GIUGNO 2025

INTELLIGENZA ARTIFICIALE E DATI SANITARI: impatto, governance e opportunità per modernizzare la sanità

Maria Rosaria Della Porta, Gabriele Licheri, Thomas Osborn

Negli ultimi anni, la sanità digitale ha rivoluzionato il SSN, il mondo della ricerca e quello delle cure. Attraverso un'ampia gamma di strumenti innovativi, che vanno dalla diagnostica avanzata basata su immagini all'impiego di robot per interventi chirurgici fino all'utilizzo di algoritmi per efficientarne gli aspetti organizzativi e di pianificazione, la disponibilità di dati sanitari e di strumenti di IA sempre più precisi offrono enormi potenzialità tanto in ambito clinico quanto in termini di efficienza nella programmazione operativa e finanziaria. Al contempo i vari settori legati al mondo della sanità rimangono tra i più esposti ai rischi legati alla gestione delle informazioni sanitarie sensibili e agli attacchi cyber, mentre è ancora insufficiente l'offerta formativa digitale per chi si appresta ad entrare nel mondo delle professioni sanitarie.

- *Il FSE 2.0, che rappresenta un'infrastruttura di avanguardia a livello europeo e globale, non presenta ancora i dati auspicati in termini di utilizzo e fiducia da parte dei cittadini e pazienti;*
- *Lo EHDS segna un punto di svolta normativo e operativo fondamentale per l'intero ecosistema della salute europea. Questo punta a facilitare la condivisione dei dati sanitari, rendendoli accessibili per la ricerca e l'innovazione all'interno di un quadro normativo strutturato, con misure di sicurezza e meccanismi di controllo;*
- *L'IA in salute sta già dando grandi risultati per quel che riguarda la ricerca scientifica, la diagnostica per immagini, la precisione degli interventi, e l'efficientamento in termini organizzativi e di pianificazione sanitaria – ad esempio sulle liste d'attesa;*
- *L'IA si sta rivelando uno strumento prezioso anche per migliorare il coinvolgimento del paziente nel proprio percorso di cura e per cambiare il modo in cui il paziente può accedere alle informazioni sanitarie, ricevere cure e gestire le proprie condizioni di salute. Questo è fondamentale per costruire la fiducia di cittadini e pazienti circa le nuove tecnologie;*
- *Fondamentali restano i temi della sicurezza dei dati e delle infrastrutture digitali e della formazione del personale. Sulla prima, preoccupa che 56% delle organizzazioni sanitarie dedica meno del 10% del proprio budget IT alla cybersecurity; sulla seconda, sono ancora troppo pochi i corsi su sicurezza del dato e IA nei corsi legati alla sanità nelle università italiane.*

INTRODUZIONE

Negli ultimi anni, la sanità digitale ha rivoluzionato il Sistema Sanitario Nazionale italiano (SSN) attraverso un'ampia gamma di strumenti innovativi, che vanno dalla diagnostica avanzata basata su immagini all'impiego di robot per interventi chirurgici fino all'utilizzo di algoritmi per efficientarne gli aspetti organizzativi e di pianificazione. Questo processo sta delineando il futuro dell'assistenza sanitaria e della ricerca innovativa, settori sempre più coinvolti nelle opportunità di crescita offerte dall'uso dei dati e dall'intelligenza artificiale (IA), ma al contempo esposti ai rischi legati alla gestione delle informazioni sanitarie sensibili.

In questo documento verranno analizzate le potenzialità del digitale per la sanità italiana, concentrandoci sugli effetti di queste tecnologie nella riduzione delle criticità derivanti dalla frammentazione territoriale, dal decentramento del SSN e dal divario digitale tra le regioni. In particolare, è importante valutare lo stato di avanzamento del FSE 2.0 in vista dell'omologazione europea dell'EHDS e dell'interoperabilità dei dati. La digitalizzazione della sanità ha ormai assunto un ruolo centrale a livello europeo, rientrando tra i settori strategici del processo di transizione digitale. In particolare, il settore sanitario è considerato una delle aree chiave per il raggiungimento di un mercato unico digitale europeo, in linea con l'Obiettivo 1 – *"Un'Europa più intelligente: trasformazione ecologica, innovativa e digitale"* – previsto nell'attuale ciclo di programmazione delle politiche di coesione 2021-2027.

L'interoperabilità e la gestione di volumi sempre maggiori di dati si configurano come pilastri fondamentali della sanità del futuro, strettamente connessi alle nuove applicazioni dell'intelligenza artificiale. Queste tecnologie stanno accelerando l'integrazione di macchine e algoritmi nel lavoro medico, offrendo strumenti avanzati che spaziano dalla prevenzione alla diagnosi, fino alla robotica e all'analisi dei dati. Sebbene tali innovazioni promettano di semplificare e migliorare l'attività clinica, sollevano al contempo questioni cruciali legate alla privacy e all'etica nell'utilizzo delle informazioni sanitarie, aspetti imprescindibili per garantire un'evoluzione sicura e sostenibile del settore.

Il settore sanitario, infatti, è tra i più vulnerabili agli attacchi informatici, una fragilità che comporta costi elevati per la protezione dei dati, aggravando ulteriormente una gestione economica già caratterizzata da risorse limitate, spesso insufficienti persino per garantire un'adeguata assistenza primaria. Per questo motivo, sia l'Italia che l'Europa stanno investendo nel rafforzamento della cybersicurezza, con particolare attenzione alla nascita dell'Ecosistema dei dati sanitari. Questo sistema integrato mira a raccogliere, gestire, scambiare e utilizzare i dati sanitari in modo sicuro ed efficiente, con l'obiettivo di migliorare l'assistenza sanitaria, potenziare la ricerca scientifica e supportare l'elaborazione di politiche sanitarie basate su dati affidabili e interoperabili.

1. FSE ED EHDS, IL DATO SANITARIO E LA SUA INTEROPERABILITÀ

Nel cuore della trasformazione digitale della sanità, il dato sanitario assume oggi un ruolo strategico, non solo come strumento clinico, ma come vero e proprio asset infrastrutturale. La capacità di raccogliere, gestire e valorizzare queste informazioni è diventata essenziale per migliorare l'efficienza dei servizi, promuovere la medicina personalizzata e potenziare le politiche di sanità pubblica. In questo contesto, strumenti come il Fascicolo Sanitario Elettronico (FSE) rappresentano un tassello fondamentale di un disegno più ampio, che trova piena espressione nella costruzione dell'Ecosistema dei Dati Sanitari nazionale e nell'ambizioso progetto europeo dello *European Health Data Space* (EHDS). È dunque sempre più evidente che la sfida non riguarda solo l'adozione tecnologica, ma anche la capacità del sistema di garantire accesso equo, sicurezza, interoperabilità e una governance trasparente del dato.

1.1. L'avanzamento del FSE 2.0

Il Fascicolo Sanitario Elettronico (FSE) rappresenta uno dei principali strumenti della sanità digitale in Italia e una *best practice* a livello internazionale. Inoltre, è stato al centro di significativi investimenti grazie ai fondi stanziati con il PNRR e alla strategia europea di unificazione e interoperabilità dei sistemi di dati sanitari. Nonostante la recente critica di *The Lancet*[1] alla sanità italiana abbia sollevato dubbi sugli sforzi compiuti a livello nazionale negli ultimi anni, evidenziando in particolare la frammentazione e il divario tra le regioni, il processo di digitalizzazione del SSN procede a ritmo sostenuto, integrando nuovi elementi e allineandosi alle normative europee. In particolare, l'Italia si distingue finalmente rispetto ad altri Paesi europei grazie a un sistema di dati già esistente e interoperabile tra le regioni, pronto a contribuire allo sviluppo del sistema europeo dei dati sanitari.

Con l'introduzione del Fascicolo Sanitario Elettronico 2.0, le aspettative sono cresciute, soprattutto in relazione alla sua integrazione con tecnologie emergenti e dibattute, come l'AI generativa e la gestione dei dati e della privacy. Tra la fine del 2024 e l'inizio del 2025 sono state introdotte nuove disposizioni sull'FSE, con scadenze precise per Regioni ed enti coinvolti. I documenti, pubblicati sul sito del FSE, riguardano: la gestione delle deleghe nel FSE 2.0, l'interoperabilità tra sistemi regionali (versione 2.6) e la tracciabilità delle operazioni sul FSE.

A inizio 2025 sono state inoltre definite le regole per l'indicizzazione delle prescrizioni e prestazioni da parte del Sistema TS, la gestione dell'oscuramento di referti e prescrizioni dematerializzate e l'accesso ai dati relativi al consenso o diniego alla donazione di organi e tessuti. Le specifiche tecniche per la gestione delle deleghe, elaborate da DTD e CNR, stabiliscono un sistema sicuro e standardizzato per consentire a un delegato di operare per conto dell'assistito. Sono previste deleghe automatiche (per genitori, tutori, curatori) e volontarie, sincronizzazione tra sistemi regionali e nazionali, e verifica del consenso alla consultazione. L'attuazione è prevista entro il 30 settembre 2025.

L'aggiornamento sull'interoperabilità, a cura di AgID, CNR, DTD e Sogei, introduce la tanto ambita e ricercata uniformità nei processi e nei dati tra i sistemi regionali e l'Infrastruttura Nazionale per l'Interoperabilità (INI). Include nuove terminologie e metadati, regole di validazione (CDA e FHIR),

[1] *The Italian health data system is broken, The Lancet Regional Health – Europe, 2025, DOI: 10.1016/j.lanepe.2024.101206*

maggiore tracciabilità e gestione del consenso secondo il GDPR. L'entrata in vigore è prevista entro il 31 marzo 2026.

Infine, le Linee operative per la registrazione e consultazione delle operazioni sul FSE, pubblicate a dicembre 2024, garantiscono la tracciabilità delle attività svolte e la possibilità per l'assistito di consultarle, nel rispetto della trasparenza e della protezione dei dati personali. Su questo, l'attuazione e l'adeguamento delle Regioni era previsto entro il 31 marzo 2025.

Tutte queste novità si integrano in un sistema già complesso, che oggi offre non solo un'interfaccia intuitiva e un accesso consultivo alla cartella clinica, ma anche una gestione attiva dei propri dati sanitari e delle funzionalità correlate. Tuttavia, nonostante il sistema sia ufficialmente operativo ed efficace, il suo utilizzo da parte di cittadini e operatori rimane frammentato a livello regionale, dimostrando che non è ancora pienamente sfruttato nella sua interezza. In particolare, come evidenziato nella Fig. 1.1, l'adozione da parte dei cittadini è ancora limitata, segnalando una carenza di cultura digitale sanitaria, soprattutto nel Sud Italia: solo l'18% di cittadini italiani aveva utilizzato il proprio FSE nei 90 giorni precedenti al periodo di riferimento[2] e solo il 42% aveva espresso il consenso alla consultazione dei propri documenti, evidenziando la presenza di importanti barriere culturali e informative.

L'adozione da parte dei cittadini è ancora limitata, segnalando una carenza di cultura digitale sanitaria. La percentuale di italiani che usa il FSE è ancora molto bassa rispetto allo stato di avanzamento, con valori preoccupanti anche relativamente alla disponibilità a condividere i dati sanitari.

La limitata diffusione di questi strumenti evidenzia una problematica strutturale legata alla disparità tra le innovazioni tecnologiche e la loro effettiva accessibilità e conoscenza da parte dei cittadini. Il *digital divide* è infatti determinato non solo dalla cosiddetta bassa "alfabetizzazione digitale", ma anche dalla difficoltà di accesso alle tecnologie, soprattutto nelle aree interne e non urbanizzate del Paese. Per affrontare questa sfida, è essenziale adottare una gestione del cambiamento che sia inclusiva, garantendo che anche le fasce più vulnerabili possano accedere ai servizi sanitari. Questo richiede l'impiego a rendere tali tecnologie sempre più intuitive, sicure e fruibili, affiancate da iniziative di comunicazione istituzionale e programmi di alfabetizzazione digitale a livello nazionale.

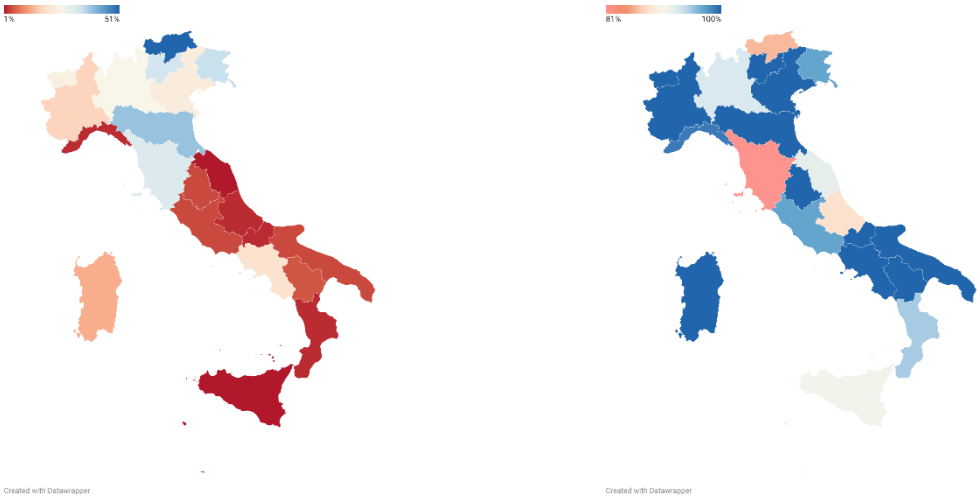
La diffusione e l'accessibilità di strumenti di sanità digitali, come appunto il FSE, sono perdipiù centrali nel superare le disuguaglianze di accesso (percepite e reali) ai sistemi di cura tra le varie fasce della popolazione. Come dimostra un'ampia letteratura scientifica, strumenti come il FSE possono rappresentare uno strumento particolarmente utile per chi dispone di minori risorse relazionali, aiutando a colmare il divario informativo e a favorire un dialogo più efficace con i professionisti sanitari. Studi come quello di Ahn S. et al. (2024)[3] mostrano, ad esempio, come l'uso di un sistema paragonabile al FSE negli USA ha avuto un effetto indiretto e positivo sulla comunicazione tra pazienti e operatori sanitari su tutta la popolazione, ma con un risultato

[2] *Settembre – Novembre 2024; per il Friuli-Venezia Giulia gennaio - marzo 2024*
[3] *Ahn S, Lee C, Bae Patients' Use of Electronic Health Records Facilitates Patient-Centered Communication: Findings From the 2017 Health Information National Trends Survey, J Med Internet Res 2024;26:e50476 - URL: https://www.jmir.org/2024/1/e50476 - DOI: 10.2196/50476*

statisticamente significativi soprattutto tra i pazienti “con basso supporto sociale”, per i quali il FSE americano ha avuto un effetto positivo sia sull’efficacia informativa sia, indirettamente, sulla comunicazione con i medici.

