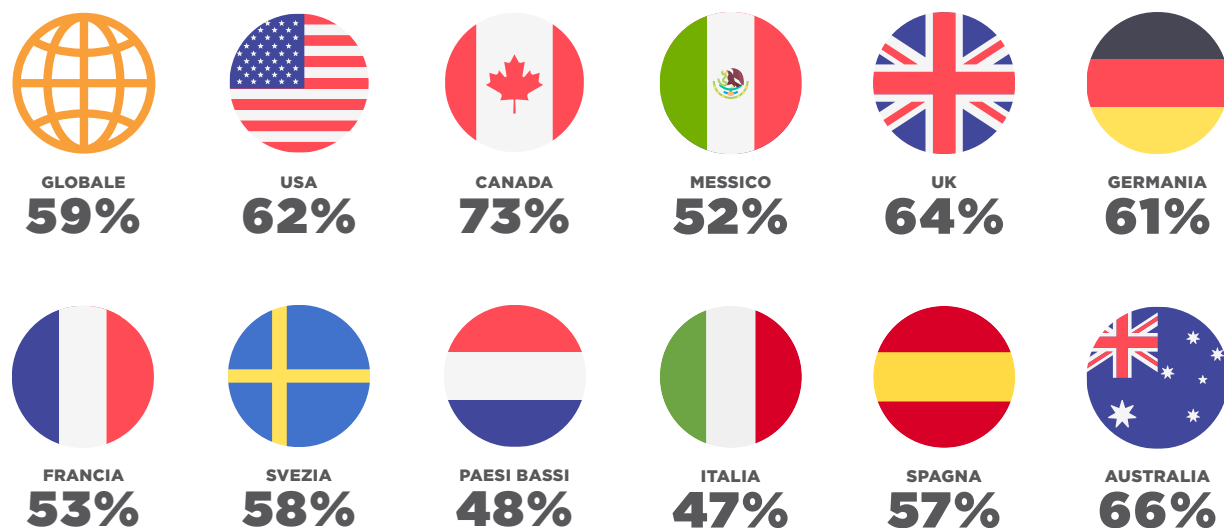
	2025	2024		2025	2024
	45%	36%		54%	27%
	44%	39%		55%	25%
	51%	43%		40%	37%
	39%	35%		37%	-
	43%	40%		41%	-
	45%	33%		53%	39%

Quattro su dieci (38%) non possono supportare i dispositivi da remoto o ottenere informazioni dettagliate sui problemi dei dispositivi, e uno su cinque (20%) sostiene di non poter rilevare i nuovi dispositivi che si connettono al sistema. L'IT ereditata è in uso nel 97% delle organizzazioni sanitarie. Sulla base della ricerca di quest'anno, continuano a verificarsi problemi di integrazione, manutenzione e sicurezza.

I SISTEMI LEGACY CREANO PIÙ LAVORO PER I TEAM

Problemi tecnici frequenti e tempi di inattività rappresentano un'ulteriore sfida quando si utilizzano dispositivi interconnessi e dispositivi di telemedicina. Il **59%** delle organizzazioni ne risente quest'anno, in aumento dal **52%** del 2022.

Si sono verificati frequenti problemi tecnici/tempi di inattività nella tua organizzazione utilizzando dispositivi medici IoT/di telemedicina?



I tempi tecnici di inattività nelle strutture sanitarie possono causare interruzioni dell'assistenza ai pazienti, compromettendo l'efficienza complessiva delle operazioni. Le organizzazioni devono affrontare sfide legate agli aggiornamenti e alla manutenzione del sistema, che portano a flussi di lavoro inefficienti e a una diminuzione della qualità dell'assistenza sanitaria.

Sebbene si tratti di problematiche globali, le interruzioni operative e le difficoltà tecniche risultano particolarmente accentuate in Canada (**73%**), Australia (**66%**) e Regno Unito (**64%**).

