AI e sicurezza dei dati: un equilibrio necessario per la Sanità Digitale

Tecnologie a supporto, non in sostituzione, della competenza medica

Speaker: Ing. Claudio Stamile, PhD, MBA

Manager of AI R&D and Market Solution, Fastweb+Vodafone

Il contesto

Trasformazione in atto

La medicina sta vivendo una **trasformazione digitale** profonda: cartelle elettroniche, imaging, dispositivi connessi, referti digitali. I **dati** sono diventati **parte integrante della pratica clinica.**

Cosa comporta questa evoluzione

Più dati vuol dire più complessità.
Aumenta il carico lavorativo per i medici, con il rischio di perdere tempo clinico su attività burocratiche o tecniche.

Il ruolo potenziale dell'AI

L'Intelligenza Artificiale può essere un alleato per semplificare l'accesso ai dati, velocizzare analisi e sintesi, supportare decisioni cliniche complesse. Ma **deve essere uno strumento, non un sostituto.**

AI specializzata sul dominio medico

Modelli Generalisti

Addestrati su **dati generici** (web, forum, documenti vari).

Ottimi per **compiti trasversali** e linguaggio naturale quotidiano.

Rischiano ambiguità, errori di contesto, interpretazioni superficiali, perché centrati su forme e linguaggi della quotidianità.

Non comprendono la terminologia o i flussi clinici.

Modelli Specialistici

Specializzati su **dati medici**, come documentazione clinica, referti, linee guida.

Conoscono **terminologia medica**, codifiche, pattern tipici.

Possono seguire logiche diagnostiche e ragionamento clinico.

Meglio controllabili, auditabili e più sicuri in ambito sanitario.

La comprensione del dominio è essenziale: **senza contesto clinico, un'AI non può essere uno strumento sicuro per il medico.**

Come passare da un modello generalista ad uno specialista

1

Selezione del modello di base: Partire da un LLM generalista già addestrato su grandi moli di dati. Deve avere capacità linguistiche solide ed essere compatibile con il fine-tuning.

2

Raccolta di dati clinici di qualità: Raccogliere documentazione medica reale (referti, cartelle cliniche, linee guida, note di dimissione, ecc.). Curare la qualità, l'anonimizzazione, e la rappresentatività dei dati.

3

Adattamento al dominio (fine-tuning): Eseguire un fine-tuning supervisionato sul contenuto clinico, mantenendo controlli per evitare errori e imprecisioni. Includere casi d'uso realistici e terminologia specialistica.

4

Validazione e audit clinico: Valutare le prestazioni con esperti clinici. Testare il modello su casi concreti, verificare comportamenti in ambiguità, negazioni, contesto patologico. Misurare sicurezza, affidabilità e aderenza ai protocolli.

Cosa serve davvero in ambito clinico

Affidabilità > creatività

Un modello specializzato, addestrato su contenuti medici, è più vicino agli obiettivi reali della pratica clinica: **chiarezza, coerenza, precisione**. I modelli generalisti, pensati per compiti generici o creativi, possono produrre risposte scorrette o fuori contesto.

Sicurezza e protezione del dato

I dati sanitari sono sensibili e devono essere trattati in **ambienti controllati**. Niente esposizione a servizi cloud non conformi, tracciabilità garantita, e protezione by design.

Trasparenza e tracciabilità

Il medico deve poter **risalire al perché di una risposta**. Servono log, spiegazioni e la capacità del modello di dire "non so".

Integrazione nel flusso clinico

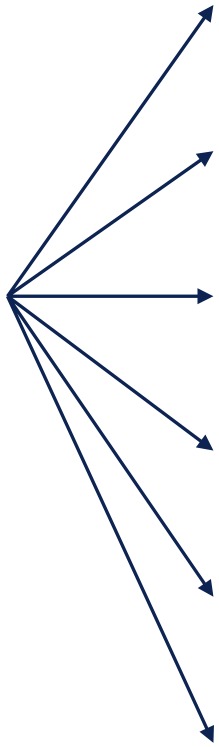
L'AI deve **inserirsi nei flussi decisionali e operativi** del medico in modo naturale, senza stravolgere pratiche consolidate. Deve ridurre il carico, non aggiungere nuovi passaggi o complessità.

