

Policy Brief

PANDEMIA DIGITALE QUANDO I SISTEMI DIGITALI FALLISCONO **Impatti sistemici sulla salute pubblica, sugli ospedali e sulla resilienza sanitaria**

Analisi del report UNDRR–ITU “When Digital Systems Fail”

Maggio 2026

PANDEMIA DIGITALE

QUANDO I SISTEMI DIGITALI FALLISCONO

Impatti sistemici sulla salute pubblica, sugli ospedali e sulla resilienza sanitaria

Analisi del report UNDRR–ITU “*When Digital Systems Fail*”

Federico Serra

Segretario Generale dell’Osservatorio sulla salute bene comune dell’Università cattolica Sacro Cuore

Presidente Health City Institute

Direttore Generale del Planetary Health Inner Circle

Vicepresidente Health Ecosystem Institute

Senior member Royal institute of international affairs - Chatham House

Capo segreteria tecnica Intergruppo parlamentare sulla sanità digitale e sulle terapie digitali

Consulente parlamentare

Claudio Cricelli

Presidente emerito vicario della Società Italiana di medicina generale e delle cure primarie

Presidente Health Ecosystem Institute

Presidente MG LAB

Walter Ricciardi

Direttore dell’Osservatorio sulla salute bene comune dell’Università cattolica Sacro Cuore

Presidente del Planetary Health Inner Circle

Professore Ordinario di Igiene Università Cattolica Sacro Cuore

EXECUTIVE SUMMARY

La trasformazione digitale della sanità rappresenta una delle più profonde rivoluzioni organizzative, tecnologiche e culturali che i sistemi sanitari abbiano conosciuto nel corso della loro storia recente. Negli ultimi anni, ospedali, servizi territoriali, centrali operative, laboratori, sistemi di emergenza e piattaforme di sanità pubblica hanno progressivamente integrato tecnologie digitali sempre più avanzate, modificando radicalmente il modo in cui vengono erogate cure, gestite informazioni cliniche e coordinate le attività assistenziali.

Cartelle cliniche elettroniche, telemedicina, piattaforme cloud, interoperabilità dei dati sanitari, sistemi di monitoraggio remoto, intelligenza artificiale applicata alla diagnostica, connected care e strumenti digitali di sorveglianza epidemiologica stanno contribuendo a rendere la sanità più veloce, integrata e predittiva. Questa evoluzione ha migliorato la continuità assistenziale, la capacità di monitorare i pazienti cronici, l’appropriatezza clinica, l’accessibilità ai servizi e la

governance sanitaria, aprendo prospettive straordinarie per la medicina personalizzata e la gestione delle grandi transizioni demografiche ed epidemiologiche del XXI secolo.

Tuttavia, proprio mentre la digitalizzazione viene considerata una leva fondamentale di innovazione e resilienza, il report internazionale *When Digital Systems Fail*, pubblicato da International Telecommunication Union (ITU), United Nations Office for Disaster Risk Reduction (UNDRR) e Sciences Po, richiama l'attenzione su una vulnerabilità emergente ancora largamente sottovalutata nel dibattito pubblico e nelle strategie di preparedness sanitaria: la crescente dipendenza delle società contemporanee da infrastrutture digitali profondamente interconnesse sta creando nuove forme di fragilità sistemica capaci di compromettere simultaneamente salute pubblica, servizi sanitari, protezione civile, economia, mobilità e governance democratica.

Il documento introduce il concetto di “systemic digital risk”, ovvero il rischio che guasti, malfunzionamenti o interruzioni delle infrastrutture digitali critiche possano propagarsi rapidamente attraverso sistemi interdipendenti, generando effetti a cascata su scala urbana, nazionale e globale. La caratteristica più preoccupante di questi eventi è che spesso non si manifestano con segnali immediatamente visibili: non vi sono necessariamente esplosioni, crolli o danni fisici evidenti, ma sistemi che improvvisamente smettono di funzionare, dati che diventano inaccessibili, reti che collassano e servizi essenziali che si interrompono simultaneamente.

A differenza delle tradizionali minacce cyber, il report concentra l'attenzione soprattutto sulle interruzioni non intenzionali e sulle vulnerabilità infrastrutturali sistemiche. Tra i principali fattori di rischio vengono citati eventi climatici estremi, blackout energetici, sovraccarichi dei data center, guasti satellitari, rotture dei cavi sottomarini, tempeste geomagnetiche e crisi multi-settoriali capaci di compromettere contemporaneamente energia, telecomunicazioni, cloud computing e reti digitali. Fig. 1

LA POSSIBILE PANDEMIA DIGITALE

Quando i sistemi digitali falliscono, il mondo si ferma.

Una pandemia digitale è un'interruzione diffusa e simultanea di infrastrutture digitali interconnesse che compromette servizi essenziali in più settori e Paesi, con effetti a cascata su società, economie e salute.

FINO ALL' 89%
DELLE INTERRUZIONI DIGITALI CAUSATE DA EVENTI NATURALI È DOVUTO A EFFETTI A CASCATA

Le persone colpite possono essere fino a **10 volte** superiori a quelle direttamente esposte.



