

DECRETO

N. 1176 del 01/07/2026

ADOTTATO

dal DIRETTORE GENERALE Dott. Luigi CAJAZZO
nominato con D.G.R. n.XII/1638 del 21/12/2023

**OGGETTO: APPROVAZIONE DEL DOCUMENTO DI INDIRIZZO PER
L'IMPIEGO DI INTELLIGENZA ARTIFICIALE IN SANITÀ – ASST
DEGLI SPEDALI CIVILI DI BRESCIA.**

**SU PROPOSTA DEL RESPONSABILE DEL PROCEDIMENTO:
Dott. Gian Luca FORNARI**

Acquisiti i pareri del
DIRETTORE AMMINISTRATIVO
DIRETTORE SANITARIO
DIRETTORE SOCIO SANITARIO

Dott. Fabio AGRÒ
Dott.a Frida FAGANDINI
Dott. Enrico BURATO



IL DIRETTORE GENERALE

Premesso che lo sviluppo delle tecnologie dell'Intelligenza Artificiale sta determinando trasformazioni profonde nei sistemi sanitari, con particolare impatto sui processi in ambito diagnostico, prognostico, terapeutico, gestionale e di ricerca biomedica, pur mantenendo sempre il Medico al centro del processo decisionale;

Considerato che l'utilizzo delle applicazioni di Intelligenza Artificiale comporta significative opportunità in termini di miglioramento del governo e dell'efficienza operativa in ambito ospedaliero, ma ha anche rilevanti implicazioni etiche, giuridiche e organizzative che richiedono una valutazione attenta e multidisciplinare;

Richiamati:

- il Regolamento (UE) n.2024/1689 del Parlamento Europeo e del Consiglio del 13/06/2024 che stabilisce regole armonizzate sull'Intelligenza Artificiale (c.d. Regolamento sull'Intelligenza Artificiale);
- il Regolamento (UE) n.2022/868 del Parlamento Europeo e del Consiglio del 30/05/2022 relativo alla governance europea dei dati, che modifica il Regolamento (UE) n.2018/1724 (c.d. Regolamento sulla governance dei dati);
- la Decisione (UE) n.2022/2481 del Parlamento Europeo e del Consiglio del 14/12/2022 che istituisce il programma strategico per il decennio digitale 2030;
- la Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'Intelligenza Artificiale (direttiva sulla responsabilità da Intelligenza Artificiale), COM/2022/496 final;
- il Documento "Ethics and governance of artificial intelligence for health: Guidance on large multi-modal models", elaborato dall'Organizzazione Mondiale della Sanità nell'anno 2024;
- la Dichiarazione Europea sui Diritti e i Principi Digitali per il decennio digitale n.2023/C 23/01;
- la Strategia Italiana per l'Intelligenza Artificiale 2024-2026 redatta dall'Agenzia per l'Italia Digitale (AGID);
- la Legge n.132/2025 in materia di Intelligenza Artificiale;

Richiamato, altresì, il Decreto n.1104 del 11/06/2025, con il quale è stato istituito il Comitato di Indirizzo per il governo delle applicazioni di Intelligenza Artificiale nei processi assistenziali e gestionali dell'ASST degli Spedali Civili di Brescia, organismo propositivo e consultivo, costituito da esperti di provata capacità ed esperienza dell'Azienda e dell'Università degli Studi di Brescia nell'ambito dell'Intelligenza Artificiale (IA);

Dato atto che il Comitato ha redatto e approvato, nella seduta del 20/05/2026, il "Documento di Indirizzo per l'Impiego di Intelligenza Artificiale in Sanità", successivamente trasmesso, con nota del 09/06/2026, al Direttore Generale dell'ASST degli Spedali Civili di Brescia e al Magnifico Rettore dell'Università degli Studi di Brescia;

Rilevato che tale Documento:

- rappresenta l'esito di un percorso basato su un confronto e un approfondimento multidisciplinare che ha coinvolto i membri appartenenti sia a questa Azienda che all'Università degli Studi di Brescia;



ASST Spedali Civili

- ha l'obiettivo di definire principi, criteri e indicazioni operative per un utilizzo appropriato, sicuro ed efficace delle soluzioni di Intelligenza Artificiale nei processi clinici, di ricerca, gestionali e organizzativi all'interno dell'Azienda, nel pieno rispetto degli aspetti etici e normativi;

Considerato che la regolamentazione delle nuove tecnologie legate all'Intelligenza Artificiale assume una funzione strategica nell'ottica del governo responsabile di questa transizione tecnologica, orientandone lo sviluppo verso finalità compatibili con la tutela dei diritti fondamentali, la sicurezza, la trasparenza e l'interesse collettivo;

Ritenuto, pertanto, di procedere all'approvazione del "Documento di Indirizzo per l'Impiego di Intelligenza Artificiale in Sanità", come da Allegato A (composto da n.81 pagine), unito al presente provvedimento a costituirne parte integrante, così strutturato:

- Documento di Indirizzo per l'Impiego di Intelligenza Artificiale in Sanità;
- Allegato 1: Panoramica strutturata dell'uso clinico dell'IA in Medicina;
- Allegato 2: Panoramica strutturata sulle applicazioni di IA nella Ricerca
- Allegato 3: IA Enti Regolatori, Privacy e Cybersecurity;
- Allegato 4: Survey sull'impiego di sistemi IA all'interno di ASST degli Spedali Civili di Brescia;
- Allegato 5: Manuale operativo per la gestione delle richieste relative ai sistemi di Intelligenza Artificiale;

Dato atto, altresì, che il presente Documento verrà pubblicato sul sito istituzionale aziendale;

Preso atto che il Direttore della S.C. Affari Generali e Legali Dott. Gian Luca FORNARI, Responsabile del procedimento, proponente il presente provvedimento, ne ha dichiarato la completezza, la regolarità tecnica e le legittimità;

Acquisito il parere del Direttore Amministrativo,

Acquisito il parere del Direttore Sanitario,

Acquisito il parere del Direttore Sociosanitario,

DECRETA

a) di procedere, per le motivazioni esposte in pressa, all'approvazione del Documento di Indirizzo per l'Impiego di Intelligenza Artificiale in Sanità", come da Allegato A (composto da n.81 pagine), unito al presente provvedimento a costituirne parte integrante, così strutturato:

- Documento di Indirizzo per l'Impiego di Intelligenza Artificiale in Sanità;
- Allegato 1: Panoramica strutturata dell'uso clinico dell'IA in Medicina;
- Allegato 2: Panoramica strutturata sulle applicazioni di IA nella Ricerca
- Allegato 3: IA Enti Regolatori, Privacy e Cybersecurity;
- Allegato 4: Survey sull'impiego di sistemi IA all'interno di ASST degli Spedali Civili di Brescia;
- Allegato 5: Manuale operativo per la gestione delle richieste relative ai sistemi di Intelligenza Artificiale;

b) di dare mandato al Comitato di Indirizzo di proporre momenti formativi per i dipendenti, di concerto con la S.C. Gestione e Sviluppo Risorse Umane, ad integrazione del Piano Formativo Aziendale anno 2026 approvato con Decreto n.1156 del 29/06/2026;

c) di procedere alla pubblicazione del presente Documento sul sito istituzionale aziendale;

d) di dare atto che dal presente provvedimento non discendono oneri per l'Azienda;



