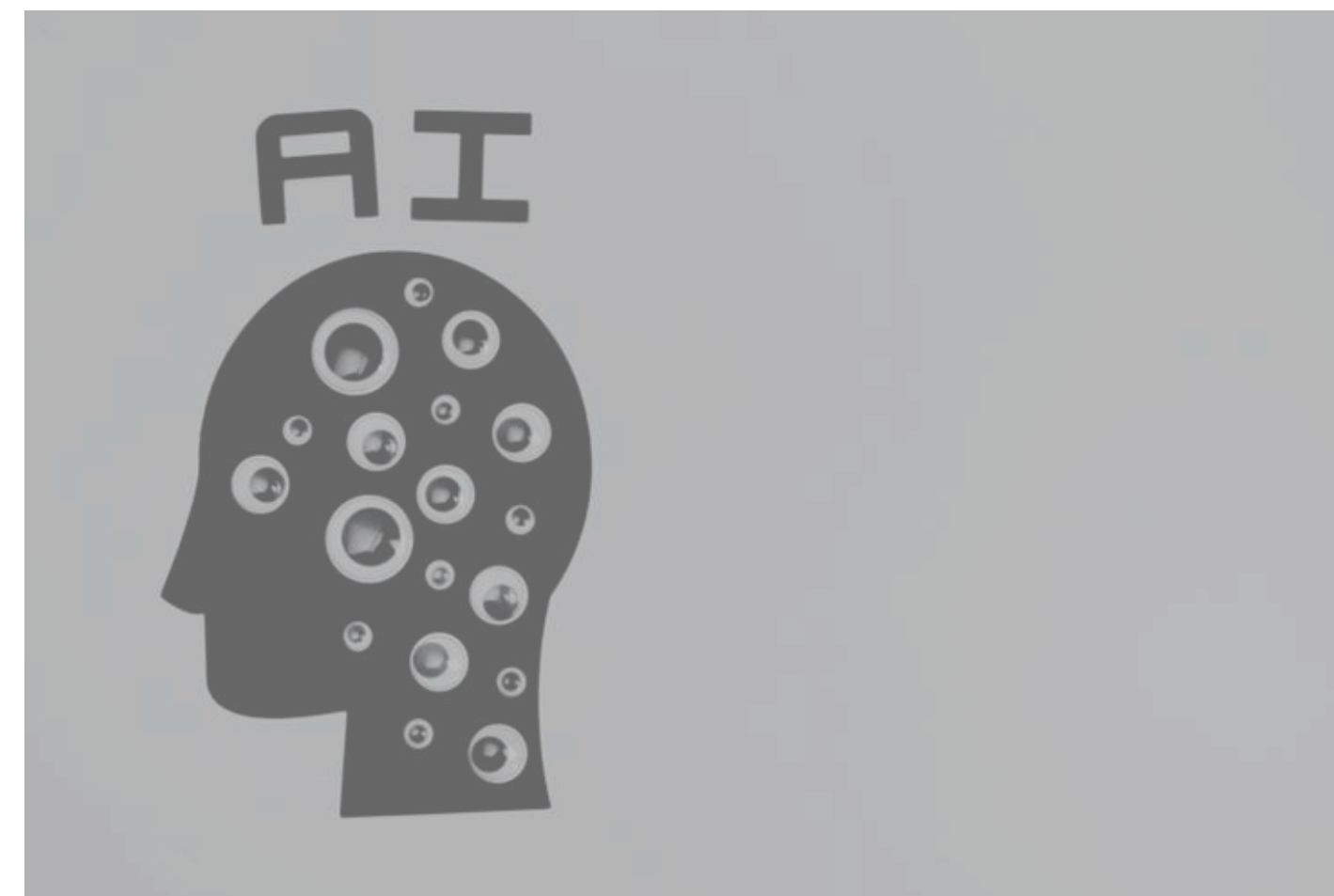


Cybersecurity nell'area dell'Intelligenza Artificiale in Sanità

Simona Dei
Direttrice Generale ISPRO



Laboratorio Sanità 20/30 AI

- **Contesto e Obiettivi: L'IA in Sanità, Innovare con Responsabilità**
- L'IA nella Pratica Clinica: Cosa fa l'IA per noi e per i nostri pazienti oggi
- Il Valore e la Tutela del Dato Sanitario : perchè il dato sanitario è “speciale”
- Minacce Cyber Potenziate dall'IA: Quando l'IA diventa un'arma, gli attacchi del presente
- Le basi normative da ieri a domani : Ricerca Scientifica e Dati Sanitari
- Quadro Normativo e AI Act: il triangolo delle compliance in un sistema normativo integrato
- Regole d'Oro : L'IA e i Dati Sono una Risorsa, Governarli È un Dovere.

**L'Intelligenza Artificiale ha smesso di essere
una promessa futura
per diventare uno strumento concreto del presente clinico.**

Entro il 2030
**Integrazione dell'IA nei percorsi di cura capillare:
dalla diagnostica alla gestione dei flussi ospedalieri,
dall'analisi predittiva delle popolazioni
all'automazione della documentazione medica.**

Lavora in modo PREDITTIVO o GENERATIVO

Laboratorio Sanità 20/30 AI



**Vision: adottare l'IA
per migliorare la qualità delle cure
e l'efficienza del sistema,
ma farlo in modo consapevole, sicuro e
nel pieno rispetto dei diritti dei pazienti.**

**L'*innovazione* tecnologica in sanità
non è un'alternativa alla *tutela* dei diritti.
È possibile solo attraverso di essa.**

SVILUPPARE L'I.A. nel rispetto:

**della tutela dei dati
GDPR**

**della protezione delle infrastrutture
Cybersecurity –NIS2-**

**della valorizzazione del patrimonio informativo della sanità pubblica
nuove Linee Guida europee 1/2026**