EFFETTI A CASCATA UN COLLASSO CHE SI PROPAGA



Secondo il report, fino all'89% delle interruzioni digitali associate a eventi naturali non deriva dal danno iniziale, ma dagli effetti secondari a cascata che si propagano tra sistemi interdipendenti. Inoltre, il numero di persone colpite può essere fino a dieci volte superiore rispetto alla popolazione direttamente esposta all'evento originario. Questo significa che una crisi apparentemente limitata — come il surriscaldamento di un data center o un'interruzione energetica regionale — può rapidamente trasformarsi in un'emergenza sanitaria diffusa, capace di compromettere ospedali, reti territoriali, sistemi di emergenza e continuità assistenziale.

Per i sistemi sanitari, questo scenario apre una nuova frontiera della sicurezza sanitaria globale. Ospedali, centrali operative del 118, piattaforme regionali, sistemi vaccinali, telemedicina, farmacie, supply chain farmaceutiche e reti territoriali dipendono oggi da un'infrastruttura invisibile composta da energia elettrica continua, reti internet, cloud computing, telecomunicazioni, data center, sincronizzazione satellitare e piattaforme interoperabili. La sanità contemporanea è quindi sempre più efficiente, ma anche sempre più esposta a vulnerabilità che spesso sfuggono ai tradizionali modelli di gestione del rischio.

Il report dimostra come il fallimento di una singola infrastruttura critica possa compromettere rapidamente l'accesso ai dati clinici, la gestione delle emergenze, il coordinamento delle ambulanze, la distribuzione dei farmaci, la continuità assistenziale e la capacità di risposta delle autorità sanitarie. In uno degli scenari descritti, un'ondata di calore estrema provoca il sovraccarico energetico dei sistemi di raffreddamento dei data center, rendendo inaccessibili le piattaforme di scambio dati sanitari e rallentando il coordinamento delle emergenze ospedaliere.

Particolarmente rilevante è l'identificazione di quattro vulnerabilità strutturali emergenti. La prima riguarda la crescente concentrazione delle infrastrutture digitali sanitarie, sempre più dipendenti da pochi grandi cloud provider e da data center altamente centralizzati. La seconda riguarda la fragilità climatica dei sistemi energetici e delle infrastrutture digitali, sempre più esposte a heatwaves, alluvioni e blackout. La terza è rappresentata dalla dipendenza invisibile dei servizi sanitari da infrastrutture esterne spesso non governate direttamente dal settore salute. La quarta riguarda la progressiva perdita delle capacità analogiche di emergenza: molti operatori sanitari oggi lavorano esclusivamente attraverso piattaforme digitali e non sono più addestrati a gestire procedure manuali o offline.

Le implicazioni di queste vulnerabilità risultano particolarmente rilevanti per i sistemi sanitari urbani e per le smart cities, dove la concentrazione di ospedali ad alta intensità tecnologica, infrastrutture critiche metropolitane, reti energetiche complesse e piattaforme digitali rende le città contemporanee particolarmente esposte ai rischi sistemici. In questo contesto, la resilienza sanitaria non può più essere separata dalla resilienza climatica, infrastrutturale e digitale.

Per questo il report suggerisce la necessità di sviluppare un nuovo paradigma di “digital health resilience”, capace di integrare resilienza climatica, sicurezza infrastrutturale, preparedness sanitaria, governance digitale, urban health e continuità operativa. Non si tratta soltanto di proteggere i sistemi informatici, ma di ripensare la capacità stessa dei sistemi sanitari di continuare a funzionare durante crisi infrastrutturali prolungate e multi-settoriali.

La vera sfida del prossimo decennio non sarà quindi soltanto digitalizzare la sanità, ma costruire sistemi sanitari capaci di restare operativi, coordinati e accessibili anche quando le infrastrutture digitali su cui si fondano diventano improvvisamente fragili o indisponibili.

INTRODUZIONE

La nuova vulnerabilità invisibile dei sistemi sanitari

Negli ultimi vent'anni i sistemi sanitari di tutto il mondo hanno attraversato una trasformazione tecnologica senza precedenti. La progressiva digitalizzazione della sanità ha modificato profondamente il modo in cui vengono organizzati i servizi, gestiti i percorsi clinici e coordinate le attività assistenziali, contribuendo a rendere le cure più rapide, integrate ed efficienti.

L'introduzione delle cartelle cliniche elettroniche, delle piattaforme di telemedicina, dei sistemi di monitoraggio remoto, dell'interoperabilità dei dati sanitari e delle tecnologie di intelligenza artificiale ha consentito di migliorare significativamente la continuità assistenziale, ridurre gli errori clinici, velocizzare l'accesso alle informazioni sanitarie e rafforzare le capacità di monitoraggio epidemiologico in tempo reale. Allo stesso tempo, l'evoluzione delle infrastrutture digitali ha favorito una maggiore integrazione tra ospedali, medicina territoriale, servizi di emergenza e sistemi di sanità pubblica, rendendo possibile una governance sanitaria sempre più basata sull'analisi dei dati e sulla condivisione delle informazioni.

Questa accelerazione tecnologica ha rappresentato uno dei pilastri dell'innovazione sanitaria contemporanea, contribuendo a costruire sistemi più connessi, predittivi e capaci di affrontare sfide complesse come l'invecchiamento della popolazione, la gestione delle cronicità e le emergenze pandemiche. Tuttavia, parallelamente ai benefici della digitalizzazione, si è sviluppata una crescente dipendenza strutturale da infrastrutture digitali altamente interconnesse e spesso invisibili ai tradizionali modelli di gestione del rischio.