- e) di disporre la trasmissione del presente provvedimento al Collegio Sindacale, ai sensi dell'art.3-ter del D.Lgs. n.502/1992 e s.m.i. e dell'art.12, comma 14 della L.R. n.33/2009, così come modificata dalla L.R. n.23/2015;
- f) di pubblicare il presente provvedimento nell'Albo on-line sul sito istituzionale dell'Azienda, ai sensi dell'art.32 della Legge n.69/2009, dell'art.17, comma 6 della L.R. n.33/2009, così come modificata dalla L.R. n.23/2015.

~~~~~

Firmato digitalmente

Il Direttore Generale  
ASST degli Spedali Civili di Brescia  
Dott. Luigi Cajazzo

Versione n. 1 del 09/06/2026

ALL. A

# Documento di Indirizzo per l'Impiego di Intelligenza Artificiale in Sanità

*A cura del Comitato di Indirizzo per l'impiego dell'Intelligenza Artificiale in Sanità- ASST-  
Spedali Civili di Brescia e Università di Brescia*

## Sommario

|                                                                                 |    |
|---------------------------------------------------------------------------------|----|
| Acronimi.....                                                                   | 1  |
| Introduzione.....                                                               | 3  |
| Cenni storico-filosofici.....                                                   | 5  |
| Il Sistema Intelligenza Artificiale (IA) .....                                  | 9  |
| IA in Medicina .....                                                            | 13 |
| IA e Ricerca Clinica Applicata.....                                             | 13 |
| IA e Ricerca Traslazionale .....                                                | 15 |
| Intelligenza artificiale e modelli organizzativi sanitari .....                 | 18 |
| Considerazioni Giuridiche.....                                                  | 21 |
| Considerazioni Giuridiche in contesto clinico .....                             | 21 |
| AI Act (Reg. UE 1689/2024) .....                                                | 21 |
| MDR (Reg. UE 745/2017): Profili di concordanza e discordanza con l'AI Act ..... | 25 |
| Principali fonti normative nazionali .....                                      | 27 |
| Indicazioni e linee guida .....                                                 | 28 |
| Considerazioni Giuridiche e ricerca biomedica .....                             | 34 |
| Quadro normativo di riferimento .....                                           | 34 |
| Specificità: Dati sintetici e protezione dei dati personali .....               | 35 |
| Considerazioni Economiche .....                                                 | 37 |
| IA e Sistemi Organizzativi e Gestionali in Sanità .....                         | 41 |
| Approvvigionamento tecnologia AI .....                                          | 43 |
| Formazione Digitale Continua .....                                              | 46 |
| Autori .....                                                                    | 48 |

## Acronimi

IA: Intelligenza Artificiale

ADMET: Assorbimento, Distribuzione, Metabolismo, Escrezione, Tossicità

AIFA: Agenzia Italiana del Farmaco

AGENAS: Agenzia Nazionale per i Servizi Sanitari Regionali

AGI: Intelligenza Artificiale Generale (*Artificial General Intelligence*)

ANI: Intelligenza Artificiale Ristretta (*Artificial Narrow Intelligence*)

ASI: Superintelligenza Artificiale

AUC-ROC: area sotto la curva ROC (Area Under the Curve ROC)

CDSS: *Clinical Decision Support Systems*

CMC: *Chemistry, Manufacturing and Controls*

CSR: *Corporate Social Responsibility*

CTD: *Common Technical Document*

DPIA: impatto sulla protezione dei dati (*Data Protection Impact Assessment*)

DPO: *Data Protection Officer*

ECM: Educazione Continua in Medicina

EMA: European Medicines Agency

FDA: *Food and Drug Administration*

GAN: Reti Generative Avversarie (*Generative Adversarial Networks*)

GDPR: *General Data Protection Regulation*

GVHD: Malattia del trapianto contro l'ospite (*Graft Versus Host Disease*)

HB: *Hospital Based*

HTA: *Health Technology Assessment*

ISS: Istituto Superiore di Sanità

LLM: *Large Language Models*

MDR: *Medical Device Regulation*

MDAI: *Medical Device Artificial Intelligence*

MISE: Ministero dello Sviluppo Economico

NLP: Natural Language Processing

NRM: mortalità non correlata alla recidiva (*Non-Relapse Mortality*)

PACS: *Picture Archiving and Communication System*

PNRR: Piano Nazionale di Ripresa e Resilienza

PSM: *Propensity Score Matching*

QSAR: *Quantitative Structure-Activity Relationship*

SaMD: *Software as a Medical Device*

SAP: Sistema Informativo Gestionale

SDO: Schede di Dimissione Ospedaliera

TCO: *Total Cost of Ownership*

VAE: *Variational Autoencoders*

VBP: *Value Based Procurement*

## Introduzione

Negli ultimi anni l'intelligenza artificiale (IA) ha assunto un ruolo sempre più rilevante nel processo di evoluzione del settore sanitario.

La transizione digitale e la crescente disponibilità di dati clinici, genetici, biomolecolari, radiologici e istopatologici hanno reso non solo possibile, ma anche necessario, lo sviluppo di sistemi intelligenti capaci di supportare il personale sanitario in campo diagnostico, prognostico, gestionale e della ricerca, concorrendo al potenziamento degli standard qualitativi delle cure, dell'efficienza organizzativa e, in ultima istanza, della stessa sostenibilità del sistema sanitario.

Affinché l'elevato potenziale di tali tecnologie si traduca in benefici concreti, è imprescindibile assicurare i massimi livelli di qualità, governance e interoperabilità delle procedure mediante l'adozione di standard rigorosi e di sistemi di tracciabilità volti a certificare l'affidabilità, la sicurezza e la riproducibilità dei processi.

Risulta, pertanto, necessario strutturare un solido impianto di governance per l'impiego dell'IA in un ecosistema ad elevata complessità quale quello sanitario, un ambito in cui la centralità della componente clinica si interseca ineludibilmente con le determinanti gestionali e con i vincoli etici e regolatori.

In tale cornice, la protezione dei dati personali, la trasparenza algoritmica, la mitigazione dei bias e la piena aderenza al quadro normativo vigente devono essere integrati sin dalle fasi della progettazione. Parimenti, i modelli predittivi impongono una rigorosa validazione clinica, supportata primariamente da studi prospettici che comprovino l'efficacia ed il reale impatto sugli outcome di salute.

Sotto il profilo gestionale, è poi necessario valutare attentamente la sostenibilità organizzativa, analizzando l'impatto dell'IA non solo sui processi assistenziali ma anche sull'allocazione delle risorse disponibili, affinché l'innovazione tecnologica elevi gli standard delle cure prevenendo al contempo inefficienze e aggravii economici.

Infine, l'integrazione dell'IA nei percorsi di ricerca in ambito ospedaliero non rappresenta una mera opzione accessoria, bensì un asset strategico imprescindibile. Tale sinergia consente, infatti, di coniugare eccellenza

scientifica, innovazione dei modelli organizzativi e responsabilità etica, ponendo le basi per un sistema sanitario più competitivo, sostenibile e autenticamente centrato sui bisogni del paziente.

Alla luce delle premesse formulate, emerge, quindi, l'esigenza di adottare il presente *Documento di Indirizzo per l'Impiego di Intelligenza Artificiale in Sanità* quale fondamentale strumento istituzionale per orientare le scelte strategiche dell'ASST. Il testo si articola in una disamina multidisciplinare volta a comprendere come si è arrivati oggi all'IA, quali problemi etici-filosofici essa pone all'uomo e alla società; che cosa è e cosa non è l'IA dal punto di vista tecnico, o meglio, logico-matematico; quali sono le principali applicazioni nella medicina, sia clinica che di ricerca; quali sono le leggi e i regolamenti attuativi che ne regolano le applicazioni in ambito sanitario; quali le regole economiche che ne ottimizzano l'uso; e ultimo, ma non ultimo, il suo governo in un ambito sanitario complesso come quello di un ospedale, grande o piccolo che sia.

## Cenni storico-filosofici

Nel pioneristico articolo *Computing Machinery and Intelligence* (1950), l'informatico Alan Turing introduceva *l'imitation game* (o test di Turing), partendo da un interrogativo fondamentale:

“Se una macchina riesce a ingannare un interlocutore umano, attesta per ciò stesso di essere “intelligente” in quanto capace di comunicare una sequenza logicamente conseguenziale di concetti?”

Lo stesso Turing, tuttavia, tracciava una netta distinzione tra fenomeno ed entità intelligente (ovvero tra l'apparenza dell'intelligenza e la sua reale sussistenza); egli riteneva, infatti, che, pur raggiungendo tale scopo, l'algoritmo si sarebbe configurato essenzialmente come una sorta di “pappagallo ammaestrato”.

L'espressione “Intelligenza Artificiale” fu proposta per la prima volta cinque anni più tardi, all'interno di un documento (proposta di Dartmouth) stilato il 31 agosto del 1955 da un gruppo di giovani ricercatori guidati dall'informatico John McCarthy<sup>1</sup>. Tale testo, presentato l'anno dopo alla Conferenza di Dartmouth (Dartmouth Summer Research Project on Artificial Intelligence) presso il Dartmouth College di Hanover (New Hampshire), recitava in apertura:

“proponiamo di condurre uno studio di 2 mesi e 10 persone sull'intelligenza artificiale durante l'estate del 1956 al Dartmouth College di Hanover. Lo studio deve procedere sulla base della congettura che ogni aspetto dell'apprendimento o di qualsiasi altra caratteristica dell'intelligenza in linea di principio può essere descritto in modo così preciso da poter essere simulato da una macchina. Si cercherà come far sì che le macchine usino il linguaggio, formino astrazioni e concetti, risolvano tipi di problemi ora riservati agli esseri umani e migliorino la loro capacità di apprendimento.”

L'obiettivo originario consisteva nell'*ottenere dalle macchine prestazioni che, se compiute da esseri umani, sarebbero state definite «intelligenti»*. Il fine ultimo, pertanto, non risiedeva nella perfetta riproduzione dell'intelligenza umana, ma

---

<sup>1</sup> Il documento originale (13 pp.) datato 31 agosto 1955, ha le firme seguenti: J. McCarthy, Dartmouth College M. L. Minsky, Harvard University N. Rochester, I.B.M. Corporation C.E. Shannon, Bell Telephone Laboratories.

nell'abilitare le macchine alla risoluzione di problemi complessi assumendo quale parametro fondamentale l'intelligenza umana.

Nel 1959 l'informatico Arthur Samuel realizzò il giocatore di dama: l'intento, ancora una volta, non era replicare l'intelligenza umana, bensì fare in modo che il programma potesse autoperfezionarsi illimitatamente, giungendo a superare le capacità del suo stesso inventore. A tal fine, Samuel istruì la macchina a competere contro sé stessa, dimostrando l'assunto (ecco la nostra tesi) secondo cui un sistema capace di auto-apprendimento genera una potenza di calcolo inedita. Implementando una funzione matematica in grado di analizzare la scacchiera in ogni fase della partita e di selezionare la mossa con la più alta probabilità statistica di vittoria, Samuel inaugurò di fatto l'apprendimento automatico (*machine learning*), orientando la tecnologia verso l'autonomia del sistema.

L'assunzione dell'intelligenza umana quale parametro di riferimento poggia su un duplice fondamento: in primis, l'assunto filosofico di matrice hobbesiana secondo cui la ragione umana è essenzialmente calcolo; in secundis, l'evidenza che la ragione umana abbia dimostrato di essere l'intelligenza più abile nel dominare la realtà attraverso strategie computazionali supportate da linguaggi. Per ottenere un'intelligenza artificiale fondata su simili premesse, si è resa necessaria l'unione tra scienze matematiche-informatiche e discipline antropologiche-psicologiche.

L'IA manifesta, fin dai suoi albori, alcuni tratti caratteristici:

- essa ha carattere organico, relazionale, totalizzante;
- ha come fine l'accrescimento della capacità computazionale per la risoluzione autonoma di problemi complessi;
- non vuole imitare l'intelligenza umana, ma la assume come parametro di riferimento;
- opera una sintesi tra saperi e linguaggi tradizionali (ingegneria, logica, filosofia, neuroscienze, diritto) fondendoli in una unità che li trascende e la cui comprensione esige il superamento delle rigide divisioni disciplinari.

Perché è stato usato il termine intelligenza? Perché è ampio: tale concetto non si esaurisce nella razionalità, ma abbraccia uno spettro più vasto che include le

abilità percettive come la *visione artificiale*. Non definisce dunque una mente, ma un insieme di “capacità” nel senso chiarito sopra.

La nascita dell’IA rappresenta, pertanto, l’esito di un lunghissimo percorso di indagine filosofico e logico-matematico sui significati di mente, come unità di attività e passività, di ragione come calcolo, di limitatezza dei sistemi formali (teoremi di incompletezza di Gödel) o potenzialità non ancora comprese (funzionalismo di Hilary Putnam, esperimento della stanza cinese di John Searle, dibattito su IA forte e debole) fino a giungere all’odierna classificazione in Intelligenza Artificiale Ristretta (ANI - *Artificial Narrow Intelligence*), Intelligenza Artificiale Generale (AGI, *Artificial General Intelligence*), Superintelligenza Artificiale (ASI). In questo scenario di profonda trasformazione, la riflessione filosofica risulta direttamente coinvolta e chiamata in causa con il compito cruciale di guidare il nostro tempo attraverso le sfide etiche e sociali poste da questa rivoluzione tecnologica.

Nell’aprile 2018 gli Stati membri dell’Unione Europea hanno firmato una dichiarazione di cooperazione per lo sviluppo coordinato dell’Intelligenza Artificiale, muovendo dalla consapevolezza che:

- l’IA sta trasformando ogni settore produttivo, economico e sociale;
- Cina e USA stanno investendo massicciamente in IA;
- se l’Europa vuole essere competitiva deve cambiare paradigmi.

La Commissione Europea ha pubblicato due documenti (IA per l’Europa e Piano coordinato sull’IA) e istituito un gruppo di esperti per definire «gli orientamenti etici e le politiche di investimento sull’IA in Europa». Contestualmente, ogni Stato Membro è stato incaricato di sviluppare una strategia nazionale. In Italia il Ministero dello Sviluppo Economico (MISE) ha elaborato la Strategia Nazionale per lo sviluppo dell’IA (dicembre 2020), mettendo al centro l’esigenza di affrontare l’IA con approccio olistico.

Da allora si è diffusa progressivamente la consapevolezza che un sapere fatto di conoscenze e competenze meramente tecnologiche risulta inadeguato per governare i processi legati all’IA: è necessaria, di contro, una visione olistica e interdisciplinare, capace di rilevare implicazioni, prevedere scenari, approntare soluzioni efficaci.

Le parole-chiave che richiamano l'attenzione filosofica sono cinque: **intelligenza, artificiale, sistema, autonomia, indifferenza di fisico e virtuale (digitale).**

Nella definizione di IA del 29 marzo 2021 del Parlamento Europeo si ritrovano proprio le caratteristiche che ci sono parse da subito primarie: «L'Intelligenza Artificiale (IA) è l'abilità di una macchina di mostrare capacità umane quali il ragionamento, l'apprendimento, la pianificazione e la creatività. L'IA permette ai sistemi di capire il proprio ambiente, mettersi in relazione con quello che percepisce e risolvere problemi, e agire verso un obiettivo specifico.... I sistemi di IA sono capaci di adattare il proprio comportamento analizzando gli effetti delle azioni precedenti e lavorando in autonomia».

Il principio dell'autonomia sistemica viene ulteriormente sancito dall'*AI Act* del 2024, che inquadra l'IA quale «**sistema** basato su una macchina progettata per operare con livelli diversi di **autonomia** [...] che, per obiettivi espliciti o impliciti, inferisce dagli input ricevuti come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti **fisici o virtuali**».

**Il vero discrimine tecnologico che separa l'IA dalla non IA risiede, pertanto, proprio nella capacità di autonomia.** *Autonomia* è la parola decisiva. Dal punto di vista filosofico, essa rappresenta la massima espressione della potenza<sup>2</sup>, in quanto elimina i vincoli eteronomi che diluiscono il raggiungimento del fine.

Tuttavia, proprio questa capacità di operare al di fuori di un controllo diretto solleva delle questioni etiche: un'IA autonoma è, infatti, un'IA che non si controlla e ciò può rappresentare un pericolo per l'Umano, laddove l'Etica nasce e vive al fine di tutelare l'Umano.

Si presenta qui una questione di fondo: quale Umano? Esiste una natura in sé dell'Umano? La riflessione filosofica contemporanea suggerisce di abbandonare l'idea di una natura statica e immutabile delle cose (e dell'Umano): l'identità umana è una dimensione storicamente determinata, dinamica e soggetta ad essere costantemente plasmata e ridefinita dal progresso tecnologico e dall'innovazione.

---

<sup>2</sup> Si permette di rimandare a N. Cusano, *Automatos. Intelligenza Artificiale e Tecnica: la potenza è autonomia*, Mimesis, Milano-Udine 2025.

In questa prospettiva, viene meno la tradizionale supremazia della realtà fisica su quella virtuale. Prende così forma il processo di biologizzazione dell'artificiale e artificializzazione del biologico, verso una ibridazione delle due dimensioni, che in ambito medico si traduce in frontiere inedite: dagli ospedali nel Metaverso ai *Digital Twin*, dai percorsi di cura, diagnosi e terapia fino all'impiego dei chip cerebrali.

Nel contesto clinico, l'IA sta profondamente trasformando l'agire del Medico. Se da una parte affianca e guida, direttamente o indirettamente, il professionista nello svolgimento di una mole di lavoro sempre più consistente, dall'altra rischia di innescare una dinamica di subordinazione, rendendolo sempre più dipendente. Accanto alle enormi potenziali opportunità offerte dall'IA, è imperativo evidenziarne i rischi: il farsi sempre più passivi e dipendenti da *input*; la perdita di pensiero critico e di capacità decisionale nonché di visione dei nessi e delle relazioni.

## **Il Sistema Intelligenza Artificiale (IA)**

L'Intelligenza Artificiale (IA) nasce come disciplina scientifica nel 1956. Nel corso degli anni sono state proposte numerose definizioni accademiche, che ne mettono in evidenza differenti aspetti teorici, metodologici e applicativi.

Con riferimento al recente EU Artificial Intelligence Act dell'Unione Europea (2024), che disciplina l'utilizzo dei sistemi di IA, una definizione non puramente accademica di sistema di Intelligenza Artificiale è quella già sopracitata:

*“un sistema basato su una macchina progettata per operare con diversi livelli di autonomia, che può mostrare adattività dopo il dispiegamento e che, per obiettivi espliciti o impliciti, inferisce dagli input ricevuti come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali.”*

Da un punto di vista tecnico-scientifico, l'IA di tale macchina si concretizza primariamente nella parte software che la implementa. Un software può essere considerato sistema di IA se implementa algoritmi che svolgono almeno una delle seguenti funzioni:

- a) Apprendono da dati e compiono inferenze sulla base di quanto appreso (tecniche di Machine Learning, tra cui il Deep Learning e il Reinforcement Learning),
- b) Elaborano rappresentazioni simboliche di conoscenza attraverso metodi di ragionamento automatico e autonomo (tecniche di IA “classica”; ad esempio sistemi basati su regole, modelli formali logici, ricerca euristica e pianificazione automatica),
- c) Utilizzano Modelli di Linguaggio (Large Language Models – LLM), Modelli Visuali (Large Visual Models – LVM), o entrambi, per generare contenuti in forma di testi, immagini, video, audio e documenti multimodali.

Va osservato che gli LLM e i VLM utilizzano modelli di deep learning di grande scala, e perciò sono un caso specifico del punto (a), ma per la loro rilevanza scientifica e applicativa, la specificità tecnico-metodologica e l’ampia diffusione, si possono considerare una categoria separata.

Un vasto insieme di tecniche di Machine Learning e di IA classica è disponibile per costruire sistemi e applicazioni di IA di varia tipologia e in molteplici settori, tra cui quello sanitario. Un testo di riferimento per una panoramica scientifica di queste tecniche è [S. Russell & P. Norvig, *Artificial Intelligence: A Modern Approach* (4th Edition), 2021, Pearson Education].