Nell'ambito dello sviluppo di iniziative strategiche, i reparti informatici devono comunque dedicare risorse significative alla gestione di problematiche operative minori, tra cui malfunzionamenti delle periferiche, criticità di connessione e altre attività di assistenza ricorrenti. Gran parte di questo problema è causato da sistemi IT obsoleti, con il **39%** dei decision maker IT che afferma di dedicare troppo tempo alla risoluzione di problemi. Questa inefficienza compromette la capacità di concentrarsi su iniziative più strategiche che guidano il miglioramento organizzativo. Le organizzazioni sanitarie devono prendere in considerazione la possibilità di implementare soluzioni che aiutino a integrare le tecnologie esistenti e quelle nuove.

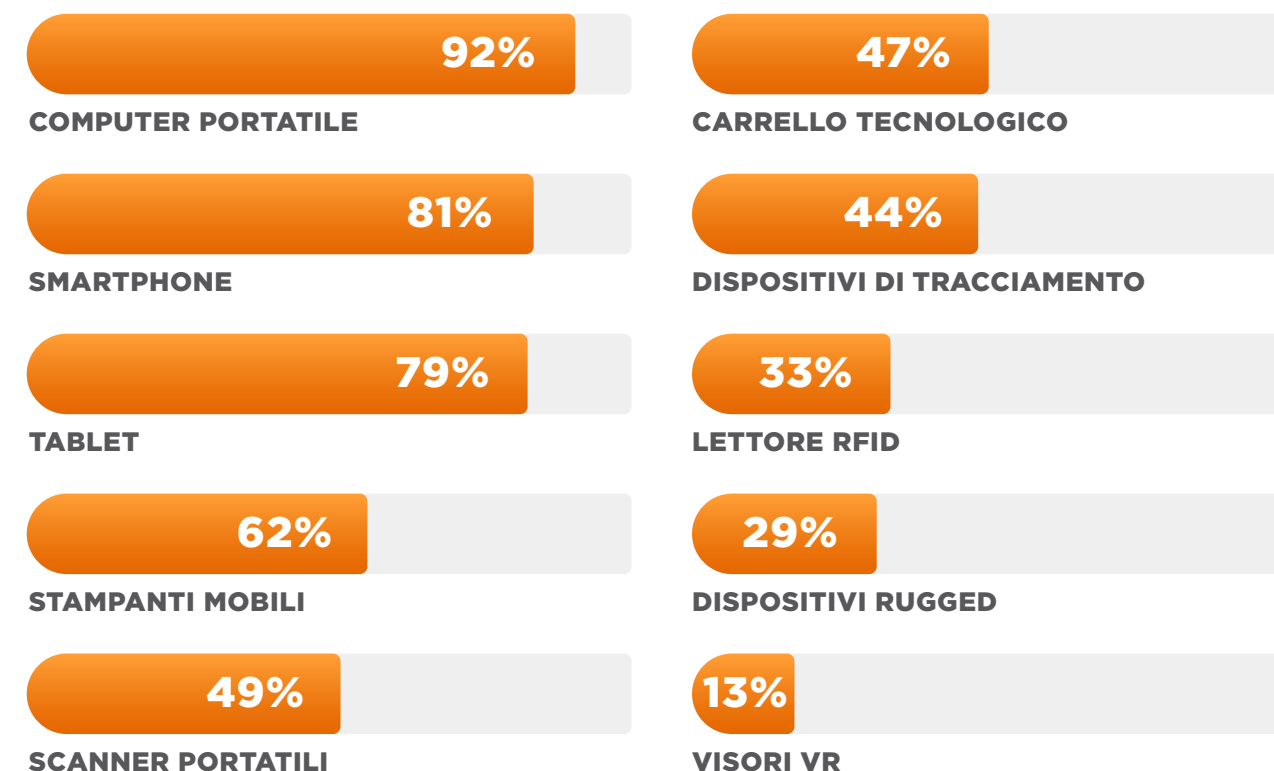


I PROSSIMI PASSI: LA GESTIONE DELLA MOBILITÀ AZIENDALE HA SOSTITUITO QUELLA DEI DISPOSITIVI MOBILI

L'aumento dell'integrazione di vari dispositivi mobili, un uso più ampio delle stampanti e un'ampia gamma di applicazioni nelle operazioni sanitarie quotidiane richiede una soluzione solida di gestione dei dispositivi.

Quali dei seguenti tipi di dispositivi mobili vengono utilizzati nella tua organizzazione?