Il report *When Digital Systems Fail*, pubblicato da International Telecommunication Union (ITU), United Nations Office for Disaster Risk Reduction (UNDRR) e Sciences Po, evidenzia come questa dipendenza stia progressivamente trasformando la sanità in uno dei settori più vulnerabili ai collassi digitali sistemici.

Il problema centrale non riguarda più soltanto il rischio di cyberattacchi, ormai relativamente consolidato nelle strategie di cybersecurity sanitaria, ma soprattutto la possibilità che crisi infrastrutturali complesse e multi-settoriali possano compromettere contemporaneamente energia, telecomunicazioni, cloud computing, data center e reti digitali da cui dipendono ospedali e servizi sanitari.

Queste crisi possono avere origine da eventi apparentemente molto diversi tra loro: ondate di calore estreme che sovraccaricano i sistemi energetici e i data center, blackout elettrici prolungati, guasti satellitari che compromettono le comunicazioni e la sincronizzazione delle reti, rotture dei cavi sottomarini che interrompono la connettività internazionale, eventi climatici estremi, stress termici sulle infrastrutture digitali o sovraccarichi improvvisi delle reti di telecomunicazione.

La caratteristica più insidiosa di questi eventi è la loro iniziale invisibilità. A differenza dei disastri tradizionali, non sempre si manifestano con immagini immediate di distruzione fisica o con danni chiaramente identificabili. Le città continuano apparentemente a funzionare, gli edifici restano in piedi, le strade sono percorribili, ma improvvisamente sistemi fondamentali smettono di operare: le piattaforme cliniche diventano inaccessibili, i dati sanitari non sono più disponibili, le comunicazioni tra ospedali si interrompono, le centrali operative rallentano, i sistemi di emergenza perdono capacità di coordinamento.

È proprio questa invisibilità iniziale a rendere il rischio digitale sistemico particolarmente difficile da riconoscere e gestire. Spesso le organizzazioni coinvolte percepiscono il problema come un semplice malfunzionamento locale o temporaneo, senza comprendere immediatamente che il guasto è parte di una crisi molto più ampia e interconnessa. Nel frattempo, però, gli effetti si propagano rapidamente attraverso sistemi tra loro dipendenti, trasformando una criticità tecnologica in una vera emergenza sanitaria.

Il report sottolinea come le moderne infrastrutture sanitarie dipendano oggi da una complessa architettura invisibile fatta di energia elettrica continua, cloud computing, telecomunicazioni, data center, sincronizzazione satellitare e reti interoperabili. Quando una di queste componenti viene meno, anche per poche ore, le conseguenze possono rapidamente compromettere l'accesso alle cure, la gestione delle emergenze, il coordinamento delle ambulanze, la distribuzione dei farmaci e la continuità assistenziale. Fig.2



La vulnerabilità dei sistemi sanitari contemporanei nasce dunque proprio dal paradosso della trasformazione digitale: più la sanità diventa efficiente, connessa e tecnologicamente avanzata, più aumenta la sua esposizione a rischi sistemici legati al funzionamento delle infrastrutture digitali che la sostengono.

Per questo motivo, la resilienza sanitaria del XXI secolo non può più essere considerata esclusivamente una questione clinica o ospedaliera. Essa dipende sempre di più dalla capacità delle società di costruire infrastrutture digitali resilienti, sistemi energetici affidabili, reti di emergenza interoperabili e modelli di governance capaci di affrontare crisi simultanee, multi-settoriali e prolungate.

SANITÀ DIGITALE E INTERDIPENDENZE INVISIBILI

Uno degli aspetti più innovativi e allo stesso tempo più preoccupanti evidenziati dal report *When Digital Systems Fail* riguarda il concetto di:

“hidden interdependencies”

ovvero le interdipendenze nascoste che legano tra loro infrastrutture digitali, sistemi energetici, telecomunicazioni, reti cloud e servizi sanitari.

Il documento sottolinea come le moderne piattaforme sanitarie non funzionino più come sistemi autonomi e indipendenti, ma come elementi inseriti all'interno di una rete estremamente complessa di infrastrutture digitali interconnesse. Molto spesso queste connessioni rimangono poco visibili persino agli stessi decisori sanitari, ai manager ospedalieri o alle autorità pubbliche che governano i servizi di salute.

Un ospedale contemporaneo, infatti, non dipende soltanto dalle proprie apparecchiature cliniche o dalla disponibilità di personale sanitario, ma da una lunga catena di infrastrutture esterne che operano simultaneamente e in modo coordinato. Dietro il funzionamento quotidiano di un pronto soccorso, di una terapia intensiva o di una centrale operativa del 118 esiste un ecosistema invisibile composto da cloud provider internazionali, data center geograficamente concentrati, reti energetiche, telecomunicazioni mobili, sistemi satellitari GPS, piattaforme regionali interoperabili, sistemi di raffreddamento e infrastrutture di backup spesso limitate.