Più recentemente si è altresì diffusa una varietà di potenti LLM e VLM (tra i più noti GPT, Claude, Gemini, LLaMA e relative versioni “vision”), che possono essere utilizzati “stand-alone”, aumentati con informazioni esterne (ad esempio tramite la Retrieval Augmented Generation), oppure integrati in software specifici (ad esempio OpenEvidence realizzato per la medicina) e in sistemi di “Agentic AI”, che interagiscono con strumenti software tradizionali, come un database aziendale.

Un software che utilizza IA non deve essere confuso con un software che, per quanto avanzato, sia realizzato con metodologie informatiche e modelli di programmazione tradizionali.

In generale, un software che non include una componente con almeno una delle caratteristiche (A)-(B)-(C) non è da considerarsi implementazione di una IA. Tale software segue regole esplicite implementate da uno o più programmatori, descritte in algoritmi specifici e applicate in modo deterministico; non sono

regole apprese dalla macchina stessa e nemmeno inferenze che il software può svolgere autonomamente a partire da conoscenza formalizzata nella macchina. Alcuni semplici esempi sono: il software di una calcolatrice, un foglio Excel con formule statiche, un software gestionale di fatturazione, un database relazionale, un simulatore che usa equazioni fisiche, un software di rendering grafico tradizionale, un sistema di allerta basato su soglia statica.

Il software tradizionale segue metodologie di sviluppo e validazione (Ingegneria del Software) consolidate, mentre la validazione di un software di IA richiede una specifica metodologia che ha profonde differenze. In generale, nel software tradizionale la validazione verifica che il software implementi correttamente le regole specificate. È una verifica di conformità rispetto a requisiti deterministici. Viceversa, per un software che utilizza Machine Learning, la validazione verifica che il modello appreso produca prestazioni adeguate su dati rappresentativi del mondo reale. Ciò richiede:

*Validazione del dataset* (un modello può essere perfetto ma validato su dati non rappresentativi): qualità dei dati, rappresentatività, eventuali bias, completezza, distribuzione statistica;

*Validazione delle performance* (non si verifica “output corretto”, ma probabilità e distribuzioni): utilizzo di metriche statistiche quali ad esempio accuracy, sensibilità / specificità, area sotto la curva ROC (AUC-ROC), F1-score, precision / recall, calibration;

*Validazione esterna* (un modello che funziona in un ospedale può fallire in un altro): test su dataset indipendenti, validazione multicentrica, validazione prospettica;

*Robustezza e stress test* (il software IA può degradare nel tempo): “Drift” dei dati, rumore, input anomali e/o mancanti, attacchi adversariali;

*Monitoraggio post-deployment* (monitoraggio continuo e re-valutazione periodica): L’IA implementata può cambiare comportamento, può essere ri-addestrata, può subire data drift.

In estrema sintesi, la differenza fondamentale tra software tradizionale e di IA non risiede nella complessità del codice, ma nella presenza di meccanismi di

apprendimento, inferenza o generazione autonoma non interamente determinati da regole esplicite scritte dal programmatore.

## **IA in Medicina**

L'intelligenza artificiale (IA) applicata in medicina sta evolvendo rapidamente e sta modificando sia la pratica clinica quotidiana che la ricerca traslazionale.

Non si tratta di un singolo "strumento", ma, come precedentemente illustrato, di un insieme di tecniche (machine learning, deep learning, modelli generativi, Natural Language Processing (NLP)) che, integrate nei sistemi sanitari, spostano il baricentro dall'interpretazione manuale di dati frammentati a una gestione più automatizzata, predittiva e, in alcuni contesti, personalizzata. Occorre tuttavia sottolineare come il grado di maturità tecnologica di queste applicazioni risulti oggi estremamente eterogeneo: alcune rappresentano già standard operativi e regolamentati, altre sono promettenti ma ancora "fragili" sul piano metodologico, organizzativo o normativo.

### ***IA e Ricerca Clinica Applicata***

Nel campo della ricerca clinica applicata, il dominio più consolidato è la diagnostica per immagini.

In radiologia, gli algoritmi di deep learning sono spesso integrati nei flussi Picture Archiving and Communication System (PACS) come strumenti di triage, prelettura e prioritizzazione, con l'obiettivo di ridurre i tempi di refertazione e intercettare precocemente reperti patologici tempo-dipendenti come emorragie intracraniche, embolie polmonari, fratture o noduli polmonari. In parallelo, la segmentazione automatica sta diventando un tassello operativo essenziale per la pianificazione terapeutica, perché trasforma immagini complesse in strutture misurabili e utilizzabili per i piani di radioterapia o le procedure interventistiche.

Qui la dimensione regolatoria è già presente: questi sistemi, quando impattano l'atto medico, devono essere validati in modo rigoroso e mantenuti sotto controllo in termini di performance nel tempo.

### **Un'evoluzione analoga sta interessando l'anatomia patologica digitale.**

La digital pathology permette di applicare modelli di visione artificiale alla classificazione di pattern istologici, alla quantificazione di biomarcatori come Ki-67 o PD-L1, all'identificazione di cellule rare e alla valutazione dei margini chirurgici. Il vantaggio clinico non è solo la velocità, ma anche la riduzione della

variabilità inter-osservatore, un tema strutturale nella diagnostica. La frontiera emergente è la patologia computazionale integrata, in cui immagine istologica, genotipi e fenotipi clinici vengono combinati da modelli multimodali per generare stratificazioni più informative rispetto a quelle basate su una singola sorgente di dato.

**La medicina di precisione e l'analisi genomica rappresentano un terzo pilastro, con un impatto crescente nella pratica clinica, in particolare in campo oncologico.**

L'IA accelera l'interpretazione delle varianti genomiche, la predizione dell'impatto funzionale e la classificazione secondo criteri standardizzati; in oncologia ed ematologia si sta affermando l'uso di modelli che integrano mutazioni con variabili cliniche longitudinali per stimare rischi di evoluzione, identificare driver biologici e selezionare pazienti candidabili a terapie target. Il passaggio più rilevante, nel medio periodo, sarà la normalizzazione dei modelli multimodali in grado di unire sequenziamento, imaging e storia clinica per generare sistemi di decision support realmente personalizzati, a condizione che la qualità del dato e la governance siano all'altezza della complessità.

Ancora, in ambiti come la terapia intensiva, la nefrologia, la cardio-oncologia, l'oncologia e il trapianto, modelli di machine learning vengono utilizzati per predire mortalità, recidiva, tossicità, infezioni, mortalità non correlata alla recidiva (NRM Non-Relapse Mortality), Malattia del trapianto contro l'ospite (GVHD - *Graft Versus Host Disease*) o risposta a terapie complesse come CAR-T e trapianto allogenico. Si tratta di ambiti clinic-decisionali molto delicati: il valore potenziale è alto, ma l'adozione reale dipende dalla robustezza dei dataset, dalla applicabilità generale anche e soprattutto fuori dal centro che ha costruito il modello e da un livello di spiegabilità sufficiente a renderlo clinicamente e legalmente accettabile. In quest'ottica, il rigore metodologico non rappresenta un fattore accessorio, bensì il discriminante che separa una soluzione tecnologica strutturale e implementabile da un mero prototipo accademico.

**Un altro vettore di penetrazione è l'automazione dei flussi clinici.**

In tale contesto, l'IA non compete con la diagnosi specialistica, ma riduce inefficienze e rischio di errore documentale: trascrizione e sintesi delle visite, refertazione assistita, compilazione di campi strutturati negli EHR, riconciliazione farmacologica, supporto alla codifica amministrativa e alla gestione delle priorità in pronto soccorso o nelle agende ambulatoriali. In questa dimensione l'IA diventa un moltiplicatore di produttività e sicurezza, perché libera tempo clinico e riduce errori di trascrizione e omissioni. È anche l'ambito dove l'adozione può essere più rapida, purché vi siano controlli di qualità, tracciabilità e gestione dei rischi.

### *IA e Ricerca Traslazionale*

La ricerca biomedica, in parallelo, è un terreno in cui l'IA sta ridefinendo pipeline consolidate.

Nella fase preclinica accelera la discovery di target e il riposizionamento farmacologico attraverso l'analisi di reti biologiche e di interazioni gene-proteina, e riduce tempi e costi con screening virtuale e modelli generativi in grado di progettare molecole con proprietà desiderate. L'analisi multiomica integra genomica, trascrittomica, proteomica e fenotipo clinico per identificare sottotipi molecolari, vulnerabilità terapeutiche e biomarcatori compositi. Inoltre, abilita modelli longitudinali di progressione di malattia, biomarcatori digitali da imaging, audio e wearable, e contribuisce all'ottimizzazione della sperimentazione clinica tramite selezione dei pazienti, design adattativi, estrazione di endpoint complessi da note cliniche non strutturate e, in alcuni contesti, costruzione di bracci di controllo sintetici basati su real-world data quando eticamente e metodologicamente difendibile.

### **La generazione di nuovi farmaci è una delle aree più trasformative.**

L'IA può intervenire dalla selezione del target fino alla lead optimization: identifica nodi critici in reti biologiche, predice l'effetto funzionale di mutazioni, integra dati multiomici per derivare target più specifici, e riduce il carico sperimentale con screening virtuale e modelli Quantitative Structure-Activity Relationship (QSAR) avanzati. Con la chimica generativa, modelli come Variational Autoencoders (VAE), Generative Adversarial Networks (GAN) e diffusion possono proporre strutture de novo ottimizzate multi-obiettivo, bilanciando potenza, selettività e profilo di assorbimento, distribuzione,

metabolismo, escrezione, tossicità (ADMET). La previsione di assorbimento, distribuzione, metabolismo, escrezione e tossicità è una delle applicazioni più consolidate, perché anticipa fallimenti che tradizionalmente emergerebbero tardi. La biologia strutturale guidata dall' IA, resa celebre da piattaforme di predizione strutturale, ha inoltre aumentato la velocità con cui si passa dall'ipotesi biologica a candidati razionali, e sta aprendo spazi anche per farmaci o prodotti biologici come anticorpi e peptidi ingegnerizzati.

**Molto recentemente, l'IA ha mostrato un notevole potenziale nella modellizzazione delle malattie o nella simulazione di trial clinici, inclusi quelli di Fase III, utilizzando dati clinici provenienti da fasi precedenti degli studi o da coorti storiche.**

Attraverso modelli computazionali avanzati e *machine learning*, i modelli di IA si sono dimostrati utili non solo nella diagnosi delle malattie, ma anche nella previsione degli esiti e nell'ottimizzazione del disegno sperimentale, rappresentando così uno strumento potente nello sviluppo di nuovi farmaci.

Ad esempio, un modello di IA può essere utilizzato per stimare gli esiti attesi del trattamento standard, apprendendo dai dati clinici storici le associazioni tra le variabili basali dei pazienti e i risultati ottenuti. In questo modo, è possibile generare un gruppo di controllo virtuale da confrontare con una coorte trattata con una nuova terapia, evitando la necessità di uno studio randomizzato di Fase III. Questo approccio può affiancare in modo complementare il Propensity Score Matching (PSM), offrendo una base per confrontare i due metodi e rafforzare l'affidabilità delle evidenze prodotte.

La configurazione metodologica di questo approccio innovativo, potenzialmente alternativo a uno studio di Fase III, rappresenta un modello di ricerca di straordinaria rilevanza etica e scientifica. L'impiego di dati retrospettivi, ottenuti da una coorte storica ampia e ben caratterizzata, integrato dal confronto con una coorte sperimentale sottoposta a trattamenti innovativi, consente di generare evidenze cliniche solide senza la necessità di sottoporre ulteriori soggetti a sperimentazioni gravose o potenzialmente dannose.

Questo approccio, oltre a minimizzare i rischi legati all'arruolamento di nuovi partecipanti, permette un'accelerazione significativa nella generazione dei

risultati, con un impatto positivo sulla disponibilità e sull'ottimizzazione delle strategie terapeutiche per un numero più ampio di pazienti.

Sebbene la rilevanza etica di uno studio non costituisca, in senso stretto, una base giuridica sufficiente per il trattamento dei dati personali in assenza di consenso informato, come chiarito nel Provvedimento n. 298/2024, essa sostiene comunque l'avanzamento della ricerca biomedica in modo responsabile e rispettoso dei principi etici.

La capacità di generare conoscenze clinicamente rilevanti senza aumentare il rischio per i pazienti rappresenta una scelta metodologica che non solo soddisfa i criteri del rigore scientifico, ma si allinea anche a una visione etica del progresso medico orientato al bene comune.

**In questo scenario l'acquisizione e gestione dei dati è centrale e i dati sintetici sono spesso proposti come soluzione di equilibrio tra utilità e privacy.**

I dati sintetici derivati da dati reali sono generati per replicare proprietà statistiche e pattern, senza riprodurre direttamente le informazioni individuali. In sanità possono abilitare addestramento e test di modelli senza esporre dataset originali, facilitare la condivisione tra team e partner e simulare condizioni rare. Tuttavia, dal punto di vista della privacy, non esiste una garanzia automatica: se il processo generativo "memorizza" e riproduce punti troppo vicini ai reali, o replica outlier e combinazioni uniche, resta possibile la re-identificazione o l'inferenza su individui originali. Per questo la qualità di un dataset sintetico non si misura solo sull'utilità analitica, ma anche su metriche di rischio privacy, su procedure di audit e su tecniche di mitigazione come privacy differenziale, controlli di similarità e stress test di attacco. In termini di compliance, la linea di confine è pragmatica: se con mezzi ragionevoli non è possibile risalire agli individui, il dataset può avvicinarsi al concetto di anonimizzazione; se invece esistono percorsi realistici di re-identificazione, quel dataset resta sostanzialmente nel perimetro dei dati personali e deve essere trattato come tale.

**Lo sviluppo di nuovi percorsi diagnostici, prognostici e terapeutici, ha necessariamente costretto le Autorità Regolatorie Sanitarie a considerare nuove metodologie di analisi e rivedere le procedure di rilascio di nuovi farmaci e validazione di nuove terapie.**

Gli Enti regolatori (Food and Drug Administration - FDA, European Medicines Agency - EMA, Agenzia Italiana del Farmaco - AIFA) non “delegano” l’approvazione all’IA, ma la impiegano (e ne valutano l’impiego da parte delle aziende) come leva per gestire complessità e volumi: triage e classificazione documentale, estrazione e confronto di dati tra moduli CTD (Common Technical Document), controllo di coerenza tra protocollo, SAP (sistema informativo gestionale) e CSR (Corporate Social Responsibility), e identificazione di criticità ricorrenti. In qualità e CMC (Chemistry, Manufacturing and Controls, la parte del dossier dedicata a qualità farmaceutica, processo produttivo, controlli, specifiche, stabilità e integrità del prodotto) l’attenzione è su trend di processo, deviazioni e integrità dei dati, con un approccio sempre più risk-based. In farmacovigilanza, l’IA supporta signal detection e case processing, accelerando prioritizzazione e riducendo carico manuale, pur mantenendo supervisione. EMA tende a un’impostazione prudente e centrata sulla governance, con forte attenzione a tracciabilità, qualità dei dati e gestione del bias; FDA storicamente enfatizza auditing, replicabilità e stress test di generalizzabilità, e mostra una propensione più operativa all’uso di strumenti avanzati nella sorveglianza e nelle ispezioni; AIFA, nel contesto italiano, incrocia l’innovazione con i bisogni di HTA (Health Technology Assessment), prezzo e rimborso, registri e appropriatezza, dove l’AI può diventare rilevante nella valutazione di valore su real-world data e nella qualità dei registri e dei Managed Entry Agreements.

### *Intelligenza artificiale e modelli organizzativi sanitari*

Oltre all’ambito strettamente clinico, l’intelligenza artificiale sta assumendo un ruolo sempre più importante anche nella gestione e nell’organizzazione dei sistemi sanitari. Le tecnologie di analisi avanzata dei dati permettono infatti di supportare i processi decisionali strategici e migliorare l’efficienza delle strutture sanitarie.

Attraverso l’analisi automatizzata di grandi volumi di dati amministrativi e clinici, l’IA può supportare la pianificazione strategica, valutando l’impatto potenziale di nuove tecnologie o modelli organizzativi su costi, qualità dell’assistenza ed esiti clinici. Gli strumenti di simulazione consentono inoltre di prevedere gli

effetti di cambiamenti nella disponibilità di posti letto, nella turnazione del personale o nella distribuzione delle risorse diagnostiche e terapeutiche.

L'intelligenza artificiale può essere utilizzata anche per individuare colli di bottiglia nei reparti ad alta complessità, come il pronto soccorso o le terapie intensive, e per simulare scenari di stress organizzativo legati a eventi straordinari, come epidemie o emergenze sanitarie.

Nel campo della sicurezza e della qualità delle cure, sistemi intelligenti possono contribuire alla sorveglianza epidemiologica e alla gestione del rischio clinico, identificando precocemente focolai infettivi, eventi avversi o situazioni di potenziale criticità. L'intelligenza artificiale può migliorare la gestione dei flussi di pazienti e dei percorsi assistenziali, attraverso modelli predittivi che stimano il numero di accessi ai servizi sanitari e algoritmi in grado di personalizzare i percorsi di cura in base alla complessità clinica e alle risorse disponibili.

Infine, integrare l'IA nei processi e nei percorsi di ricerca rappresenta oggi una scelta strategica per un Ospedale che intenda consolidare il proprio ruolo nel panorama della ricerca biomedica. L'IA, infatti, non si configura come un semplice strumento tecnologico, ma come un'infrastruttura abilitante capace di elevare la qualità scientifica, potenziare l'analisi e l'interpretazione dei dati e accelerare la produzione di evidenze robuste, riproducibili e trasferibili nella pratica clinica. In un contesto caratterizzato da crescente complessità assistenziale e disponibilità massiva di dati, l'impiego consapevole di metodologie avanzate di analisi consente di trasformare il patrimonio informativo aziendale in conoscenza strutturata e in valore per i pazienti.

L'adozione consapevole dell'AI nel contesto di ricerca può rafforzare la competitività dell'Ente, aumentare la capacità di attrarre finanziamenti per la ricerca, consolidare il posizionamento nel panorama della ricerca biomedica nazionale ed internazionale. In questa prospettiva, l'Intelligenza Artificiale si configura come una leva strategica per lo sviluppo, l'innovazione e la sostenibilità del sistema sanitario.

Per un Ospedale, già strutturato per promuovere e supportare i percorsi di ricerca, investire in IA significa adottare un approccio multidisciplinare e

integrato che coinvolga clinici, ricercatori, data scientist, Clinical Trial Center e Direzione Strategica in una visione condivisa. È necessario definire priorità chiare per l'implementazione dell'IA nella ricerca clinica, individuando ambiti ad alto impatto e coerenti con le linee di sviluppo aziendali. Parallelamente, occorre promuovere partnership strutturate con enti di eccellenza nazionali e internazionali, valorizzando lo scambio di competenze e la partecipazione a progetti collaborativi.

Fondamentale è anche l'investimento nella formazione interna, attraverso programmi dedicati allo sviluppo di competenze digitali, metodologiche e regolatorie che consentano al personale sanitario e tecnico di utilizzare in modo critico e responsabile gli strumenti di IA.