Risultati globali



Con una gamma così diversificata di dispositivi, le organizzazioni sanitarie devono affrontare la sfida di mantenere la sicurezza, condurre la risoluzione dei problemi a distanza e garantire che tutti i dispositivi funzionino in modo ottimale. Per i decision maker informatici, risulta cruciale assicurare un'interconnessione senza connessioni con le apparecchiature medicali. Per soddisfare queste esigenze, le organizzazioni sanitarie devono andare oltre la gestione dei dispositivi mobili tradizionale e adottare un approccio più completo e integrato.

LA CRESCENTE NECESSITÀ DI SOLUZIONI EMM

Indubbiamente, la tecnologia mobile è molto utile, in quanto l'**86%** dei decision maker IT sostiene che renda il loro lavoro più veloce. Tuttavia, il numero in circolazione suggerisce che ci sono molti dispositivi mobili da monitorare, mantenere e gestire, e la maggioranza utilizza MDM per scopi di sicurezza (**90%**). Questo include la gestione delle policy di sicurezza, la protezione dalle minacce informatiche e l'identificazione di dispositivi non autorizzati che accedono alla rete - tutti aspetti critici per ridurre le vulnerabilità e minimizzare il rischio di violazioni.



Gestione della sicurezza	63%
Protezione dalle minacce informatiche/identificazione dei dispositivi esterni che accedono alla rete	56%
Riduzione dell'esposizione al rischio esterno esterne/riduzione delle opportunità per gli hacker	48%
Risoluzione dei problemi da remoto	47%
Gestione delle app	47%
Monitoraggio dei dispositivi	45%
Conformità e applicazione delle politiche	44%
Limitazione dell'accesso alle funzionalità dei dispositivi in determinati ambienti	38%
NET: Relativo alla sicurezza (gestione della sicurezza o protezione da minacce informatiche/identificazione di dispositivi esterni che accedono alla rete o modi per ridurre le vulnerabilità alle minacce esterne/riduzione delle opportunità per gli hacker)	90%

Molte organizzazioni sanitarie utilizzano soluzioni MDM per la sicurezza di base e la gestione dei dispositivi, ma si tratta solo del livello minimo essenziale. Nell'attuale ambiente sanitario in rapida evoluzione, una MDM di base non è più sufficiente.

Con un'assistenza ai pazienti sempre più complessa e un numero in aumento di dispositivi collegati, le organizzazioni devono passare da strategie reattive a strategie proattive per rilevare ed evitare i problemi prima che ostacolino l'assistenza. Ciò significa andare oltre le sole funzioni di base per attuare il monitoraggio in tempo reale e prevedere le violazioni della sicurezza e le interruzioni operative.

Due terzi (**65%**) dei responsabili IT riferiscono che la loro organizzazione ha sperimentato una violazione di dati da una fonte esterna o un attacco ransomware DDoS negli ultimi 12 mesi. Questo evidenzia la necessità di andare oltre le misure basilari e implementare protocolli di sicurezza più avanzati e completi.



La sicurezza dei dati è ancora in cima alla lista delle preoccupazioni IT, menzionata dal **30%** dei decision maker. La percentuale che la indica come principale preoccupazione continua ad aumentare in modo significativo rispetto al **16%** del 2023 e al **23%** del 2024. Aggiungiamo il **13%** che identifica nella gestione della sicurezza dei dispositivi condivisi la principale criticità del 2024, e vediamo che quasi la metà (**43%**) considera problematiche relative alla sicurezza la priorità assoluta per i reparti IT.

Qual è attualmente la principale criticità per l'IT nella tua organizzazione?

Preoccupazioni sulla sicurezza dei dati o sulla gestione della sicurezza dei dispositivi condivisi					
	2025	2024		2025	2024
	43%	35%		51%	25%
	41%	43%		39%	33%
	53%	39%		31%	28%
	43%	32%		36%	-
	39%	43%		50%	-
	41%	24%		53%	39%

La sicurezza dei dati è la priorità assoluta per tutti i Paesi quest'anno, con alcune nazioni che registrano un incremento particolarmente marcato:

-  la **Francia** considera tematiche security come top priority per il **25%** delle organizzazioni sanitarie (dati 2024) e dal **51%** nel 2025
-  in **Canada** è salito dal **39%** lo scorso anno, e si attesta ora sul **53%**
-  in **Australia** è salito dal **39%** al **53%**
-  e in **Germania** dal **24%** al **41%**.