La crescente digitalizzazione della sanità ha certamente aumentato efficienza e capacità organizzativa, ma ha anche creato nuove dipendenze sistemiche che rendono i servizi sanitari vulnerabili a crisi che possono originarsi molto lontano dagli ospedali stessi. Un problema energetico in un data center, un'interruzione delle telecomunicazioni, una crisi climatica o un guasto satellitare possono oggi produrre conseguenze immediate sulla capacità di cura, di coordinamento delle emergenze e di accesso ai dati clinici.

Il report evidenzia come il rischio principale non risieda soltanto nel singolo guasto, ma nella capacità di questi malfunzionamenti di propagarsi rapidamente tra sistemi interdipendenti, generando effetti a cascata difficili da prevedere e ancora più difficili da gestire. In infrastrutture fortemente connesse, infatti, la perdita di una singola componente può compromettere progressivamente anche tutte le altre reti che dipendono da essa.

Uno degli scenari più significativi descritti nel documento riguarda un'ondata di calore estrema che colpisce una grande area urbana altamente digitalizzata. Inizialmente il fenomeno produce uno

stress energetico diffuso dovuto all'aumento dei consumi elettrici e alla difficoltà dei sistemi di raffreddamento di mantenere operative le infrastrutture critiche. Progressivamente, il surriscaldamento compromette il funzionamento di alcuni data center, causando il rallentamento delle reti cloud e l'interruzione della piattaforma nazionale di scambio dati sanitari.

Le conseguenze diventano rapidamente sanitarie. Gli ospedali non riescono più ad accedere tempestivamente alle informazioni cliniche, le centrali operative incontrano difficoltà nel coordinamento delle ambulanze, le reti di emergenza rallentano e i tempi di risposta aumentano significativamente. Nel caso descritto dal report, il tempo di intervento dei servizi di emergenza cresce del 34%, con inevitabili ripercussioni sulla gestione dei pazienti più critici.

Questo scenario dimostra in maniera molto chiara come il rischio sanitario contemporaneo non sia più confinato esclusivamente all'interno delle strutture ospedaliere. Oggi la capacità di garantire cure, coordinare le emergenze e mantenere la continuità assistenziale dipende sempre di più da infrastrutture digitali esterne che spesso il settore sanitario non controlla direttamente.

La salute pubblica è quindi diventata profondamente interdipendente con:

- infrastrutture energetiche;
- sistemi cloud;
- telecomunicazioni;
- reti satellitari;
- piattaforme digitali globali;
- supply chain tecnologiche.

Questa nuova realtà modifica radicalmente il concetto stesso di resilienza sanitaria. Non basta più garantire posti letto, personale e dispositivi medici: occorre assicurare anche la resilienza delle infrastrutture invisibili che sostengono il funzionamento dell'intero ecosistema sanitario digitale.

Il report evidenzia inoltre un ulteriore elemento critico: molte di queste dipendenze non vengono ancora considerate nei tradizionali modelli di risk assessment sanitario. In molti casi, le autorità sanitarie non conoscono esattamente:

- dove siano fisicamente ospitati i dati clinici;
- quali data center supportino i sistemi regionali;
- quanto tempo possano resistere i sistemi di backup;
- quali servizi dipendano da infrastrutture satellitari;
- o quali conseguenze potrebbe produrre il collasso simultaneo di energia, cloud e telecomunicazioni.

È proprio questa invisibilità sistemica a rendere il rischio digitale particolarmente pericoloso. Le crisi non si manifestano più soltanto attraverso danni fisici immediatamente evidenti, ma attraverso il progressivo deterioramento delle capacità operative di sistemi interconnessi che smettono improvvisamente di comunicare tra loro.

Per questo motivo il report suggerisce la necessità di sviluppare nuove strategie di “digital health resilience”, capaci di integrare:

- resilienza energetica;
- preparedness climatica;
- continuità digitale;
- governance multisettoriale;
- sistemi di backup;
- capacità analogiche di emergenza;
- pianificazione urbana resiliente.

La sanità del XXI secolo non dovrà essere soltanto digitale e interconnessa, ma anche capace di continuare a funzionare quando le infrastrutture digitali su cui si fonda diventano improvvisamente fragili o indisponibili.

IL CAMBIAMENTO CLIMATICO COME MOLTIPLICATORE DEL RISCHIO SANITARIO DIGITALE

Uno degli aspetti più innovativi e strategicamente rilevanti del report *When Digital Systems Fail* riguarda il rapporto sempre più stretto tra cambiamento climatico, infrastrutture digitali e salute pubblica. Il documento evidenzia come la crisi climatica non rappresenti più soltanto una minaccia ambientale o sanitaria diretta, ma stia progressivamente diventando anche un potente fattore di destabilizzazione delle infrastrutture digitali su cui si fondano i sistemi sanitari contemporanei.

Negli ultimi anni il dibattito internazionale si è concentrato soprattutto sugli effetti sanitari immediati del cambiamento climatico — aumento della mortalità durante le ondate di calore, diffusione di malattie infettive, eventi estremi, impatti sulla qualità dell’aria — ma il report introduce un ulteriore livello di vulnerabilità ancora poco esplorato: quello delle “climate-induced digital disruptions”, ovvero delle interruzioni digitali provocate direttamente o indirettamente dagli eventi climatici estremi.