**Il compendio non è completo senza considerare la sicurezza informatica, perché l'adozione dell'IA aumenta la superficie di attacco dei sistemi sanitari e, contemporaneamente, offre strumenti più potenti per difenderli.**

L'IA è già utilizzata nella difesa per anomaly detection su rete, endpoint, identità e cloud, per correlazione di threat intelligence e per automazione di incident response, migliorando i tempi di rilevazione e risposta e riducendo falsi positivi. Ma la stessa tecnologia rende gli attaccanti più efficaci: phishing e spear phishing iper-personalizzati, frodi con deepfake, malware adattivo e ricognizione automatizzata abbassano la soglia tecnica dell'offensiva e aumentano la scalabilità dell'attacco. Inoltre, l'IA stessa diventa un asset da proteggere: modelli e pipeline possono essere colpiti con data poisoning, model inversion, membership inference e prompt injection, soprattutto quando LLM vengono integrati nei processi aziendali o clinici. Ne deriva una necessità di governance specifica: controllo dei dati di training, tracciabilità e versioning dei modelli, testing avversariale, monitoraggio di drift e performance, e gestione del rischio della supply chain (modelli esterni, dipendenze cloud, componenti terze).

**In conclusione,** l'IA in medicina è già una trasformazione in atto, ma non è una trasformazione "solo tecnologica": è organizzativa, regolatoria, etica e di sicurezza. Dove i flussi sono già digitali e i dati sono di qualità, l'IA migliora velocità, precisione e capacità predittiva; dove i dati sono poveri, frammentati o non governati, l'IA amplifica rumore e bias.

Il punto di equilibrio non è scegliere tra entusiasmo e rifiuto, ma costruire infrastrutture, regole e responsabilità che rendano l'IA uno strumento clinicamente utile, difendibile in un contesto regolatorio e sicuro nel tempo per gli operatori e per i pazienti.

## **Considerazioni Giuridiche**

### *Considerazioni Giuridiche in contesto clinico*

L'impiego di sistemi di intelligenza artificiale (IA) in clinica, con particolare riferimento ai medical devices con IA (cd. MDAI - Medical Device Artificial Intelligence), è regolato da un quadro normativo integrato che prevede un approccio risk-based complementare, ove talora si intrecciano la normativa unionale (Fonti normative Unione Europea) in materia di IA e quella già vigente in materia di dispositivi medici. Ritenere, tuttavia, che tutti i sistemi di IA per fini medici siano anche dispositivi medici è scorretto.

#### *AI Act (Reg. UE 1689/2024)*

Secondo l'**AI Act (Reg. UE 1689/2024)**, i sistemi di IA vengono suddivisi in quattro classi di rischio, ove per rischio si intende la combinazione tra la probabilità di verificarsi di un danno e la gravità del danno, da parametrarsi secondo la potenziale lesione dei valori della salute, della sicurezza e dei diritti fondamentali. Per ciò che qui interessa, le classi di rischio vengono di seguito così definite:

#### **INACCETTABILE (art. 5):**

Per ciò che interessa il contesto sanitario, rientrano in questa classe le pratiche manipolative che alterano il comportamento umano causando un danno significativo, a meno che tale attività non sia lecita pratica medica, con finalità terapeutica validata (cons. 29).

Non è poi consentita la categorizzazione biometrica in base a informazioni sensibili, che deduce, dunque, orientamento sessuale, religione, etnia dal volto o dalla voce del paziente. Altra questione attiene alla classificazione clinica del

paziente, che è invece consentita e considerata come dal Regolamento come ad alto rischio.

Di là dalle eccezioni qui menzionate, l'impiego di questi sistemi di IA è proibito.

### **RISCHIO ALTO (art. 6):**

In questa classe di rischio rientrano i cd. Medical Device Artificial Intelligence (MDAI), sottoposti a procedura di valutazione della conformità da parte di un organismo notificato (all. I AI Act) secondo le norme armonizzate, ossia, nel caso di specie, il Medical Device Regulation (MDR) (Reg. UE n. 745/2017 sui dispositivi medici); per esempio, Clinical Decision Support Systems (CDSS), ossia i sistemi di IA che vengono impiegati a sostegno delle attività di diagnosi, prognosi e individuazione della terapia. V. infra per integrazione con MDR.

Nei sistemi ad alto rischio rientrano anche macchine che possono essere utilizzate nel contesto di cura, ma potrebbero non essere dispositivi medici perché non svolgono attività terapeutiche, come l'impiego di sistemi di IA per il riconoscimento delle emozioni (finalità mediche/sanitarie). Ancora, appartengono a questa categoria anche diversi sistemi impiegati in attività prodromiche alla presa in carico del paziente, quali sono quelli deputati alla valutazione di ammissibilità del paziente a prestazioni e servizi di assistenza sanitaria; determinazione dei rischi e prezzi assicurativi; oppure definizione dei triage e delle priorità nelle chiamate di emergenza (All. III). In tutti questi casi, la valutazione di conformità viene fatta ai sensi e secondo le procedure dell'AI Act.

Per tutti i sistemi di IA ad alto rischio l'AI Act prevede il rispetto di requisiti stringenti e di procedure da garantire e osservare, quali misure di gestione della qualità; misure di gestione del rischio; qualità e governance dei dati; documentazione tecnica; conservazione delle registrazioni; trasparenza; accuratezza, robustezza e cybersicurezza; e sorveglianza umana.

Tutti i requisiti appena menzionati sono immaginati per essere pienamente rispettati. Tuttavia, è possibile che lo sviluppo di alcuni requisiti possa andare a detrimento di altri. L'esempio più noto in letteratura è il conflitto tra accuratezza e trasparenza: i sistemi più accurati sono tendenzialmente quelli meno interpretabili, perché più complessi; viceversa, ad una maggiore trasparenza si accompagna generalmente una minore complessità e, di riflesso, accuratezza.

Inoltre, l'*AI Act* applica talvolta delle formule vaghe, nel senso che indica il risultato da raggiungere ma non i parametri per ottenerlo. Ad esempio, i sistemi di IA ad alto rischio devono essere 'sufficientemente' trasparenti; i rischi residui devono essere 'accettabili', ecc. Il bilanciamento in concreto sul grado di 'sufficienza' della trasparenza o di 'accettabilità' dei rischi residui dev'essere quindi compiuto dal fornitore. Quest'ultimo potrà godere però di una presunzione di conformità ai requisiti qualora rispetti le norme armonizzate. È verosimile sostenere, allora, che queste ultime diventeranno lo standard da seguire. Ciò comporta dei rischi, perché tali norme armonizzate vengono elaborate da organismi privati (gli organismi europei di standardizzazione), a scarso o nullo controllo pubblico e giurisdizionale, e a composizione principalmente tecnica ed ingegneristica. All'esito, si può paventare il rischio che i bilanciamenti in concreto vengano operati da organismi che hanno scarse competenze in materia di salute, sicurezza e diritti fondamentali.

I sistemi di IA devono sottoporsi a una valutazione di conformità:

- a) Operata autonomamente dal fornitore se ricadono tra i sistemi di IA dell'All. III (cfr. punto 2, voce 'Rischio alto'), a meno che non si tratti di sistemi di identificazione biometrica da remoto: in questo caso sarà necessario passare attraverso la valutazione di un organismo notificato (ente terzo di valutazione della conformità notificato in conformità dell'*AI Act* e di altre pertinenti normative di armonizzazione dell'Unione);
- b) Per gli MDAI di cui all'All. I (cfr. punto 1, voce 'Rischio alto') l'intera procedura di valutazione è attratta da quella del Reg. UE 745/2017, cui andrà aggiunto il rispetto dei requisiti previsti dall'*AI Act*. Ciò nel caso in cui tale Regolamento imponga la valutazione da parte di un organismo notificato, ossia il caso dei dispositivi medici che sono software o li integrano come componenti di sicurezza, laddove rientrino nella classe IIa, IIb o III (esclusi quindi i dispositivi di classe I).

Per ciò che riguarda i Diritti degli interessati previsti dall'*AI Act* (cioè coloro che sono destinatari dell'output del sistema): l'art. 86 dà diritto a ottenere informazioni significative sul ruolo del sistema e sugli elementi principali della

decisione, tuttavia l'art. 86 si applica ai soli sistemi di IA ad alto rischio dell'All. III, non si applica agli MDAI dell'All. I.

### **RISCHIO LIMITATO:**

Riguarda, in particolare, Chatbot sanitari informativi/ assistenti virtuali che forniscono informazioni generali su sintomi e servizi

In questi casi vi è l'obbligo di informare l'interessato che interagisce con IA. Nessuna procedura di conformità strutturata. L'AI Act promuove la volontaria osservanza da parte dei fornitori ai requisiti previsti per i sistemi ad alto rischio.

### **RISCHIO MINIMO:**

Riguarda, in particolare, il Miglioramento (ottimizzazione) dell'amministrazione sanitaria (turni, logistica); sistemi di IA di wellness e fitness.

In questo caso si può prevedere una Libertà d'uso, fermo restando il rispetto del GDPR (General Data Protection Regulation) e della normativa vigente. Anche qui, l'AI Act promuove la volontaria osservanza da parte dei fornitori ai requisiti previsti per i sistemi ad alto rischio.

Vi sono poi Modelli di IA per finalità generali: essi sono destinatari di un capo apposito all'interno dell'AI Act, in quanto sono addestrati su gigantesche quantità di dati per eseguire una notevole pluralità di compiti diversi (mentre i sistemi di IA tendenzialmente compiono uno o più compiti specifici). In ragione di queste caratteristiche, sono sottoposti a particolari misure di trasparenza tecnica, nonché nei confronti del pubblico presso cui sono distribuiti.

I sistemi di IA per finalità generali sono sistemi di IA che operano sulla base di un modello di IA per finalità generali. Il sistema di IA per finalità generali, per parte propria, apparterrà ad una delle classi di rischio dei sistemi di IA (proibito, alto, medio o minimo).

Per fare un esempio, GPT-4.5 è un modello di IA per finalità generali; ChatGPT è il sistema di IA per finalità generali basato su GPT-4.5.

Il Regolamento prevede rilevanti obblighi soggettivi per gli attori che intervengono nella catena del valore dei sistemi di IA ad alto rischio. Qui

interessa, in particolare, la figura dei *deployer* (cioè coloro che utilizzano per ragioni professionali e sotto la propria responsabilità i sistemi di IA ad alto rischio), dal momento che tale figura sarà rivestita dalle strutture sanitarie e medici liberi professionisti:

- osservanza delle istruzioni per l'uso nell'utilizzo del sistema di IA;
- monitoraggio del sistema, dovere di sospensione del sistema in caso di malfunzionamento e di segnalazione di eventuali violazioni da parte del fornitore o malfunzionamenti;
- conservazione per almeno sei mesi dei log generati durante l'utilizzo
- delega (nel caso di specie da parte della struttura sanitaria) a soggetti qualificati (nel caso di specie i medici impiegati) dei compiti di sorveglianza umana.

Esistono poi degli obblighi di carattere generale rilevanti nell'ambito medico: l'art. 4 AI Act impone a fornitori e *deployer* oneri di alfabetizzazione in materia di IA rispettivamente dei propri clienti e collaboratori in merito alla conoscenza e al corretto impiego dei sistemi di IA. L'alfabetizzazione in materia di IA è un obbligo delle strutture sanitarie, saldandosi con i pregnanti doveri che si aggiungono in particolare per coloro che sono delegati (i medici) alle funzioni di sorveglianza umana.

#### *MDR (Reg. UE 745/2017): Profili di concordanza e discordanza con l'AI Act*

Alcune delle più rilevanti implicazioni pratiche includono: (i) obbligo di aggiornamento continuo del modello IA per variazioni dati/post-market (MDR art. 10, par. 9); (ii) responsabilità del fabbricante per decisioni totalmente autonome senza sorveglianza umana (AI Act art. 29); (iii) integrazione con linee guida nazionali ex Legge 23 settembre 2025, n. 132, attraverso l'adozione dei corrispondenti decreti di attuazione, con specifico riguardo ai dati sanitari; (iv) necessità di autorizzazione da parte dei comitati etici territoriali per i trial clinici con IA (D.Lgs. 52/2019 di recepimento del MDR). La doppia conformità MDR/AI Act richiede piani di qualità integrati, audit algoritmici e notifica incidenti entro 15 giorni (AI Act art. 73; MDR art. 87).

Per quanto riguarda i profili di concordanza tra *AI Act* e MDR, va sottolineato come la nozione di fornitore (*AI Act*) e fabbricante (MDR) siano sostanzialmente sovrapponibili. Inoltre, entrambi i Regolamenti disciplinano in maniera strutturata i requisiti di gestione della qualità, gestione del rischio e documentazione tecnica. In questi casi, gli specifici obblighi previsti dall'*AI Act* andranno aggiunti ed integrati dentro le procedure già previste dal MDR.

Sono, tuttavia, notevoli anche i profili di discordanza. In primo luogo, differiscono le nozioni di *deployer* (*AI Act*) e utilizzatore (MDR): quest'ultimo comprende anche l'utilizzatore profano (cioè il paziente), mentre l'*AI Act*, come già sottolineato, individua nel *deployer* solo l'utilizzatore professionale. L'ambito di applicazione dell'*AI Act* è poi più esteso del MDR: potrebbero esserci dispositivi medici prodotti all'estero ma non commercializzati in UE che sono considerati sistemi di IA ad alto rischio e vedono applicato l'*AI Act* ma non il MDR.

Differente è la nozione di rischio nel MDR, che lo parametrizza alla potenzialità di lesione organica (psico-fisica) del paziente da parte del dispositivo (classe I rischio minimo, classe III rischio massimo), mentre nell'*AI Act* i parametri di riferimento sono salute, sicurezza e diritti fondamentali. Va evidenziato che la classe di rischio alta ai sensi dell'*AI Act* non incide sulla classe di rischio del MDR: ci possono quindi essere dispositivi medici ad alto rischio ma di classe IIa (peraltro la generalità dei casi per i dispositivi medici software).

I parametri di bilanciamento sono spesso diversi: i rischi nel MDR devono essere eliminati 'per quanto possibile' (*as far as possible*), secondo il limite è lo stato dell'arte. Nell'*AI Act*, invece, i rischi devono essere eliminati 'per quanto possibile dal punto di vista tecnico' (*as far as technically feasible*). Il limite è qui meno stringente, perché introduce nella valutazione costi-benefici l'incidenza di ragioni di carattere economico.

### *Principali fonti normative nazionali*

#### *L. 219/2017*

Questa legge rappresenta il punto di riferimento dell'attività clinica. Si individua nel consenso informato il luogo di incontro tra l'autonomia del paziente e competenza, l'autonomia professionale e la responsabilità del medico. La circostanza che si parli di 'incontro' lascia intendere che l'assunzione del medico di un ruolo deliberativo, ovverosia della capacità di guidare il paziente verso la scelta più coerente all'orizzonte valoriale di quest'ultimo. Tant'è che si parla espressamente di tempo della comunicazione come tempo di cura.

Perché ciò sia possibile, la legge prevede che al paziente sia fornita un'informazione completa, aggiornata e a lui comprensibile (e che questi può sempre rifiutare) su diagnosi, trattamento suggerito e alternative terapeutiche, con il limite dell'informazione 'terroristica' (ossia sproporzionata e nociva perché tale da ingenerare desistenza dalle cure a fronte di probabilità estremamente risibili di avveramento della controindicazione clinica o prognostica).

L'autonomia del paziente è salvaguardata dal diritto al rifiuto e alla revoca delle cure (già tutelato, invero, dall'art. 32 co. 2 Cost.), a fronte del quale il medico è esente da responsabilità civile e penale.

In ogni caso al medico è fatto divieto di dare luogo a una ostinazione irragionevole delle cure (nozione nota un tempo come 'accanimento terapeutico'), cui si aggiunge il dovere di garantire l'accompagnamento palliativo.

L'autonomia e la competenza professionale del medico viene tutelata, in particolare, dalla previsione che lo libera da obblighi professionali di fronte a richieste contrarie a norme di legge, deontologia professionale e buone pratiche clinico assistenziale. Ciò non equivale a dire che il medico possa esercitare una obiezione di coscienza di fronte al rifiuto o alla richiesta di revoca delle cure da parte del paziente: tale facoltà deve essere espressamente prevista dalla legge (non è questo il caso) e si configura come un comportamento omissivo, cioè di astensione del medico da una certa attività, risultando quindi incompatibile con comportamenti attivi, qual è la somministrazione forzata di una cura.

### *L. 24/2017*

La cd. legge Gelli-Bianco ha individuato un regime di responsabilità contrattuale per la struttura sanitaria e il medico libero professionista, e un regime di responsabilità extracontrattuale del medico dipendente della struttura e libero professionista di cui tale struttura si avvalga.

### *L. 132/2025*

Art. 7 co. 3: “L'interessato ha diritto di essere informato sull'impiego di tecnologie di intelligenza artificiale”;

Art. 7 co. 5: “I sistemi di intelligenza artificiale in ambito sanitario costituiscono un supporto nei processi di prevenzione, diagnosi, cura e scelta terapeutica, lasciando impregiudicata la decisione, che è sempre rimessa agli esercenti la professione medica”.

La l. 132/2025 quindi individua, da un lato, un preciso obbligo informativo in capo al medico e nei confronti del paziente rispetto all'impiego dello strumento di IA. Sotto altro profilo, dichiara espressamente che i sistemi di IA vanno considerati strumenti di ausilio alla decisione del curante.

### *Indicazioni e linee guida*

L'integrazione dell'intelligenza artificiale nei processi clinici e di ricerca introduce rischi giuridici strutturali che necessitano di mitigazione e governance specifica. L'opacità dei modelli (cd. black box) impedisce la verifica della causalità predittiva, minando la fiducia scientifica della ricerca; l'automazione delle ipotesi privilegia correlazioni statistiche su meccanismi biologici plausibili, mentre overfitting e falsi positivi accentuano la crisi di riproducibilità. Sotto il profilo clinico, si traduce in una mancanza di trasparenza e quindi nella difficoltà di comprendere e interpretare il funzionamento e i risultati dell'IA da parte del medico.

La presenza di modelli opachi, unita alle maggiori capacità computazionali della macchina, ingenera il rischio di un affidamento acritico del medico rispetto agli output prodotti (cd. automation bias) e, a lungo andare, la progressiva

sostituzione dell'essere umano comporta la perdita di capacità e competenze da parte del professionista sanitario (cd. deskilling). Per le medesime ragione, il deskilling può compromettere anche le capacità analitiche dei ricercatori.

I bias algoritmici, derivanti da dataset non rappresentativi della complessità sociale, amplificano disparità demografiche o cliniche, producendo risultati distorti e raccomandazioni discriminatorie, specie ai fini della medicina di precisione.

Sotto il profilo gestionale, le disuguaglianze digitali concentrano benefici in grandi strutture avanzate, ampliando i divari con le realtà territoriali. Sul punto è rilevante il riferimento dell' art. 7 L. 132/2025, che vieta l'uso di IA che determinino discriminazioni nell'accesso alle cure.

Infine, l'IA, per tutte le ragioni appena esposte, può alterare gli equilibri della relazione medico-paziente, producendo un impoverimento sul piano comunicativo, dell'empatia e della fiducia.

In particolare, le conseguenze dell'impiego di sistemi intelligenti si misurano dal punto di vista della 1. RELAZIONE DI CURA e della 2. RESPONSABILITÀ SANITARIA.

Il canone fondamentale da tenere a mente è che il sistema intelligente rimane un mero strumento di cui il medico decide di avvalersi nell'esecuzione della prestazione di cura. Ciò in quanto le macchine non eseguono ancora in piena autonomia e senza mediazione umana né la prestazione di cura né segmenti di essa.

Altro aspetto centrale da considerare è che, nella relazione di cura, verranno impiegati prevalentemente dispositivi medici di supporto alla diagnosi, prognosi, terapia e monitoraggio (Clinical Decision Support System o CDSS), quindi tutti dispositivi medici di IA ad alto rischio. Le considerazioni che seguono sono quindi specificamente ritagliate sulle specificità di questi dispositivi all'interno del contesto clinico.

#### 1) Relazione di cura

La relazione di cura si realizza nel momento in cui il paziente compie una scelta consapevole e coerente con il proprio orizzonte valoriale.