Fig.1.1: *Sinistra*: **Cittadini che hanno utilizzato il Fascicolo Sanitario Elettronico nei 90 giorni precedenti alla data di rilevazione.** *Destra*: **MMG e PLS che hanno effettuato almeno un'operazione sul Fascicolo nel periodo di riferimento**

Fonte: Ministero della Salute
Nota: per periodo di riferimento si intende: settembre - novembre 2024



L’uso del FSE da parte dei medici si conferma dunque un elemento chiave, sia per l’accesso alle informazioni sanitarie, sia per migliorare la relazione con i pazienti, essendo il primo strumento per la creazione e la operabilità di un ecosistema digitale. Gli operatori sanitari lo utilizzano ormai quotidianamente nella maggior parte delle regioni, con Abruzzo, Bolzano e Toscana che registrano valori leggermente inferiori al 90%, ma comunque superiori all’80%. Questi dati evidenziano la necessità di proseguire nell’implementazione e nella diffusione del FSE, soprattutto per coinvolgere quei pazienti ancora diffidenti o poco abituati alla sanità digitale, dove il ruolo dei medici di famiglia (MMG) può risultare fondamentale per aumentarne la capillarità e la fiducia.

È in questo contesto che lo scorso 5 marzo diventa una data rivoluzionaria per la sanità digitale. In questa data, infatti, sono stati ufficialmente pubblicati due importanti provvedimenti: sulla Gazzetta Ufficiale dell’Unione Europea (GUUE) è apparso il Regolamento (UE) 2025/327, che istituisce lo Spazio Europeo dei Dati Sanitari (*European Health Data Space* - EHDS), mentre sulla Gazzetta Ufficiale italiana è stato pubblicato il Decreto del Ministero della Salute del 31 dicembre 2024, che introduce l’Ecosistema dei Dati Sanitari (EDS). Questi atti normativi rappresentano un passo cruciale verso un sistema sanitario più integrato, sicuro e accessibile, sia a livello nazionale che europeo.

1.2. EDS e la rivoluzione dei dati

L’Ecosistema dei Dati Sanitari (EDS), istituito ufficialmente tramite il decreto del 31 dicembre 2024 (n. 53 del 5-3-2025), individua i contenuti, le modalità di alimentazione, nonché i soggetti che vi hanno accesso, le operazioni eseguibili e le misure di sicurezza per assicurare i diritti degli interessati, aprendo ad una rivoluzione sull’utilizzo del dato sanitario.

Secondo quanto stabilito dall'articolo 3 del Decreto Ministeriale sull'EDS, l'ecosistema si alimenta con i dati del FSE, che includono informazioni anagrafiche e amministrative dei pazienti (ad esempio, esenzioni per reddito o patologia, contatti e delegati), oltre a una vasta gamma di documenti sanitari: referti, lettere di dimissione, verbali di pronto soccorso, prescrizioni farmaceutiche e specialistiche, cartelle cliniche, registri delle vaccinazioni e dell'erogazione di farmaci, prestazioni specialistiche e annotazioni personali dell'assistito.

Inoltre, vengono integrati i dati disponibili tramite il Sistema Tessera Sanitaria. Queste informazioni possono essere consultate ed elaborate all'interno dell'EDS attraverso operazioni di ricerca, estrazione e analisi, con la possibilità di sviluppare strumenti innovativi come il Dossier Farmaceutico. Quest'ultimo, introdotto come novità normativa, raccoglie dati dettagliati sulle prescrizioni e l'erogazione dei farmaci, compresi i piani terapeutici e le modalità di somministrazione, contribuendo a una gestione più efficace delle terapie.

Rivoluzionario è anche l'approccio all'accesso all'EDS, regolato in base alle finalità specifiche per cui i dati vengono utilizzati:

- Per la cura dei pazienti (art. 13 del DM EDS), possono accedere le strutture sanitarie e sociosanitarie, i medici convenzionati e altri professionisti sanitari coinvolti nell'assistenza, escludendo però soggetti come periti, compagnie assicurative, datori di lavoro e personale medico-legale;
- per la prevenzione (art. 14), l'accesso è consentito agli enti del Servizio Sanitario Nazionale (SSN) e ai servizi sociosanitari regionali, attraverso i dipartimenti competenti in materia di prevenzione;
- per la profilassi internazionale (art. 15), i dati possono essere consultati dagli uffici del Ministero della Salute responsabili della sanità marittima, aerea e di frontiera, nel rispetto delle normative sanitarie internazionali;
- per il governo del sistema sanitario (art. 16), l'accesso è riservato agli uffici del Ministero della Salute, Agenas e alle autorità regionali competenti;
- per la ricerca scientifica (art. 17), l'EDS rappresenta un'opportunità significativa, con un'apertura regolamentata che potrebbe contribuire a superare molte delle attuali criticità del settore, consentendo l'accesso a soggetti pubblici e privati che istituzionalmente perseguono finalità di studio e di ricerca scientifica in campo medico, biomedico ed epidemiologico.

Questo sistema innovativo punta a trasformare la gestione dei dati sanitari in Italia, migliorando la qualità dell'assistenza e promuovendo un utilizzo più efficiente e sicuro delle informazioni. Il decreto stabilisce che l'accesso ai dati anonimizzati dell'EDS è riservato al personale qualificato del Ministero della Salute, di Agenas e delle regioni e province autonome, attraverso appositi servizi di estrazione, ma introduce anche un'importante apertura verso il settore privato, consentendo anche a enti pubblici e privati impegnati nella ricerca medica, biomedica ed epidemiologica di richiedere ad Agenas l'estrazione di dati anonimizzati; tale richiesta dovrà essere accompagnata da un progetto di ricerca conforme agli standard metodologici, etici e, se applicabile, alle norme deontologiche previste per il trattamento dei dati a fini statistici e di ricerca scientifica.

1.3. European Health Data Space (EHDS): l'ecosistema europeo per la condivisione dei dati sanitari

Le novità introdotte in Italia si collocano all'interno di un contesto europeo più ampio, in cui l'Unione Europea compie un passo decisivo verso la creazione di uno strumento digitale condiviso, interno, interoperabile e armonizzato tra gli Stati membri. Il tanto atteso Regolamento sullo *European Health Data Space* (EHDS), che si inserisce nel filone del Data Governance Act, di cui è un importante e strategico filone verticale, ha infatti l'obiettivo di rafforzare l'accesso e il controllo delle persone fisiche sui propri dati sanitari elettronici nell'ambito dell'assistenza sanitaria. Inoltre, mira a favorire l'utilizzo dei dati sanitari elettronici per finalità di interesse collettivo come la ricerca, l'innovazione, la definizione di politiche sanitarie, la preparazione e la risposta alle minacce per la salute (incluse la prevenzione e la gestione di future pandemie), la sicurezza dei pazienti, la medicina personalizzata, le statistiche ufficiali e le attività normative.

Il sistema dell'EDS si colloca quindi all'interno di una più ampia strategia europea volta alla trasformazione e alla gestione dei dati sanitari, con la creazione dello EHDS. Il regolamento relativo all'EHDS è strutturato in tre sezioni principali, ciascuna indirizzata a specifici destinatari:

- Capitolo II - Uso primario dei dati: rafforza i diritti dei pazienti e definisce l'infrastruttura tecnica necessaria per garantirne l'attuazione. Gli Stati membri sono tenuti a predisporre le infrastrutture necessarie a livello nazionale e ad assicurare che gli operatori sanitari siano connessi al sistema.
- Capitolo III - Sistemi di cartella clinica elettronica (EHR): riguarda i produttori e gli operatori economici che immettono sul mercato questi sistemi. Introduce requisiti in materia di interoperabilità e tracciabilità, oltre a stabilire meccanismi di sorveglianza del mercato, demandando agli Stati membri la designazione delle autorità competenti per il controllo e la supervisione del settore.
- Capitolo IV - Uso secondario dei dati: disciplina l'accesso e l'utilizzo dei dati sanitari da parte dei detentori e degli utenti di tali informazioni. Impone agli enti che gestiscono i dati l'obbligo di renderli disponibili e definisce le modalità di utilizzo per la ricerca e altre finalità. Inoltre, prevede l'istituzione degli organismi di accesso ai dati sanitari (Health Data Access Bodies – HDABs) e l'infrastruttura necessaria al loro funzionamento.

Con lo EHDS i pazienti potranno invece accedere ai servizi di consultazione dei dati sanitari e far valere i propri diritti a partire dal 26 marzo 2029 per le prime categorie prioritarie e dal 26 marzo 2031 per le restanti.

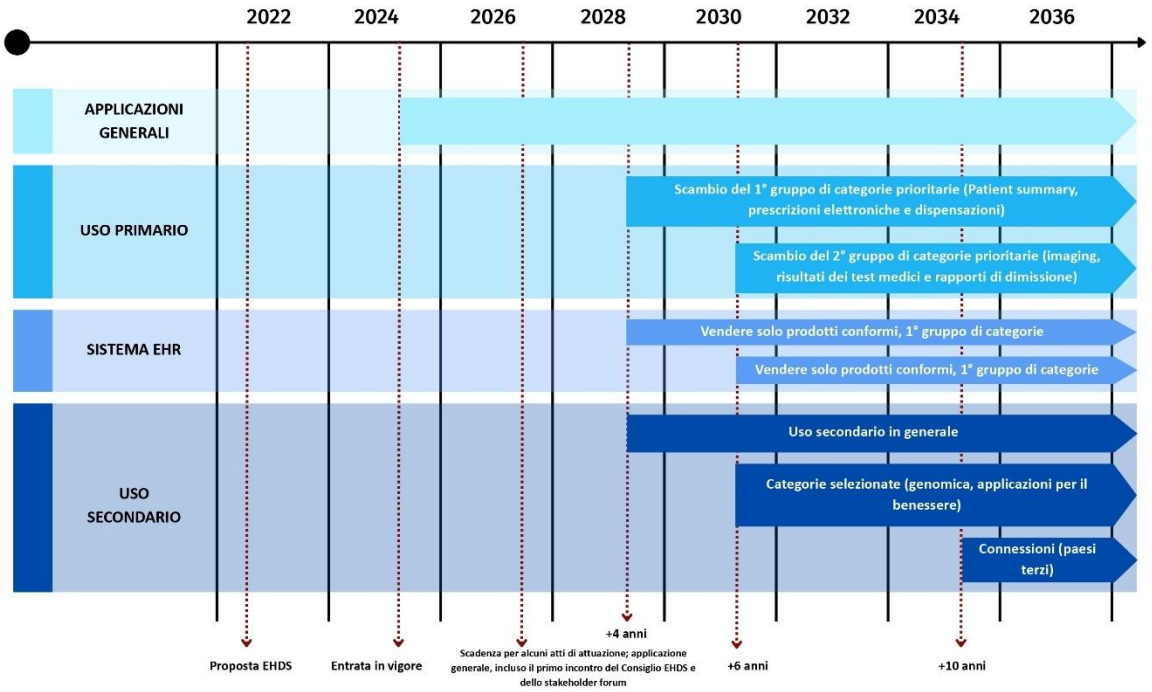
Le disposizioni entreranno in funzione gradualmente, si prevede una prima fase per i Capitoli II e III, entro il 26 marzo 2029, che riguarderà i sommari clinici, le ricette elettroniche e la dispensazione elettronica, mentre la seconda fase, entro il 26 marzo 2031, estenderà l'applicazione agli studi di imaging medico ai risultati di test diagnostici e alle lettere di dimissione. I pazienti potranno invece accedere ai servizi di consultazione dei dati sanitari e far valere i propri

diritti a partire dal 26 marzo 2029 per le prime categorie prioritarie e dal 26 marzo 2031 per le restanti[4].

Fondamentale infine evidenziare l'impegno che lo EHDS richiede agli Stati membri anche in termini organizzativi. Difatti, questi dovranno istituire le proprie *autorità per la sanità digitale* e designare i punti di contatto nazionali entro il 26 marzo 2027, mentre entro il 26 marzo 2029 dovranno garantire l'operatività dei servizi previsti dal Capitolo II ed entro il 26 marzo 2031 dovranno estenderli alla seconda categoria di dati prioritari.

Fig.1.2: Prossimi passi dell'EHDS (2022-2036)

Fonte: Elaboraziome I-Com su European Commission



Una volta disponibile l'infrastruttura i pazienti avranno il diritto di accedere in modo sicuro e gratuito ai propri dati sanitari attraverso una piattaforma digitale che consentirà di visualizzare, scaricare e gestire le informazioni personali. Sarà possibile verificare chi ha consultato i dati, segnalare eventuali inesattezze, limitare l'accesso a determinate informazioni e impostare deleghe per terzi.