Le heatwaves descritte nel documento rappresentano un esempio concreto e particolarmente realistico di questo fenomeno. Le temperature estreme, infatti, non colpiscono soltanto la salute delle persone, ma mettono sotto pressione anche le infrastrutture energetiche e digitali che consentono il funzionamento quotidiano degli ospedali, delle piattaforme sanitarie e dei sistemi di emergenza. Durante le ondate di calore aumenta drasticamente la domanda energetica per il raffreddamento degli edifici e dei data center; contemporaneamente, però, il calore riduce l’efficienza delle reti elettriche e compromette la capacità dei sistemi di raffreddamento di mantenere operative le infrastrutture digitali critiche.

Il report descrive uno scenario in cui il surriscaldamento progressivo dei data center porta al rallentamento delle piattaforme cloud e all’interruzione dei sistemi di scambio dati sanitari. Le conseguenze diventano rapidamente sanitarie: ospedali che non riescono ad accedere alle cartelle

cliniche, ambulanze rallentate, sistemi di emergenza congestionati, difficoltà nel coordinamento territoriale e incremento significativo dei tempi di risposta.

Questo scenario evidenzia come il cambiamento climatico stia diventando un vero e proprio moltiplicatore di rischio per la sanità digitale. Con l'aumento progressivo delle temperature medie globali, delle ondate di calore, delle alluvioni, degli incendi e dei fenomeni meteorologici estremi, cresce inevitabilmente anche la probabilità che infrastrutture digitali essenziali subiscano interruzioni o malfunzionamenti prolungati.

Le città contemporanee risultano particolarmente vulnerabili a questi fenomeni perché concentrano contemporaneamente:

- ospedali ad alta intensità tecnologica;
- infrastrutture digitali centralizzate;
- reti energetiche complesse;
- sistemi di mobilità intelligente;
- grandi piattaforme cloud;
- data center energivori;
- servizi di emergenza digitalizzati.

Le smart cities, costruite per essere efficienti e connesse, rischiano quindi di diventare estremamente fragili durante eventi climatici estremi se non adeguatamente progettate in ottica di resilienza sistemica.

Per questo motivo il report suggerisce di superare la tradizionale separazione tra politiche climatiche e politiche sanitarie. La resilienza climatica e la resilienza sanitaria digitale devono essere considerate due dimensioni inseparabili della sicurezza urbana contemporanea. Pianificare città resilienti significa oggi non soltanto proteggere ospedali e popolazioni vulnerabili dal caldo o dalle alluvioni, ma anche garantire la continuità energetica, la protezione dei data center, la ridondanza delle reti digitali e la capacità dei sistemi sanitari di continuare a funzionare durante crisi climatiche prolungate.

DATA CENTER, CLOUD E CONCENTRAZIONE DEL RISCHIO SANITARIO

Il report identifica i data center come uno dei principali “blind spot” della governance contemporanea del rischio digitale. Sebbene siano ormai diventati il cuore invisibile dell'economia digitale e dei sistemi sanitari moderni, i data center rimangono spesso poco considerati nei modelli tradizionali di preparedness sanitaria e di gestione delle emergenze.

Negli ultimi anni molti sistemi sanitari nazionali e regionali hanno accelerato la migrazione verso infrastrutture cloud sempre più centralizzate. Cartelle cliniche elettroniche, piattaforme di interoperabilità, sistemi di telemedicina, intelligenza artificiale applicata alla diagnostica, piattaforme di prenotazione e database sanitari vengono sempre più frequentemente ospitati

all'interno di hyperscale cloud infrastructures gestite da un numero limitato di grandi provider globali.

Questa trasformazione ha indubbiamente prodotto enormi vantaggi in termini di:

- efficienza;
- scalabilità;
- interoperabilità;
- rapidità di accesso ai dati;
- integrazione dei servizi;
- sviluppo dell'AI healthcare.

Tuttavia, il report sottolinea come questa centralizzazione stia producendo una nuova forma di vulnerabilità sistemica: la concentrazione geografica del rischio.

Molte piattaforme sanitarie critiche dipendono infatti da pochi grandi data center collocati in aree specifiche. Ciò significa che un singolo evento climatico, energetico o infrastrutturale può compromettere contemporaneamente ospedali, laboratori, farmacie, servizi territoriali, piattaforme regionali e sistemi di emergenza.

Il rischio principale non deriva soltanto dalla possibilità di un guasto tecnico, ma dal fatto che la crescente centralizzazione crea veri e propri:

“single points of failure” sistemici

Un blackout energetico, un'alluvione, un incendio, un'ondata di calore o un problema di raffreddamento possono interrompere simultaneamente l'accesso ai dati clinici e compromettere l'intero ecosistema sanitario di una regione o di un Paese.

Il report evidenzia inoltre come molte autorità sanitarie non abbiano piena consapevolezza delle proprie dipendenze infrastrutturali. Spesso i decisori sanitari non conoscono:

- dove siano fisicamente ospitati i dati;
- quali data center sostengano le piattaforme regionali;
- quanto possano durare i sistemi di backup;
- o quali infrastrutture energetiche supportino le reti cloud utilizzate dagli ospedali.

Questa opacità rende estremamente difficile valutare la reale resilienza dei sistemi sanitari digitali.