Perché ciò avvenga è necessario un processo continuo, che a partire da una corretta diagnosi si sviluppa attraverso il momento informativo fino ad arrivare, attraverso l'ascolto e la comunicazione con il paziente, ad una decisione consapevole.

Il ruolo contemporaneo del medico, lo si ribadisce, è di carattere deliberativo, nel senso di accompagnamento dell'ammalato verso l'aderenza valoriale alla scelta terapeutica per lui più opportuna.

L'IA consente di velocizzare i processi di diagnosi e formulazione di ipotesi e proposte terapeutiche e offrire soluzioni 'ritagliate' sulle caratteristiche specifiche del paziente (obiettivo della medicina delle 4P: precisa, preventiva, predittiva e partecipativa).

L'integrazione dell'IA nella relazione di cura è da ritenersi efficace se consente di dedicare più tempo alla comunicazione del paziente e rispetta la dimensione valoriale di quest'ultimo.

La compressione dei tempi di visita e cura da parte delle strutture sanitarie, laddove motivata dall'adozione di strumenti di calcolo più veloci e performanti, è quindi verosimilmente destinata al fallimento, perché amplifica i rischi di automation bias e deskilling e rischia di ridurre ulteriormente i momenti di comunicazione, già ridotti al minimo dall'assenza di adeguate risorse, specialmente umane.

Ciò premesso, l'assenza di trasparenza è un fattore capace di pregiudicare la piena comprensione dell'output da parte del medico senza, tuttavia, poter giustificare il venir meno dell'assunzione di responsabilità da parte di questi. Il professionista sanitario deve essere in grado di dominare e controllare le indicazioni fornite dalla macchina, anche al fine di potersene discostare.

Particolare attenzione va prestata alla presenza di eventuali bias, a partire dalla verifica della rappresentatività sociale dei dataset impiegati dalla macchina alle peculiarità fisiologiche e geografiche del paziente. Infatti, le modalità di programmazione – i dati sulla base dei quali la macchina è stata addestrata – condizionano l'esattezza delle indicazioni diagnostiche e terapeutiche in relazione al singolo paziente del caso concreto, le cui caratteristiche potrebbero, per converso, non essere adeguatamente rappresentate nei dataset impiegati.

Tutti gli obblighi anzidetti discendono anche specificamente dalle norme individuate dall'AI Act in materia di sorveglianza umana: il sorvegliante deve conoscere il dispositivo, resistere all'automation bias, saper interpretare correttamente l'output, sapersene discostare ove necessario, capace di decidere di non usare il sistema o sospenderne il funzionamento.

Fondamentali diventano quindi le misure in materia di alfabetizzazione in materia di IA e specifica formazione dei medici che applicheranno i dispositivi. Attenzione particolare andrà riposta anche nelle istruzioni per l'uso, dal momento che contengono tutte le misure di trasparenza ritenute necessarie da parte del fornitore.

N.B.: Attesa la presenza di necessari bilanciamenti tra requisiti, dei diversi parametri che informano i bilanciamenti tra AI Act e MDR, e delle potenziali lacune delle norme armonizzate, è fondamentale non ingenerare automatismi tra la presenza di una marcatura CE e la sicurezza o affidabilità del CDSS: il dispositivo andrà sempre validato all'interno della struttura, con particolare attenzione al contesto specifico e alla tipologia di destinatari su cui verrà impiegato.

### 1.1. Incidenza dell'IA sul momento informativo

L'art. 7 L. 132/2025 prevede che i medici informino adeguatamente il paziente in ordine all'utilizzo dell'IA.

Il paziente, tuttavia, non deve autorizzare, con il suo consenso informato, il professionista a impiegare il sistema intelligente, perché questa decisione rientra nell'autonomia professionale del medico o nelle valutazioni operate dalla struttura sanitaria di riferimento.

In ipotesi, la persona malata non può pretendere che il medico desista dall'impiegare l'IA a beneficio di una tecnologia meno performante; tuttavia, egli ha il diritto di conoscere la logica decisionale sottostante all'indicazione fornita dal sistema: di conoscere, in altri termini, sulla scorta di quale valore o bene giuridico la macchina ha indicato o preferito una determinata opzione terapeutica. La conoscenza della logica decisionale consente di preservare l'autodeterminazione della persona malata anche a fronte dell'impiego della macchina, senza che l'output sia imposto al paziente come l'unico possibile (dal

paternalismo del medico al paternalismo dell'IA), bensì inserendolo in un processo relazionale funzionale all'acquisizione di un consenso/dissenso informato.

Il medico che ottemperi alla richiesta del paziente di utilizzare una tecnologia meno efficace rispetto a quella a disposizione potrà ritenersi civilmente responsabile del pregiudizio eventualmente così cagionato al paziente medesimo. La richiesta del paziente, infatti, non esonera il medico dal dovere di comportarsi secondo diligenza, in relazione alle conoscenze dello stato dell'arte.

### 1.2. Incidenza dell'IA sulla dimensione valoriale del paziente

Va rifiutata l'idea di una pretesa 'neutralità tecnologica' del CDSS: la macchina incardina dei valori che potrebbero discostarsi da quelli del paziente. Essa può, ad esempio, operare con l'obiettivo di massimizzare la vita del paziente, oppure di garantirne il più possibile la qualità della vita, oppure ancora preferire terapie farmacologiche a interventi chirurgici, sulla base dei valori di programmazione.

Sta dunque al medico, una volta

- Verificata la rappresentatività del paziente all'interno del sistema di IA;
- Informato il paziente del suo utilizzo;
- Forniti eventuali chiarimenti sui benefici attesi e le logiche decisionali impiegati, nonché risolte eventuali ritrosie all'impiego da parte del paziente;
- Validato l'output fornito dalla macchina;

Verificare la corrispondenza tra la terapia suggerita e la volontà del paziente. Quest'ultimo aspetto è da considerarsi tendenzialmente residuale per la fase diagnostica, ove minori sono i profili valoriali da considerare ed è invece di primaria importanza la corretta individuazione della patologia in corso, poiché altrimenti si pregiudica, a cascata, l'intero svolgimento della relazione e la sicurezza delle cure.

## 2. Il regime di responsabilità

La disciplina della responsabilità e la valutazione della diligenza professionale in ambito sanitario non hanno subito modifiche o aggiustamenti in relazione

all'impiego dell'IA, con riguardo agli interventi di diritto sia nazionale sia sovranazionale.

L'art. 7 della legge n. 132/2025 (Uso dell'intelligenza artificiale in ambito sanitario e di disabilità) lascia impregiudicata l'autonomia professionale del medico (la cui responsabilità continua a essere disciplinata ai sensi della legge c.d. Gelli-Bianco n. 24/2017); oltre ai doveri informativi già citati, richiede che i sistemi d'intelligenza artificiale siano affidabili e verificati e ne esclude l'utilizzo per condizionare e selezionare l'accesso alle prestazioni sanitarie secondo criteri discriminatori.

L'impiego dell'intelligenza artificiale non altera, in conclusione, il regime della responsabilità professionale (dell'operatore e della struttura), che resta, dunque, il medesimo, secondo la disciplina tradizionalmente predisposta dagli artt. 1176, 1218, 2043 e 2236 c.c.

Vale a dire:

- l'IA non rende la pratica medica un'attività pericolosa ai sensi dell'art. 2050 c.c. (ipotesi di responsabilità oggettiva);

- l'IA non interrompe il nesso causale tra l'evento dannoso e la condotta del medico: atteso che su di esso spetta la decisione ultima, non pare necessaria la comprensione di cosa abbia determinato l'erroneo risultato prodotto dall'IA. Tuttavia, questa soluzione potrebbe venire meno nel caso in cui la macchina, in futuro, esegua autonomamente la prestazione di cura o parti di essa;

- l'obbligazione del medico rimane 'di mezzi' e la sua diligenza continua a fondarsi sul criterio della colpa: il paziente non può pretendere un 'risultato' corretto per il solo fatto che sia impiegata l'IA, così come il curante non può invocare le criticità sollevate dall'IA per trincerarsi dietro lo speciale regime delle prestazioni caratterizzate dalla soluzione di problemi tecnici di speciale difficoltà (art. 2236 c.c.), che continua ad avere natura eccezionale;

- i sistemi di IA non sono ancora assimilati alle linee guida o alle buone pratiche clinico-assistenziali (ai fini dell'esenzione di responsabilità), ma si prestano a divenire parte dello stato dell'arte richiesto per la corretta esecuzione delle prestazioni;

-all'ultimo rilievo si accompagna il possibile irrigidimento del dovere di diligenza del medico rispetto alle 'modalità' con cui abbia impiegato lo strumento. In particolare, si parla di *duty to stay abreast* per indicare il dovere di formarsi e tenersi costantemente aggiornato sullo strumento impiegato, così come di profili di negligenza nell'inserimento di dati scorretti in input oppure di mancata verifica di corretto funzionamento del sistema prima di impiegarlo;

-la struttura sanitaria continua a rispondere in via contrattuale per le condotte di cui sopra da parte dei propri medici, nonché a titolo di 'difetto di organizzazione': la struttura sanitaria deve formare adeguatamente il proprio personale; aggiornare tempestivamente il sistema; monitorare e verificare il corretto funzionamento dello strumento prima dell'impiego, potendo essa andare esente da responsabilità solo laddove dimostri che il malfunzionamento sia stato determinato da difetti di fabbricazione o da cause non rilevabili con un'ispezione diligente. → in caso di autonoma prestazione da parte della macchina, si ventila il possibile scivolamento del regime di responsabilità in capo al produttore oppure all'ente certificatore.

## *Considerazioni Giuridiche e ricerca biomedica*

### *Quadro normativo di riferimento*

L'impiego di sistemi di intelligenza artificiale nella ricerca biomedica richiede la contestualizzazione in un quadro normativo multilivello, caratterizzato dall'integrazione di fonti europee e nazionali.

La Legge 23 settembre 2025, n. 132 ("Disposizioni e deleghe al Governo in materia di intelligenza artificiale") qualifica come di rilevante interesse pubblico - ai sensi dell'art. 9, par. 2, lett. g, GDPR - il trattamento di dati sanitari e genetici finalizzato alla ricerca e sperimentazione scientifica nella realizzazione di sistemi di IA per scopi terapeutici e farmacologici.

Il Regolamento (UE) 2024/1689 (AI Act) classifica come ad alto rischio i sistemi di IA destinati alla valutazione e assegnazione di trattamenti sanitari o all'elaborazione di decisioni clinicamente rilevanti, imponendo requisiti stringenti di gestione del rischio, trasparenza algoritmica, human oversight e sorveglianza post-commercializzazione.

Il Regolamento (UE) 2016/679 (GDPR) disciplina il trattamento dei dati sanitari come categorie particolari (art. 9), richiedendo basi giuridiche specifiche, minimizzazione dei dati, pseudonimizzazione e DPIA (Data Protection Impact Assessment) per trattamenti ad alto rischio. L'art. 89 riconosce deroghe per la ricerca scientifica, purché adottate garanzie tecniche e organizzative adeguate.

Allo stato delle attuali conoscenze tecniche e normative, non è possibile garantire l'assoluta anonimizzazione dei dati, potendosi invece unicamente procedere a un processo di pseudonimizzazione. Tale metodologia minimizza la possibilità di re-identificazione del soggetto interessato, mantenendo un livello di tutela adeguato e conforme ai principi del Regolamento (UE) 2016/679.

In sintesi, si ritiene pertanto necessario chiarire che, in assenza di specifiche linee guida nazionali sull'anonimizzazione, l'approccio metodologico condiviso con il Data Protection Officer (DPO) prevede il ricorso alla pseudonimizzazione dei dati come misura tecnica e organizzativa appropriata per il perseguimento delle finalità di ricerca, senza necessità di sottoporre la questione al preventivo esame del Garante per la protezione dei dati personali.

È inoltre opportuno chiarire che quando gli algoritmi sviluppati in ricerca vengono incorporati in dispositivi medici (cd. software as medical device, o SaMD), interviene il Regolamento (UE) 2017/745 (MDR), che disciplina la marcatura CE, la validazione clinica e la sorveglianza post-market per prodotti con funzioni di diagnosi, monitoraggio o supporto decisionale. L'intersezione tra MDR e AI Act genera un regime di doppia conformità, con requisiti complementari di performance clinica e robustezza algoritmica.

#### *Specificità: Dati sintetici e protezione dei dati personali*

L'impiego dei dati sintetici nei progetti di ricerca biomedica con intelligenza artificiale solleva questioni giuridiche di primaria importanza. I dati sintetici, generati algoritmicamente a partire da dataset reali attraverso tecniche quali, GAN, modelli di diffusione o privacy differenziale, non determinano automaticamente l'uscita dall'ambito di applicazione del GDPR (Regolamento UE 2016/679). Ai sensi del Considerando 26, i dati possono considerarsi anonimi soltanto qualora non si riferiscano a una persona fisica identificata o identificabile, ovvero qualora sia impossibile o non più possibile identificarne gli interessati. I dati sintetici mantengono la qualifica di dati personali

ogniquale volta, mediante tecniche di inferenza statistica, attacchi di membership inference o correlazione con altri dataset, risulti ragionevolmente possibile ricondurli a singoli individui o a informazioni sensibili relative agli stessi.

L'anonimizzazione irreversibile richiede l'applicazione rigorosa di metriche quantitative che attestino l'assenza di rischi realistici di riconducibilità agli interessati originari. Nel contesto sanitario, l'utilizzo di dati sintetici per l'addestramento o la validazione di modelli di IA impone una valutazione d'impatto sulla protezione dei dati (DPIA) ai sensi dell'art. 35 GDPR, che analizzi specificamente:

- i rischi di re-identificazione diretta o indiretta;
- le basi giuridiche del trattamento (art. 9 par. 2 lett. g/j GDPR per ricerca scientifica di interesse pubblico);
- le misure tecniche e organizzative di sicurezza implementate;
- il coinvolgimento del Comitato Etico e del Responsabile della Protezione dei Dati.

Tali cautele risultano tanto più rilevanti alla luce dell'art. 8, comma 4, della Legge 23 settembre 2025, n. 132, che demanda la definizione di linee guida nazionali per le procedure di anonimizzazione e creazione di dati sintetici nell'ambito della ricerca con IA per finalità terapeutiche e farmacologiche.

## Considerazioni Economiche

Le applicazioni della IA in medicina dal punto di vista economico-sociale vanno valutate seguendo le linee classiche dei modelli di valutazione economica e HTA.

Le dimensioni chiave da tenere presente sono

- Impatto economico (quindi costi ed efficienza, costo efficacia)
- Accessibilità ed equità alle cure
- Possibile riorganizzazione amministrativa (quindi nuovi modelli di business) per gestire le nuove tecnologie/i nuovi percorsi

Il tipo di analisi da condurre si può ricondurre sostanzialmente a tre filoni

**Minimizzazione del costo.** Questa analisi è appropriata quando l'outcome atteso dell'intervento (di solito misurato in termini di anni di vita statistici attesi guadagnati (eventualmente pesati per la qualità della vita) non cambia. In questo caso l'analisi può essere fatta solo sui costi attesi dei diversi metodi. Va fatta particolare attenzione in questa valutazione ad analizzare tutti i costi che un cambiamento di percorso può comportare e anche una analisi degli eventuali diversi rischi economici che possono derivare (rischi per esempio legati a possibili controversie legali, richieste di danni da parte di pazienti che riterranno che una certa scelta fatta dalla AI ha portato loro un danno).

**Analisi costo efficacia classica.** È appropriata per un intervento/HTA rivolto al trattamento di una patologia per cui non esiste una cura efficace, un percorso già prestabilito. In questo caso, partendo dai risultati dei trial clinici comunque conclusi, si andrà a valutare il costo per unità di efficacia e si valuterà se tale costo è sopportabile. Anche in questo caso attenzione ai possibili rischi economici.

**Analisi costo efficacia incrementale.** Probabilmente quella di più comune utilizzo per valutare l'opportunità dell'utilizzo dell'intelligenza artificiale in molte applicazioni di ricerca. Si tratta di valutare rispetto ad una tecnologia/percorso già esistente l'opportunità di sostituirla con una nuova. In questo caso si andrà a valutare i benefici in termini incrementali (i maggiori benefici) rispetto ai maggiori costi. Anche in questo caso vanno valutati i diversi rischi che possono derivare dalla applicazione dei diversi processi

Per quanto riguarda il secondo punto (accessibilità ed equità) alle cure, questa analisi si rende necessaria in due contesti

Quando l'utilizzo di uno strumento diagnostico o di cura può richiedere competenze da parte del paziente o l'utilizzo di tecnologie che non tutti potrebbero avere. Per esempio, alcuni strumenti di controllo richiedono l'utilizzo di internet e di banda larga che potrebbe non essere disponibile a tutta la popolazione

Studiare quali tipi di pazienti beneficerebbero della tecnologia per evitare di concentrare tutte le risorse solo su quelle patologie che portano ai benefici maggiori.

Entrambi questi aspetti potrebbero essere meno importanti nella gestione clinica ospedaliera in cui gli operatori sono formati e la disponibilità dei sistemi informatici accessori è già stata verificata. Possono invece essere (soprattutto il primo) elementi importanti nel caso di prescrizione di percorsi terapeutici che prevedano anche un controllo del paziente da remoto.

Per quanto riguarda la ricerca, l'applicazione della valutazione economica andrà in parallelo con quella tradizionale legata ad accertare se i nuovi farmaci/devices sono costo efficaci. In questo caso le nuove potenzialità della AI hanno messo in luce come talvolta alcune fasi del percorso di ricerca possano essere sostituite/affiancate/ridotte da analisi condotte con AI. In questo caso, previo riscontro positivo dalla clinica medica, si può fare una analisi costo efficacia relativa all'uso della AI in alternativa/in parallelo nella sperimentazione secondo i principi generali dell'analisi costo-beneficio. In particolare, in questo caso può essere interessante distinguere alcune figure diverse, in particolare

Utilizzo di strumenti di AI nel corso di una sperimentazione clinica, anche dove tale percorso possa essere cambiato a seguito dell'utilizzo della AI.

Sviluppo di strumenti di AI da utilizzare in applicazioni cliniche o di ricerca.

Utilizzo di strumenti di AI per attività correlate alla divulgazione della ricerca/applicazione clinica della stessa.

Nel primo caso la valutazione economica è abbastanza lineare in quanto il principio da usare è sempre lo stesso: valutare i benefici rispetto ai costi. In questo caso diventa importante elaborare anche un solido modello di rischio legato all'uso di possibili pratiche non consolidate.

Nel secondo caso, un aspetto che nel tempo potrebbe diventare importante è legato alla sostenibilità dal punto di vista economico e ambientale della tecnologia. Va ricordato che la AI è una tecnologia energivora il cui consumo di risorse non è ancora stato completamente internalizzato nei prezzi del suo utilizzo. In questo caso gli enti regolatori potrebbero chiedere ulteriore documentazione, analisi più approfondite, un diverso protocollo per la registrazione e ovviamente l'analisi economica dovrà essere adeguata alle nuove indicazioni.

Nel terzo caso mentre il vantaggio economico in termini di tempo è indubbio, ci sono altri rischi che devono essere presi in considerazione: la possibilità che il documento non sia preciso, "allucinazioni" da parte della AI, utilizzo di materiale soggetto a copyright.

Va inoltre considerato che molti di questi processi sono altamente regolati per quanto riguarda sia il loro utilizzo (mediante una registrazione presso un ente regolatorio e/o la loro rimborsabilità) che la divulgazione scientifica. Il regolatore stesso potrebbe prevedere strumenti ad hoc per la valutazione economica dei risultati della ricerca a cui sarà ovviamente necessario adeguarsi.