Inoltre, il sistema EHR europeo permetterà ai pazienti di integrare le proprie cartelle cliniche con dati provenienti da app e dispositivi per il benessere, mantenendo una distinzione chiara tra dati inseriti dagli utenti e quelli dei professionisti sanitari. Le app dovranno rispettare requisiti tecnici, essere interoperabili e registrate in un database UE.

[4] *Per quanto riguarda i produttori di sistemi EHR, dal 26 marzo 2029 questi potranno immettere sul mercato solo sistemi conformi alle specifiche comuni per la gestione dei primi dati prioritari, mentre dal 26 marzo 2031 l'obbligo si estenderà anche ai sistemi che trattano le altre categorie di dati. I detentori di dati sanitari dovranno inviare agli organismi di accesso ai dati sanitari (HDAB) la descrizione dei dataset detenuti entro il 26 marzo 2029 o 2031, a seconda della categoria di appartenenza ai sensi dell'Articolo 51, e potranno essere obbligati a rendere disponibili i dati in seguito a specifiche autorizzazioni.*

L'invio dei dati avverrà solo con il consenso dell'utente, che potrà definirne modalità e frequenza. Il regolamento EHDS migliorerà anche la portabilità dei dati sanitari nell'UE, favorendo la continuità delle cure tra Stati membri.

È prevista inoltre l'integrazione di Paesi terzi nel sistema *MyHealth@EU*, previo rispetto di standard equivalenti a quelli europei. Una volta approvati, potranno scambiare informazioni sanitarie con l'UE, pur restando osservatori e non membri decisionali della governance.

1.3.1. GDPR ed EHDS: l'uso secondario dei dati sanitari

Un aspetto fondamentale dello EHDS riguarda l'utilizzo secondario dei dati sanitari, ovvero l'impiego delle informazioni raccolte non per la cura diretta del paziente, ma per finalità più ampie di interesse collettivo. Il secondo pilastro dell'iniziativa, *HealthData@EU*, promuove infatti l'uso di dati sanitari pseudonimizzati o anonimizzati per sostenere la ricerca scientifica, l'innovazione medica, lo sviluppo di farmaci e dispositivi, oltre che per ottimizzare l'organizzazione dei sistemi sanitari. Questo approccio, imprescindibile per cogliere appieno i vantaggi e le potenzialità derivanti dalle ingenti quantità di informazioni digitali, mira a trasformare i dati sanitari in una leva strategica per migliorare la salute pubblica e accelerare il progresso della medicina.

È previsto che l'impiego di tali dati sia rigorosamente regolato: potranno accedervi solo enti autorizzati, sotto controllo di autorità competenti, e le richieste saranno valutate caso per caso per garantire il rispetto della privacy e dei diritti dei cittadini. Importante inoltre evidenziare come l'UE preveda di garantire comunque il diritto di opposizione (*opt-out*), che permetterà ai cittadini di escludere i propri dati da questi utilizzi, fatta eccezione per alcune situazioni specifiche legate all'interesse pubblico[5]. Per rafforzare la tutela dei diritti individuali, il regolamento vietata esplicitamente l'adozione dei dati sanitari per finalità discriminatorie, come decisioni in ambito assicurativo o creditizio. Questo garantisce che le informazioni mediche non possano essere usate per danneggiare le persone in base al loro stato di salute.

L'EHDS si inserisce nel solco del GDPR, ma con l'obiettivo di ampliare, in modo controllato e trasparente, le possibilità di utilizzo dei dati sanitari per fini secondari: mentre il GDPR pone limiti precisi e lascia margine alle normative nazionali, l'EHDS intende offrire un quadro armonizzato e proattivo a livello europeo, che valorizzi il potenziale dei dati sanitari, mantenendo al contempo un elevato livello di protezione per i dati sensibili. In questo scenario, il regolamento si propone di rispondere a una sfida complessa: bilanciare il diritto alla riservatezza dei cittadini con la necessità di disporre di dati completi e accessibili per promuovere cure più efficaci, ricerche più rapide e una sanità più sostenibile.

L'EHDS punta, dunque, a facilitare la condivisione dei dati sanitari, rendendoli accessibili per la ricerca e l'innovazione all'interno di un quadro normativo strutturato, con misure di sicurezza e meccanismi di controllo.

Per realizzare questo obiettivo, il regolamento stabilisce che i titolari dei dati individuino e classificano le diverse categorie di informazioni sanitarie in loro possesso, rendendole accessibili agli organismi responsabili dell'accesso ai dati (*Health Data Access Bodies*, HDAB), designati dagli Stati membri dell'UE. Questi organismi fungono da intermediari tra i titolari dei dati e gli utenti

[5] *Ad esempio, casi di gestione di emergenze sanitarie o la ricerca su malattie gravi.*

autorizzati, come ricercatori, enti pubblici e soggetti privati con finalità di ricerca o innovazione, gestendo le richieste e fornendo i dati tramite una piattaforma sicura[6].

I titolari dei dati - pubblici o privati attivi nei settori della sanità, dell'assistenza o della ricerca - sono tenuti a condividere le informazioni, salvo eccezioni previste per le microimprese e i ricercatori indipendenti. Non sussiste l'obbligo se i dati non sono accessibili dal titolare, come nel caso delle app che archiviano le informazioni esclusivamente sul dispositivo dell'utente.

Per garantire un equilibrio tra apertura dei dati e tutela dei diritti, è riconosciuta la possibilità di segnalare all'HDAB la presenza di contenuti protetti da proprietà intellettuale o segreti commerciali. In questi casi, l'organismo può imporre misure di protezione specifiche o negare l'accesso, se sussistono rischi concreti per i diritti del titolare.

L'EHDS punta a facilitare la condivisione dei dati sanitari, rendendoli accessibili per la ricerca e l'innovazione all'interno di un quadro normativo strutturato, con misure di sicurezza e meccanismi di controllo

[6] *Inoltre, alcuni soggetti con comprovata esperienza nella gestione di dati sanitari possono essere designati come "trusted health data holders". Pur non avendo potere decisionale, possono ricevere richieste e fornire raccomandazioni all'HDAB. Per semplificare le procedure, gli Stati membri possono anche creare enti di intermediazione che supportano l'invio e la gestione delle richieste, senza tuttavia assumere il ruolo di titolari fidati né alterare il processo formale di valutazione da parte dell'HDAB.*

2. INTELLIGENZA ARTIFICIALE E MEDICINA DEL FUTURO: DALL'IA GENERATIVA A QUELLA PREDITTIVA

Dopo aver approfondito il ruolo cruciale dei dati sanitari e gli strumenti normativi e infrastrutturali predisposti per garantirne l'accessibilità e la condivisione è fondamentale analizzare le potenzialità che tali dati offrono quando vengono valorizzati attraverso tecnologie avanzate. In particolare, l'intelligenza artificiale rappresenta uno degli ambiti più promettenti per trasformare la sanità, migliorando diagnosi, percorsi terapeutici e organizzazione dei servizi al fine di raggiungere livelli di efficienza che possano sostenere la sostenibilità del nostro modello di cura. Questo secondo Capitolo è dunque dedicato a esplorare come l'IA stia entrando nel mondo della salute e quali siano le sfide normative, etiche e operative da affrontare per un suo utilizzo sicuro ed efficace.

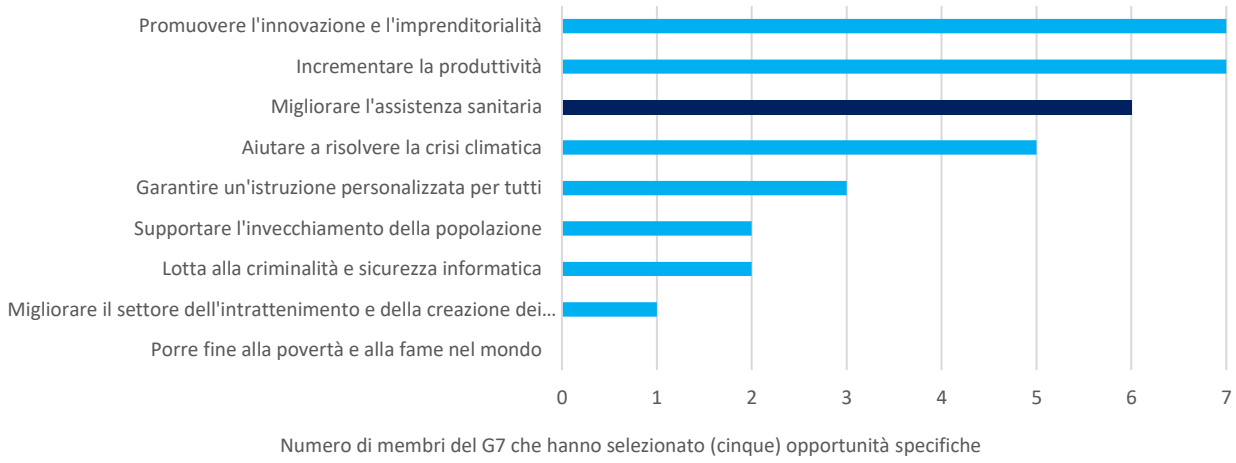
1.1. Le potenzialità dell'intelligenza artificiale in ambito sanitario

L'assistenza sanitaria, a livello globale, è alle prese con numerose sfide, tra cui l'invecchiamento della popolazione, l'aumento del carico di malattie croniche e non trasmissibili, l'aumento dei costi, il burnout dei medici, la carenza di forza lavoro nonché l'evoluzione delle aspettative di cura dei pazienti. Molte di queste sfide potrebbero essere sostenute e affrontate, se non addirittura superate, cogliendo il potenziale dell'intelligenza artificiale nel settore sanitario. Negli anni, la consapevolezza di tali opportunità è andata man mano crescendo, con evidenze e garanzie che hanno favorito il superamento dell'iniziale diffidenza e dei timori legati all'applicazione dell'IA in ambiti estremamente sensibili, come la salute.

Secondo la relazione redatta dall'OECD per il G7 di Hiroshima, nel 2023, infatti, sei Paesi su sette già erano giunti a ritenere che il miglioramento dell'assistenza sanitaria - insieme all'aumento della produttività, alla promozione dell'innovazione e alla risoluzione della crisi climatica - sia una delle principali opportunità rese possibili dallo sviluppo e dall'implementazione dell'intelligenza artificiale generativa[7] (Fig. 2.1).

Fig. 2.1: Le cinque principali opportunità dell'IA generativa per raggiungere gli obiettivi nazionali e regionali secondo i membri del G7

Fonte: OECD (2023)



[7] *OECD, G7 HIROSHIMA PROCESS ON GENERATIVE ARTIFICIAL INTELLIGENCE (AI) TOWARDS A G7 COMMON UNDERSTANDING ON GENERATIVE AI (2023)*

Difatti, a livello mondiale sempre più organizzazioni sanitarie riconoscono le potenzialità delle tecnologie di IA per migliorare l'assistenza sanitaria. Secondo un sondaggio di Deloitte[8], il 92% dei leader mondiali vede nell'IA generativa una promessa per migliorare l'efficienza in sanità: nello specifico, l'82% delle organizzazioni sanitarie mondiali ha o prevede di implementare strutture di governance e supervisione per l'IA generativa mentre il 65% ritiene che sia un valido strumento per consentire un processo decisionale più rapido. Anche tra le aziende del settore c'è grande ottimismo e il 75% di queste dichiara di star sperimentando o pianificando di utilizzare l'IA generativa al proprio interno.

L'IA in salute sta già dando grandi risultati per quel che riguarda la ricerca scientifica, la diagnostica per immagini, la precisione degli interventi, e l'efficientamento in termini organizzativi e di pianificazione sanitaria

In effetti, le tecnologie IA stanno già dando prova di saper rivoluzionare la medicina e l'assistenza dei pazienti (Fig. 2.2), offrendo numerosi benefici. Queste, infatti, sono in grado, di migliorare le capacità di ricerca clinica, supportare il processo decisionale clinico nonché consentire cure sempre più precise e personalizzate in grado di migliorare sensibilmente gli *outcome* di salute dei pazienti. Grazie all'IA, si stanno compiendo passi da gigante nella diagnostica per immagini dove tali tecnologie consentono una lettura precisa delle immagini mediche e di rilevare tempestivamente eventuali anomalie.

Inoltre, l'intelligenza artificiale è in grado di ottimizzare l'efficienza operativa e liberare tempo prezioso per gli operatori sanitari consentendogli di concentrarsi sulla cura dei pazienti, migliorandone significativamente il livello di assistenza.

Fig. 2.2: Applicazione dell'intelligenza artificiale in vari ambiti dell'assistenza sanitaria

Fonte: elaborazione I-Com su Journal of Personalized Medicine

[8] *https://www2.deloitte.com/us/en/pages/life-sciences-and-health-care/articles/generative-ai-in-healthcare.html*

L'IA si sta rivelando uno strumento prezioso anche per migliorare il coinvolgimento del paziente nel proprio percorso di cura e per cambiare il modo in cui il paziente può accedere alle informazioni sanitarie, ricevere cure e gestire le proprie condizioni di salute. Secondo un recente sondaggio condotto da McKinsey & Company[9], il coinvolgimento nonché il miglioramento dell'esperienza di cura del paziente sono il secondo ambito - dopo la produttività clinica - in cui l'intelligenza artificiale generativa esprime un elevato potenziale. Ben oltre il 60% degli intervistati, provenienti da alcune organizzazioni sanitarie statunitensi, ritiene che l'esperienza del paziente possa beneficiare di numerosi vantaggi grazie all'integrazione di queste tecnologie nel percorso di cura, in termini di maggiore appropriatezza delle cure, efficienza nonché autonomia.