Dati sanitari = Dati Critici

- I dati sanitari sono tra le informazioni personali più sensibili che esistano. Raccontano la storia clinica di una persona, il suo stato di salute, le sue fragilità.
- La loro gestione non è solo una questione tecnica, ma un atto che ha implicazioni **etiche**, **legali** e **sociali**.
- In ambito sanitario, non basta che i dati siano "protetti": è fondamentale sapere **dove si trovano fisicamente**, **chi può accedervi** e **sotto quale giurisdizione ricadono**.
- I dati devono essere sempre anonimizzati per il training. L'unica eccezione è quando vengono utilizzati per correggere un bias e non sono possibili altri modi per farlo.
- Le soluzioni che si affidano a infrastrutture generiche o cloud distribuiti su scala globale non rispondono ai requisiti di trasparenza e controllo richiesti dalla pratica clinica.
- La protezione del dato deve essere parte integrante del sistema di cura, non una considerazione accessoria.

Rischi reali: uso improprio dell'AI

L'adozione non controllata di modelli di intelligenza artificiale può introdurre **vulnerabilità cliniche, legali e sistemiche**.



Hallucinations: Generazione di contenuti errati ma plausibili. In sanità, può significare diagnosi o trattamenti inesistenti.

Bias nei dati: Rappresentazione distorta di sesso, etnia, età o condizioni cliniche. Rischio di decisioni discriminatorie o imprecise.

Black-box models: Impossibilità di verificare il ragionamento alla base della risposta. Nessuna auditabilità o tracciabilità.

Esposizione di dati critici: Uso di servizi cloud non conformi può comportare perdita di controllo su localizzazione e accesso ai dati.

Over-reliance: Fiducia eccessiva nel sistema AI da parte del personale sanitario, che porta ad una riduzione del pensiero critico.

… E molte altre!

Requisiti per un ambiente sicuro

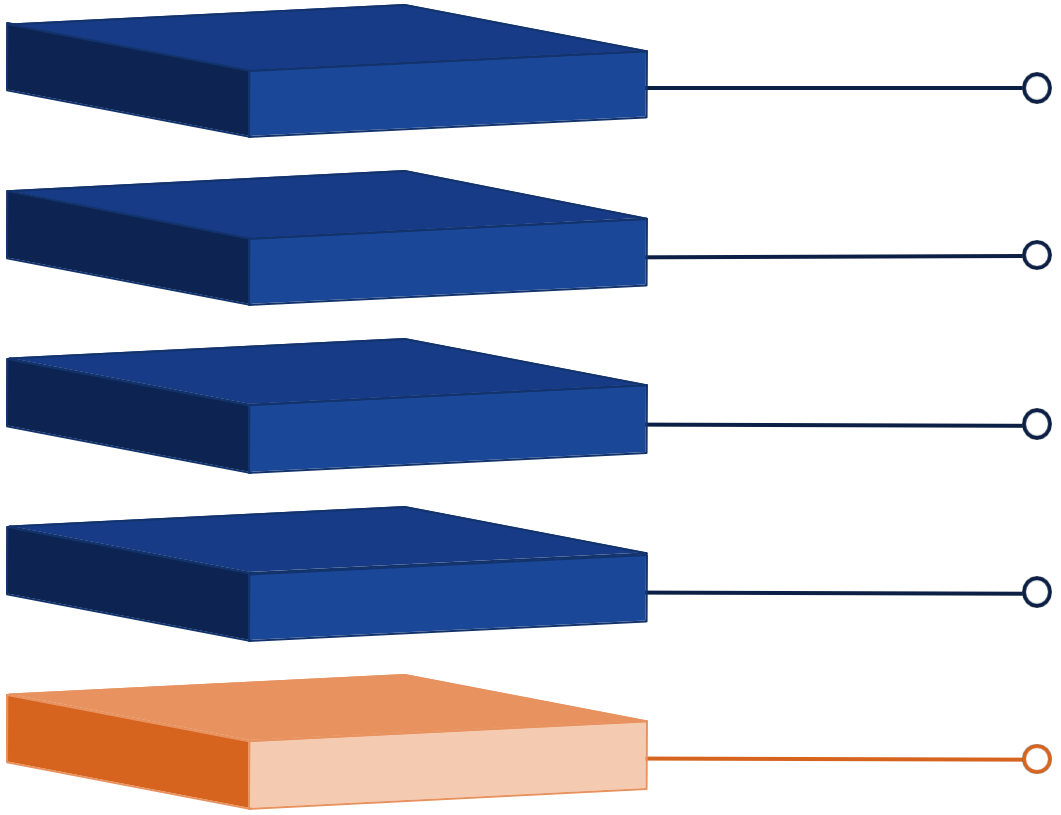
I dati devono essere custoditi in infrastrutture fisicamente localizzate e sotto controllo sanitario. Serve piena trasparenza su **dove sono e chi li gestisce**.