La natura dei dispositivi mobili richiede che siano gestiti da più utenti. Non sorprende, quindi, che la gestione della sicurezza dei dispositivi condivisi rimanga una delle principali preoccupazioni IT. A ciò si aggiunge la sfida rappresentata dai sistemi legacy, che rendono quasi impossibile la gestione remota di questi dispositivi, trasformando i device mobili in un'arma a doppio taglio.

Le caratteristiche MDM di base non sono più sufficienti per il mondo tecnologico moderno e tutti i dispositivi e sistemi complessi in atto. Le tradizionali funzionalità MDM hanno raggiunto i loro limiti. Oggi, la necessità di soluzioni tecnologiche avanzate è più critica che mai. I moderni strumenti EMM danno alle organizzazioni sanitarie una maggiore visibilità nell'intero ecosistema dei dispositivi, consentendo loro di monitorare meglio le operazioni, rafforzare la sicurezza dei dati e rispondere più rapidamente alle minacce emergenti.

PRIORITÀ ALLA SICUREZZA DEI DISPOSITIVI MOBILI: COPRIRE TUTTI GLI ASPETTI

Le organizzazioni stanno dando priorità alle misure per garantire la sicurezza dei dispositivi mobili. Alcune organizzazioni adottano un approccio human-centric, con il **45%** che forma il personale su minacce alla sicurezza, best practice e normative sulla protezione dei dati, mentre una percentuale simile limita l'accesso ai dati sensibili in base a ruoli e responsabilità. Eppure, solo un terzo (**33%**) dispone di un piano di risposta agli incidenti se qualcosa dovesse andare storto.

Effettuare aggiornamenti periodici è la misura di sicurezza più implementata, attuata dal **51%**. Una percentuale significativamente più alta tra coloro che non hanno subito incidenti alla sicurezza dei dati negli ultimi 12 mesi (**60%**) adotta questo approccio, rispetto al solo **49%** tra chi ha sperimentato un incidente). L'utilizzo di autenticazione multi-fattore è una priorità per il **44%**, mentre la crittografia per il **42%**.

È evidente che tutte le organizzazioni stanno attuando misure per proteggere i dispositivi mobili, ma poche stanno facendo tutto il possibile.



ESIGENZA DI STRATEGIE PIÙ EFFICACI PER LA GESTIONE DEI DISPOSITIVI MOBILI

La sicurezza non è l'unico ambito in cui le soluzioni MDM obsolete stanno mostrando carenze. Molte organizzazioni sanitarie riscontrano incoerenze nell'applicazione di queste soluzioni su vari dispositivi, il che complica il monitoraggio e il supporto dei dispositivi. Questa incoerenza spesso porta a sostituire inutilmente i dispositivi e a inefficienze nelle operazioni globali.

Quasi la metà (**47%**) dei decisori IT sostiene che una soluzione MDM sia fondamentale per risolvere i problemi della loro organizzazione da remoto e il **45%** dichiara che sia essenziale per il monitoraggio dei dispositivi; tuttavia, il **38%** delle organizzazioni non è in grado di distribuire e gestire facilmente nuovi dispositivi e stampanti a causa dei sistemi legacy e il **38%** non è in grado di supportare i dispositivi da remoto o di ottenere informazioni dettagliate sui problemi dei dispositivi per questo stesso motivo.

La ricerca evidenzia la necessità per le organizzazioni sanitarie di adottare soluzioni EMM solide e centralizzate che garantiscano la sicurezza e la conformità dei dispositivi. Queste soluzioni dovrebbero anche supportare la risoluzione dei problemi da remoto, semplificare la configurazione e fornire informazioni azionabili.

Gli strumenti avanzati che forniscono analisi e intelligenza operativa su tutti i dispositivi consentono ai team IT di identificare in modo proattivo i problemi di performance dei dispositivi. Può anche monitorare le tendenze di utilizzo, fornendo alle organizzazioni approfondimenti utili a prendere decisioni informate. Questo approccio riduce i tempi di inattività, riduce al minimo le inefficienze e migliora la qualità complessiva dell'assistenza ai pazienti.