L'IA si sta rivelando uno strumento prezioso anche per migliorare il coinvolgimento del paziente nel proprio percorso di cura e per cambiare il modo in cui il paziente può accedere alle informazioni sanitarie, ricevere cure e gestire le proprie condizioni di salute

Box 1: Foresight e liste di attesa: l'IA nella pianificazione sanitaria - il caso dell'NHS

Tra le applicazioni più promettenti dell'IA in sanità vi è la sua capacità di poter ridurre le liste di attesa. L'utilizzo dell'IA su dati storici può fornire preziose informazioni per prevedere la domanda e consentire una pianificazione più efficace delle risorse e una maggiore gestione dei flussi dei pazienti, evitando così il formarsi di lunghe liste d'attesa. La capacità di anticipare picchi di richiesta e adeguare di conseguenza le risorse è un vantaggio competitivo significativo per gli operatori sanitari. Attraverso l'uso di algoritmi avanzati, l'IA è in grado di effettuare un triage dei pazienti in modo più efficiente e preciso. I sistemi di IA possono analizzare i dati clinici per determinare l'urgenza delle condizioni dei pazienti, consentendo di dare priorità a quelli che necessitano di cure immediate. Questo approccio garantisce che le risorse siano utilizzate in modo più efficace, riducendo i tempi di attesa per i pazienti più critici[10].

Il Servizio Sanitario Nazionale del Regno Unito (NHS) sta esplorando l'uso dell'intelligenza artificiale per gestire in modo più equo ed efficace proprio le liste d'attesa, soprattutto dopo la crisi causata dalla pandemia[11]. Gli strumenti di IA consentono di calcolare un "punteggio di rischio" per ciascun paziente, valutando la probabilità che le sue condizioni di salute peggiorino durante l'attesa. Questo approccio non si limita a considerare il solo ordine cronologico o il bisogno clinico, ma inizia a includere anche fattori legati alle disuguaglianze sociali e demografiche, come il livello di deprivazione o l'appartenenza a minoranze etniche. I primi studi mostrano come questa metodologia possa ridurre le disuguaglianze negli esiti di salute e migliorare l'efficacia degli interventi.

Alcune esperienze hanno dimostrato che strumenti di IA ben progettati possono supportare interventi mirati anche fuori dal contesto clinico, per esempio con programmi di preabilitazione o supporto sociale ed economico. Questo approccio apre la strada a una

[9] https://www.mckinsey.com/industries/healthcare/our-insights/generative-ai-in-healthcare-adoption-trends-and-whats-next
[10] https://www.healthtech360.it/strategie-globali-per-la-salute-digitale/liste-attesa-sanita-digitale-tecnologie/
[11] https://www.kingsfund.org.uk/insight-and-analysis/reports/health-inequalities-nhs-waiting-lists

gestione delle liste più sostenibile nel lungo termine, orientata non solo all'efficienza, ma anche alla riduzione delle disuguaglianze strutturali.

Per la prima volta, inoltre, un modello di intelligenza artificiale generativa è stato applicato all'intero archivio di dati sanitari di una popolazione nazionale. Il modello, chiamato *Foresight*[12], è stato sviluppato per prevedere ospedalizzazioni, infarti e centinaia di altre condizioni cliniche, ed è stato addestrato su dati anonimizzati provenienti da 57 milioni di pazienti del Servizio Sanitario Nazionale inglese (NHS).

Una versione precedente di Foresight era stata addestrata sui dati sanitari di circa 1,5 milioni di persone a Londra, dimostrando buone capacità nel prevedere gli esiti clinici futuri sulla base della storia medica individuale. Il modello integra dati provenienti da diverse fonti: cartelle ospedaliere, vaccinazioni, visite dal medico di base e registri nazionali dei decessi. L'attuale versione è stata addestrata su eventi medici registrati tra il 2018 e il 2022, per un totale di circa 10 miliardi di voci.

Cresce anche in Italia l'interesse per l'integrazione dell'intelligenza artificiale nei processi decisionali del sistema sanitario, la Regione Liguria, per esempio, ha avviato un progetto innovativo denominato #Reg4IA[13], che utilizza l'intelligenza artificiale per ottimizzare la gestione delle liste d'attesa sanitarie. Questo progetto è stato selezionato dal Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei ministri come progetto pilota nazionale e ha ricevuto un finanziamento di 6,5 milioni di euro. Il progetto prevede l'implementazione di algoritmi predittivi e adattativi capaci di analizzare in tempo reale la domanda e l'offerta di prestazioni sanitarie, ottimizzando l'allocazione delle risorse e personalizzando i percorsi di cura per i pazienti. L'obiettivo è ridurre i tempi di attesa e migliorare l'efficienza del sistema sanitario.

La Liguria è capofila di questa iniziativa, che coinvolge anche altre regioni italiane, tra cui Piemonte, Sicilia, Lazio, Calabria, Molise, Basilicata e la Provincia Autonoma di Trento. Le attività operative saranno avviate nei prossimi mesi, con l'obiettivo di completare il progetto entro la fine del 2026.

Infine, la *drug discovery* è sicuramente un altro ambito in cui l'intelligenza artificiale, specie quella generativa, può esprimere il suo massimo potenziale: dalla progettazione di nuovi composti alla valutazione dell'efficacia e della sicurezza dei medicinali, fino alla selezione dei partecipanti alla sperimentazione clinica. Si stima[14] che tale tecnologia possa infatti generare da $60 a $110 miliardi all'anno di valore economico per le industrie farmaceutiche e dei prodotti medicali, in gran parte perché può aumentare la produttività accelerando il processo di identificazione dei composti per possibili nuovi farmaci, accelerare lo sviluppo e i processi di approvazione e migliorare il modo in cui i medicinali vengono commercializzati. Diverse sono ormai le società biotech che stanno conducendo studi clinici approvati dalla Food and Drug Administration (FDA) su trattamenti antitumorali progettati utilizzando modelli di intelligenza artificiale generativa[15].

[12] *https://www.nature.com/articles/d41586-025-01422-3*

[13] *https://www.regione.liguria.it/cgr/item/42886-progetto-liguria-vince-intelligenza-artificiale.html*

[14] *https://www.mckinsey.com/industries/life-sciences/our-insights/generative-ai-in-the-pharmaceutical-industry-moving-from-hype-to-reality#/*

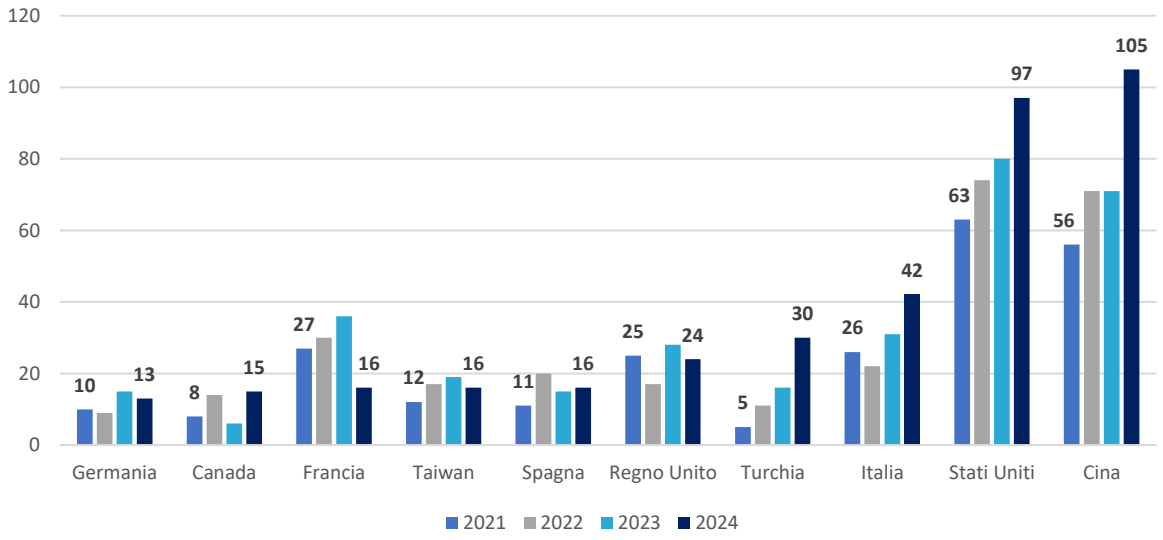
[15] *OECD, INITIAL POLICY CONSIDERATIONS FOR GENERATIVE ARTIFICIAL INTELLIGENCE (2023)*

A livello globale, gli studi clinici basati sull'intelligenza artificiale sono aumentati notevolmente. L'Italia con 42 studi nel 2024 si colloca sul podio, in terza posizione dietro Cina e Stati Uniti per numero di studi condotti utilizzando modelli di IA

Difatti, l'utilizzo dell'IA nel campo della ricerca clinica è sempre più frequente e sono ormai tantissimi i ricercatori a livello mondiale che cercano di sviluppare metodologie innovative basate su modelli IA per la diagnosi di numerose patologie. Secondo recenti dati della Stanford University[16], a livello globale, gli studi clinici basati sull'intelligenza artificiale sono aumentati notevolmente e tra i principali poli di studio in materia figura anche l'Italia: con 42 studi nel 2024 il nostro Paese si colloca in terza posizione globale dietro Cina e Stati Uniti per numero di studi condotti utilizzando modelli di IA (Fig. 2.3).

Fig. 2.3: Numero di studi clinici basati su IA, per area geografica

Fonte: Stanford University (2025)



Box 2: l'applicazione dell'IA nella lotta al cancro

Recentemente, alcuni ricercatori provenienti dalla Daffodil University in Bangladesh, dalla Charles Darwin University, dall'Università di Calgary e dall'Australian Catholic University hanno collaborato per sviluppare un nuovo modello di IA chiamato ECgMPL[17], che ha raggiunto una precisione del 99,26% nella diagnosi del cancro dell'endometrio, grazie ad un'analisi minuziosa delle immagini istopatologiche (ossia immagini microscopiche di tessuti utilizzate nell'analisi delle malattie). Il modello è stato poi testato su ulteriori dataset di immagini istopatologiche e anche in tal caso ha prodotto risultati straordinari: ad esempio

[16] *https://hai-production.s3.amazonaws.com/files/hai_ai_index_report_2025.pdf*

[17] *https://www.sciencedirect.com/science/article/pii/S2666990025000059#:~:text=ECgMLP%20offers%20a%20novel%20approach%20for%20automated%20diagnosis,achieves%2099.26%20%25%20accuracy%2C%20surpassing%20prior%20diagnostic%20techniques.*

per il cancro colorettale ha raggiunto una precisione del 98,57%, per il cancro al seno del 92,20% e per il cancro orale una precisione del 97,34%. Dunque, si tratta di una tecnologia che potrebbe presto migliorare le tempistiche e l'accuratezza delle diagnosi e potenzialmente salvare molte vite. E come questa ce ne sono ormai diverse.

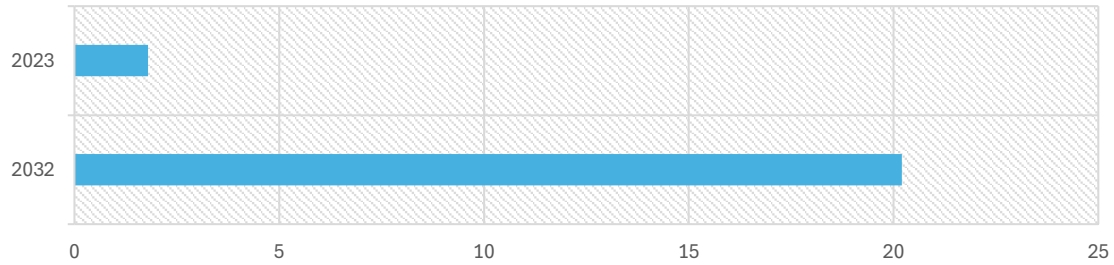
Un'altra importante novità è stata presentata lo scorso marzo, quando il comitato per i medicinali per uso umano (CHMP) dell'EMA ha emesso il primo Qualification Opinion (QO) su una metodologia di sviluppo innovativa basata sull'intelligenza artificiale. Lo strumento, chiamato AIM-NASH, aiuta i patologi ad analizzare le scansioni bioptiche epatiche per identificare la gravità della MASH (steatoepatite associata a disfunzione metabolica; precedentemente nota come steatoepatite non alcolica NASH) negli studi clinici[18].

Il crescente interesse nei confronti dell'IA da parte del mondo sanitario trova conferma anche nei dati di mercato. Secondo alcune stime[19], emerge che il valore dell'IA generativa si è attestato a $1,8 miliardi nel 2023 e si prevede raggiungerà i $20,2 miliardi entro la fine del 2032 con un tasso di crescita medio annuo (CAGR) del +33,2% nel periodo 2024-2032 (Fig. 2.4).

A trainare principalmente tale mercato sono le applicazioni nel campo della scoperta e sviluppo dei farmaci e nel segmento di analisi e diagnostica delle immagini mediche – dove l'IA generativa ha raggiunto un volume di ricavi di $655,4 milioni di dollari nel 2023.

Fig. 2.4: Il valore dell'IA generativa nel mercato sanitario globale (miliardi di $)

Fonte: Global Market Insights (2024)



1.1.1. Applicazioni di IA nelle strutture sanitarie in Italia

Numerosi sono, dunque, i vantaggi offerti da queste tecnologie e tante sono ormai le strutture sanitarie che si affidano ad esse. Anche in Italia[20] non mancano casi interessanti di utilizzo dell'intelligenza artificiale in sanità.

