IA in Sanità e Cybersecurity: obblighi legali, rischi reali e soluzioni concrete

AVV. CIRO GALIANO

PRICIPALI NORMATIVE UE

- **AI ACT Regolamento (UE) 2024/1689** che stabilisce norme armonizzate sull'intelligenza artificiale) è il primo quadro giuridico globale in assoluto sull'IA a livello mondiale. L'obiettivo delle norme è promuovere un'IA affidabile in Europa.
- **NIS (Network and information Security) 2 Direttiva 2022/2555** adottata per rafforzare il livello di sicurezza delle reti e dei sistemi informativi in Europa (sostituisce la NIS 2016/1148)
- **Reg. UE 2016/679 GDPR** Tutela dei dati personali e favorisce la circolazione degli stessi in ambito unionale;
- **REGOLAMENTO N. 2017/745 SUI DISPOSITIVI MEDICI** entrato in vigore in tutti gli stati membri il 26 maggio 2021. (Medical Dispositive Regulation) L'obiettivo del nuovo regolamento è di garantire un elevato livello di sicurezza, tracciabilità e protezione della salute.

E in ITALIA

- **D.LGS 101/2018** norma di attuazione ed integrazione del Reg. UE 2016/679 novella il D.Lgs 196/2003 (codice privacy);https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196!vig
- **D.lgs 138/2024** attuazione della NIS 2 in ambito nazionale;https://www.acn.gov.it/portale/nis/la-normativa
- **L. 90/2024** Disposizioni per il rafforzamento di cyber sicurezza nazionale e dei reati informatici : contrasto ai cyber crimini come l'accesso abusivo dei sistemi informatici e la diffusione di strumenti per intercettare le comunicazioni. Amplia i poteri della Agenzia per la cybersicurezza nazionale (ACN)https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2024-06-28;90
- **Legge n. 132/2025 sull'AI https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2025-09-23;132**
- **Strategia Italiana per l'intelligenza artificiale 204-2026** https://innovazione.gov.it/notizie/articoli/strategia-italiana-per-l-intelligenza-artificiale-2024-2026/

TAPPE AI ACT (ART. 113)

2 febbraio 2025 – Inizio applicazione concreta dell'AI Act

-**Divieto delle pratiche di IA a rischio inaccettabile** (art. 5).

-**Obbligo di alfabetizzazione AI** per operatori, personale, organismi

2 agosto 2025

- **Autorità di notifica – AI office europeo (Bruxelles)**
- autorità nazionali competenti in Italia AgID e ACN (L.132/2025)
- **Obblighi per i fornitori di modelli GPAI obbligo di** dichiarare quando un contenuto è generato da IA, documentare dataset e rischi, rispettare obblighi di trasparenza e sicurezza.
- **Attivazione del sistema sanzionatorio**

Da qui in avanti si applicano effettivamente le sanzioni previste dall'art. 99.

- **Periodo transitorio per modelli preesistenti**

I modelli GPAI commercializzati **prima del 2 agosto 2025** hanno tempo **fino al 2 agosto 2027** per adeguarsi.

TAPPE AI ACT (ART. 113)

2 agosto 2026 – Obblighi per i sistemi ad alto rischio

Chi utilizza o sviluppa sistemi AI ad alto rischio dovrà:

1. **Implementare un sistema di gestione del rischio**
   Attivo per tutto il ciclo di vita dell'IA (progettazione → uso → aggiornamenti → manutenzione).
2. **Garantire qualità dei dati e mitigazione dei bias**
3. **Garantire supervisione umana significativa e documentata**
4. **Implementare misure avanzate di cybersecurity**
5. **Prodotti e software: documentazione tecnica + marcatura CE**
6. **Obbligo di FRIA (Fundamental Rights Impact Assessment)**
   Obbligatoria per **tutti i sistemi ad alto rischio utilizzati nel settore pubblico**, sanità inclusa quando l'ente è pubblico o svolge attività di interesse pubblico.
7. **Registrazione nel database pubblico europeo**
   Tutti i sistemi ad alto rischio devono essere registrati nel database UE.