TECNOLOGIA MEDICA MONOUSO

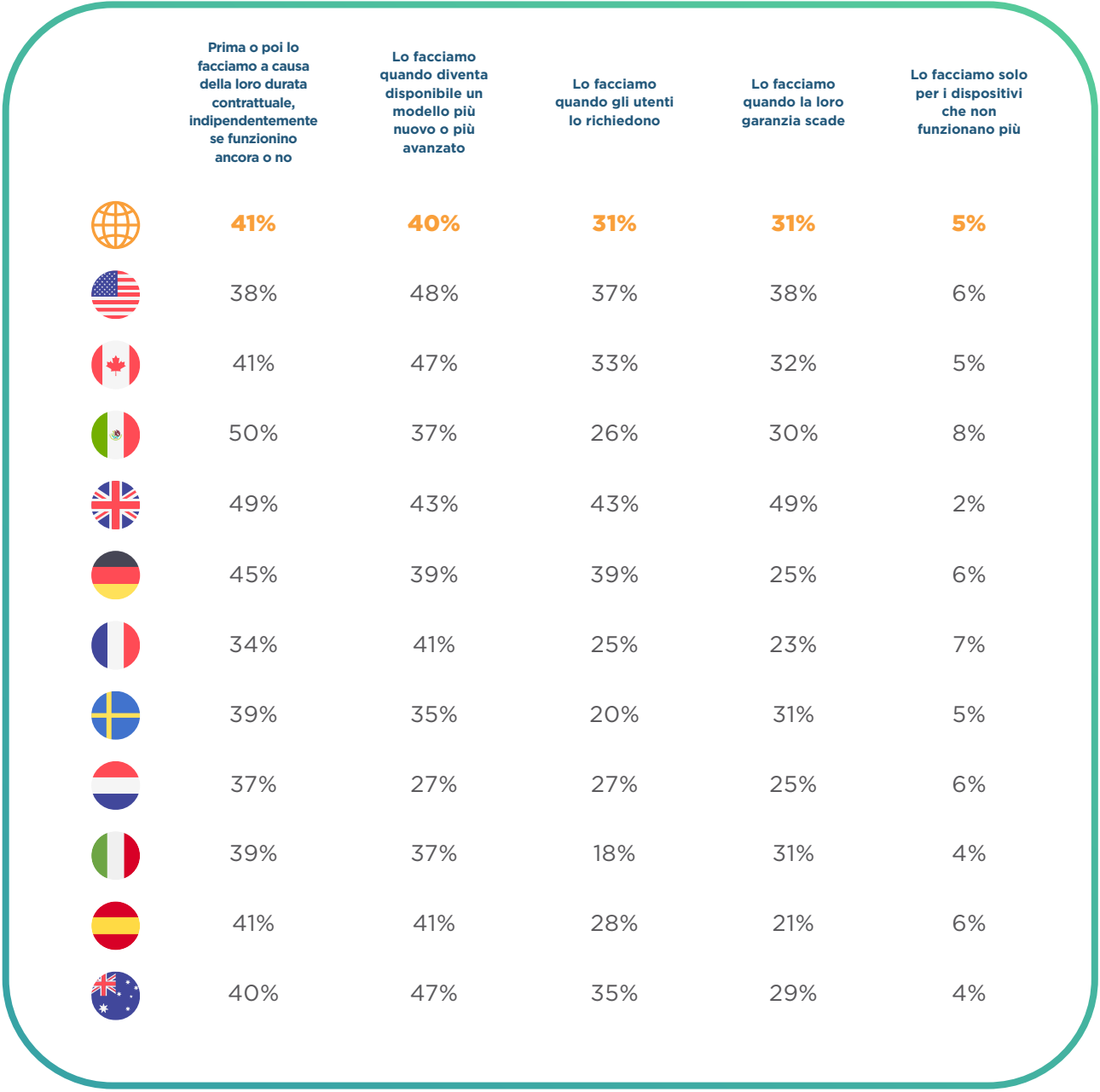
Le preoccupazioni non si esauriscono nel momento in cui un dispositivo mobile non è più in uso; anzi, spesso aumentano. Infatti, l'**81%** dei decisori IT ha espresso preoccupazioni riguardo alla sicurezza dei dati dei pazienti durante lo smaltimento dei dispositivi.