L'Università Campus Bio-Medico di Roma, ad esempio, è in prima linea con la sua unità di ricerca in *"Intelligent Health Technology"*, in sperimentazioni che includono l'IA generativa nello studio delle malattie rare. Un ulteriore esempio riguarda l'Ospedale Universitario Sant'Andrea di Roma in cui, da giugno 2022, viene utilizzato un software che identifica autonomamente le fratture che potrebbero sfuggire all'occhio umano, specialmente alla fine di un turno. Ogni immagine che arriva al pronto soccorso viene inviata a un sistema esterno di machine learning, che la elabora ed

[18] https://www.ema.europa.eu/en/news/ema-qualifies-first-artificial-intelligence-tool-diagnose-inflammatory-liver-disease-mash-biopsy-samples
[19] https://www.gminsights.com/industry-analysis/generative-ai-in-healthcare-market
[20] https://romebusinessschool.com/wp-content/uploads/2024/07/RBS_Report-2024_Limpatto-dellIntelligenza-Artificiale-in-Italia.pdf

in due minuti indica se c'è o meno una frattura, grazie ad un algoritmo addestrato precedentemente su un vasto dataset di vari tipi di fratture. Si tratta di una prima lettura che il radiologo deve poi confermare. Pertanto, la tecnologia supporta il radiologo, non lo sostituisce. Sempre a Roma, al Policlinico Gemelli, è stato sviluppato il *Generator Heart Failure DataMart*, una piattaforma digitale che integra e combina una grande quantità di dati e informazioni di fonte e contenuto eterogeneo (consulti cardiologici, misurazione eco-cardiografiche, farmaci assunti, esami di laboratorio, diagnosi cliniche standard, ricoveri, eventi in urgenza, diari infermieristici, contatti familiari e sociali) per progettare e addestrare dei modelli predittivi a più parametri allo scopo di individuare in anticipo la re-ospedalizzazione del paziente dopo l'ultima dimissione ospedaliera per scompenso cardiaco.

All'IRCCS Policlinico di Sant'Orsola, l'intelligenza artificiale supporta le attività di diagnosi precoce di noduli ai polmoni. Funziona incrociando in tempo reale i dati della TAC e le immagini della radiologia fluoroscopica. Con queste informazioni il Body Vision Lung System ricostruisce una immagine tridimensionale della realtà che non sarebbe possibile visualizzare altrimenti. Riproduce fedelmente una broncoscopia e indirizza i medici che la utilizzano, come un piccolo e sofisticato "navigatore" intelligente, così da arrivare in posti dove non sarebbe stato possibile arrivare con la normale navigazione e scovare precocemente anche le tracce meno visibili di noduli polmonari periferici. Questi sarebbero infatti difficilmente evidenziabili con gli attuali dispositivi disponibili, anche i più recenti come il broncoscopio ultrasottile o le minisonde ecografiche radiali.

Lo strumento consente un incremento della capacità diagnostica di circa il 10% che, unità al 70% già registrato con i metodi in uso, consentirà una capacità di far diagnosi precise fino a circa l'80%[21].

L'Università Aldo Moro e il Politecnico di Bari hanno invece sviluppato un algoritmo di intelligenza artificiale in grado di rilevare cambiamenti patologici nelle immagini di risonanza magnetica associati alla malattia di Alzheimer già nella fase di lieve declino cognitivo. Questa fase è critica, poiché le alterazioni non sono ancora visibili clinicamente, ma è proprio il momento in cui i trattamenti sperimentali possono avere maggiore efficacia. Tale modello, invece, offre spiegazioni dettagliate, evidenziando i distretti anatomici rilevanti nella diagnosi dell'Alzheimer e rendendo il processo decisionale più trasparente e comprensibile.

Anche il San Raffaele di Milano è in prima linea nell'uso dell'Intelligenza Artificiale per predire l'Alzheimer. Inoltre, un recente studio[22], condotto dal Consiglio Nazionale delle Ricerche (CNR) in collaborazione con l'Università di Firenze e l'Azienda Ospedaliera Universitaria Careggi, rappresenta un importante passo avanti nell'applicazione dell'apprendimento automatico per l'individuazione precoce dell'Alzheimer. La ricerca, pubblicata sul Journal of the Franklin Institute, è caratterizzata dall'utilizzo innovativo di metodi di apprendimento automatico topologico applicati ai dati di spettroscopia Raman. Questo approccio consente di rilevare alterazioni biochimiche associate alla malattia di Alzheimer con un'accuratezza maggiore rispetto ai risultati precedenti[23].

---

[21] *https://www.aosp.bo.it/it/content/l%E2%80%99intelligenza-artificiale-supporta-le-attivit%C3%A0-di-diagnosi-precoce-di-noduli-ai-polmoni#:~:text=All%E2%80%99IRCCS%20Policlinico%20di%20Sant%E2%80%99Orsola%20l%E2%80%99intelligenza%20artificiale%20supporta%20le,della%20TAC%20e%20le%20immagini%20della%20radiologia%20fluoroscopica.*

[22] *Conti, F., Banchelli, M., Bessi, V., Cecchi, C., Chiti, F., Colantonio, S., ... & Matteini, P. (2024). Harnessing topological machine learning in Raman spectroscopy: Perspectives for Alzheimer's disease detection via cerebrospinal fluid analysis. Journal of the Franklin Institute, 361(18), 107249.*

[23] *https://www.healthtech360.it/salute-digitale/intelligenza-artificiale/intelligenza-artificiale-sanita-esempi-studi-ricerche/#:~:text=Intelligenza%20Artificiale%20in%20Sanit%C3%A0%3A%20esempi%2C%20sperimentazioni%20e%20casi,pancreas%3A%20il%20progetto%20dell%E2%80%99Ospedale%20Cardarelli%20...%20Altri%20elementi*

Box 3: In Liguria un progetto pilota di IA per abbattere le liste d'attesa

Cresce anche in Italia l'interesse per l'integrazione dell'intelligenza artificiale nei processi decisionali del sistema sanitario, la Regione Liguria, per esempio, ha avviato un progetto innovativo denominato #Reg4IA[24], che utilizza l'intelligenza artificiale per ottimizzare la gestione delle liste d'attesa sanitarie.

Questo progetto è stato selezionato dal Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei ministri come progetto pilota nazionale e ha ricevuto un finanziamento di €6,5 milioni. Il progetto prevede l'implementazione di algoritmi predittivi e adattativi capaci di analizzare in tempo reale la domanda e l'offerta di prestazioni sanitarie, ottimizzando l'allocazione delle risorse e personalizzando i percorsi di cura per i pazienti. L'obiettivo è ridurre i tempi di attesa e migliorare l'efficienza del sistema sanitario.

La Liguria è capofila di questa iniziativa, che coinvolge anche altre regioni italiane, tra cui Piemonte, Sicilia, Lazio, Calabria, Molise, Basilicata e la Provincia Autonoma di Trento. Le attività operative saranno avviate nei prossimi mesi, con l'obiettivo di completare il progetto entro la fine del 2026.

1.2. Implicazioni etiche e principali ostacoli dell'IA in sanità

L'impiego e la diffusione dei dati e dell'intelligenza artificiale nel settore sanitario comporta una serie di effetti positivi, che intessano sia il personale sanitario, sia i pazienti ma in generale il sistema nel suo complesso. Sebbene le tante potenzialità, l'IA pone però anche una serie di rischi. Uno dei principali è il potenziale bias negli algoritmi. I pregiudizi (o bias) dell'intelligenza artificiale possono essere di genere, di natura razziale, culturale e il loro impatto sulla società può essere veramente dannoso, incrementando le disuguaglianze esistenti e le violazioni dei diritti fondamentali. Ad esempio, uno studio[25] pubblicato su Science ha scoperto che un algoritmo di previsione del rischio sanitario era basato su pregiudizi razziali, il che ha portato i pazienti neri ad avere una gestione delle cure meno adeguata e non in grado di rispondere ai reali bisogni di queste persone.

Altri rischi, specie dell'IA generativa, si riferiscono alla propensione di tali modelli di fornire informazioni errate o completamente inventate e farle passare come fatti reali. Questi rischi, che in gergo tecnico vengono chiamati "allucinazioni", costituiscono un serio problema in ambito sanitario e non solo.

Al di là di questi rischi più specifici, vi sono poi quelli relativi alla violazione della privacy, ai rischi informatici, nonché - specie in ambito sanitario - alla responsabilità dei processi decisionali elaborati con l'IA. Quando le decisioni mediche basate sugli algoritmi di IA danneggiano gli individui, i processi di responsabilità dovrebbero identificare chiaramente chi ha causato il danno. Tuttavia, alcune caratteristiche delle tecnologie di intelligenza artificiale, tra cui la loro "opacità", la dipendenza dall'input umano, l'interazione, la discrezione, la scalabilità, la capacità di generare intuizioni nascoste e la complessità del software, rendono difficile attribuire chiaramente le

[24] *https://www.regione.liguria.it/cgr/item/42886-progetto-liguria-vince-intelligenza-artificiale.html*
[25] *https://www.scientificamerican.com/article/racial-bias-found-in-a-major-health-care-risk-algorithm/*

responsabilità e pertanto si tratta di una sfida in continua evoluzione che rimane incerta nelle leggi della maggior parte dei paesi[26].

Box 4: I 6 principi etici dell'OMS per l'uso dell'IA in sanità

L'OMS ha pubblicato il documento "Ethics and governance of artificial intelligence for health. Guidance on large multi-modal models"[27] che individua sei principi etici che dovrebbero guidare lo sviluppo e l'impiego dell'IA in sanità.

Il primo principio è quello della protezione dell'autonomia degli esseri umani secondo il quale l'autonomia decisionale della macchina non deve pregiudicare quella umana. Nel contesto sanitario, ciò significa che gli esseri umani dovrebbero mantenere il pieno controllo del processo decisionale. Tale principio, ricalca l'approccio antropocentrico, spesso richiamato quando si parla di intelligenza artificiale, secondo cui le nuove tecnologie devono essere progettate ed adoperate per estendere o aumentare le capacità intellettuali e le abilità sociali umane, e non per comprometterle o entrare in conflitto con esse.

Il secondo principio riguarda, invece, la promozione del benessere delle persone, della loro sicurezza e del pubblico interesse. Dunque, le tecnologie di intelligenza artificiale non dovrebbero danneggiare le persone. Al contrario, dovrebbero soddisfare i requisiti normativi in materia di sicurezza, accuratezza ed efficacia prima dell'implementazione e dovrebbero essere messe in atto misure per garantire il controllo e il miglioramento della qualità.

Secondo l'OMS è fondamentale, inoltre, la predisposizione di adeguate garanzie in materia di trasparenza, spiegabilità e comprensibilità dei sistemi di IA (terzo principio). Nel quarto principio OMS, viene suggerito, per evitare la diffusione della responsabilità, in cui "il problema di tutti diventa responsabilità di nessuno", un modello di responsabilità impeccabile ossia di "responsabilità collettiva", in cui tutti gli agenti coinvolti nello sviluppo e nell'implementazione di una tecnologia di IA sono ritenuti responsabili. Tale modello potrebbe incoraggiare tutti gli attori ad agire con integrità e ridurre al minimo i danni.

Gli ultimi due principi individuati dal gruppo di esperti dell'OMS si riferiscono infine alla garanzia dell'inclusione e dell'equità nello sviluppo e nell'uso di tali tecnologie e alla promozione di un IA sostenibile.

Dunque, il successo dell'integrazione di tale tecnologia in ambito sanitario dipende dalla capacità di saper controbilanciare i benefici con i possibili rischi. Proprio un recentissimo studio[28] dell'OCSE, condotto in collaborazione con l'Associazione Medica Mondiale (WMA), ha evidenziato che è fondamentale trovare un equilibrio tra innovazione e sicurezza per poter sfruttare le potenzialità dell'IA in sanità.

Secondo il sondaggio OCSE, il 72% delle associazioni mediche intervistate ritiene che i benefici dell'IA nel settore sanitario superino i rischi e credono fortemente che tali strumenti trasformeranno in modo significativo il campo della medicina, ma il 70% concorda anche sul fatto

[26] *Eurispes, Enpam, 3° Rapporto sulla Salute e sul Sistema Sanitario (2024)*
[27] *https://iris.who.int/bitstream/handle/10665/375579/9789240084759-eng.pdf?sequence=1*
[28] *https://www.oecd.org/en/publications/artificial-intelligence-and-the-health-workforce_9a31d8af-en.html*

che il ruolo dei medici rimarrà centrale. Tuttavia, la stragrande maggioranza (94%) ha espresso preoccupazione per le questioni etiche che possono derivare dalle applicazioni dell'IA nella pratica medica e il 71% ritiene che la responsabilità dei medici aumenterà a causa dell'uso di soluzioni di IA.

Pertanto, gli esperti sottolineano la necessità e l'importanza di coinvolgere i medici nella progettazione e nell'implementazione degli strumenti IA per garantire che rispondano alle esigenze del settore sanitario. Inoltre, questioni come qualità e interoperabilità dei dati, infrastrutture digitali obsolete, scarsa alfabetizzazione digitale nonché rischi legati alla violazione della privacy preoccupano molto le associazioni intervistate, le quali concordano sulla necessità di educare i medici sull'uso degli strumenti IA, sia a livello accademico che durante la carriera in modo da fare un uso responsabile di tali tecnologie. Dunque, un chiaro quadro normativo, politiche solide nonché formazione e coinvolgimento attivo dei professionisti sanitari sono gli ingredienti fondamentali per abilitare il futuro dell'IA nel settore sanitario e massimizzare i benefici.