Laboratorio Sanità 20/30 AI

- **Contesto e Obiettivi: L'IA in Sanità, Innovare con Responsabilità**
- **L'IA nella Pratica Clinica: Cosa fa l'IA per noi e per i nostri pazienti oggi**
- **Il Valore e la Tutela del Dato Sanitario : perchè il dato sanitario è “speciale”**
- **Minacce Cyber Potenziate dall'IA: Quando l'IA diventa un'arma, gli attacchi del presente**
- **Le basi normative da ieri a domani : Ricerca Scientifica e Dati Sanitari**
- **Quadro Normativo e AI Act: il triangolo delle compliance in un sistema normativo integrato**
- **Regole d'Oro : L'IA e i Dati Sono una Risorsa, Governarli È un Dovere.**

I.A. in Diagnostica per immagini:

algoritmi di machine learning analizzano immagini, evidenziano anomalie impercettibili, riducono i margini di errore, accelerano la diagnosi.

Secondo la letteratura internazionale, Integrare con IA la lettura delle mammografie riduce del 30% i falsi negativi

Riducono le possibilità di errore e migliorano la capacità di diagnosi

I.A. Scribes:

strumenti basati su modelli linguistici avanzati trascrivono automaticamente la visita, compilano la cartella clinica, riassumono la storia farmacologica del paziente.

Riducono il tempo "burocratico" a favore del tempo "cura"



I.A. in Ricerca farmacologica

Accelera l'identificazione di target terapeutici analizzando milioni di dati genomici

Consente sperimentazioni cliniche più rapide e personalizzate

Ha un potenziale rivoluzionario per le malattie rare e oncologiche

Accelera i tempi di scelta di una terapia aumentando la capacità di cura

Deep learning in I.A.

Utilizza reti neurali profonde, cioè strati di algoritmi ispirati al funzionamento del cervello umano, per imparare dai dati.