La sfida del prossimo decennio sarà quindi costruire modelli di sanità digitale non soltanto efficienti e interoperabili, ma anche decentralizzati, resilienti e capaci di evitare concentrazioni eccessive di vulnerabilità critica.

Tempeste solari e sicurezza sanitaria globale

Tra gli scenari più allarmanti descritti dal report vi è quello relativo a un possibile evento geomagnetico estremo simile al cosiddetto “Carrington Event”, la grande tempesta solare che nel 1859 colpì la Terra causando gravi danni ai sistemi telegrafici dell’epoca.

Oggi, però, una tempesta geomagnetica di simile intensità avrebbe conseguenze immensamente più gravi. Le società contemporanee dipendono infatti in modo capillare da satelliti, telecomunicazioni, reti elettriche, sistemi GPS e infrastrutture digitali interconnesse.

Secondo il report, un evento geomagnetico estremo potrebbe provocare:

- blackout continentali;
- perdita di connettività globale;
- guasti satellitari;
- interruzione dei sistemi GPS;
- collasso delle telecomunicazioni;
- danni ai trasformatori elettrici ad alta tensione.

Per il settore sanitario questo scenario aprirebbe una crisi senza precedenti. Gli ospedali potrebbero perdere accesso alle piattaforme cliniche digitali, i sistemi di emergenza potrebbero smettere di comunicare, le supply chain farmaceutiche verrebbero interrotte e la telemedicina diverrebbe inutilizzabile. Anche la sorveglianza epidemiologica e il monitoraggio dei pazienti cronici risulterebbero gravemente compromessi.

Il report sottolinea inoltre un elemento particolarmente critico: la sostituzione dei grandi trasformatori elettrici danneggiati potrebbe richiedere mesi o addirittura anni. Questo significa che alcune crisi digitali potrebbero trasformarsi in emergenze sanitarie prolungate, mettendo sotto pressione i sistemi sanitari ben oltre le capacità dei tradizionali piani di continuità operativa.

Lo scenario evidenzia quindi come la sicurezza sanitaria globale sia oggi strettamente connessa anche alla resilienza delle infrastrutture spaziali, energetiche e satellitari.

LA PERDITA DELLE CAPACITÀ ANALOGICHE

Uno dei temi più originali e profondi affrontati dal report riguarda la progressiva erosione delle cosiddette:

“analogue fallback capacities”

Negli ultimi decenni la digitalizzazione ha progressivamente sostituito procedure manuali, sistemi cartacei e strumenti analogici all’interno dei sistemi sanitari. Ospedali e servizi di

emergenza sono oggi fortemente dipendenti da piattaforme digitali integrate, reti cloud, software di gestione clinica e sistemi di comunicazione online.

Questa trasformazione ha migliorato enormemente l'efficienza operativa, ma ha anche prodotto un effetto collaterale poco considerato: molte competenze analogiche sono progressivamente scomparse.

Molti operatori sanitari non sono più addestrati a lavorare senza:

- cartelle cliniche elettroniche;
- piattaforme online;
- sistemi di comunicazione cloud;
- reti digitali interoperabili.

Il report sottolinea come protocolli cartacei, radio analogiche, procedure manuali e capacità offline siano stati progressivamente abbandonati o non più testati attraverso esercitazioni realistiche.

In caso di crisi digitale sistemica, questa perdita potrebbe trasformarsi in una grave vulnerabilità sanitaria. Se le piattaforme cliniche diventassero improvvisamente inaccessibili, molti ospedali avrebbero difficoltà a:

- recuperare informazioni sui pazienti;
- coordinare i percorsi assistenziali;
- gestire manualmente i flussi clinici;
- mantenere la continuità delle cure.

Per questo motivo il report suggerisce di recuperare e mantenere capacità operative analogiche come parte integrante della preparedness sanitaria contemporanea.

IMPLICAZIONI PER LE POLITICHE URBANE DELLA SALUTE

Le implicazioni del report risultano particolarmente rilevanti per le politiche urbane della salute e per il futuro delle smart cities.

Le città contemporanee dipendono sempre più da ecosistemi digitali complessi per gestire:

- mobilità urbana;
- sistemi di emergenza;
- monitoraggio ambientale;
- telemedicina;
- active ageing;
- servizi sociali;
- protezione civile;

- gestione energetica;
- sicurezza urbana.

Il report dimostra però che queste infrastrutture possono collassare simultaneamente durante crisi climatiche o digitali sistemiche.

Per questo motivo emerge la necessità di sviluppare una nuova generazione di:

“healthy resilient cities”

Le future politiche urbane dovranno integrare:

- resilienza digitale;
- adattamento climatico;
- salute pubblica;
- preparedness sanitaria;
- governance multisettoriale;
- sicurezza energetica;
- continuità operativa delle infrastrutture critiche.

La città del futuro non dovrà essere soltanto intelligente e connessa, ma anche capace di continuare a proteggere salute e servizi essenziali durante crisi simultanee e prolungate.