L'attività clinica lascia invece più margini di libertà agli operatori in quanto ad oggi non esistono delle specifiche linee guida per quanto riguarda la valutazione economica legata al loro utilizzo. In questo contesto, oltre alla sostenibilità della tecnologia nel lungo periodo è importante valutare il punto di vista dell'analisi e cioè rispetto a chi (il provider, l'acquirente, il paziente, la società) si considerano costi e benefici. Questo aspetto è per esempio molto importante nei casi di cambiamenti di percorsi terapeutici o riorganizzazioni che possano cambiare l'assetto dell'offerta di prestazioni.

Nel caso di valutazioni economiche applicate alle attività gestionali, l'ambito è quello non tanto di un percorso terapeutico clinico che produce un cambiamento organizzativo (tale valutazione andrà gestita all'interno della valutazione economica in ambito clinico) quanto di applicazioni di IA che abbiano come oggetto il cambiamento dell'organizzazione del lavoro al livello amministrativo.

In questo caso le regole da seguire sono simili a quelle elencate in precedenza, sebbene uno strumento di analisi costo-beneficio classico sia probabilmente più appropriato di uno strumento di analisi costo-efficacia, data la natura del tipo di variabili in gioco per cui la valutazione in termini monetari è molto più semplice. L'analisi da svolgere in questo caso è molto simile al modello dell'analisi costo beneficio finanziaria con le opportune modifiche per tenere conto della natura non profit dell'attività ospedaliera.

## IA e Sistemi Organizzativi e Gestionali in Sanità

L'adozione strutturale dell'IA nei sistemi sanitari non può prescindere da un'analisi delle implicazioni organizzative e delle trasformazioni necessarie in termini di governance, competenze e infrastrutture. L'integrazione di questa tecnologia nei processi di valutazione e decisione richiede infatti un adattamento non solo metodologico, ma anche istituzionale. Dal punto di vista delle strutture sanitarie, l'utilizzo di dati sintetici implica la disponibilità di infrastrutture digitali ad alte prestazioni, capaci di supportare processi di generazione, validazione e archiviazione dei dati. Questo comporta investimenti in architetture cloud, potenza computazionale e soluzioni di cybersecurity, coerenti con i più recenti standard europei in materia di interoperabilità e sicurezza dei dati.

Sul piano delle risorse umane, si evidenzia la necessità di competenze interdisciplinari che integrino conoscenze di tipo biomedico, statistico, informatico e regolatorio.

Il personale coinvolto nei processi HTA, nei comitati etici, nei centri di ricerca e nelle agenzie dovrà essere formato per comprendere e valutare le logiche di generazione dei dati sintetici e il loro impiego in modelli di simulazione e valutazione.

Dal lato istituzionale, occorre rafforzare il ruolo di enti pubblici (come Agenzia Nazionale per i Servizi Sanitari Regionali - AGENAS, Istituto Superiore di Sanità - ISS e i centri HTA regionali) nella definizione di standard metodologici e nella funzione di terza parte per la certificazione di dataset sintetici e modelli predittivi. Questo è cruciale per evitare asimmetrie informative tra sponsor industriali e valutatori pubblici.

In particolare, per garantire la validità dei modelli economici alimentati da dati sintetici, è essenziale che questi siano integrati con fonti amministrative, come i flussi Schede di Dimissione Ospedaliera (SDO), farmaceutica e ambulatoriale. L'accesso a tali dati (in forma aggregata o anonimizzata) consente di calibrare e validare gli algoritmi generativi, migliorando la credibilità e l'accettabilità regolatoria dei profili simulati.

Infine, i dati sintetici non sono solo uno strumento tecnico per la ricerca e l'HTA, ma potrebbero rappresentare anche un vero e proprio asset strategico per la governance dei sistemi sanitari. La loro capacità di simulare artificialmente scenari possibili offre ai decisori pubblici nuove possibilità operative, tra cui:

valutare ex ante l'impatto di nuove tecnologie o modelli organizzativi;

stimare la sostenibilità economica e l'equità distributiva di diverse strategie di rimborso;

anticipare squilibri tra domanda e offerta in specifiche aree terapeutiche o territori.

Nel medio periodo, i dati sintetici potranno essere utilizzati anche per analisi di budget impact a livello nazionale o regionale, nonché integrati nei processi di programmazione sanitaria. Affinché ciò avvenga in modo efficace, sarà però essenziale garantire: trasparenza metodologica, validazione indipendente dei modelli e una governance condivisa delle infrastrutture dati.

## Approvvigionamento tecnologia AI

Le procedure per l'introduzione di dispositivi di IA devono seguire i percorsi ordinari previsti per le tecnologie già presenti nella struttura ospedaliera. Tuttavia, esse devono essere integrate con strumenti di valutazione che permettano di evidenziare le peculiarità della specifica tecnologia IA proposta dal clinico.

In particolare, è opportuno affiancare ai criteri tradizionali (economici, tecnici e organizzativi) ulteriori elementi di analisi, quali la validazione clinica degli algoritmi, la trasparenza e spiegabilità dei modelli, il livello di integrazione con i sistemi informativi esistenti, nonché gli aspetti etici, legali e di sicurezza dei dati.

Solo attraverso un approccio valutativo integrato è possibile garantire che l'adozione di tecnologie di IA in ambito ospedaliero sia non solo conforme alle normative vigenti, ma anche realmente efficace, sicura e sostenibile nel contesto clinico-organizzativo.

Pertanto, è opportuno utilizzare come strumento l'HTA, già citata nei paragrafi precedenti, e il *value based procurement* che può tradurre al meglio l'efficienza e l'efficacia dei nuovi strumenti tecnologici in ambito diagnostico.

In modo particolare, considerando la velocità di innovazione nel campo dell'IA, è utile l'applicazione dell'*Hospital Based (HB) HTA* al fine di rispettare i tempi dei processi interni. L'HB HTA è l'applicazione del processo di valutazione delle tecnologie sanitarie all'interno delle singole strutture ospedaliere ed è in genere utilizzata dal gruppo di HTA aziendale che si rapporta anche con la commissione regionale. Infatti, a differenza dell'HTA nazionale, che definisce linee guida generali, l'HB-HTA supporta la direzione strategica dell'ospedale nel decidere se introdurre, mantenere o dismettere una specifica tecnologia basandosi sul contesto reale e sulle risorse di quella specifica struttura.

Il Value Based Procurement (VBP) rappresenta l'evoluzione del tradizionale approccio agli acquisti pubblici e privati, orientando le decisioni di procurement non al prezzo più basso, ma al valore complessivo generato dalla soluzione lungo l'intero ciclo di vita. Il valore è inteso in senso ampio e multidimensionale economico, operativo, organizzativo, sociale e, in alcuni contesti, ambientale e

viene valutato considerando benefici attesi, performance, rischi e costi indiretti nel medio-lungo periodo.

A differenza del procurement tradizionale, centrato sull'ottimizzazione del costo iniziale, il VBP mira a massimizzare l'impatto complessivo della fornitura in coerenza con gli obiettivi strategici dell'organizzazione. Sulla base della definizione sopra delineata, è possibile individuare quattro **obiettivi** principali del VBP:

**Massimizzazione del valore nel ciclo di vita**: attraverso la considerazione del *Total Cost of Ownership (TCO)*, che include costi di implementazione, integrazione, manutenzione, aggiornamento, gestione operativa e dismissione;

**Allineamento strategico**: volto a garantire che le decisioni di acquisto siano coerenti con gli obiettivi strategici dell'organizzazione;

**Orientamento agli outcome**: per cui l'acquisto è valutato non solo in base alle caratteristiche della fornitura, ma in relazione ai risultati concreti che consente di ottenere (ad esempio riduzione dei tempi di processo, miglioramento dell'accuratezza decisionale, incremento della produttività);

**Integrazione della gestione del rischio**: che considera, oltre ai rischi finanziari, anche quelli operativi, tecnologici, normativi e reputazionali, al fine di selezionare soluzioni robuste e sostenibili nel tempo.

La **struttura** del VBP si articola in quattro capisaldi operativi:

**Definizione del valore atteso**: individuazione degli outcome strategici e dei benefici che l'organizzazione intende conseguire attraverso l'acquisto;

**Valutazione multidimensionale delle alternative**: analisi comparativa basata su criteri economici, tecnici e organizzativi, includendo il TCO e gli impatti lungo il ciclo di vita;

**Selezione orientata agli outcome**: scelta della soluzione che massimizza il valore complessivo rispetto agli obiettivi strategici, superando la logica del minor prezzo;

**Monitoraggio e verifica delle performance**: definizione di indicatori (KPI) *a priori* e meccanismi di controllo per assicurare che il valore previsto sia effettivamente realizzato nel tempo.

L'attuale sviluppo di strumenti di IA è sicuramente indirizzato all'ambito clinico-diagnostico, ma sono presenti sul mercato diverse soluzioni anche per l'ambito tecnico-amministrativo, che saranno sempre più presenti nel prossimo futuro. Si citano a esempio le applicazioni nei processi di acquisto (supporto alle commissioni di valutazione, supporto alla stesura delle specifiche tecniche, strumenti integrati ai software gestionali delle ingegnerie cliniche, etc.)

Oltre che l'acquisto di nuove tecnologie con o senza IA è necessario considerare anche il problema della loro gestione. L'IA non è una tecnologia tradizionale, di conseguenza richiede una multidisciplinarietà nella gestione per la quale è strategica la collaborazione tra più attori, il cui core sono Ingegneria Clinica (IC), Sistemi Informativi Aziendali (SIA) e i Clinici, ma a seconda della tecnologia possono essere coinvolte altre figure (es. Fisica Medica per la gestione delle applicazioni in diagnostica per immagini).

È quindi necessario che per tali tecnologie, siano esse acquisti, sperimentazioni, università, noleggi, donazioni..., si segua il percorso di richiesta formale come per qualsiasi altra tecnologia medica (P-SIC709 Approvvigionamento di beni e servizi, P-SIC704 Emissione proposte d'ordine e ModSIC70401 Check-list donazione apparecchiature). Il processo vale anche per la richiesta visione di apparecchiature o software caratterizzati dalla presenza di AI (P-SIC706 Prova visione).

Le soluzioni AI che vengono introdotte all'interno delle aziende sanitarie devono essere opportunamente tracciate; è necessario quindi avere un database dedicato che contenga le opportune informazioni che permettano l'Azienda anche un facile interfacciamento con le ditte fornitrici in caso di eventuali problematiche.

Risulta inoltre altrettanto strategica la stipula di contratti che prevedano al loro interno l'inclusione di eventuali aggiornamenti tecnologici, fondamentali affinché la tecnologia AI risulti adeguata alle ultime release.

## **Formazione Digitale Continua**

L'intelligenza artificiale (IA) si configura come una leva strategica e trasformativa per il potenziamento e l'aggiornamento continuo delle competenze dei professionisti sanitari.

Attraverso algoritmi di apprendimento adattivo e tecniche di machine learning, l'IA è in grado di personalizzare i percorsi formativi in tempo reale, modulando contenuti e modalità didattiche in funzione del profilo professionale, del livello di esperienza, delle performance pregresse e degli specifici ambiti di pratica clinica.

Un contributo particolarmente rilevante riguarda l'evoluzione degli ambienti di simulazione avanzata. L'integrazione tra IA, realtà virtuale e realtà aumentata consente di sviluppare scenari clinici altamente realistici e immersivi, ulteriormente potenziati da modelli generativi capaci di produrre casi clinici strutturati e personalizzati. Tali strumenti favoriscono l'addestramento interdisciplinare e multiprofessionale, contribuendo al perfezionamento delle competenze cliniche, decisionali e relazionali (es.: counseling etico-familiare), in contesti controllati che riducono il rischio clinico reale e promuovono la sicurezza delle cure.

Parallelamente, i sistemi di tutoring intelligente, tra cui chatbot basati su modelli linguistici avanzati, supportano lo sviluppo del ragionamento clinico. Analizzando dati provenienti da cartelle cliniche elettroniche e altre fonti sanitarie, questi strumenti facilitano l'interpretazione di pattern complessi (ad esempio biomarcatori in malattie rare) e contribuiscono a migliorare l'appropriatezza prescrittiva, limitando fenomeni di sovra-utilizzo diagnostico.

Un ulteriore ambito di applicazione riguarda la valutazione delle competenze. L'IA consente di implementare sistemi di assessment continui e oggettivi, basati su analisi predittive delle performance in simulazioni e test adattivi. Ne derivano feedback granulari, tempestivi e personalizzati, utili per monitorare in tempo reale i progressi formativi, individuare specifiche aree di miglioramento (ad esempio in ambito di bioetica digitale) e pianificare interventi mirati, superando i limiti delle valutazioni tradizionali, spesso episodiche e soggettive.

In questo quadro, l'intelligenza artificiale deve essere intesa come uno strumento complementare e non sostitutivo del ruolo centrale dei formatori e dei tutor clinici, i quali garantiscono qualità pedagogica, supervisione critica,

contestualizzazione culturale ed etica, inclusa l'attenzione ai potenziali bias algoritmici, nonché una dimensione relazionale ed empatica imprescindibile.

L'integrazione dell'IA nei percorsi formativi biomedici richiede pertanto un solido ancoraggio a principi normativi e regolatori (quali l'AI Act dell'Unione Europea e le linee guida AGENAS), promuovendo un uso consapevole e critico delle tecnologie, lo sviluppo della digital literacy e la costruzione di un sistema sanitario sempre più competente, integrato, resiliente e centrato sulla persona.

I programmi di formazione digitale per le professioni sanitarie sono oggi molto diffusi e offrono corsi ECM (Educazione Continua in Medicina) online e FAD, focalizzati su telemedicina, intelligenza artificiale, sicurezza informatica e strumenti digitali. Piattaforme come [IkosECM.it](https://www.ikosecm.it), [ACCMED](https://www.accmед.it), e iniziative del Piano Nazionale di Ripresa e Resilienza ([PNRR](https://www.pnrr.it)) [Salute](https://www.salute.gov.it) rispondono all'obbligo formativo, potenziando le competenze tecniche e manageriali del personale sanitario.

Considerando l'alto grado di specializzazione e i differenti ambiti formativi, è consigliabile non rivolgersi ad un unico programma formativo, tanto più se questo programma è generalista. Piuttosto, è opportuno che il programma di formazione digitale sia scelto in base al proprio interesse e soprattutto in base alle esigenze della propria professione sanitaria.

Questi programmi sono essenziali per l'aggiornamento continuo, la gestione della telemedicina e l'integrazione delle tecnologie digitali nel lavoro quotidiano.

#### **Ambiti Chiave della Formazione Digitale Sanitaria sono:**

- **Sanità Digitale e Telemedicina:** Corsi sulla gestione del paziente a distanza e strumenti innovativi.
- **Intelligenza Artificiale (IA) in Medicina:** Applicazioni dell'IA nelle discipline specialistiche.
- **Intelligenza Artificiale (IA) per le Attività Gestionali:** Applicazioni dell'IA nel settore gestionale sanitario, opportunità e rischi.
- **Sicurezza e Data Protection:** Corsi in cybersecurity e protezione dei dati in ambito sanitario.
- **Digital Marketing in Sanità:** Strategie di comunicazione online, gestione social e CRM.

## **Autori**

Il presente testo è stato composto e redatto da parte dei componenti del Comitato di Indirizzo per l'Impiego dell'Intelligenza Artificiale.

### *Coordinatori:*

Prof. Domenico Russo

Dott. Aldo Maria Roccaro

### *Componenti:*

Dott.ssa Francesca Brognoli

Dott.ssa Simona Cacace

Prof.ssa Nicoletta Cusano

Dott.ssa Rosa Coppola

Ing. Claudia Duri

Dott.ssa Frida Fagandini

Prof. Alfonso Gerevini

Prof.ssa Rosella Levaggi

Dott.ssa Gemma Marelli

Ing. Fabio Marinoni

Ing. Giovanni Poggialini

Dott.ssa Elena Tratta

Ing. Gian Luca Viganò

Ing. Davide Zanchi

## **1 Allegato 1: Panoramica Strutturata dell'uso clinico dell'IA in Medicina**

Di seguito una panoramica strutturata, con particolare attenzione agli ambiti più maturi, ai modelli organizzativi e ai limiti regolatori.

### ***1.1 Diagnostica per immagini***

L'area più avanzata e regolata. Gli algoritmi di deep learning sono oggi integrati nei PACS come strumenti di triage, pre-lettura o prioritizzazione. Impatti operativi: riduzione dei tempi di refertazione, identificazione precoce di findings critici (emorragie intracraniche, embolie polmonari, fratture, noduli polmonari), segmentazione automatica per la pianificazione terapeutica. I dispositivi sono soggetti a marcatura CE e FDA, con validazioni multicentriche.

### ***1.2 Anatomia patologica digitale***

La digital pathology consente l'uso di modelli di visione artificiale per classificare pattern istologici, quantificare biomarcatori (Ki-67, PD-L1), identificare rare cellule patologiche, valutare margini chirurgici. Si riducono variabilità inter-osservatore e tempi di refertazione. Si affaccia ora la patologia computazionale integrata: correlazione tra immagine istologica, genotipi e fenotipi clinici mediante modelli multimodali.

### ***1.3 Analisi genomica e medicina di precisione***

L'IA accelera l'interpretazione di varianti, la predizione dell'impatto funzionale, la classificazione ACMG e la definizione di driver. Nei tumori ematologici, gli algoritmi sono impiegati per: predire rischi di evoluzione (es. CH verso tMN), integrare mutazioni con dati clinici, selezionare candidati a terapie target. In prospettiva, modelli multimodali (sequenziamento, imaging, dati clinici longitudinali) alimenteranno sistemi di decision support personalizzati.

## *1.4 Applicazioni consolidate nei laboratori*

- Interpretazione automatica di emocromi e strisci periferici con reti neurali.
- Microbiologia: identificazione rapida di pattern in immagini di colonie, predizione resistenze da dati fenotipici/genotipici.
- Anatomia patologica digitale: quantificazione di marker, grading tumori, identificazione di rare cellule.

## *1.5 Supporto diagnostico*

Applicazioni ormai standardizzate, integrate nei flussi clinici.

- Radiologia: algoritmi di triage e prioritizzazione degli esami (es. sospetta emorragia cerebrale, embolia polmonare, fratture).
- Cardiologia: interpretazione automatica avanzata di ECG, eco con quantificazione automatica, rilevazione precoce di insufficienza cardiaca.
- Dermatologia: classificazione di lesioni cutanee sospette con performance comparabile allo specialista nei casi definiti.
- Endoscopia: assistenza in tempo reale nella rilevazione di polipi (CADE) e nella caratterizzazione (CADx), con aumento del tasso di individuazione.

## *1.6 Identificazione precoce del deterioramento clinico*

L'AI supporta sistemi di allerta intraclinica per i pazienti ricoverati.

- Early Warning Systems (EWS) basati su machine learning: predizione rischio di arresto cardiaco, shock settico, deterioramento respiratorio.
- Automazione del monitoraggio: analisi continua dei parametri vitali, riduzione dei falsi allarmi e interventi più tempestivi.

## *1.7 Chirurgia e procedure interventistiche*

L'AI affianca robotica e sistemi di imaging intraoperatorio.

- Navigazione chirurgica con segmentazione automatica delle strutture.

- Predizione dinamica della traiettoria ottimale dell'intervento.
- Supporto nella radiologia interventistica (fusion imaging, needle guidance, riduzione dose radiazioni).

### *1.8 Personalizzazione terapeutica*

Viene utilizzata per ottimizzare trattamenti complessi o con margine terapeutico ristretto.

- Oncologia: predizione di tossicità, risposta, NRM, recidiva; selezione dei candidati a terapie target o CAR-T.
- Ematologia e trapianto: modelli per stimare probabilità di GVHD, infezioni severe, mortalità a 100 giorni, rischio di recidiva post-HSCT.
- Nefrologia: ottimizzazione della dialisi e predizione precoce della necessità di CRRT in terapia intensiva.
- Terapia intensiva: modelli di dose optimization per sedazione, ventilazione e fluid management.

### *1.9 Automazione dei flussi clinici*

Incrementa produttività e riduce errori documentali.