Nell' AI predittiva, queste reti possono identificare profili complessi presenti nei dati difficili da rilevare tramite metodi statistici tradizionali. *analisi demografica, processi decisionali*

Nell' AI generativa, le reti neurali sono addestrate per generare nuovi dati che imitano gli input di addestramento. *telemedicina, sviluppo di digital twins*

- **Contesto e Obiettivi: L'IA in Sanità, Innovare con Responsabilità**
- **L'IA nella Pratica Clinica: Cosa fa l'IA per noi e per i nostri pazienti oggi**
- **Il Valore e la Tutela del Dato Sanitario : perchè il dato sanitario è “speciale”**
- **Minacce Cyber Potenziate dall'IA: Quando l'IA diventa un'arma, gli attacchi del presente**
- **Le basi normative da ieri a domani : Ricerca Scientifica e Dati Sanitari**
- **Quadro Normativo e AI Act: il triangolo delle compliance in un sistema normativo integrato**
- **Regole d'Oro : L'IA e i Dati Sono una Risorsa, Governarli È un Dovere.**



Il Dato Sanitario

PREZIOSO, VULNERABILE, SPECIALE

“dato particolare”

ai sensi dell'Art. 9 GDPR UE/2016/679:

(regolamento generale sulla protezione dei dati)

il cui trattamento richiede

una “base giuridica rafforzata”

**Contiene informazioni su diagnosi, terapie,
abitudini di vita, genetica, stato mentale**

**Una sua violazione può compromettere il lavoro,
le relazioni, la dignità di una persona**

Laboratorio Sanità 20/30 AI

Le misure di salvaguardia obbligatorie

Misura	Descrizione
Pseudonimizzazione	Separazione dell'identità del paziente dai dati clinici tramite un codice univoco
Ambienti sicuri	Accesso ai dati solo in Data Access Environment verificabili
Accessi limitati	Solo a personale autorizzato del Comitato Etico secondo il di ricerca
Trasparenza stratificata	Informativa: estesa a portali web / synth per esperti • sintesi invece per pubblico
Divieto di re-identificazione	Obbligo contrattuale e sanzione per tutti i soggetti coinvolti

CONDIZIONI IRRINUNCIABILI

Privacy by design

Sistemi IA previsti nella progettazione, non aggiunti successivamente (art 25 GDPR)

Valutazione di Impatto sulla protezione dei dati

Prima di attivare qualsiasi sistema di IA che tratti dati sanitari su larga scala, è obbligatoria una Valutazione di Impatto sulla Protezione dei Dati (art. 35 del GDPR.) Tutela reale e non formale

Consenso informato:

I pazienti devono sapere se e come un sistema di IA interviene nel loro percorso di cura e devono poter contestare una decisione automatizzata. (art. 22 del GDPR)

DPO

Data protection officer, figura obbligatoria nelle strutture sanitarie pubbliche (art. 37 38 39 GDPR)



In una Azienda sanitaria gli organi direttivi devono:

Approvare le misure di gestione dei rischi informatici

Seguire una formazione specifica in materia di cybersecurity

Vigilare sull'attuazione degli obblighi

Non è sufficiente delegare.

- **Contesto e Obiettivi: L'IA in Sanità, Innovare con Responsabilità**
- **L'IA nella Pratica Clinica: Cosa fa l'IA per noi e per i nostri pazienti oggi**
- **Il Valore e la Tutela del Dato Sanitario : perchè il dato sanitario è “speciale”**
- **Minacce Cyber Potenziate dall'IA: Quando l'IA diventa un'arma, gli attacchi del presente**
- **Le basi normative da ieri a domani : Ricerca Scientifica e Dati Sanitari**
- **Quadro Normativo e AI Act: il triangolo delle compliance in un sistema normativo integrato**
- **Regole d'Oro : L'IA e i Dati Sono una Risorsa, Governarli è un Dovere.**

Piattaforme come ChatGPT, Gemini, Copilot non sono:

- **Dispositivi medici certificati
(nessuna marcatura CE come medical device)**
- **Ambienti sicuri per dati sanitari
(nessuna garanzia contrattuale GDPR-compliant)**



**Nessun dato sanitario — anche anonimizzato in apparenza —
deve essere inserito in piattaforme IA non contrattualizzate e non certificate
secondo i requisiti dell'AI Act e del GDPR.**

Rischi concreti

Allucinazioni con Conseguenze Cliniche



L'IA genera informazioni false con tono autorevole :
dosaggi errati, interazioni farmacologiche inesistenti, diagnosi imprecise
senza supervisione umana il rischio clinico è reale e documentato.