TAPPE AI ACT (ART. 113) e SANZIONI

2 agosto 2027 – Ampliamento degli elenchi ad alto rischio in base all'evoluzione tecnologica.
2 agosto 2028 – Revisione generale del Regolamento

SANZIONI (ART. 99):
Violazione delle pratiche vietate (art. 5)
€ 35 milioni € o 7% del fatturato mondiale
Violazione di altri obblighi dell'AI Act
€ 15 milioni € o 3% del fatturato mondiale
Informazioni false, incomplete o fuorvianti alle autorit
€ 7,5 milioni € o 1% del fatturato mondiale
PMI e startup
Applicazione proporzionale.
Si applica l'importo **più basso** tra valore assoluto e percentuale.

NOVITA' 19.11.2025: DIGITAL OMNIBUS POSSIBILE MORATORIA AL 2027 E ALLEGGERIMENTODEGLI OBBLIGHI

Definizione della Direttiva NIS 2 e il suo recepimento in Italia

La **Direttiva NIS 2** (*Network and Information Security Directive 2*), formalmente **Direttiva (UE) 2022/2555**, è la normativa europea volta a **rafforzare la sicurezza informatica** e la **resilienza delle infrastrutture digitali e dei servizi essenziali** negli Stati membri dell'Unione Europea.

LA SANITA' E' COINVOLTA DIRETTAMENTE

Misure di sicurezza rafforzate:

Le aziende devono adottare misure tecniche e organizzative adeguate per la gestione dei rischi informatici, garantendo la sicurezza delle reti e dei sistemi informativi. È inoltre previsto l'obbligo di notifica immediata degli incidenti di sicurezza significativi all'ACN. 24 ORE/72 ORE/1 MESE RELAZIONE FINALE.

OBBLIGO SCATTA PER TUTTI i soggetti importanti ed essenziali DA GENNAIO 2026.

SANZIONI 10 MLN O 2% FATTURATO

7 MLN 0 1,4% FATTURATO

Cos'è un algoritmo di Intelligenza Artificiale?

Art 3 2024/1689 AI act. «Sistema di IA»: «*un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali*»

Il sistema dell'apprendimento automatico (machine learning), si basa sull'elaborazione di grandi quantità di dati grazie al quale l'algoritmo di AI riesce a trovare correlazioni per raggiungere a risultati/decisioni autonomi.

Questo approccio, avviene attraverso strutture chiamate reti neurali, perché traggono ispirazione dalla struttura del cervello umano, funziona sicuramente molto meglio del sistema basato su regole predefinite quando il problema da risolvere è troppo astratto o ha troppe possibili istanze per poter essere descritto precisamente

La criticità risiede che più sono complesse le reti di calcolo (le reti neurali) più l'elemento decisionale è frutto di pattern invisibili alle persone perché "nascosti" in grandi quantità di informazioni che vengono offerte per alimentare il l'apprendimento della macchina (deep learning).

In sostanza abbiamo due grandi criticità:

1. le ipotesi di partenza
2. la trasparenza nel ragionamento che porta alla decisione.

I bias (pregiudizi)- rischi e rimedi

L'AI può presentare dei "bias" (pregiudizi) che potrebbero portare a decisioni discriminatorie, errate ingiuste e aberranti. https://iusinitinere.it/intelligenza-artificiale-se-lalgoritmo-e-discriminatorio/

Tutto questo può avvenire se non vi è trasparenza nei criteri di scelta dei data set, nella qualità e caratteristiche dei dati e nel processo di apprendimento che deve essere sempre trasparente e spiegabile.

Rischi della Cybersecurity nell'IA applicata alla Medicina

L'IA potenzia il settore sanitario, ma introduce nuove vulnerabilità. Le principali minacce sono:

a. Attacchi ai dati di addestramento (bias nei modelli).

b. Manipolazione delle decisioni dell'IA (alterazione delle diagnosi).

c. Esfiltrazione di dati sanitari (violazioni della privacy e ricatti).

d. Attacchi ai dispositivi medici (interferenze con la salute dei pazienti).

e. Phishing ai medici (truffe per ottenere credenziali e installare malware).

Attacchi ai dati di addestramento (Data Poisoning)

Gli algoritmi medici apprendono da milioni di dati clinici.

Se un hacker inserisce dati manipolati nel dataset di training … l'IA impara a sbagliare.

Risultato?

- diagnosi distorte
- trattamenti errati
- protocolli clinici compromessi

Esempio: un modello oncologico addestrato così:– scambia lesioni innocue per tumori,– ignora tumori reali,– propone cure inappropriate.

Conseguenze: danno ai pazienti, responsabilità sanitarie.