Un chiaro quadro normativo, politiche solide nonché formazione e coinvolgimento attivo dei professionisti sanitari sono gli ingredienti fondamentali per abilitare il futuro dell'IA nel settore sanitario e massimizzare i benefici

Per favorire l'integrazione dell'intelligenza artificiale nel settore sanitario e beneficiare del suo potenziale, ci sarà bisogno di professionisti che svolgeranno ruoli "ibridi" basati sull'intersezione tra competenze mediche e informatiche. Più in generale, i medici e tutti gli operatori sanitari necessitano di un mix di alfabetizzazione digitale e pensiero critico fondamentale per poter utilizzare in modo responsabile tali tecnologie. Ai medici e agli altri operatori sanitari sarà sempre più spesso chiesto di dare una seconda opinione, la prima delle quali è stata ricavata da un algoritmo. Ciò richiederà che il medico abbia una comprensione di base di come funzionano queste applicazioni, sia in grado di comprendere i loro limiti e se sono state utilizzate in modo appropriato.

3. GOVERNANCE DEL DATO: NUOVE SFIDE E OPPORTUNITÀ

Man mano che la tecnologia diventa sempre più integrata nelle nostre vite, la governance dei dati nell'intelligenza artificiale e nel mondo dei dati sanitari assume un ruolo cruciale, soprattutto in termini di sicurezza, tanto per i pazienti quanto per l'intera infrastruttura della pubblica e privata alle prese con la gestione di dati così sensibili. Come dimostrato nei paragrafi precedenti, le istituzioni e le aziende fanno sempre più affidamento sull'AI per elaborare enormi quantità di dati, ma questo comporta anche rischi significativi, come violazioni e usi impropri, ma soprattutto, come vedremo, rischi di cybersicurezza e violazione delle normative. Per questi motivi è sempre più necessaria una governance efficace dei dati che fornisca un quadro di riferimento per gestire le informazioni in modo responsabile, garantendo al contempo solide misure di sicurezza.

La governance dei dati nell'IA è fondamentale per garantire un uso responsabile e sicuro delle informazioni. Si basa su un insieme di politiche e linee guida che regolano la raccolta, l'analisi e la condivisione dei dati, assicurando il rispetto delle normative e rafforzando la fiducia di clienti e stakeholder. In questo contesto, la trasparenza gioca un ruolo chiave, permettendo alle organizzazioni di spiegare chiaramente come i sistemi di IA utilizzano i dati, aumentando la fiducia degli utenti e aiutando a individuare potenziali rischi. Un altro pilastro fondamentale in questo contesto è la qualità dei dati, che garantisce che le informazioni siano accurate, affidabili e protette da accessi non autorizzati o manipolazioni. Infine, ma non meno importante, la conformità normativa assicura che le aziende operino nel rispetto di leggi come il GDPR o il CCPA, prevenendo sanzioni e tutelando la propria reputazione.

3.1. Cybersecurity in sanità

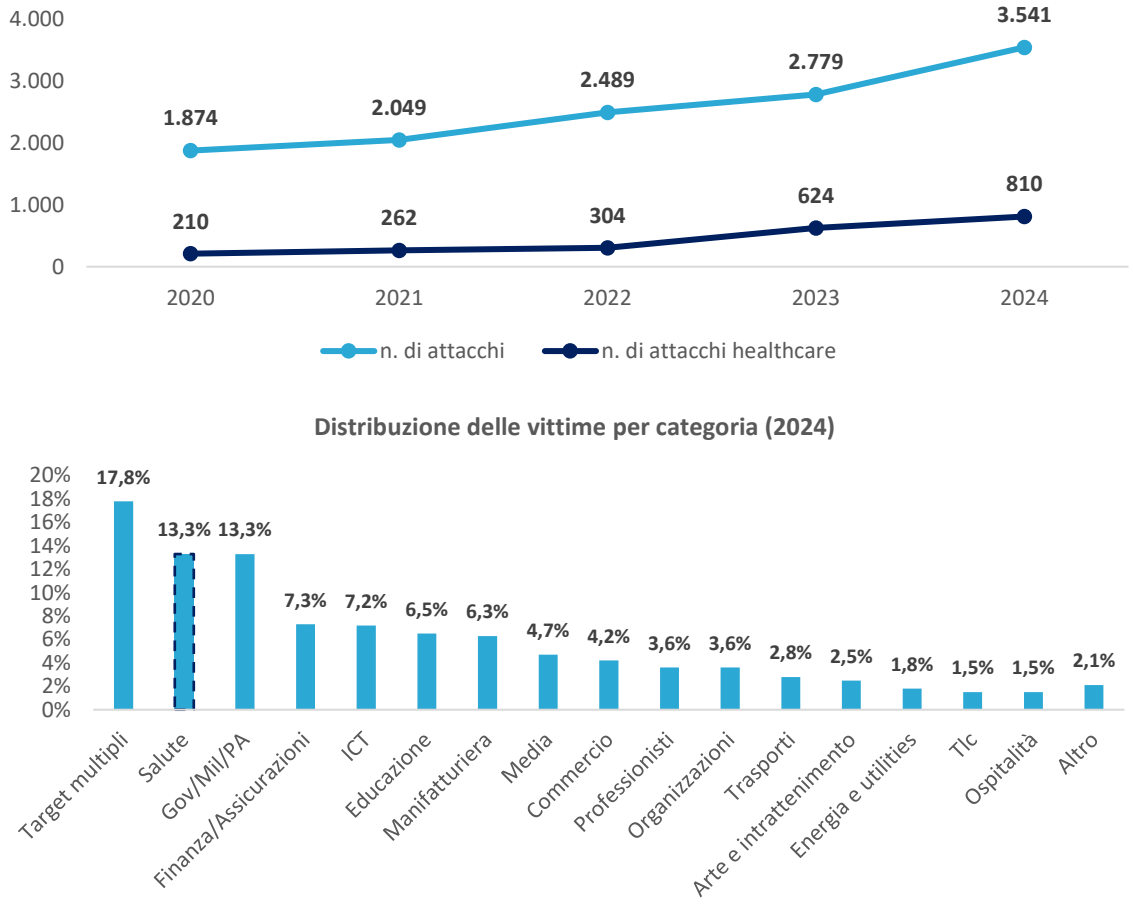
Tuttavia, anche con una solida governance dei dati e l'adozione di pratiche orientate alla trasparenza, qualità e conformità, le aziende - in particolare nel settore sanitario - restano esposte a minacce crescenti. La digitalizzazione e l'intensivo uso dell'intelligenza artificiale rendono sempre più vulnerabili le infrastrutture critiche, attirando l'interesse dei cybercriminali. Il settore sanitario, custode di enormi quantità di dati sensibili, è diventato uno dei bersagli principali, con un numero di attacchi informatici in continua crescita su scala globale.

Nel solo 2024 sono stati registrati 810 incidenti informatici di pubblico dominio, segnando un aumento del +30% rispetto all'anno precedente e un incremento di quattro volte rispetto al 2020 e 2021. La quasi totalità di questi attacchi (806 su 810) è stata motivata da attività cybercriminali, mentre solo pochi casi (4 in totale) sono riconducibili a hacktivism o cyber espionage.

Il continente americano continua a essere il più colpito, rappresentando il 78% degli attacchi, sebbene con una leggera diminuzione rispetto all'80% del 2023. Parallelamente, si registra un aumento degli incidenti in Europa, che passa dal 12% al 14%, e in Asia, che cresce dal 4% al 5%, mentre Oceania e Africa restano stabili con percentuali rispettivamente del 2% e dell'1%.

Fig.3.1: Andamento degli attacchi informatici per anno (2020-2024) e distribuzione delle vittime per categoria (2024)

Fonte: Rapporto Clusit



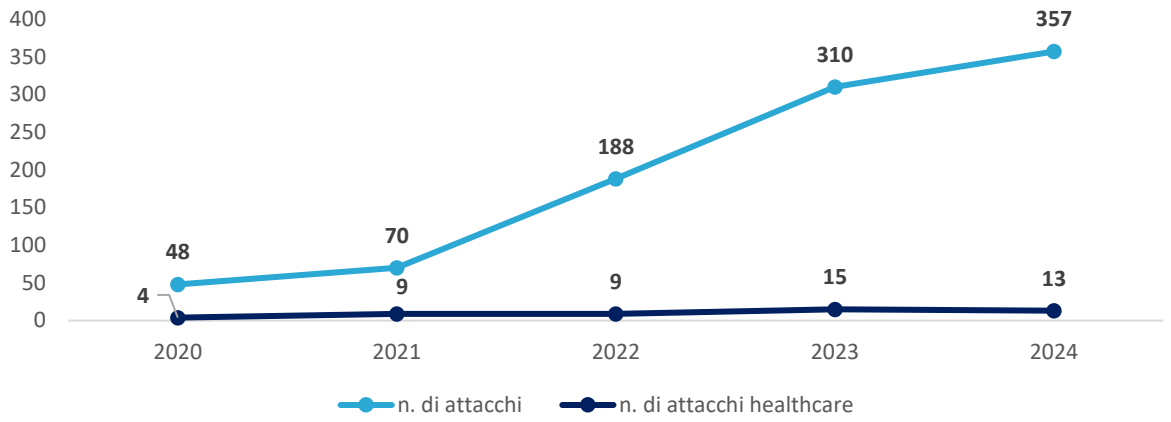
In Italia, gli attacchi informatici contro il settore sanitario mostrano una lieve diminuzione rispetto all'anno precedente, passando da 15 a 13 incidenti di pubblico dominio, rappresentando il 3% degli attacchi registrati nel Paese. A differenza del 2023, il Cybercrime emerge come unica motivazione alla base di questi attacchi, mentre scompaiono altre categorie come hacktivism ed espionage/sabotage, ancora presenti a livello globale.

In Italia, gli attacchi informatici contro il settore sanitario mostrano una lieve diminuzione rispetto all'anno precedente, rappresentando il 3% degli attacchi registrati nel Paese.

Le tecniche di attacco continuano a privilegiare l'uso del Malware, responsabile del 54% degli incidenti, con il ransomware che si conferma il metodo preferito dai cybercriminali per colpire le strutture sanitarie nazionali. Tuttavia, sebbene il ransomware rimanga la principale minaccia, il suo utilizzo è in calo rispetto all'anno precedente, mentre cresce significativamente lo sfruttamento delle vulnerabilità della supply chain, che in Italia registra un aumento senza precedenti del 31%. Questo dato evidenzia come la catena di approvvigionamento rappresenti un punto critico sempre più esposto agli attacchi, specialmente nel settore sanitario, rendendolo un obiettivo strategico per le attività malevole.

Fig.3.2: Distribuzione degli incidenti cyber in Italia (2020-2024)

Fonte: Rapporto Clusit



Il crescente livello di sofisticazione degli attacchi informatici, unito alla rapida evoluzione tecnologica e all'elevato valore dei dati sanitari, impone un rafforzamento costante delle strategie di cybersecurity. La sola governance dei dati, per quanto fondamentale, non è più sufficiente: è necessario un approccio integrato che combini prevenzione, monitoraggio continuo e risposta tempestiva agli incidenti. Investire nella sicurezza dell'intera filiera - inclusa la supply chain - diventa cruciale per proteggere non solo le infrastrutture digitali, ma anche la fiducia dei cittadini e la qualità dei servizi sanitari, solo così sarà possibile affrontare con efficacia le minacce di oggi e prepararsi a quelle di domani. Allo stesso tempo la data governance europea e nazionale si arricchisce sempre di più di elementi innovativi, che cercano di regolamentare tutti gli aspetti del dominio digitale sanitario, dall'IA generativa alla sicurezza del dato sensibile, passando per la protezione di queste preziose informazioni con nuove norme sulla cybersicurezza.

Box 5: L'UE risponde agli attacchi cyber in sanità: lo *European action plan on the cybersecurity of hospitals and healthcare providers*

Il settore sanitario europeo è sempre più nel mirino dei cybercriminali, negli ultimi anni, gli attacchi informatici sono infatti cresciuti in modo significativo, soprattutto a causa della crescente digitalizzazione dei servizi sanitari. Sebbene questa trasformazione offra grandi opportunità di crescita e innovazione, espone al tempo stesso il sistema sanitario a nuove vulnerabilità.

In particolare, nel 2024 il ransomware ha rappresentato il 60% degli incidenti di cybersicurezza nel settore, con conseguenze gravi o gravissime nel 90% dei casi, come ritardi nelle cure, difficoltà di accesso ai servizi di emergenza e rischi per la sicurezza dei pazienti. Il valore elevato dei dati sanitari rende il settore particolarmente appetibile, con l'83% degli attacchi motivato da interessi economici.

Considerata la situazione, diventa fondamentale disporre di un'infrastruttura digitale sicura e resiliente, anche per garantire la piena operatività dello EHDS. La Presidente della Commissione Europea, Ursula von der Leyen, ha sottolineato la necessità di rafforzare la resilienza della sanità europea nelle *Linee Guida Politiche 2024–2029.* Sebbene la sicurezza resti una competenza nazionale, il settore sanitario è tra quelli critici previsti dalla Direttiva

NIS2. Le minacce informatiche non conoscono confini: per questo la cooperazione tra Stati membri è essenziale, così come la condivisione di pratiche e strategie comuni.

L'UE ha quindi avviato un *Piano d'Azione per rafforzare la cybersicurezza nel settore sanitario*. Tra le misure principali: l'istituzione di un *Centro europeo di supporto alla cybersicurezza* gestito da ENISA, che fornirà strumenti e linee guida pratiche per prevenzione, preparazione e risposta agli attacchi. Sarà promosso anche l'uso del Portafoglio di Identità Digitale UE, che ridurrà la dipendenza da password deboli e introdurrà un sistema armonizzato di autenticazione elettronica sicura per gli operatori sanitari, obbligatorio entro la fine del 2027.