Esfiltrazione Involontaria

I prompt inseriti dagli utenti possono contenere dati identificativi non visibili
(metadati, codici nosologici, riferimenti indiretti).

Il paziente non viene mai informato. Il consenso non viene mai acquisito

Data Leakage

dati inseriti da parte di sanitari a fini diagnostici in piattaforme IA pubbliche
illecitamente memorizzati nei server del provider, usati per addestrare il modello, esposti a terzi.

1. Phishing Ultra-Personalizzato (Spear Phishing con LLM)

L'IA analizza i profili LinkedIn, i siti istituzionali e le comunicazioni pubbliche del personale sanitario
Genera email perfette, nel tono giusto, con il nome del diretto superiore
In un ospedale del nord Italia (2025): un operatore ha cliccato su un link fraudolento
credendo fosse una circolare della direzione. *Accesso al sistema HIS compromesso.*

2. Deepfake Medici e Audio Clonati

Clonazione della voce del Direttore Sanitario per autorizzare bonifici urgenti o procedure straordinarie
Videochiamate false con avatar realistici per estorcere credenziali di accesso
Il personale non è addestrato a riconoscerli: *la nuova ingegneria sociale*

3. Ransomware Intelligente (AI-Assisted)

Il malware studia autonomamente la rete ospedaliera prima di attivarsi
Identifica i sistemi più critici (cartelle cliniche, sistemi di allerta, apparecchiature connesse)
Colpisce in modo sincronizzato per massimizzare il danno e il riscatto
Costo medio di un attacco ransomware a un ospedale europeo: *4,4 milioni di euro*

COSA FARE?

- **Formare tutto il personale**
 - **Aggiornare i sistemi**
 - **Simulare gli attacchi**
- **Non aspettare che accada.**

- **Contesto e Obiettivi: L'IA in Sanità, Innovare con Responsabilità**
- **L'IA nella Pratica Clinica: Cosa fa l'IA per noi e per i nostri pazienti oggi**
- **Il Valore e la Tutela del Dato Sanitario : perchè il dato sanitario è “speciale”**
- **Minacce Cyber Potenziate dall'IA: Quando l'IA diventa un'arma, gli attacchi del presente**
- **Le basi normative da ieri a domani : Dati Sanitari e Ricerca Scientifica**
- **Quadro Normativo e AI Act: il triangolo delle compliance in un sistema normativo integrato**
- **Regole d'Oro : L'IA e i Dati Sono una Risorsa, Governarli È un Dovero.**

Regolamento generale per la Protezione dei Dati (GDPR- Regol UE 2016/679)

Codice Privacy (Decreto legislative 196/2003)

Legge sulla Intelligenza Artificiale (AI ACT – Regol UE 2024/1689)

Legge dello stato Italiano n. 132 del 23 Settembre 2025

Direttiva NIS 2 (UE 2022/2555)

Dcreto legislative 138/2024 (recepimento NIS 2)

Cybersecurity Act (Regol. UE 2025/37)

Guidelines European Data Protection Board 1/2026

6 criteri qualificano un'attività come "ricerca scientifica" ai sensi dell'Art. 89 GDPR:

Finalità genuinamente scientifica
non commerciale, con obiettivi conoscitivi verificabili

Metodologia rigorosa
approvazione etica e protocollo scientifico documentato

Pubblicazione dei risultati
trasparente, anche in caso di risultati negativi

Misure di salvaguardia proporzionate pseudonimizzazione,
accessi limitati, ambienti sicuri

Supervisione indipendente
Comitato Etico o organismo equivalente

Interesse pubblico dimostrabile
beneficio collettivo prevalente sull'interesse individuale

Laboratorio Sanità 20/30 AI



I principi cardine di una ricerca che utilizza dati sanitari (GDPR)

Principio	Significato pratico
Minimizzazione	Raccogliere solo i dati strettamente necessari allo scopo
Limitazione della finalità	I dati raccolti per la cura non possono essere usati liberamente per altri scopi
Responsabilizzazione	Il titolare del trattamento risponde delle scelte organizzative e tecnologiche

Sinergia con lo Spazio Europeo dei Dati Sanitari (EHDS):

Le Guidelines 1/2026 con il Regolamento EHDS, creano un ecosistema normativo coerente per il riutilizzo secondario dei dati clinici su scala europea.