POLICY OPTIONS

1. Definire la resilienza digitale sanitaria come priorità strategica nazionale

Uno dei principali messaggi che emerge dal report *When Digital Systems Fail* è che la resilienza digitale non può più essere considerata esclusivamente una questione tecnica o informatica, ma deve diventare una componente centrale delle strategie nazionali di sicurezza sanitaria. Le infrastrutture digitali che sostengono il funzionamento quotidiano dei sistemi sanitari rappresentano oggi un elemento essenziale per la continuità delle cure, la gestione delle emergenze e la protezione della salute pubblica.

Per questo motivo i governi dovrebbero riconoscere formalmente:

- piattaforme sanitarie digitali;
- reti ospedaliere interoperabili;
- centrali operative di emergenza;
- infrastrutture cloud sanitarie;
- sistemi di telemedicina;

- piattaforme di sorveglianza epidemiologica

come vere e proprie infrastrutture critiche nazionali.

Questa classificazione consentirebbe di integrare il settore sanitario all'interno delle strategie nazionali di protezione delle infrastrutture critiche, rafforzando:

- investimenti in resilienza;
- coordinamento interministeriale;
- preparedness infrastrutturale;
- continuità operativa;
- pianificazione multi-rischio.

La resilienza sanitaria del XXI secolo dipende infatti non soltanto dalla disponibilità di ospedali e personale sanitario, ma anche dalla capacità di proteggere reti energetiche, data center, telecomunicazioni e sistemi digitali da cui i servizi sanitari dipendono sempre più profondamente.

2. Creare audit obbligatori di resilienza sanitaria digitale

Il report evidenzia come molti sistemi sanitari non abbiano ancora una piena consapevolezza delle proprie vulnerabilità infrastrutturali e delle interdipendenze che collegano piattaforme cliniche, reti energetiche, telecomunicazioni e cloud computing.

Per questo motivo diventa necessario introdurre audit obbligatori di resilienza sanitaria digitale capaci di valutare non soltanto la cybersecurity tradizionale, ma anche la capacità dei sistemi sanitari di resistere a crisi infrastrutturali sistemiche.

Tali audit dovrebbero includere:

- digital stress test;
- simulazioni di blackout prolungati;
- esercitazioni multi-settoriali;
- analisi delle dipendenze energetiche;
- valutazioni integrate clima-digitale;
- mapping delle interconnessioni sistemiche;
- valutazioni della resilienza dei data center;
- test di continuità operativa offline.

L'obiettivo non dovrebbe essere esclusivamente quello di prevenire il collasso tecnologico, ma soprattutto comprendere:

- quali sistemi siano più vulnerabili;
- quali servizi sanitari possano essere compromessi;
- quali dipendenze infrastrutturali rappresentino i maggiori punti critici;
- quanto tempo possano resistere i sistemi di backup;

- quali effetti a cascata possano propagarsi durante una crisi.

La preparedness sanitaria dovrà evolvere verso modelli di simulazione sistemica capaci di integrare salute, energia, telecomunicazioni, clima e infrastrutture critiche.

3. Rafforzare le capacità analogiche ospedaliere

Uno degli aspetti più preoccupanti evidenziati dal report riguarda la progressiva perdita delle capacità operative analogiche all'interno dei sistemi sanitari contemporanei. La digitalizzazione ha certamente migliorato efficienza e rapidità dei processi clinici, ma ha anche ridotto la capacità di lavorare in assenza di reti digitali funzionanti.

Molti ospedali oggi dipendono completamente da:

- cartelle cliniche elettroniche;
- piattaforme cloud;
- comunicazioni online;
- software di gestione;
- sistemi digitali di triage;
- reti interoperabili.

In caso di blackout digitale sistemico, questa dipendenza potrebbe trasformarsi rapidamente in una vulnerabilità clinica e organizzativa.

Per questo motivo gli ospedali dovrebbero mantenere e aggiornare:

- procedure cartacee di emergenza;
- sistemi offline di accesso ai dati essenziali;
- radio analogiche;
- protocolli manuali di coordinamento;
- sistemi energetici autonomi;
- backup locali;
- esercitazioni periodiche offline.

La resilienza sanitaria del futuro non dipenderà soltanto dalla qualità delle tecnologie digitali, ma anche dalla capacità delle organizzazioni sanitarie di continuare a operare quando tali tecnologie diventano improvvisamente indisponibili.

Recuperare competenze analogiche non significa tornare indietro rispetto alla digitalizzazione, ma costruire sistemi sanitari più robusti, adattivi e resilienti.

4. Integrare salute, clima e infrastrutture

Il report dimostra con grande chiarezza che il cambiamento climatico rappresenta sempre più anche una minaccia per la stabilità delle infrastrutture digitali e sanitarie. Heatwaves, alluvioni, incendi, stress energetici e fenomeni meteorologici estremi possono compromettere simultaneamente reti elettriche, telecomunicazioni, data center e servizi sanitari.

Per questo motivo le politiche di adattamento climatico non possono più essere separate dalla pianificazione sanitaria e infrastrutturale.

I piani climatici nazionali, regionali e urbani dovrebbero includere:

- protezione fisica dei data center sanitari;
- continuità energetica per ospedali e piattaforme critiche;
- ridondanza delle telecomunicazioni;
- sistemi resilienti di raffreddamento;
- infrastrutture ospedaliere climate-proof;
- strategie di continuità digitale durante eventi estremi;
- protezione delle supply chain farmaceutiche.