Le organizzazioni sanitarie gestiscono enormi volumi di dati sensibili e senza processi di smaltimento standardizzati i dispositivi non più utilizzati presentano gravi rischi di violazione dei dati e di non conformità normativa. Mentre la maggior parte delle organizzazioni prende misure per proteggere i dati durante lo smaltimento dei dispositivi, le incongruenze rimangono elevate. Quest'anno, otto decisori informatici su dieci hanno espresso ancora preoccupazione.

Gli aggiornamenti frequenti complicano il problema. Il **31%** delle organizzazioni sostituisce i dispositivi su richiesta dell'utente; il **40%** lo fa quando sono disponibili nuovi modelli; il **41%** li sostituisce in base alle condizioni contrattuali e il **31%** alla scadenza della garanzia. Ciò comporta preoccupazioni importanti in materia di sicurezza e sostenibilità.

Per ridurre i rischi, le organizzazioni devono implementare protocolli standardizzati, tra cui la cancellazione remota dei dati e una solida gestione del ciclo di vita per garantire un adeguato monitoraggio e smaltimento. Il personale dovrebbe anche ricevere una formazione periodica sulle pratiche di smaltimento sicuro. Dando priorità a processi sicuri e sostenibili, le organizzazioni sanitarie possono proteggere meglio i dati dei pazienti e soddisfare gli standard di conformità.

Qual è la politica della tua organizzazione riguardo all'aggiornamento/rinnovo/sostituzione dei dispositivi come quelli sopra menzionati, ad esempio smartphone, tablet, dispositivi rugged, ecc.?



Gli Stati Uniti, il Canada e l'Australia hanno la percentuale più alta di sostituzione dei dispositivi quando una nuova versione diventa disponibile. Tuttavia, è importante notare che questa è una tendenza comune a livello globale. È fondamentale trovare un equilibrio tra sostenibilità e performance dei dispositivi. Se i dispositivi vengono smaltiti solo quando smettono di funzionare, i team IT passeranno ancora più tempo a risolvere problemi minori.

GESTIONE DELLO STATO DELLA BATTERIA: PREVENIRE È MEGLIO CHE CURARE

Un monitoraggio inefficiente della salute della batteria può essere un ulteriore motivo per i guasti imprevisti dei dispositivi nel settore sanitario. Costi più elevati dovuti alle sostituzioni premature dei dispositivi sono comuni e comportano vincoli finanziari e preoccupazioni ambientali in materia di smaltimento dei rifiuti elettronici. Il **97%** delle organizzazioni monitora attivamente la salute della batteria dei dispositivi, ma solo un terzo (**31%**) sostiene di controllarla solo quando sorgono problemi.

Per il **41%**, la politica prevede di sostituire le batterie a cadenza fissa, indipendentemente dalla salute della batteria. Fortunatamente, la metà effettua controlli manuali regolari, il **44%** utilizza il monitoraggio automatico della salute della batteria e il **41%** dispone di un sistema di manutenzione predittiva.

In definitiva, i risultati suggeriscono che mentre i dispositivi mobili offrono vantaggi innegabili, la loro gestione deve essere ottimizzata implementando soluzioni EMM per stabilire le migliori pratiche per il tracciamento dei dispositivi, il monitoraggio della salute delle batterie e strategie di sostituzione sostenibili. Tali misure permetterebbero non solo di semplificare le operazioni quotidiane, ma anche di aprire la strada a iniziative informatiche più strategiche in tutto il panorama sanitario.





CONCLUSIONE

Il settore sanitario sta progredendo rapidamente nel suo percorso di trasformazione digitale, eppure la strada rimane complessa. Nonostante l'utilizzo diffuso di IoT e dispositivi di telemedicina, i sistemi legacy presentano problemi quali una raccolta dei dati incompleta e frequenti interruzioni tecniche, che impediscono ai team IT di sfruttare i vantaggi del loro percorso di trasformazione digitale.