Le strutture sanitarie che alimentano l'EHDS devono già oggi adeguare i propri sistemi ai requisiti di qualità, interoperabilità e governance previsti.



Riferimenti normativi:

GDPR — Artt. 5, 9, 89

**Guidelines EDPB 1/2026 sul trattamento
dei dati per finalità di ricerca scientifica**

Codice Privacy — Art. 75 e ss. (D.Lgs. 196/2003)

Il consenso si evolve e si sceglie:

Broad Consent (Consenso Ampio)

Il paziente autorizza il riutilizzo dei propri dati per categorie ampie di ricerca future
(es. oncologia, malattie cardiovascolari, neurologia)

Deve essere accompagnato da trasparenza stratificata e dalla possibilità di revoca in qualsiasi momento
-biobanks, registri clinici -

Dynamic Consent (Consenso Dinamico)

Il paziente gestisce le proprie preferenze in tempo reale tramite portali digitali dedicati

Può autorizzare, limitare o revocare il consenso per singoli progetti di ricerca

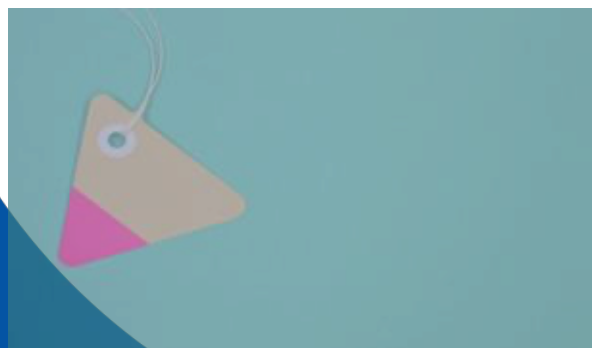
- ricerca longitudinale, studi multicentrici, progetti ad alto impatto -

- **Contesto e Obiettivi: L'IA in Sanità, Innovare con Responsabilità**
- **L'IA nella Pratica Clinica: Cosa fa l'IA per noi e per i nostri pazienti oggi**
- **Il Valore e la Tutela del Dato Sanitario : perchè il dato sanitario è “speciale”**
- **Minacce Cyber Potenziate dall'IA: Quando l'IA diventa un'arma, gli attacchi del presente**
- **Le basi normative da ieri a domani : Ricerca Scientifica e Dati Sanitari**
- **Quadro Normativo e AI Act: il triangolo delle compliance in un sistema normativo integrato**
- **Regole d'Oro : L'IA e i Dati Sono una Risorsa, Governarli È un Dovere.**

Il Triangolo della Compliance: GDPR + AI Act + NIS 2: Tre regolamenti, un unico ecosistema:

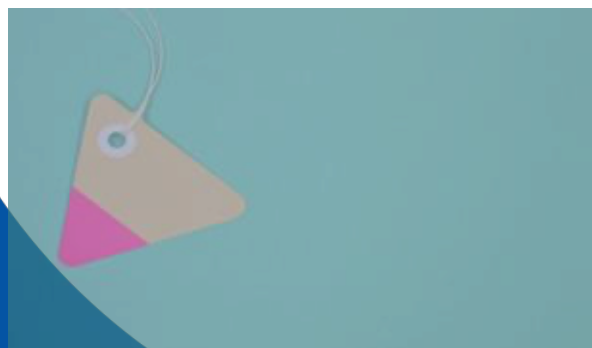
- **L'AI Act** regola i sistemi,
- **il GDPR** tutela i dati
- **le Guidelines EDPB** definiscono le regole specifiche per il riutilizzo a fini di ricerca.

Tre livelli di protezione, sovrapposti e complementari.