Il Piano prevede inoltre test di preparazione e valutazioni della maturità della cybersicurezza, coordinati dal Centro Europeo di Competenza per la Cybersicurezza (ECCC), e l'introduzione dei Cybersecurity Vouchers per sostenere economicamente gli ospedali più piccoli nell'adozione di misure adeguate, anche attraverso fondi UE come il FESR e il *Digital Europe Programme*.

Particolare attenzione è rivolta anche alle catene di fornitura ICT, che includono dispositivi medici e sistemi connessi, attraverso il *Cyber Resilience Act*, che stabilisce requisiti di sicurezza per tutto il ciclo di vita dei prodotti. ENISA svilupperà linee guida per la gestione sicura del cloud e dei fornitori esterni, promuovendo un approccio "Security by Default and by Design".

La condivisione di informazioni sugli incidenti e le vulnerabilità tra gli Stati membri, tramite i CSIRTs, sarà potenziata per rafforzare i sistemi di allerta precoce e migliorare l'analisi delle minacce, in collaborazione con Europol e gli ISACs. In caso di gravi emergenze, l'UE potrà intervenire attraverso la Cybersecurity Reserve.

Infine, il successo del piano dipenderà dall'impegno concreto degli Stati membri, che dovrebbero istituire Centri Nazionali di Supporto alla Cybersicurezza e sviluppare piani d'azione nazionali per identificare rischi e misure prioritarie. La condivisione delle risorse tra strutture sanitarie, un maggiore investimento nella sicurezza informatica e la cooperazione tra settore pubblico e privato - anche tramite un nuovo Comitato Consultivo sulla Cybersicurezza Sanitaria - saranno elementi chiave per garantire la protezione dei dati, la continuità dei servizi e la fiducia dei cittadini.

3.2. La sfida della Sanità Digitale e della sua sicurezza: formazione di operatori sanitari e cittadini

3.2.1. Cybersicurezza e la sicurezza del dato sanitario

Queste innovazioni, unite a livelli disomogenei di consapevolezza informatica tra il personale ospedaliero e i dirigenti, rappresentano una sfida complessa per la protezione dei sistemi sanitari. Ad esempio, secondo l'Eurobarometro 2024[29] sulle competenze informatiche, solo il 25% delle

[29] https://europa.eu/eurobarometer/surveys/detail/3176?utm

aziende nei settori della sanità, dell'istruzione e dell'assistenza sociale ha fornito formazione o attività di sensibilizzazione sulla cybersecurity nell'ultimo anno, rendendo necessario promuovere una cultura della sicurezza informatica tra i professionisti sanitari in prima linea. L'uso di postazioni di lavoro condivise, una gestione inadeguata delle autenticazioni, l'impiego di supporti rimovibili e i frequenti cambi di personale sono ulteriori fattori di vulnerabilità per la sicurezza informatica degli operatori sanitari. In molti casi, i servizi IT e OT sono almeno in parte esternalizzati. Difatti, l'Eurobarometro 2024 ha rilevato che il settore sanitario, dell'istruzione e dell'assistenza sociale è quello che esternalizza di più la cybersecurity, con il 57% delle aziende che delega almeno alcune attività di sicurezza informatica.

Inoltre, vi è una crescente tendenza alla migrazione verso il cloud, spinta dalla necessità di soluzioni scalabili per l'archiviazione e la gestione dei dati, dall'efficienza dei costi, dal miglioramento della collaborazione e dal supporto per tecnologie avanzate come l'IA e l'Internet of Medical Things, basti pensare che nel 2022, il 58% delle organizzazioni sanitarie ha utilizzato una piattaforma sanitaria digitale basata su cloud. Tuttavia, se da un lato questa transizione offre vantaggi significativi, dall'altro introduce nuovi rischi che richiedono decisioni informate sulla scelta dei fornitori e sulla configurazione sicura delle infrastrutture.

L'uso continuato di strumenti obsoleti e sistemi legacy, le risorse limitate per prevenire o rispondere agli incidenti e le lacune nella maturità della cybersecurity derivano spesso da carenze di finanziamenti. Gli ospedali devono costantemente trovare un equilibrio tra l'aggiornamento e la sicurezza delle infrastrutture digitali e altri investimenti essenziali per migliorare l'assistenza ai pazienti, come l'assunzione di medici e operatori sanitari, l'implementazione di nuovi metodi diagnostici e terapeutici e l'acquisto di dispositivi medici. Secondo un rapporto di IANS Research[30] pubblicato nel marzo 2025 le aziende sanitarie destinano in media circa il 15% del loro budget IT alla sicurezza informatica. Tuttavia, un'analisi più dettagliata rivela che il 56% delle organizzazioni sanitarie dedica meno del 10% del proprio budget IT alla cybersecurity[31], evidenziando una sotto-prioritizzazione della sicurezza digitale in un settore altamente sensibile.

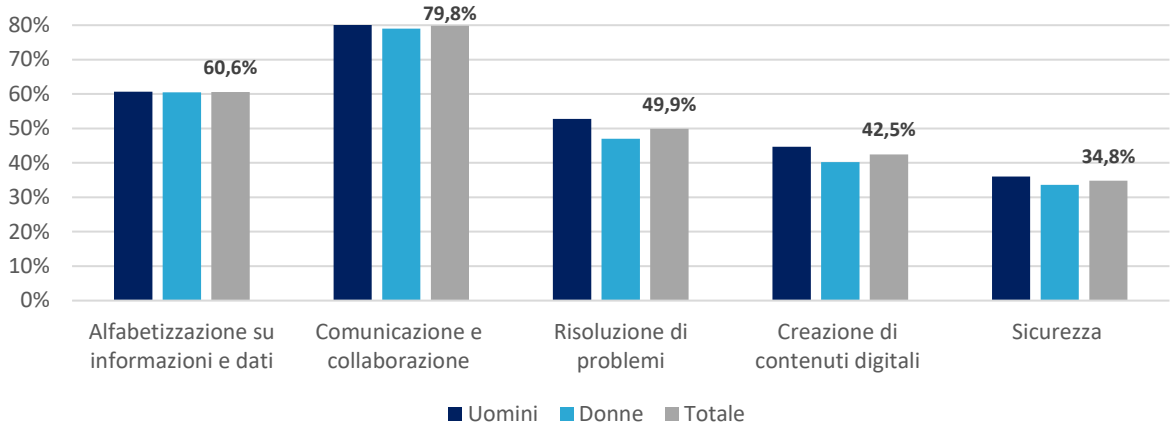
Il 56% delle organizzazioni sanitarie dedica meno del 10% del proprio budget IT alla cybersecurity

Andando però oltre la sicurezza informatica, uno degli elementi strategici da cui passa la lotta al cybercrimine è certamente il livello di competenze in campo digitale dei cittadini. L'ultima rilevazione Eurostat (2023) ci dà modo di ragionare sulla situazione in essere nel campo in questione, restituendoci un quadro certamente non confortante né per l'Europa, né tantomeno per l'Italia; il dato relativo alla popolazione italiana complessiva con competenze almeno di base si attesta al 45,8% contro una media europea del 55,6%. Se poi approfondiamo i cinque domini del digitale emerge chiaramente come il lato sicurezza rimanga il settore in cui le competenze elevate sono presenti in minoranza, per solo il 34,8% degli individui tra i 16 e i 74 anni (Fig.3.3).

[30] *https://www.iansresearch.com/resources/all-blogs/post/security-blog/2025/03/27/healthcare-security-comp-and-budgets-decline--access-key-report-data-and-trends*
[31] *https://www.dialoghealth.com/post/healthcare-cybersecurity-statistics*

Fig.3.3: Individui tra 16-74 anni in Italia con competenze elevate nei 5 domini del digitale (2023)

Fonte: Istat



Nonostante tutto, l'Italia si distingue come il paese con la crescita più significativa tra le principali nazioni europee, negli ultimi 5 anni, in termini di digitalizzazione complessiva dell'economia e società. Subito dopo l'Italia, tra i paesi con le migliori performance, troviamo Germania, Irlanda, Francia e Polonia, che completano la *top five* dell'UE.

Negli ultimi anni, l'Unione Europea ha infatti investito circa €205 miliardi per sostenere la *Digital Decade*, sfruttando appieno le proprie risorse di finanziamento. La trasformazione digitale è una delle principali priorità politiche della Commissione, considerata essenziale per la prosperità economica, la ripresa e la resilienza dell'UE. Secondo il rapporto della Commissione Europea[32] nel biennio 2021-2022, l'UE ha destinato €131,9 miliardi (incluso il NextGenerationEU) alla transizione digitale, pari a circa il 17,4% del bilancio complessivo dell'Unione, di questi €15,223 miliardi (11,54%) sono stati destinati alle misure per il target e-health. In particolare, i Piani Nazionali di Ripresa e Resilienza (PNRR), che combinano investimenti e riforme per €651,7 miliardi di euro, rappresentano una fonte chiave di finanziamento per la digitalizzazione a livello nazionale, integrando i grandi progetti strategici europei finanziati attraverso il Programma Europa Digitale (DIGITAL), Horizon Europe e il Connecting Europe Facility (CEF).

Emergono con sempre maggiore evidenza due tendenze parallele: da un lato, una crescente attenzione alla centralità del dato e alla necessità di proteggerlo, e in particolare in Italia una grande accelerazione nella creazione di un ecosistema digitale del dato sanitario sicuro ed efficiente; dall'altro, persistenti criticità legate alla carenza di professionisti adeguatamente formati nel settore. A queste si aggiunge, come approfondiremo nel paragrafo successivo, la limitata preparazione del personale sanitario nell'utilizzo degli strumenti digitali. Un gap che si sta cercando di colmare anche grazie alle risorse messe a disposizione dal PNRR, con l'obiettivo di promuovere una trasformazione digitale più sicura ed efficace.

3.2.2. *La formazione per le competenze digitali del personale sanitario*

In un contesto digitale così ampio la formazione degli operatori si conferma un elemento chiave per un utilizzo efficace del sistema e per la sua diffusione tra i pazienti. Per i professionisti sanitari

[32] *https://digital-strategy.ec.europa.eu/it/factpages/digital-decade-2024-report-country-fact-pages*

in formazione, l'integrazione di competenze digitali nei percorsi universitari è ormai imprescindibile. L'attuale generazione di studenti può essere definita "nativa digitale", essendo cresciuta in un'epoca caratterizzata dalla diffusione della tecnologia e dalla costante connettività, tuttavia, la familiarità con gli strumenti digitali non si traduce automaticamente nella capacità di utilizzarli in ambito sanitario, specialmente per la prevenzione, la diagnosi e la cura dei pazienti. Per questo motivo, è fondamentale collaborare con le università affinché i corsi di laurea, sia quelli a ciclo unico in medicina sia quelli triennali per le professioni sanitarie, includano una formazione specifica sulle competenze digitali. Tuttavia, ancora più emergenziale appare la realtà dei laureati con competenze di cybersicurezza e più in particolare quelle dedicate alla protezione del SSN.

Secondo i dati più recenti nell'anno solare 2023 i laureati in corsi universitari esplicitamente dedicati alla *sicurezza informatica* sono stati 333, pari allo 0,09% del totale dei laureati italiani, comprendendo un totale di 14 corsi dedicati in tutto il panorama formativo. Anche in questo dato mostriamo un ritardo rispetto ad altri paesi europei, infatti con solo lo 0,1% di laureati nel field *"Database and network design and administration"* ci posizioniamo diciannovesimi in Europa[33].

L'osservatorio Cyber di I-Com fornisce dati ancora più dettagliati e interessanti: per l'anno accademico 2024/2025, su un totale di 99 Università statali e non statali (private, straniere e telematiche) riconosciute dal MIUR, si registra la presenza di 774 corsi di formazione universitaria sulla cybersicurezza, in notevole crescita rispetto ai 520 individuati a inizio 2024, il che fa segnare un incremento di circa il 48% su base annua[34]. Tra questi, si osservano 323 insegnamenti singoli all'interno di corsi di laurea magistrale, 158 insegnamenti singoli all'interno delle lauree triennali, 86 progetti di ricerca in dottorati, 69 corsi singoli in master di II livello e 54 in master di I livello, a fronte di 31 lauree magistrali, 30 master, 16 corsi all'interno di dottorati di ricerca, 11 corsi singoli all'interno di master di I e II livello e 7 lauree triennali interamente dedicate alla cybersecurity. Interessante notare come le lauree specifiche sul tema della cibersicurezza abbiano raggiunto le 38 unità. Tuttavia, queste appaiono ancora relativamente poche e quasi tutte collocate, salvo rare eccezioni (7), nel ciclo magistrale.

Circoscrivendo ulteriormente questi dati, osserviamo come i corsi dedicati al cyber nel mondo sanitario siano un numero esiguo, solamente due gestiti direttamente dalle facoltà di medicina, di cui uno è un percorso di dottorato. Si contano interamente 27 insegnamenti singoli in 26 percorsi differenti distribuiti in tutto il territorio nazionale, che si dividono in corsi ingegneristici e altri dedicati alla sanità digitale e alla protezione del dato.

I professionisti della salute si trovano spesso ad affrontare carenze infrastrutturali, limitazioni di tempo e competenze digitali inadeguate, fattori che compromettono l'utilizzo efficiente di strumenti come i sistemi di cartella clinica elettronica e le piattaforme di telemedicina. Ciononostante, diversi studi evidenziano come il personale maggiormente predisposto all'adozione di nuove tecnologie sia quello con una formazione più recente, di livello elevato e appartenente a fasce d'età più giovani. Al contrario, nel nostro contesto attuale, il personale sanitario tende a trovarsi più vicino all'età pensionabile che alla fase post-universitaria, riflettendo una dinamica generazionale meno favorevole alla rapida integrazione di innovazioni.