La crisi climatica e la crisi digitale sono ormai profondamente intrecciate. Per questo la resilienza sanitaria dovrà essere progettata attraverso un approccio integrato capace di unire:

- salute pubblica;
- pianificazione urbana;
- energia;
- infrastrutture critiche;
- governance climatica;
- protezione civile.

5. Creare osservatori urbani di resilienza sanitaria digitale

Le città rappresentano oggi i luoghi in cui si concentra la maggiore esposizione ai rischi sistemici digitali e climatici. Ospedali ad alta intensità tecnologica, sistemi di mobilità intelligente, data center, piattaforme cloud, reti energetiche e servizi di emergenza convivono infatti all'interno di ecosistemi urbani fortemente interdipendenti.

Per questo motivo le grandi aree urbane dovrebbero sviluppare veri e propri osservatori di resilienza sanitaria digitale capaci di monitorare vulnerabilità, rischi emergenti e capacità di risposta delle infrastrutture critiche cittadine.

Questi strumenti potrebbero includere:

- urban resilience dashboards;
- piattaforme integrate salute-clima-digitale;

- sistemi di monitoraggio delle vulnerabilità infrastrutturali;
- mappe dinamiche delle interdipendenze critiche;
- centri di coordinamento multisettoriale;
- modelli predittivi di rischio climatico-digitale;
- sistemi di allerta precoce.

L'obiettivo dovrebbe essere quello di costruire città non soltanto intelligenti e connesse, ma anche capaci di mantenere operativi servizi sanitari, emergenze e reti essenziali durante crisi simultanee e prolungate.

La resilienza urbana dovrà quindi diventare una componente strutturale delle future politiche di urban health.

6. Sviluppare standard internazionali di digital health resilience

La crescente interdipendenza globale delle infrastrutture digitali rende evidente che nessun Paese può affrontare da solo il rischio di crisi digitali sistemiche. Data center, piattaforme cloud, reti satellitari, cavi sottomarini e telecomunicazioni costituiscono infatti infrastrutture globali che attraversano confini nazionali e collegano economie, sistemi sanitari e reti di emergenza.

Per questo motivo diventa necessario sviluppare una nuova architettura internazionale della resilienza sanitaria digitale.

Organizzazioni internazionali come OMS, ITU, UNDRR, OCSE e governi nazionali dovrebbero collaborare per definire:

- standard globali di resilienza ospedaliera digitale;
- linee guida internazionali per continuità operativa sanitaria;
- protocolli condivisi di gestione delle crisi digitali sistemiche;
- framework per la protezione delle infrastrutture cloud sanitarie;
- sistemi internazionali di early warning;
- standard di preparedness multi-settoriale.

La salute pubblica globale dipenderà sempre di più dalla capacità delle istituzioni internazionali di costruire modelli di governance cooperativa capaci di affrontare rischi sistemici transnazionali.

CONCLUSIONI

Il report *When Digital Systems Fail* evidenzia con straordinaria chiarezza come la sicurezza sanitaria del XXI secolo dipenderà sempre più dalla resilienza delle infrastrutture digitali che sostengono il funzionamento delle società contemporanee.

Le future crisi sanitarie potrebbero non nascere soltanto da pandemie, disastri naturali o emergenze epidemiologiche tradizionali, ma anche da:

- collassi energetici;
- blackout digitali;
- eventi geomagnetici;
- guasti dei data center;
- interruzioni delle telecomunicazioni;
- failure delle reti globali;
- crisi climatiche multi-settoriali.

La crescente interconnessione tra salute, energia, clima, cloud computing, telecomunicazioni e infrastrutture critiche sta modificando profondamente il concetto stesso di preparedness sanitaria.

La resilienza dei sistemi sanitari non potrà più essere costruita esclusivamente all'interno degli ospedali, ma dovrà integrare:

- salute pubblica;
- urban health;
- resilienza climatica;
- governance digitale;
- protezione delle infrastrutture critiche;
- continuità operativa;
- preparedness multi-rischio.

La vera sfida del prossimo decennio non sarà soltanto digitalizzare la sanità, ma costruire sistemi sanitari capaci di continuare a funzionare anche quando le infrastrutture digitali su cui si fondano diventano improvvisamente fragili o indisponibili.

In questo scenario, la resilienza sanitaria diventa sempre più una questione di resilienza sistemica delle società contemporanee.

BIBLIOGRAFIA ESSENZIALE

- International Telecommunication Union (ITU), United Nations Office for Disaster Risk Reduction (UNDRR), Sciences Po (2025). *When Digital Systems Fail – An Expert Report on the Hidden Risks of Our Digital World*.
- Koks, E. et al. (2024). *Infrastructure failure cascades quintuple risk of storm and flood-induced service disruptions across the globe*. One Earth.
- International Energy Agency (2024). *Electricity 2024: Analysis and Forecast to 2026*.
- Lloyd's of London (2013). *Solar Storm Risk to the North American Electric Grid*.
- Clare, M.A. et al. (2023). *Fast and destructive density currents created by ocean-entering volcanic eruptions*. Science.
- WHO Europe (2021). *Climate Change and Health in Europe*.
- OECD (2023). *The Digital Transformation of Health Systems*.
- UNDRR (2022). *Global Assessment Report on Disaster Risk Reduction*.