Il Triangolo della Compliance: GDPR + AI Act + NIS 2: Tre regolamenti, un unico ecosistema:

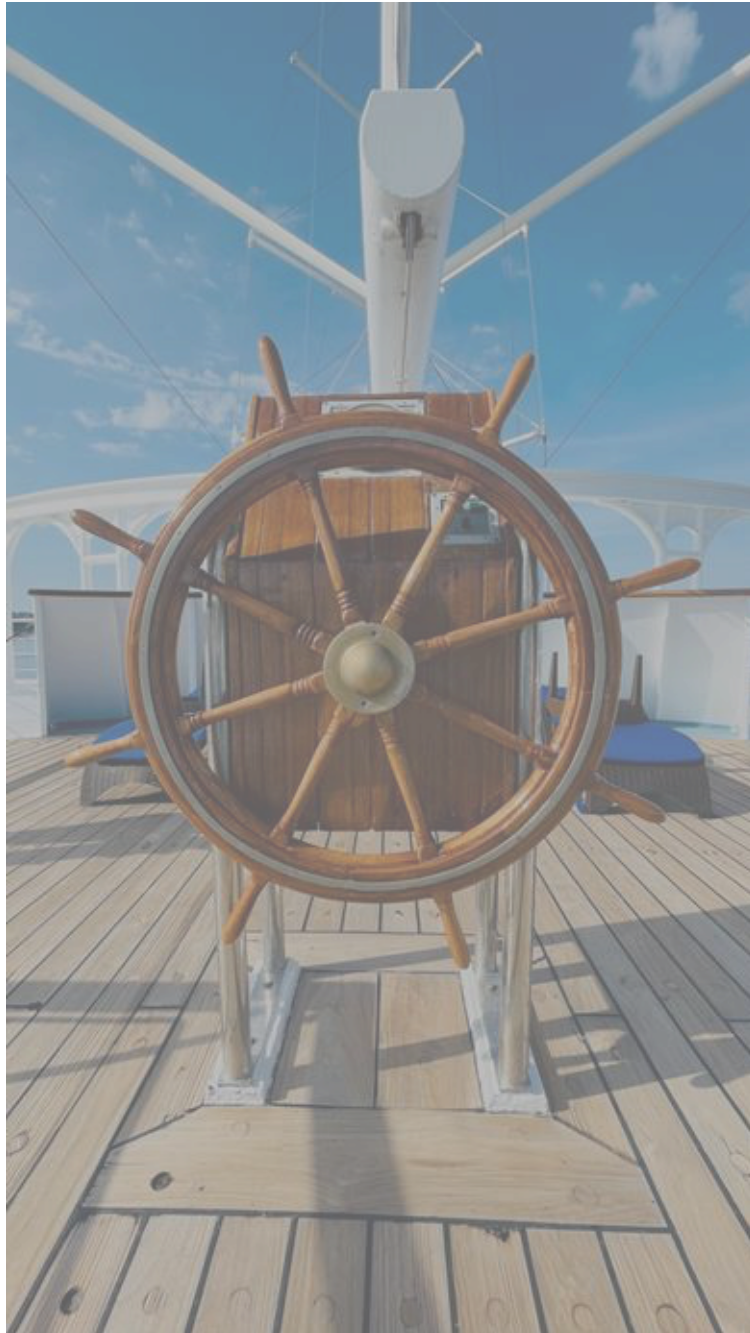
- I sistemi IA per diagnostica, triage, monitoraggio e supporto alle decisioni cliniche sono classificati **ad alto rischio** (AI Act, Allegato III)
- La struttura sanitaria che usa il Sistema (**deployer**) deve garantire:
 - **Supervisione umana** attiva
 - **Trasparenza** verso il paziente
 - **Monitoraggio** del sistema in uso
 - Registrazione delle attività nel **database EU** per sistemi ad alto rischio



Chi è il "deployer"?

Le Aziende Sanitarie che adottano sistemi di IA sono definite deployer dall'art. 26 dell'AI Act: hanno l'obbligo di usare il sistema secondo le istruzioni del fornitore, monitorarne il funzionamento nel tempo e intervenire quando necessario.

Non basta acquistare il software: bisogna governarlo.