[33] *https://www.talentsventure.com/osservatorio/*

[34] *I corsi analizzati includono sia insegnamenti singoli all'interno di corsi di laurea più generici ("offerta formativa non specializzata"), sia corsi di laurea specifici sul tema, insieme a Master e Progetti di ricerca in Dottorato ("offerta formativa specializzata"). Esempio: un insegnamento in Cybersecurity all'interno della LM in Informatica.*

Box 6: Fattori che incidono sull'adozione di competenze digitali nel personale sanitario

Uno studio pubblicato nel 2025 sugli operatori sanitari del Regno Unito[35] dimostra come i livelli di istruzione, il contesto lavorativo, le esperienze professionali e l'utilizzo medio delle soluzioni digitali, sia sul lavoro che nel tempo libero, influenzano in modo diverso le varie dimensioni della competenza digitale in ambito sanitario, tenendo conto di età e genere.

Il titolo di studio è emerso come un fattore significativo: i professionisti sanitari con un titolo post-laurea hanno mostrato una probabilità circa sei volte maggiore di possedere una competenza elevata nella consulenza remota centrata sulla persona e circa quattro volte maggiore nell'ambito delle tecnologie ICT, rispetto a chi possiede solo un diploma o un'istruzione generale. Anche i laureati triennali risultano avere una probabilità da quattro a cinque volte superiore di mostrare competenze elevate nell'uso delle soluzioni digitali nel contesto lavorativo, nelle ICT e nella valutazione delle tecnologie digitali.

Inoltre, lavorare in contesti non ospedalieri riduce la probabilità di essere associati a competenze elevate nell'uso delle ICT; al contrario, un maggior numero di anni di esperienza professionale è correlato a una maggiore competenza etica nell'utilizzo delle soluzioni digitali. Tuttavia, un utilizzo più intenso delle tecnologie digitali sia sul lavoro che nel tempo libero è risultato associato a una minore probabilità di possedere competenze elevate nella valutazione critica delle soluzioni digitali.

Risultati analoghi emergono anche dallo studio pubblicato nel 2023 in riferimento al contesto finlandese[36]: fattori come l'età, l'anno di conseguimento del titolo di studio più alto, l'ambiente clinico in cui si opera, il percorso professionale, la quantità di attività svolta con i pazienti, l'esperienza in ruoli di supporto gestionale, le pratiche organizzative a sostegno dello sviluppo delle competenze digitali, così come l'adozione delle tecnologie e l'influenza esercitata dai colleghi, risultano tutti significativamente associati a un livello più elevato di competenza nella sanità digitale.

Per quel che riguarda l'Italia, la formazione digitale del personale sanitario è riconosciuta come una leva strategica per la digitalizzazione del sistema sanitario, in linea con gli obiettivi del PNRR. In particolare, la Missione 6 – Salute, tramite l'investimento 2.2, ha stanziato €740 milioni per migliorare le competenze tecniche, professionali, digitali e manageriali del personale sanitario. Tra questi, €18 milioni sono destinati a corsi specifici per 4.500 professionisti del SSN da formare entro il 2026.

Accanto al piano nazionale, le Regioni hanno un ruolo chiave nell'attuazione di progetti locali, sostenuti dai fondi PNRR, che integrano interventi infrastrutturali e formativi. Il Decreto del 29 marzo 2023 ha affidato all'AGENAS il coordinamento delle attività e la ripartizione delle risorse tra Regioni e Province Autonome. Anche l'investimento 1.3.1, relativo all'adozione e uso del Fascicolo Sanitario Elettronico (FSE), include iniziative formative, sia tecniche che generali, per promuovere l'utilizzo diffuso del FSE da parte del personale.

Tra le esperienze regionali più rilevanti:

[35] *https://www.sciencedirect.com/science/article/pii/S0897189725000242*
[36] *https://pubmed.ncbi.nlm.nih.gov/38323687/*

- Toscana ha investito €35 milioni in formazione digitale per operatori sanitari, MMG e pediatri, all'interno di un più ampio piano di innovazione tecnologica da €125 milioni con focus su telemedicina, COT e FSE.
- In Sardegna, il progetto MEDS, promosso da ARES, coinvolgerà circa 29.000 operatori sanitari in percorsi formativi su sanità digitale, interoperabilità, FSE e sicurezza informatica, contribuendo alla trasformazione digitale regionale.
- Emilia-Romagna, insieme a Marche e Puglia, partecipa a una sperimentazione europea con il modello del "Digital Upskilling", che prevede la creazione di profili digitali personalizzati, l'autovalutazione delle competenze e percorsi formativi su misura, con l'obiettivo di creare un modello formativo replicabile a livello nazionale[37].
- In Piemonte[38], sono stati avviati corsi rivolti a 10.000 operatori sanitari, con moduli e-learning e seminari su FSE, sicurezza dei dati, privacy e gestione dei consensi. Un'attenzione particolare è riservata all'integrazione delle cartelle cliniche di MMG, pediatri e specialisti.

Parallelamente, il Dipartimento per la Trasformazione Digitale, con il Ministero della Salute, AGENAS e ProMIS, ha lanciato il contest "Formazione e Comunicazione Innovativa", per premiare i progetti regionali più efficaci nella formazione digitale legata al FSE 2.0. L'iniziativa promuove soluzioni replicabili, sostenibili e orientate alla collaborazione interregionale.

Il Fascicolo Sanitario Elettronico, oltre a essere uno strumento per la gestione dei dati clinici, si configura così come un motore di innovazione e diffusione della cultura digitale nella sanità. Un esempio significativo è Ania, il chatbot sviluppato dalla Regione Campania, che guida i cittadini nell'uso del FSE 2.0, fornendo supporto su consultazione dei documenti, gestione dei consensi e problemi di accesso, 24 ore su 24.

In sintesi, il potenziamento delle competenze digitali del personale sanitario è un elemento centrale nella trasformazione del SSN: non solo per garantire un uso efficace delle tecnologie, ma anche per costruire una sanità più innovativa, accessibile e resiliente.

[37] *Strategia Generale di Accrescimento delle Competenze Digitali DIGITAL SKILLS TO INCREASE QUALITY AND RESILIENCE OF THE HEALTH SYSTEM IN ITALY - REFORM/SC2022/047, Project funded by the European Union via the Technical Support Instrument, managed by the European Commission Directorate General for Structural Reform Support, 2023*

[38] https://www.regione.piemonte.it/web/temi/sanita/strumenti-operativi/fse-20-competenze-digitali-degli-operatori

4. CONCLUSIONI E RACCOMANDAZIONI DI POLICY

Le evidenze contenute nel presente documento confermano come l'intelligenza artificiale e la valorizzazione del dato sanitario rappresentino leve strategiche per garantire sostenibilità, equità e qualità al Servizio Sanitario Nazionale. L'integrazione del digitale nella sanità italiana - dal Fascicolo Sanitario Elettronico all'Ecosistema dei Dati Sanitari e allo Spazio Europeo dei Dati Sanitari - apre scenari promettenti, ma pone anche sfide cruciali che non possono più essere rimandate.

Anzitutto, emerge la necessità di rafforzare la governance della sanità digitale. Oggi, l'adozione frammentata di strumenti come il FSE e l'uso disomogeneo dell'IA tra regioni rischiano di accentuare il divario digitale e informativo tra cittadini, anziché ridurlo. Serve un **piano pluriennale** nazionale, con obiettivi misurabili, governance unica e fondi dedicati, capace di integrare livelli regionali e nazionali e promuovere piena interoperabilità dei sistemi. La definizione di indicatori uniformi per monitorare l'adozione del FSE e l'impatto delle tecnologie IA su esiti clinici, efficienza e accessibilità dovrebbe essere prioritaria. Inoltre, nonostante l'Italia occupi una posizione di rilievo a livello globale nei trial clinici che utilizzano l'intelligenza artificiale (3° posto nel mondo), dal confronto emerge un dato significativo: il nostro Paese si colloca solo al 13° posto per quanto riguarda lo sviluppo di brevetti. Questo evidenzia ancora una volta l'eccellenza e l'avanguardia della ricerca e del know-how italiano, che però faticano a tradursi in innovazione concretamente realizzata. Le cause principali risiedono nei **bassi investimenti in ricerca e sviluppo, nelle difficoltà strutturali e nell'eccessiva complessità burocratica**, sia a livello nazionale che europeo. Questi ostacoli spesso impediscono di valorizzare pienamente i risultati della sperimentazione, spingendo ricercatori e brevetti a trasferirsi in Paesi con normative più snelle e ambienti economici più favorevoli.

Fondamentale sarà anche **investire nella cultura digitale del personale sanitario**. Nonostante l'evidente impatto positivo delle soluzioni IA su efficienza e qualità delle cure, la formazione in materia di dati, cybersecurity e intelligenza artificiale è ancora carente nei percorsi accademici e di aggiornamento professionale. **È necessario integrare moduli formativi su IA e sicurezza del dato nei corsi universitari sanitari e non solo**; parallelamente, va rafforzata la **figura del *"medico data-literate"***, capace di integrare competenze cliniche e digitali, e promossa l'adozione di ruoli ibridi tra sanità e informatica.

Inoltre, la sicurezza informatica deve diventare priorità assoluta. A fronte di un numero crescente di attacchi cyber - con l'Italia tra i Paesi più vulnerabili - appare non più sostenibile che il 56% delle organizzazioni sanitarie destini meno del 10% del proprio budget IT alla cybersecurity. Occorre **sostenere e rafforzare la spesa per la sicurezza digitale, supportare l'adozione di sistemi resilienti nelle strutture più fragili, e rafforzare le misure di protezione della supply chain sanitaria**. Anche la recente strategia europea, con il Cybersecurity Action Plan per il settore sanitario, deve trovare un'attuazione rapida e coordinata a livello nazionale.

È altresì prioritario garantire l'accesso equo all'innovazione. **Gli strumenti di sanità digitale devono diventare alleati nella riduzione delle disuguaglianze, non amplificatori del divario**. La bassa adozione del FSE nel Mezzogiorno e tra le fasce sociali più vulnerabili richiede interventi mirati di alfabetizzazione digitale, comunicazione istituzionale e co-design delle piattaforme, con il coinvolgimento delle comunità locali. I medici di medicina generale e i pediatri di libera scelta rivestono un ruolo centrale nel rafforzare la fiducia dei cittadini nei confronti dei nuovi strumenti

digitali. In un contesto in cui la consapevolezza e il coinvolgimento dell'utente finale restano ancora limitati, il loro contributo è fondamentale per favorire l'adozione delle tecnologie; a conferma di ciò, l'utilizzo del Fascicolo Sanitario Elettronico non ha registrato significativi progressi rispetto al 2024, segnalando chiaramente come questo ambito rappresenti una delle priorità su cui intervenire nei prossimi anni.

Sarà anche fondamentale garantire la copertura dell'intero spettro che va dalla ricerca all'innovazione, includendo tutte le fasi della catena di valore, fino al deployment su larga scala, partendo dalla creazione di prototipi alla loro concreta immissione sul mercato. Le **soluzioni** devono essere pensate fin dall'inizio per essere **scalabili**: non ha senso sviluppare tecnologie fini a sé stesse, ma è necessario che **portino a reali miglioramenti per il sistema e per i pazienti**. Inoltre, tali soluzioni devono essere progettate secondo i principi del **secure by design e by default**, garantendo la sicurezza del paziente come risultato intrinseco del sistema, e non come un'aggiunta successiva. In questo contesto, è cruciale definire con chiarezza ruoli e responsabilità lungo l'intero processo di sviluppo, implementazione e utilizzo.

A livello normativo, è essenziale **valorizzare l'uso secondario del dato sanitario in modo sicuro, trasparente ed etico.** L'EDS e lo EHDS costituiscono infrastrutture essenziali per la medicina del futuro: è necessario attuarli garantendo al contempo la tutela della privacy, il diritto all'opposizione (opt-out) e la partecipazione attiva della comunità scientifica, garantendo allo stesso tempo sicurezza del dato e progresso. Serve **un'alleanza strategica tra pubblico e privato per sviluppare algoritmi predittivi e strumenti di supporto decisionale capaci di rispondere a bisogni reali, ridurre le liste di attesa e promuovere la medicina personalizzata**. Infine, l'avanzamento del Fascicolo Sanitario Elettronico rispetto alla roadmap europea consente all'Italia di posizionarsi in prima linea rispetto alle trasformazioni in atto. Grazie alla natura volontaria del sistema di partecipazione, il nostro Paese ha l'opportunità di integrarsi e contribuire all'European Health Data Space già prima delle scadenze mostrate nel documento, anticipando il percorso a partire dal 2026, anno in cui si concluderanno i piani di attuazione del PNRR per il FSE.

È importante, dunque, che le politiche sanitarie riconoscano la trasformazione digitale e l'intelligenza artificiale come investimenti strategici, non come costi. È auspicabile che il prossimo ciclo di programmazione sanitaria consideri la sanità digitale, assieme alla prevenzione, come ambito prioritario per la sostenibilità del SSN. Una quota strutturale del Fondo Sanitario Nazionale dovrebbe essere vincolata a innovazione digitale, sicurezza informatica e formazione. In parallelo, le nuove regole europee di bilancio dovrebbero escludere tali investimenti dal calcolo del deficit, riconoscendoli come fattori abilitanti della resilienza sanitaria. Infatti, sia la digitalizzazione del sistema sanitario che la prevenzione delle cronicità contribuiscono a una presa in carico più tempestiva dei pazienti, con effetti positivi su più fronti: da un lato, permettono cure più rapide ed efficaci per i cittadini; dall'altro, rendono più efficienti i processi del Servizio Sanitario Nazionale, semplificando le procedure e liberando tempo prezioso per il personale sanitario.