- Trascrizione automatica certificabile delle visite e refertazione assistita negli EHR.
- Riempimento dei campi strutturati e riconciliazione farmaci.
- Sistemi di priorità automatici in Pronto Soccorso e agenda ambulatoriale.
- Supporto alla codifica (ICD-10, DRG) con riduzione dei tempi amministrativi.

### *1.10 Supporto alla decisione clinica (CDSS)*

Integrati nei sistemi EHR, suggeriscono decisioni coerenti con linee guida aggiornate.

- Avvisi su interazioni farmacologiche, dosaggi, controindicazioni specifiche.
- Percorsi diagnostico-terapeutici automatizzati (care pathways) personalizzati sul singolo paziente.
- Analisi predittiva per stratificare i pazienti in base al rischio e ottimizzare allocazione risorse.

Uso degli Agenti Intelligenti in Gruppi Multidisciplinari a supporto decisionale per la diagnosi, prognosi e terapia dei pazienti affetti da malattie neoplastiche e non neoplastiche.

### *1.11 Sanità pubblica ed epidemiologia*

Utilizzi consolidati: predizione di focolai, modellizzazione di trasmissione, ottimizzazione delle risorse ospedaliere, sorveglianza in tempo reale. L'uso in Italia sta crescendo ma richiede infrastrutture digitali e interoperabilità.

### *1.12 Telemedicina e gestione territoriale*

Integrazione di IA nei dispositivi domiciliari e nei servizi remoti:

- Analisi automatica di dati da device wearable o sensori (aritmie, apnea, scompenso).
- Follow-up automatizzato dei pazienti cronici con stratificazione del rischio.
- Chatbot clinici certificabili per triage preliminare.

### *1.13 Governance, qualità e sicurezza*

Strumenti IA integrati nei sistemi ospedalieri per migliorare performance e sicurezza.

- Predizione carichi di lavoro e bed management.
- Ottimizzazione logistica di sale operatorie e flussi di pazienti.
- Analisi degli eventi avversi per pattern ricorrenti e prevenzione.

### *1.14 Trend*

- Modelli multimodali che integrano testo clinico, imaging, laboratorio e genomica in un'unica piattaforma.
- Assistenti clinici real-time integrati nell'EHR (anamnesi, note, referti, suggerimenti terapeutici).
- Validazioni regolatorie più rapide (EU AI Act, FDA SaMD) con versioning controllato.

### *1.15 Limiti, rischi e governance*

- Dati: qualità, eterogeneità, bias, necessità di rappresentatività.
- Privacy: compliance GDPR, pseudonimizzazione, uso secondario dei dati.
- Spiegabilità: fondamentale per ambiti ad alto rischio clinico (EMA, MDR 2017/745).
- Regolazione: necessità di audit continui, monitoraggio post-market, versioning controllato dei modelli.
- Responsabilità professionale: il medico rimane responsabile; l'AI è uno strumento, non un decisore.

## **Allegato 2: Panoramica Strutturata sulle Applicazioni di IA nella Ricerca**

Principali applicazioni dell'intelligenza artificiale nella ricerca biomedica e clinica, con particolare attenzione ai domini oggi più maturi e a quelli emergenti.

### ***1.1 Discovery di nuovi target e riposizionamento dei farmaci***

L'AI accelera le fasi precoci della ricerca preclinica.

- Analisi di reti di interazione gene–proteina per identificare target terapeutici.
- Modelli generativi per progettare molecole con proprietà farmacologiche desiderate.
- Screening virtuale ad alta capacità per individuare composti attivi.
- Drug repurposing: identificazione di farmaci già approvati potenzialmente efficaci in nuove indicazioni, riducendo tempi e costi.

### ***1.2 Analisi multiomica e medicina di precisione***

I modelli ML integrano genomica, trascrittomica, proteomica, metabolomica e fenotipo clinico.

- Identificazione di sottotipi molecolari.
- Predizione di vulnerabilità terapeutiche.
- Costruzione di biomarcatori compositi (genetici + clinici + imaging).
- Analisi evolutive del tumore e ricostruzione delle clonalità.

### ***1.3 Modellazione della progressione di malattia***

L'AI è utilizzata per costruire modelli predittivi longitudinali.

- Identificazione di pattern precoci che anticipano peggioramento clinico o recidiva.
- Modelli di sopravvivenza non lineari (random survival forests, deep survival analysis).
- Ricostruzione dei percorsi di malattia in condizioni croniche o oncologiche.

## *1.4 Sviluppo di biomarcatori digitali*

Emergono nuove tecniche che trasformano dati non strutturati in biomarcatori misurabili.

- Imaging: radiomics, pathomics, segmentazioni e feature estratte da reti neurali.
- Audio e linguaggio: biomarcatori vocali in neurologia e psichiatria.
- Wearable: segnali fisiologici continui trasformati in predittori quantitativi.

## *1.5 Ottimizzazione della sperimentazione clinica*

L'AI interviene nel design, nella conduzione e nell'analisi degli studi.

- Selezione dei pazienti mediante modelli predittivi di eleggibilità.
- Synthetic control arms basati su real-world data quando eticamente appropriato.
- Adaptive trial design con supporto algoritmico per randomizzazione e modulazione delle dose-escalation.
- Analisi automatizzata di note cliniche non strutturate per endpoint complessi.

## *1.6 Analisi di real-world data e real-world evidence*

La crescente disponibilità di EHR, registri, biobanche e dati di laboratorio consente analisi su larga scala.

- Identificazione di pattern emergenti, tossicità rare, complicanze post-terapia.
- Creazione di modelli generalizzabili validati in coorti multisito.
- Epidemiologia computazionale per studiare incidenza, burden e outcome.

## *1.7 Generazione e sintesi di conoscenza scientifica*

Modelli linguistici avanzati supportano la ricerca nella gestione della letteratura.

- Review automatizzate o semi-automatiche di studi.

- Estrazione di evidenze, relazioni, conclusioni da grandi corpus.
- Generazione assistita di ipotesi e sperimentazione concettuale.

### *1.8 Ottimizzazione dei workflow sperimentali e di laboratorio*

L'IA guida robotica e automazione.

- Pianificazione automatica di esperimenti.
- Ottimizzazione della sintesi chimica e delle condizioni di reazione.
- Analisi cellulare mediante imaging ad alta capacità.

### *1.9 Ricerca traslazionale guidata da modelli multimodali*

In rapida evoluzione.

- Integrazione di testo clinico, immagini, sequenziamento, laboratorio.
- Predizione di risposta terapeutica personalizzata.
- Identificazione di correlati biologici della risposta (mechanistic insights).

### *1.10 Frontiere emergenti*

- Foundation models biologici (modelli addestrati su scale tipo AlphaFold, ESM, Perceiver IO).
- In-silico trials: simulazioni computazionali per prevedere effetti di nuove terapie.
- AI per editing genomico (ottimizzazione guide CRISPR, predizione off-target).
- Digital twins del paziente per scenari terapeutici personalizzati.

#### *1.10.1 Applicazione di AI nella generazione di nuovi farmaci*

Applicazioni dell'intelligenza artificiale nella generazione di nuovi farmaci, dall'identificazione del target alla fase preclinica.

##### *1.10.1.1 Identificazione di nuovi target terapeutici*

L'AI accelera la fase più costosa e incerta della ricerca farmacologica.

- Analisi di reti biologiche (gene-gene, proteina-proteina) per identificare nodi critici da colpire.

- Predizione degli effetti funzionali delle mutazioni (pathogenicity ranking) per distinguere driver e passenger.

- Integrazione multiomica (genomica, single-cell, proteomica) per derivare target specifici di sottoclone tumorali o microambienti patologici.

- Identificazione di pathway attivabili o inibibili con approccio systems biology.

#### 1.10.1.2 *Screening virtuale e ranking dei composti*

L'IA riduce drasticamente il numero di esperimenti in vitro necessari.

- Accelerated virtual screening: reti neurali che predicono affinità ligando-target più velocemente dei metodi docking tradizionali.

- Filtering intelligente: modelli QSAR avanzati per escludere composti tossici o instabili.

- Prioritizzazione dinamica dei composti in base a potenza prevista, solubilità, permeabilità e ADMET.

#### 1.10.1.3 *Generazione de-novo di molecole (Generative Chemistry)*

Una delle aree più rivoluzionarie: la chimica generativa.

- Modelli generativi (VAE, GAN, diffusion models) progettano molecole da zero con proprietà target-specifiche.

- Ottimizzazione multi-obiettivo: un'unica molecola viene generata per bilanciare potenza, selectivity, logP, clearance, e profilo di sicurezza.

- Fine-tuning personalizzato: il modello si adatta a famiglie di composti o target specifici (es. KRAS, FLT3, BTK).

- Risultato: tempi di discovery ridotti da anni a mesi o settimane.

#### 1.10.1.4 *Ottimizzazione strutturale guidata da AI*

Dopo aver individuato un candidato, l'AI migliora iterativamente la molecola.

- Predizione modifiche chimiche che aumentano stabilità, riducono tossicità o migliorano biodisponibilità.

- Simulazioni rapide di interazioni proteina-ligando (AI-driven molecular dynamics).

- Saturazione virtuale del sito attivo: suggerimento di sostituzioni R-group mirate.

#### 1.10.1.5 *Previsione ADMET (Absorption, Distribution, Metabolism, Excretion, Toxicity)*

Questa è l'applicazione più consolidata e ampiamente validata.

- Modelli predittivi più accurati dei metodi tradizionali di regressione e QSAR.
- Rilevazione anticipata di epatotossicità, cardiotossicità, interazioni con CYP450, potenziale QT prolongation.
- Previsione della biodisponibilità orale e barriere di permeabilità (BBB, GI).

#### 1.10.1.6 *Biologia strutturale guidata da IA*

- AlphaFold e simili hanno rivoluzionato la predizione strutturale delle proteine.
- Modelli docking AI-native predicono binding pose più accuratamente dei motori classici.
- Possibilità di progettare biologici (anticorpi, peptidi) con binding affinities ottimizzate.

#### 1.10.1.7 *Accelerazione della ricerca preclinica*

- Pianificazione automatica di esperimenti in vitro/in vivo.
- Analisi automatizzate di immagini (microscopia, istologia, high-content screening).
- Riduzione del numero di animali necessari grazie a simulazioni in-silico.

#### 1.10.1.8 *Drug repurposing con IA*

Particolarmente utile in oncologia, malattie rare, infettivologia.

- Algoritmi che correlano profili trascrizionali di malattie e farmaci.
- Identificazione di composti noti con potenziale efficacia su nuovi target o pathway.
- Esempi clinici: farmaci antivirali, immunomodulatori, antineoplastici individuati tramite reti di similarità farmacogenomica.

#### 1.10.1.9 *In-silico trials e digital twins*

Tecnologie emergenti che anticipano efficacia e tossicità prima degli studi umani.

- Simulazione di popolazioni virtuali per valutare risposta e variabilità interindividuale.
- Test di combinazioni terapeutiche, previsione sinergie e antagonismi.
- Possibile integrazione futura con pazienti virtuali basati su modelli multiomici reali.

#### 1.10.1.10 *Impatto su tempi e costi*

I primi benchmark industriali mostrano:

- Riduzione del tempo di lead identification da 4–5 anni a 6–12 mesi.
- Diminuzione dei costi di circa il 40–60% nelle fasi early discovery.
- Maggior tasso di candidati con buon profilo ADMET, quindi minor tasso di fallimento in fase clinica.

## **1 Allegato 3: IA Enti Regolatori, Privacy e Cybersecurity**

### **1.1 IA per registrazione di farmaci da parte degli Enti Regolatori: EMA, FDA, AIFA**

L'IA sta entrando nei processi regolatori soprattutto come leva di efficienza e di qualità: non “approva” farmaci al posto degli enti, ma viene usata (o valutata) per gestire volumi documentali enormi, identificare incoerenze, supportare ispezioni, migliorare farmacovigilanza, e – in alcuni ambiti – analizzare dati complessi (real-world data, segnali di sicurezza, qualità manifatturiera). La direzione generale è abbastanza chiara: aumentare capacità operativa e robustezza delle decisioni, mantenendo tracciabilità, spiegabilità e responsabilità umana.

#### **1.1.1 Dove l'AI impatta davvero il ciclo di registrazione**

##### **1.1.1.1 Dossier e review**

- triage e classificazione: smistamento di moduli, allegati, versioni, e “pattern” di criticità ricorrenti (es. incongruenze tra CTD, protocollo e CSR).
- estrazione e confronto: estrazione automatica di dati da report clinici (CSR), tabelle, narrative, e confronto con quanto dichiarato nel label/SmPC proposto.
- quality checks: individuazione di duplicazioni, refusi con impatto regolatorio, incongruenze di definizioni endpoint, o mismatch tra SAP e analisi eseguite.

##### **1.1.1.2 Qualità e CMC**

analisi di trend produttivi e deviazioni: modelli per rilevare drift, outlier e segnali precoci su lotti, impurità, stabilità, OOS/OOT.

controllo integrità dati: supporto a risk-based inspections e detection di anomalie su audit trail e data provenance.

### 1.1.1.3 Sicurezza post-marketing (farmacovigilanza)

- signal detection: modelli su EudraVigilance/FAERS per prioritizzare segnali, cluster inattesi, e accelerare valutazioni.
- case processing: automazione parziale su codifica MedDRA, deduplicazione, triage di ICSRs, con supervisione.

### 1.1.1.4 Real-world evidence e studi non randomizzati

Non è “IA che prova efficacia”, ma strumenti per gestire bias, linkage di database, fenotipizzazione, e analisi su coorti: utile soprattutto per sicurezza, sub-popolazioni, comparators esterni, e conferme post-approvazione.

### 1.1.1.5 Prodotti che incorporano IA (SaMD/AI-medical devices) e “AI-enabled drug development”

Se l’algoritmo è parte del prodotto (diagnostico, decision support, digital biomarker), entrano requisiti specifici (validazione, change management, monitoraggio prestazionale). Per i farmaci, l’IA è spesso “strumento di sviluppo” (es. selezione target, disegno trial, analisi), e l’ente chiede: riproducibilità, governance, e evidenze che non aumenti bias o errori.

## 1.2 EMA:

Attualmente EMA ha un approccio: prudente e molto “governance-centrico” riguardo all’impiego di AI in medicina. L’EMA punta a integrare AI soprattutto su farmacovigilanza, gestione del lifecycle e qualità dei processi di assessment.

Principali topics:

- come sono stati generati, curati e ri-versionati i dataset usati per analisi (soprattutto RWE o text mining);
- tracciabilità delle trasformazioni (data lineage) e controlli di qualità;
- trasparenza metodologica: se usate modelli, quali assunzioni, performance, validazione esterna, robustezza e sensitivity analyses;
- gestione del rischio di bias (per popolazioni, centri, geografie).

## 1.3

### 1.4 FDA:

FDA mostra un approccio: storicamente più “operational” e sperimentale su strumenti di review e sorveglianza, con particolare enfasi su standard, auditing e replicabilità. In parallelo, la FDA spinge concetti come RWE quando ben governata.

Principali topics:

- aspettative forti su validazione e auditability (soprattutto se un’analisi AI/ML influenza decisioni cliniche o label);
- stress test e generalizzabilità (shift di popolazione, qualità variabile dei dati, missingness);
- attenzione al “model risk management” se l’AI è usata in processi core.

Dove è più visibile: sorveglianza sicurezza (FAERS), ispezioni e integrità dati, e, lato device, framework più espliciti per AI/ML (utile come analogia quando un farmaco dipende da un componente digitale).

### 1.5 AIFA:

AIFA svolge un ruolo e ha una specificità del tutto nazionale (italiana). AIFA non “replica” l’assessment EMA per i prodotti centralizzati: spesso il fulcro nazionale è rappresentato dal prezzo e rimborso (HTA, negoziazione), registri, appropriatezza, e monitoraggio. Qui l’IA può diventare molto rilevante in tre aree:

A) valutazione del valore e impatto sul SSN

- analisi di RWE italiana (flussi amministrativi, registri AIFA, database regionali) per stimare effectiveness, persistenza, safety in routine.
- supporto a modelli di costo-efficacia e budget impact, con gestione più efficiente di sottogruppi e scenari.

B) registri e Managed Entry Agreements

- data quality: pulizia, deduplicazione, controlli di coerenza.
- identificazione precoce di pattern di inappropriatezza o scostamenti dai criteri di eleggibilità.

### C) farmacovigilanza nazionale e segnali locali

Prioritarizzazione casi e segnali, con focus su popolazioni specifiche e co-prescrizioni tipiche.

#### *1.6 Gli Enti che valutano progetti/dossier includenti "IA" chiedono:*

- governance: chi è responsabile, quali SOP, quali controlli, quali audit.
- riproducibilità: si può rifare l'analisi e ottenere lo stesso risultato (versioni di codice, modelli, dati).
- trasparenza: anche se il modello è complesso, dovete poter spiegare cosa guida il risultato e come avete controllato l'errore.
- bias e fairness: rischio di performance diversa per età, sesso, etnia/geografia, comorbidità, centri.
- change control: cosa succede se il modello "si aggiorna" (o se cambiano i dati in input).
- impatto decisionale: l'IA è solo supporto operativo o influenza direttamente claims/label/decisioni cliniche?

#### *1.7 Implicazioni/indicazioni concrete "regulatory-ready" per la preparazione di un dossier*

- È necessario chiarire, all'interno del dossier, dove sono stati impiegati i sistemi di IA, e a quale scopo.
- L'impiego di IA va documentato in tutte le fasi del processo: dataset, preprocessing, feature engineering, training/validation, performance, limiti, sensitivity analyses.
- È consigliabile preparare un "pacchetto di audit", che includa la tracciatura delle versioni, i codici e i controlli qualità, oltre a un piano di monitoraggio post approvazione, se ritenuto pertinente.
- È consigliabile evitare i claim eccessivi.

## *1.8 Uso dei dati sintetici ricavati da dati reali e privacy*

L'uso di dati sintetici derivati da dati reali è diventato centrale nei progetti di intelligenza artificiale, soprattutto nei settori regolati come sanitario e farmaceutico, perché offre potenziali vantaggi di privacy, efficienza e condivisione dei dati. Tuttavia, il rapporto tra dati sintetici e privacy non è banale: la sicurezza non è automatica e dipende da come i dati vengono generati, validati e governati.

I dati sintetici sono set di dati generati algebricamente per riprodurre proprietà statistiche e pattern dei dati reali, senza contenere direttamente informazioni identificabili sugli individui. Possono essere creati tramite modelli statistici o tecniche di IA generativa (ad esempio GAN, modelli di diffusione, o sistemi che apprendono la distribuzione dei dati reali).

In sanità e nella ricerca clinica questi dati consentono di:

- addestrare o testare modelli senza esporre dati sensibili;
- simulare scenari rari o gruppi di controllo;
- condividere dataset tra team o partner senza trasferire dati reali.

## *1.9 Dati sintetici e privacy*

### **A) Privacy come obiettivo principale**

L'idea alla base dell'uso di dati sintetici è di ridurre al minimo o eliminare l'esposizione di informazioni personali, rendendo possibile lavorare con grandi dataset pur rispettando i requisiti di privacy imposti da norme come il GDPR nell'Unione Europea o HIPAA negli Stati Uniti.

Il GDPR definisce "dati personali" come qualunque informazione relativa a una persona identificata o identificabile. Se un dataset sintetico non permette la re-identificazione degli individui, in teoria non è soggetto alle stesse restrizioni dei dati reali.

### **B) Ridurre l'esposizione ai rischi di implicazioni legali**

Se i dati generati sono realmente non correlabili ai dati d'origine, possono essere trattati come dati anonimi, semplificando la compliance alla normativa vigente, non ricadendo più nell'ambito di applicazione del GDPR.

#### C) Rischio di re-identificazione

In alcune condizioni un dataset sintetico può riprodurre dettagli troppo simili a dati reali e consentire tecniche di re-identificazione o inferenza sugli individui originali. Questo succede soprattutto quando il modello genera punti dati troppo vicini ai reali, o gli outlier del dataset reale sono riprodotti fedelmente.

In questi casi i dati sintetici possono essere considerati ancora dati personali, e quindi soggetti a GDPR o normative equivalenti.

#### D) Difficoltà nel definire l'"anonimizzazione"

E' necessario distinguere tra:

pseudonimizzazione: trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile (Art. 4 del Regolamento UE 2016 679). Si tratta di una forma di de-identificazione reversibile, qualora si disponga di informazioni aggiuntive.

anonimizzazione: trasformazione dei dati personali in modo tale che non sia più possibile identificare l'interessato, né direttamente né indirettamente, nemmeno con l'impiego di tutte le tecnologie e le informazioni ragionevolmente utilizzabili, e che tali dati non siano più riconducibili a una persona fisica identificata o identificabile. Si tratta di un processo di de-identificazione irreversibile.