I pilastri

Trasparenza algoritmica (art. 13 AI Act)

**il sistema deve essere comprensibile
per chi lo usa professionalmente.**

Sorveglianza umana obbligatoria (art. 14 AI Act)

**l'IA decide, ma un essere umano supervisiona sempre.
Mai delegare completamente.**

Diritto alla spiegazione (art. 86 AI Act)

**il paziente ha il diritto di capire come un sistema di IA
ha contribuito a una decisione che lo riguarda.**

- **Contesto e Obiettivi: L'IA in Sanità, Innovare con Responsabilità**
- **L'IA nella Pratica Clinica: Cosa fa l'IA per noi e per i nostri pazienti oggi**
- **Il Valore e la Tutela del Dato Sanitario : perchè il dato sanitario è “speciale”**
- **Minacce Cyber Potenziate dall'IA: Quando l'IA diventa un'arma, gli attacchi del presente**
- **Le basi normative da ieri a domani : Ricerca Scientifica e Dati Sanitari**
- **Quadro Normativo e AI Act: il triangolo delle compliance in un sistema normativo integrato**
- **Regole d'Oro : L'IA e i Dati Sono una Risorsa, Governarli È un Dovere.**

1. MAI CARICARE DATI DI PAZIENTI SU IA NON CERTIFICATE CHATGPT, GEMINI, COPILOT E SIMILI NON SONO DISPOSITIVI MEDICI CERTIFICATI.

UN REFERTO CARICATO SU QUESTE PIATTAFORME PUÒ ESSERE MEMORIZZATO, RIUTILIZZATO E POTENZIALMENTE ESPOSTO.

LA REGOLA VALE PER TUTTI: MEDICI, INFERMIERI, AMMINISTRATIVI.

2. L'OCCHIO UMANO È SEMPRE L'ULTIMO OGNI DECISIONE CLINICA SUPPORTATA DALL'IA DEVE ESSERE VALIDATA DA UN PROFESSIONISTA.

L'IA SUGGERISCE, IL MEDICO DECIDE. QUESTO NON È SOLO BUON SENSO: È UN OBBLIGO DI LEGGE SANCITO DALL'AI ACT.

3. INFORMARE SEMPRE IL PAZIENTE SE UN SISTEMA DI IA INTERVIENE NEL PERCORSO DI CURA,

IL PAZIENTE HA IL DIRITTO DI SAPERLO. IL CONSENSO INFORMATO VA AGGIORNATO PER INCLUDERE L'USO DELL'IA.



4. INVESTIRE NELLA SICUREZZA INFORMATICA LA CYBERSECURITY

NON È UN CAPITOLO DI SPESA DISCREZIONALE.

**È UN OBBLIGO NORMATIVO (NIS 2) E UNA RESPONSABILITÀ DIRETTA
DELLA DIREZIONE GENERALE.**

**FORMAZIONE CONTINUA, AGGIORNAMENTO DEI SISTEMI,
SIMULAZIONI DI ATTACCO: NON SI PUÒ ASPETTARE L'INCIDENTE PER MUOVERSI.**

- 5. VERIFICARE I FORNITORI DI IA PRIMA DI ADOTTARE QUALSIASI SISTEMA DI IA,
VERIFICARE CHE SIA CERTIFICATO COME DISPOSITIVO MEDICO,
CHE SIA STATO SOTTOPOSTO A DPIA,
E CHE IL CONTRATTO CON IL FORNITORE GARANTISCA
LA NON RIUTILIZZAZIONE DEI DATI SANITARI.**



L'Intelligenza Artificiale non è il nemico della sanità pubblica.
È uno **STRUMENTO POTENTE**, e come tutti gli strumenti potenti,
RICHIEDE RISPETTO COMPETENZE REGOLE
Il nostro impegno, come sistema sanitario,
è fare in modo che l'**INNOVAZIONE** arrivi ai pazienti
insieme alla **TUTELA** dei loro diritti,
non a scapito di essa.

*«Il successo nella creazione dell'intelligenza artificiale potrebbe essere
il più grande evento nella storia umana.
Purtroppo potrebbe anche essere l'ultimo,
a meno che non impariamo a evitarne i rischi.»*

Stephen Hawking



Laboratorio Sanità 20/30 AI