Intelligenza Artificiale in Medicina - Parte quinta

Data 22 marzo 2026
Categoria Medicinadigitale

In questa serie di pillole verrà affrontata un'analisi critica dell'uso della Intelligenza Artificiale (AI) in medicina.

Il quadro normativo europeo: l'AI Act è già in vigore

La questione legata all'uso della AI in medicina non è solo clinica ma anche normativa. Dal 1° agosto 2024 è in vigore il Regolamento (UE) 2024/1689, noto come AI Act: il primo quadro giuridico globale che disciplina in modo organico lo sviluppo, l'immissione sul mercato e l'utilizzo dei sistemi di Intelligenza Artificiale. Per i clinici e le strutture sanitarie che adottano strumenti di supporto diagnostico, le implicazioni sono concrete e immediate.

I sistemi di diagnosi differenziale sono "ad alto rischio"

L'AI Act classifica i sistemi di AI in quattro categorie di rischio. I software di supporto alla decisione clinica che influenzano diagnosi o terapie rientrano a pieno titolo nella categoria "ad alto rischio" (Allegato III, punto 5): sistemi destinati ad essere utilizzati dai professionisti della salute come ausilio nelle decisioni diagnostiche o terapeutiche individuali. Per questi sistemi, il Regolamento prevede i requisiti più stringenti.
Gli obblighi per i sistemi ad alto rischio entreranno in applicazione piena il 2 agosto 2027 per i software embedded in prodotti già regolati — ma le strutture sanitarie e i vendor che intendono evitare rischi regolatori devono avviare i processi di conformità fin d'ora.

Cosa prescrive l'AI Act: trasparenza, spiegabilità, supervisione umana

L'articolo 13 del Regolamento è di particolare rilevanza. Prescrive che i sistemi di AI ad alto rischio siano progettati e sviluppati in modo da garantire che il loro funzionamento sia "sufficientemente trasparente da consentire ai deployer di interpretare l'output del sistema e utilizzarlo adeguatamente". Il deployer, in contesto sanitario, è la struttura ospedaliera o il professionista che utilizza il sistema.
L'articolo 14 aggiunge l'obbligo di supervisione umana effettiva: i sistemi devono essere progettati in modo da poter essere sorvegliati da persone fisiche competenti, che devono essere in grado di riconoscere quando il sistema produce output inaffidabili, prendere decisioni indipendenti e — se necessario — non tener conto dell'output del sistema.
L'articolo 26, che disciplina gli obblighi dei deployer, stabilisce inoltre che chi utilizza un sistema di AI ad alto rischio deve garantire che il proprio personale abbia un'adeguata alfabetizzazione in materia di AI e disponga delle competenze necessarie per interpretare criticamente gli output del sistema.

Il nodo irrisolto: trasparenza dell'output versus fedeltà del ragionamento

Qui emerge una tensione che l'AI Act riconosce implicitamente ma non risolve completamente. Il Regolamento richiede che i sistemi siano "sufficientemente trasparenti" — ma la trasparenza è definita in relazione alla capacità del deployer di interpretare l'output, non alla corrispondenza causale tra spiegazione e calcolo interno. La dottrina giuridica ha già segnalato che la spiegabilità non è sempre perseguibile per sistemi di tipo black-box, e che il Regolamento stesso ammette questo limite richiedendo livelli di trasparenza "adeguati" allo stato dell'arte.
In altre parole: l'AI Act obbliga i vendor a dichiarare i limiti dei propri sistemi e a fornire strumenti per la supervisione umana. Non obbliga — perché allo stato attuale della tecnologia non è possibile — a certificare che le spiegazioni prodotte siano causalmente fedeli al calcolo interno. Questa è la lacuna che la ricerca in interpretabilità meccanicistica sta cercando di colmare.

[i][b]Cosa prevede l'AI Act per i deployer in sanità (sintesi operativa)[/b]

Verificare che il sistema sia classificato correttamente e disponga della documentazione tecnica richiesta (art. 11).
Garantire che il personale che usa il sistema abbia ricevuto formazione adeguata sull'AI (art. 26, comma 2).
Assicurare la supervisione umana effettiva degli output — non come prassi formale, ma come competenza reale (art. 14).
Conservare i log automatici generati dal sistema per almeno sei mesi (art. 26, comma 5).
Segnalare all'autorità competente qualsiasi incidente grave o malfunzionamento che possa causare danni ai pazienti.
Non modificare l'intended purpose del sistema oltre quanto previsto dal vendor senza rivalutare la conformità.[/i]

(Continua)

NB. Le pillole precedenti di questa serie sono state pubblicate in data 22 febbraio 2026, 1 marzo 2026, 8 marzo 2026, 15 marzo 2026.

FaustoBodini