Allo stesso tempo, questioni legate alla sicurezza si sono rivelate la principale preoccupazione per il **43%** dei decisori IT; le cause sono minacce che spaziano dalla gestione di dispositivi condivisi all'aumento delle violazioni dei dati. Mentre le perdite di dati dei dipendenti pianificate sono leggermente diminuite, le perdite accidentali e i sofisticati attacchi esterni continuano a esporre le vulnerabilità. Quasi la metà dei leader IT riconosce i sistemi legacy come causa principale che rende le reti vulnerabili agli attacchi e sottolinea l'urgente necessità di modernizzare le tecnologie di base. Sembra che la questione riguardi meno la tecnologia emergente stessa e più i sistemi che la supportano.

L'adozione dell'IA è aumentata a livello globale e quest'anno viene utilizzata da un terzo di organizzazioni in più, soprattutto nel Regno Unito e in Australia. L'IA viene integrata nell'analisi dei dati medici, nella pianificazione dei trattamenti, nell'assistenza personalizzata ai pazienti e molto altro. Un'ancora di salvezza per il settore sanitario ormai sovraccarico, ma il cui utilizzo deve essere monitorato e messo in sicurezza.

Inoltre, la gestione dei dispositivi mobili si sta rivelando un notevole spreco di risorse IT e la moltitudine di dispositivi in uso ne complica il monitoraggio efficace e la gestione remota. L'inadeguatezza delle soluzioni MDM esistenti e politiche di sostituzione disomogenee aggravano ulteriormente la situazione, acuendo sia i rischi per la sicurezza che le problematiche di sostenibilità.

In definitiva, per realizzare una vera trasformazione digitale in ambito sanitario, le organizzazioni devono fare un passo indietro e considerare il quadro generale. Ciò che serve è una strategia in grado di coniugare la continua diffusione su larga scala di tecnologie innovative con investimenti mirati alla modernizzazione e integrazione delle infrastrutture IT, unitamente all'adozione di soluzioni EMM realmente adeguate alle specifiche esigenze del settore sanitario. Questo approccio equilibrato consentirà alle organizzazioni di proteggere i dati, semplificare l'uso dei dispositivi mobili e, in ultima analisi, migliorare l'assistenza ai pazienti.

CHI SIAMO

SOTI è un'azienda innovatrice e un leader di settore riconosciuto che semplifica la complessità delle soluzioni di mobilità aziendale rendendole più intelligenti, veloci e affidabili. Grazie al suo [innovativo portfolio di soluzioni](#), le organizzazioni possono affidarsi a SOTI per migliorare e per semplificare le proprie operazioni in mobilità, per massimizzare il ritorno sugli investimenti e per ridurre i tempi di inattività dei dispositivi. A livello globale, con oltre 17.000 clienti aziendali, SOTI ha dimostrato di essere il principale fornitore di piattaforme mobili per la gestione, la protezione e il supporto dei dispositivi fondamentali per le aziende. Grazie al supporto su scala internazionale di SOTI, le aziende possono portare la mobilità verso possibilità infinite.



PER SAPERNE DI PIÙ:

Per ulteriori informazioni su come SOTI può preparare la tua azienda al successo, **clicca qui**.

Per maggiori informazioni sulla piattaforma SOTI ONE, **clicca qui**.

Per scoprire come SOTI può aiutarti con i tuoi investimenti mobili, contattaci all'indirizzo **sales@soti.net**.

SOTI è un innovatore comprovato e leader del settore per la semplificazione delle soluzioni di mobilità aziendale rendendole più intelligenti, più rapide e più affidabili. SOTI aiuta le imprese di tutto il mondo a sfruttare le infinite possibilità della mobilità.

it.soti.net

© 2025, SOTI Inc. Tutti i diritti riservati. Tutti i nomi dei prodotti e delle aziende sono marchi registrati o marchi registrati dei rispettivi proprietari. L'utilizzo di questi marchi non implica alcuna affiliazione con SOTI o sponsorizzazione da parte del titolare del marchio. Offerte soggette a modifica o cancellazione senza preavviso. SOTI si riserva il diritto di modificare prodotti, servizi o prezzi in qualsiasi momento. Le informazioni sono fornite "COME SONO" senza alcuna garanzia. I prodotti e i servizi sono soggetti alle condizioni applicabili.

052725