Ogni interazione con l'AI deve essere **tracciabile e accessibile** sia a livello medico, che tecnico.

Crittografia, accesso autenticato, segmentazione dei flussi informativi: la **sicurezza** è parte dell'architettura.

L'ambiente deve permettere la **validazione clinica continua**. I professionisti devono poter intervenire quando qualcosa non va.

Per garantire tutto ciò, è essenziale che **i modelli siano eseguiti in ambienti dedicati, chiusi, performanti**. Le architetture on-prem, come un superpod, rappresentano la soluzione più solida.



Il valore di un “superpod”

Ambiente dedicato, chiuso e protetto

Il superpod è un'**infrastruttura isolata**, fisicamente e logicamente, da ambienti condivisi o pubblici.
Nessun accesso esterno, nessuna interconnessione non autorizzata.
Ideale per dati ad alta sensibilità.

Modelli sotto controllo completo

I modelli AI girano dentro il superpod, non altrove. Questo garantisce **controllo** sulle versioni, **tracciabilità** degli aggiornamenti, **audit** totale delle risposte.

Compliance, scalabilità e performance

Il superpod unisce rispetto delle **normative** (es. GDPR, policy ospedaliere), **scalabilità** verticale (potenza) e orizzontale (più utenti/modelli), tempi di risposta **rapidi** e stabili, anche in ambito clinico real-time.

Use case clinici

Supporto alla refertazione clinica

Generazione di referti a partire da appunti, dettatura vocale o moduli strutturati. Velocizza la documentazione, *riduce errori* di forma.

Sintesi della cartella clinica

Riassunto automatico di note, referti e lettere di dimissione. Utile per il passaggio di consegne e la *presa in carico* rapida.

Pre-anamnesi e triage automatizzato

Raccolta preliminare delle informazioni dal paziente (via form o chatbot). Ottimizza i *tempi di visita* e aiuta nella priorità di accesso.

Follow-up e gestione ambulatoriale

Supporto nel monitoraggio post-visita, invio reminder, gestione dell'agenda clinica. Migliora *continuità e aderenza alla cura*.

Verso un'adozione consapevole

- L’intelligenza artificiale può essere uno strumento potente per la medicina, ma solo se **adottata con consapevolezza**.
- Non basta fidarsi della tecnologia: bisogna comprenderla, supervisionarla e governarla.
- L’AI deve restare nelle mani del medico, come supporto, mai come sostituzione.
- Le istituzioni e le aziende sanitarie hanno un ruolo centrale nel garantire che l’**introduzione di questi strumenti sia etica, sicura e utile per la pratica clinica**.

Grazie per l’a tenzione