I dati sintetici potrebbero essere teoricamente anonimi. Tuttavia, possono ancora contenere segnali che permettono inferenze.

La valutazione normativa di quando un set sintetico sia davvero “anonimo” non è ancora completamente uniformata tra giurisdizioni.

#### E) Tecniche per mitigare i rischi di privacy

Per assicurare che i dati sintetici rispettino i requisiti di privacy e non violino normative come il GDPR, si adottano tecniche come:

- Privacy differenziale

Un approccio che aggiunge rumore controllato ai dati in modo da limitare la possibilità di ricavare informazioni su singoli individui pur mantenendo utilità statistica.

- Valutazioni di re-identification risk

La generazione responsabile di dati sintetici include metriche che stimano la probabilità di re-identificazione e altre misure quantitative di privacy.

- Validazioni e audit esterni

Per scenari regolati (es. studi clinici, RWE), è spesso necessario audit indipendente della qualità del dataset sintetico e delle tecniche di generazione per garantire compliance e robustezza.

### **Implicazioni regolatorie e normative**

#### A) Nel contesto del GDPR

Non è ancora del tutto chiaro se dati sintetici generati da modelli IA possano essere sempre considerati pienamente anonimizzati;

L'interpretazione tende a essere pragmatica: se i dati non consentono re-identification con metodi ragionevoli, possono essere trattati come sicuri dal punto di vista dei dati personali.

#### B) Nel contesto di regolatori di settore

Nel settore sanitario e farmaceutico, enti come EMA, FDA o autorità nazionali (ad es. AIFA) non hanno posizioni univoche ma osservano con interesse l'uso di dati sintetici come strumento per ricerca, test e addestramento di modelli purché siano accompagnati da robuste garanzie di privacy e trasparenza metodologica.

### **Conclusione operativa**

L'uso di dati sintetici può essere un potente strumento per bilanciare utilità dei dati e protezione della privacy se:

- le tecniche di generazione sono ben documentate e validate;
- vengono adottate misure per minimizzare rischi di re-identificazione;
- la governance include audit, metriche quantitative di privacy e controlli di qualità.

In assenza di questi presupposti, un dataset sintetico potrebbe non essere considerato veramente anonimo e rimanere soggetto a normative sulla protezione dei dati.

### *1.10 IA e Cybersecurity*

Il rapporto tra intelligenza artificiale e cybersecurity è ormai strutturale e bidirezionale: l'IA è contemporaneamente uno strumento di difesa sempre più indispensabile e un moltiplicatore di capacità offensive. Per questo oggi la sicurezza informatica non viene più progettata “senza IA”, ma nemmeno può fidarsi ciecamente dell'IA stessa.

#### *1.10.1 Perché l'IA è diventata centrale nella cybersecurity*

I sistemi informativi moderni producono volumi di dati (log, eventi, traffico di rete, endpoint telemetry) che superano la capacità umana e anche quella dei sistemi rule-based tradizionali. L'IA consente di:

- analizzare grandi flussi di dati in tempo reale;
- individuare pattern complessi e non ovvi;
- adattarsi a minacce nuove o mutate;
- ridurre tempi di rilevazione e risposta (MTTD, MTTR).

In sintesi: senza IA, la difesa è oggi strutturalmente in ritardo rispetto all'attacco.

#### *1.10.2 Uso dell'IA nella difesa (AI for cybersecurity)*

##### *A) Detection e anomaly detection*

L'uso più maturo è l'individuazione di comportamenti anomali rispetto a una baseline appresa automaticamente. Questo vale per:

- traffico di rete (NDR);
- endpoint (EDR/XDR);
- accessi e identità (UEBA);
- cloud e ambienti ibridi.

Il valore dell'AI non è "riconoscere una firma nota", ma identificare deviazioni sottili, movimenti laterali, living-off-the-land attacks.

#### B) Threat intelligence e correlazione

Modelli IA correlano segnali deboli provenienti da fonti diverse (log, IOC, feed esterni, dark web) e producono priorità di rischio realistiche. Questo riduce drasticamente i falsi positivi, uno dei principali problemi dei SOC tradizionali.

#### C) Incident response e automazione

L'IA supporta (e in parte automatizza) playbook di risposta:

- isolamento di endpoint;
- blocco di credenziali;
- rollback di modifiche sospette;
- triage degli alert.

La decisione finale resta umana nei contesti critici, ma l'IA accelera enormemente le fasi iniziali.

#### D) Vulnerability management

Analisi predittiva delle vulnerabilità realmente sfruttabili, integrando CVE, contesto di sistema, esposizione reale e comportamento osservato. Questo supera l'approccio puramente numerico dei CVSS score.

### *1.11 Uso dell'IA nell'attacco (cybersecurity against us)*

L'IA abbassa la soglia di competenza tecnica necessaria per attaccare.

Si riportano di seguito alcuni esempi di campi in cui l'impiego di IA può facilitare attacchi online, rendendone più difficile l'intercettazione ai sistemi di protezione attualmente in uso.

#### A) Social engineering avanzato

phishing altamente personalizzato;

spear phishing generato automaticamente;

deepfake vocali e video per frodi (CEO fraud, identity spoofing).

Questi attacchi sono molto più credibili e difficili da intercettare con filtri tradizionali.

#### B) Malware adattivo

- codice che muta dinamicamente per eludere firme;
- payload che si attivano solo in determinate condizioni;
- evasione automatica di sandbox e sistemi di analisi.

#### C) Raccolta automatizzata di informazioni

L'IA può scandagliare superfici di attacco, configurazioni cloud, repository pubblici e comportamenti umani con una velocità e profondità non raggiungibili manualmente.

#### D) Attacchi "AI-native"

Stanno emergendo attacchi progettati specificamente contro sistemi IA:

- data poisoning;
- model inversion;
- membership inference;
- prompt injection (per LLM integrati in sistemi aziendali).

### *1.12 La cybersecurity dell'IA (AI security)*

Un punto spesso sottovalutato: l'AI stessa diventa un asset critico da proteggere.

#### A) Rischi principali

- addestramento su dati compromessi o non affidabili;
- esposizione di dati sensibili attraverso il modello;
- comportamento non deterministico e non auditabile;
- dipendenza da modelli esterni (supply chain risk).

#### B) Superficie di attacco ampliata

Un sistema IA introduce nuovi vettori:

- input malevoli (prompt, immagini, segnali);

- modelli ospitati su cloud terzi;
- pipeline di training e retraining automatico.

### C) Governance e controlli

La sicurezza dell'IA richiede:

- controllo dei dati di training;
- versioning e tracciabilità dei modelli;
- testing avversariale;
- monitoraggio continuo delle performance e dei drift.

### *1.13 Regolazione e contesti ad alta criticità*

Nei settori regolati (sanità, finanza, infrastrutture critiche, difesa) l'uso dell'IA in cybersecurity è visto come necessario, ma solo se:

- spiegabile e auditabile;
- governato da SOP chiare;
- integrato con responsabilità umana;
- conforme a principi di sicurezza by design e privacy by design.

In Europa questo dialoga direttamente con GDPR (protezione dei dati), NIS2 (sicurezza delle reti e dei sistemi) ed AI Act (classificazione del rischio e obblighi).

### *1.14 Implicazioni strategiche*

Tre messaggi chiave:

1. Non usare IA in cybersecurity oggi equivale a essere strutturalmente vulnerabili.
2. Usare IA senza comprenderne limiti e rischi crea una falsa sensazione di sicurezza.
3. La vera competenza non è "implementare sistemi di IA", ma saperli governare, testare e integrare.

La cybersecurity moderna non è una guerra uomo-macchina, ma una guerra di sistemi socio-tecnici complessi, in cui l'AI è un acceleratore, non un sostituto del giudizio.



## 1 Allegato 4: Survey sull'impiego di sistemi IA all'interno di ASST Spedali Civili di Brescia

Nel mese di settembre 2025, è stata condotta una survey interna all'ASST Spedali Civili di Brescia, per rilevare quali sistemi con IA fossero in uso, sia in area clinica che in area di ricerca.

La survey è stata inviata a tutti i Responsabili di struttura complessa, ed ai titolari di incarichi quali Struttura Semplice, o Specializzazione.

Si riportano di seguito i risultati della survey, suddivisi per Area di implementazione (area ricerca o area clinica).

Area clinica:

| Cluster Funzionale                          | Tipologia di Applicazione                                                                                                                    | Strutture Coinvolte                                                       |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| Imaging & Diagnostica Avanzata              | Segmentazione automatica (sostanza bianca/grigia), analisi volumetrica e diametrica (Angio TC), studi funzionali e imaging 3D.               | Neuroradiologia, Chirurgia Vascolare, Radiologia Pediatrica, Dermatologia |
| Supporto al Trattamento & Chirurgia         | Autosegmentazione per radioterapia, generazione immagini CT sintetiche (MRCAT), realtà aumentata per planning prechirurgico.                 | Fisica Sanitaria, Radioterapia, Chirurgia Pediatrica                      |
| Analisi di Laboratorio & Citologia          | Classificazione automatica della morfologia cellulare (sospetta leucemia), pre-classificazione di preparati microscopici ed elettroforetici. | Laboratorio Analisi, Ematologia, Fisica Sanitaria                         |
| Sistemi Predittivi & Decision Support (DSS) | Previsione ipotensione intraoperatoria                                                                                                       | Anestesia e Rianimazione, Endocrinologia                                  |
| Screening e Prevenzione                     | Riconoscimento e caratterizzazione automatica di polipi coloretali durante esami endoscopici.                                                | Endoscopia Interventistica                                                |
| Sviluppo & Ricerca (Open Source)            | Creazione di reti neurali e Deep Learning per applicazioni di fisica medica; analisi radiomica e dosiomatica.                                | Fisica Sanitaria                                                          |

Studi clinici:

| Area di patologia               | Sigla dello Studio | Obiettivo dello studio                                                                                                                                                                                                                              | Impiego IA                                                                         | Status autorizzativo       |
|---------------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|----------------------------|
| <b>Oncoematologia</b>           | VEN DEC AI         | Proof of concept. Esplorativo per valutare la possibilità di confermare risultati ottenuti da uno studio farmacologico di fase II                                                                                                                   | Utilizzo di IA generativa per la generazione di dati sintetici                     | Autorizzato                |
| <b>Malattie Cardiovascolari</b> | AIM HEALTH         | Valutare l'efficacia di un sistema di IA generativa nella produzione di un documento che combini le informazioni della lettera di dimissione ospedaliera originale con quelle fornite durante il colloquio di dimissione con il personale sanitario | Utilizzo di IA generativa per la redazione del documento da consegnare al paziente | In corso di autorizzazione |
| <b>Nefrologia</b>               | AIM HEALTH         | Valutare l'efficacia di un sistema di IA generativa nella produzione di un documento che combini le informazioni della lettera di dimissione ospedaliera originale con quelle fornite durante il colloquio di                                       | Utilizzo di IA generativa per la redazione del documento da consegnare al paziente | In corso di autorizzazione |

|  |  |                                             |  |  |
|--|--|---------------------------------------------|--|--|
|  |  | dimissione con il<br>personale<br>sanitario |  |  |
|--|--|---------------------------------------------|--|--|

## **Allegato 5: Manuale Operativo per la gestione delle richieste relative ai sistemi di Intelligenza Artificiale**

Il presente allegato ha come obiettivo quello di regolamentare e fornire indicazioni pratiche su come utilizzare/ richiedere/implementare, all'interno di ASST Spedali Civili di Brescia, "sistemi" di Intelligenza Artificiale, nelle aree clinica, gestionale e di ricerca.

Il documento definisce:

- i percorsi di attivazione delle richieste;
- le strutture aziendali coinvolte;
- le modalità di trasmissione e valutazione delle richieste;
- contenuti essenziali da indicare nella richiesta

### ***Area Clinica e Area Gestionale***

L'impiego nella pratica clinica di un "sistema" di IA (dispositivo, applicazione, software, algoritmo predittivo, o altri sistemi analoghi) può avere impatto sui processi clinici, organizzativi, gestionali e decisionali aziendali.

Pertanto, come dettagliato nel Documento di Indirizzo per l'impiego dell'Intelligenza Artificiale, devono essere tenuti obbligatoriamente in considerazione:

- Le caratteristiche del sistema IA, ovvero: le caratteristiche tecniche che lo connotano come dispositivo IA; la sua certificazione; la sua validazione; il grado di "rischio" relativamente alla funzione per cui viene impiegato;
- la trasparenza nell'utilizzo del sistema IA nell'ambito dei processi aziendali sia di area clinica che gestionale;
- la tracciabilità e documentazione dell'utilizzo del sistema IA.

Per gli aspetti clinici, etici, organizzativi e regolatori si rinvia al Documento di Indirizzo per l'Impiego dell'Intelligenza Artificiale.

Qualora si volesse introdurre o implementare un nuovo "sistema" di intelligenza artificiale (IA), in ambito clinico o gestionale è necessario procedere come segue. Il richiedente, evidenziata la necessità di approvvigionarsi del sistema di IA, deve far pervenire la richiesta alla S.C. Ingegneria Clinica, compilando la modulistica necessaria ("Modulo richiesta apparecchiature", che verrà digitalizzata e avrà una sezione dedicata agli strumenti di AI). La S.C. Ingegneria Clinica attiva, per quanto di competenza, i percorsi aziendali in essere, permettendo al richiedente di monitorare lo stato della richiesta tramite l'applicativo aziendale SIC (Software Ingegneria Clinica). L'elaborazione della richiesta coinvolgerà il

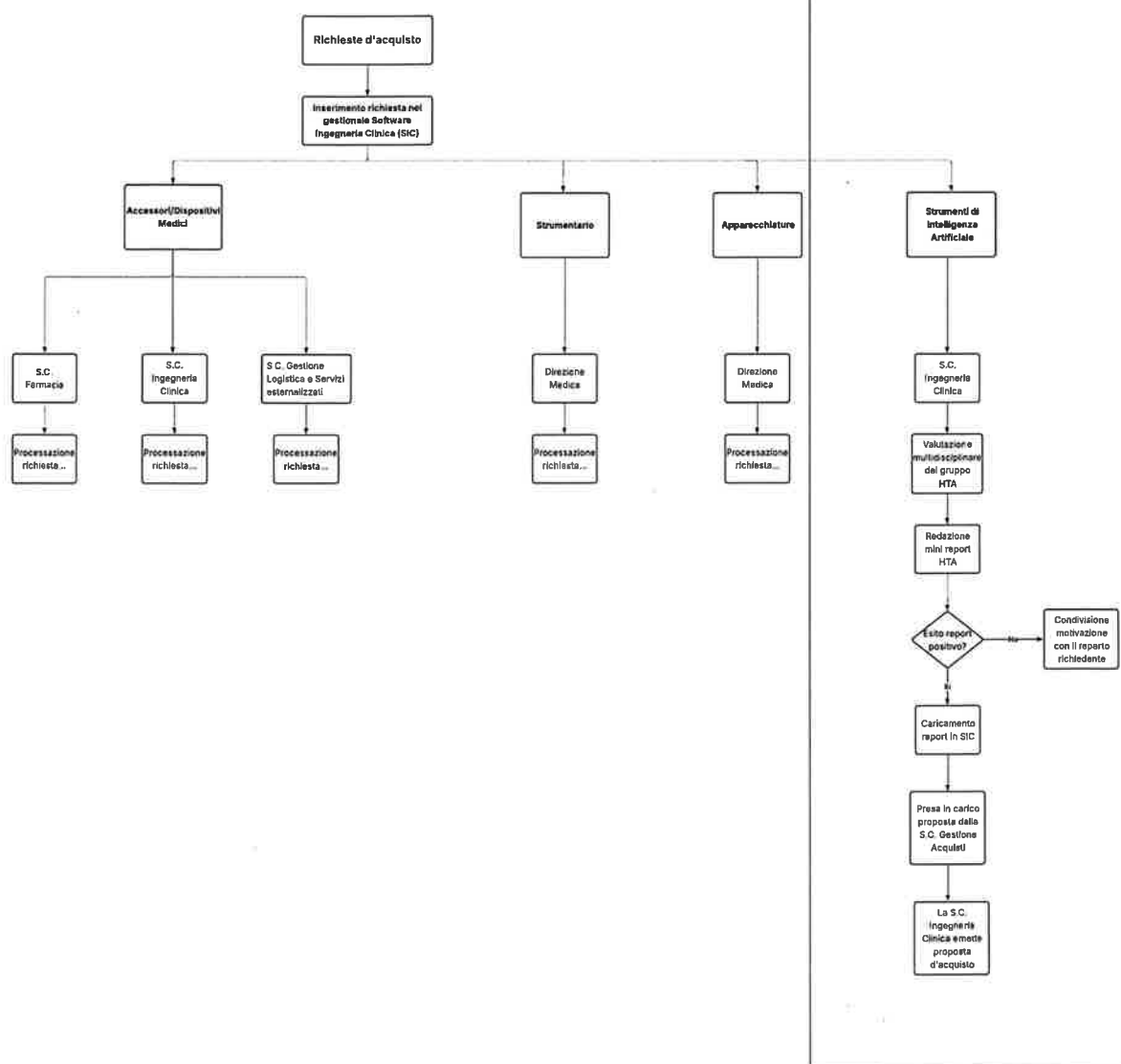
gruppo HTA (Health Technology Assessment) aziendale (comprendente Ingegneria Clinica, Sistemi Informativi Aziendali, Direzione Medica di Presidio, Reparto richiedente, altri professionisti ritenuti utili all'analisi) e produrrà un mini-report HTA con le valutazioni effettuate ed un giudizio finale, che in caso di esito positivo darà l'avvio alla verifica delle risorse necessarie ed al relativo processo di acquisto.

Il percorso è sinteticamente rappresentato nel diagramma in Figura 1.

Qualora il sistema richiesto comporti il trattamento di dati personali, riferiti a qualunque soggetto interessato, l'HTA coinvolgerà l'Ufficio Privacy che effettuerà le dovute valutazioni di competenza, di concerto con il DPO (Data Protection Officer) aziendale al fine di attuare gli adempimenti previsti dalla vigente normativa in materia di protezione dei dati personali.

La richiesta, ai fini delle rispettive valutazioni di competenza, deve contenere almeno:

- finalità del sistema e ambito di utilizzo;
- descrizione sintetica della soluzione proposta in cui viene anche dettagliata la logica algoritmica utilizzata e come il sistema di I.A intende garantire il rispetto del principio di non discriminazione.
- eventuale produttore/fornitore;
- presenza di marcatura CE (ove applicabile) e scheda tecnica;
- tipologia dei dati trattati, con indicazione dell'eventuale trattamento di dati personali/sanitari;
- eventuale utilizzo di servizi cloud o piattaforme esterne;
- eventuale necessità di interoperabilità con sistemi aziendali;
- necessità di installazione software o acquisizione dispositivi.



**Figura 1: Flusso processazione richiesta di acquisto per strumenti di intelligenza artificiale**

Al termine della procedura di acquisizione, il Gruppo HTA notificherà l'esito al richiedente e al Comitato di Indirizzo per l'Impiego di Intelligenza Artificiale, che terrà traccia dei sistemi IA introdotti in ASST degli Spedali Civili di Brescia, entro un termine massimo di 90 giorni dalla data della richiesta.

## **Area di Ricerca**

Gli studi clinici che prevedano l'impiego di "sistemi" di intelligenza artificiale possono essere distinti in due fattispecie, come previsto dalla legge 132/2025.

### ***Ricerca e sperimentazione scientifica per la realizzazione di sistemi di intelligenza artificiale in ambito sanitario***

Qualora il progetto di ricerca si proponga di realizzare "sistemi" di IA in ambito sanitario, è necessario in primo luogo redigere un protocollo di studio, redatto secondo i dettami della normativa e delle linee guida vigenti, che includa una descrizione il più possibile dettagliata del sistema che si intende sviluppare/addestrare, dei dati necessari all'addestramento, delle caratteristiche tecniche del sistema, fornendo, anche sotto forma di allegato, tutta la documentazione tecnica disponibile relativamente al "sistema" AI.

### ***Ricerca e sperimentazione tramite sistemi di intelligenza artificiale e machine learning (art. 9, primo comma)***

Anche nel caso in cui ci si intenda avvalere di un sistema di IA per la conduzione di uno studio clinico, il primo passaggio è la redazione del protocollo di studio, che includa la descrizione e le caratteristiche del "sistema" IA che si intende utilizzare, oltre che la fase dello studio in cui si prevede di utilizzarlo (esempio: fase di randomizzazione, fase di selezione dei soggetti arruolabili, etc.)

La bozza di protocollo deve essere trasmessa alla S.C. Clinical Trial Center, Laboratorio di Ricerca C.R.E.A., che effettuerà la prima revisione e le verifiche di primo livello necessarie per proseguire con la progettazione.

Effettuata la prima revisione, la S.C. Clinical Trial Center, Laboratorio di Ricerca C.R.E.A. (CTC) coordina i rapporti con altre Strutture Aziendali competenti, a seconda delle caratteristiche del singolo studio, ivi inclusi l'Ufficio Privacy e DPO aziendale, per le valutazioni di pertinenza, integrando la protezione dei dati personali fin dalla fase di progettazione.

Se, per la realizzazione dello studio, è necessario installare nuovi software sui server aziendali, o apportare modifiche tecniche a quanto già in essere, il richiedente dovrà comunicare la progettualità e richiedere il nullaosta alla S.C. Sistemi Informativi Aziendali (SIA) che, a sua volta, in collaborazione con l'Ufficio Privacy, effettuerà le verifiche tecniche di propria competenza, propedeutiche all'installazione del software, secondo i percorsi in essere.

Se, per la realizzazione dello studio, è necessario acquisire nuovi dispositivi, il richiedente dovrà contattare la S.C. Ingegneria Clinica, che effettua le verifiche di propria competenza per l'acquisizione del dispositivo, secondo i percorsi in essere all'interno dell'ASST Spedali Civili.

L'acquisizione di nuovi software, dispositivi o altri beni deve seguire le procedure aziendali in vigore presso l'Ente al momento della richiesta.

Ciascuna delle strutture coinvolte nel percorso di progettazione dello studio clinico può, qualora lo ritenga necessario, richiedere parere consultivo sullo studio al Comitato per l'impiego dell'Intelligenza Artificiale.

Una volta terminata la progettazione dello studio, e verificatane la fattibilità con tutte le strutture competenti, il CTC coordina l'invio del pacchetto documentale al Comitato Etico Territoriale competente e, se previsto dalla tipologia di studio, all'Autorità Competente, ad es. AIFA, per acquisire i necessari pareri/autorizzazioni.

Lo studio potrà iniziare solo dopo l'emissione dell'autorizzazione della Direzione Generale dell'ASST Spedali Civili di Brescia, una volta acquisiti i pareri e le necessarie autorizzazioni.

Una volta autorizzato, la S.C. Clinical Trial Center notificherà lo studio al Comitato di Indirizzo per l'Impiego dell'Intelligenza Artificiale, che terrà traccia degli studi che prevedono l'impiego di sistemi di IA promossi dall'ASST Spedali Civili di Brescia.