2. Manipolazione delle decisioni dell'IA (Model Inference Attack)

Descrizione:
Questi attacchi mirano a **modificare il comportamento** dell'IA già operativa in un sistema sanitario, alterando le decisioni diagnostiche o terapeutiche.

Come funziona l'attacco?

- Tramite **ransomware o malware**, un attaccante può modificare i parametri dell'IA.
- L'IA potrebbe **fornire indicazioni errate** ai medici o eseguire azioni sbagliate in autonomia.

Esempio pratico:

- Un attacco a un **sistema AI per l'analisi di elettrocardiogrammi** potrebbe far diagnosticare **aritmie inesistenti**, inducendo a interventi chirurgici non necessari.
- Un hacker modifica i protocolli di **un'IA che regola la somministrazione di insulina** in un paziente diabetico → Dosi errate con rischio di ipoglicemia o iperglicemia fatale.

3. Esfiltrazione di dati sanitari (Data Breach) https://www.garanteprivacy.it/data-breach

Descrizione:
I dati sanitari sono molto **preziosi**. Gli hacker cercano di rubare questi dati per **rivenderli sul dark web o usarli per estorsioni (ransomware)**.

Come funziona l'attacco?

- Un malware o un attacco phishing colpisce il database sanitario.
- L'hacker estrae cartelle cliniche, referti, dati genetici e anamnesi dei pazienti.
- I dati vengono rivenduti illegalmente o usati per frodi sanitarie.

Esempio pratico:

- Attacchi ai repository sanitari come **Fascicolo Sanitario Elettronico (FSE)** o database ospedalieri (**DSE**).
- **Accesso non autorizzato** ai dati dei wearable (dispositivi indossabili che monitorano i parametri vitali dei pazienti).

Conseguenze:

- **Violazione del GDPR** e sanzioni per le strutture sanitarie.
- **Perdita di fiducia** da parte di pazienti e operatori sanitari.
- **Uso illecito dei dati** per creare identità sanitarie false o truffe assicurative.

4. Attacchi alla Supply Chain dei dispositivi medici

Descrizione

Pacemaker, pompe di insulina, sensori cardiaci, TAC, RM e sistemi di telemonitoraggio basati su IA possono essere vulnerabili ad attacchi informatici.

Una singola vulnerabilità software può compromettere funzioni vitali.

Come avviene l'attacco

- L'attaccante sfrutta una falla nel software del dispositivo.
- Può **modificare parametri vitali**, alterare i dati, bloccare il funzionamento o prendere il controllo del dispositivo.

Esempi concreti

- Un attacco a un dispositivo di telemonitoraggio cardiaco può **alterare i dati inviati ai medici**, con diagnosi imprecise e terapie sbagliate.

Conseguenze

- **Arresto o malfunzionamento** di dispositivi critici.
- **Danni fisici** ai pazienti, soprattutto se il dispositivo regola funzioni vitali.
- **Responsabilità sanitarie**.

5. Social Engineering & Phishing ai medici e ospedali

Descrizione:
Gli attacchi di phishing sono tra i più diffusi nella sanità. I cybercriminali ingannano medici e operatori sanitari **per ottenere credenziali di accesso ai sistemi IA e ai dati sanitari**.

Come funziona l'attacco?
•L'hacker invia email o messaggi **con link fraudolenti**
•Il medico **clicca sul link e scarica un malware**.
•L'attaccante ottiene l'accesso ai database sanitari o ai sistemi IA.
Esempio pratico:
•Un medico riceve un'email che **sembra provenire dal Ministero della Salute** con oggetto "Aggiornamento obbligatorio della piattaforma AI per telemedicina".
•Cliccando sul link, installa **un ransomware che blocca il sistema informatico ospedaliero**, richiedendo un riscatto per riattivarlo.
Conseguenze:
•Blocchi operativi nelle strutture sanitarie.
•Perdita di accesso ai dati sanitari per giorni o settimane.
•Necessità di pagare riscatti per recuperare i dati.

Ridurre i rischi di cybersecurity nell'uso dell'IA in sanità

1. Appalti sicuri capitolati dettagliati.

Qualsiasi sistema di IA acquisito da ospedali o aziende sanitarie deve essere conforme a:

- **NIS2** (cybersecurity),
- **AI Act** (requisiti per sistemi ad alto rischio),
- **MDR** (software come dispositivo medico).

Fondamentale: prevedere nel capitolato di appalto requisiti stringenti di sicurezza, audit, logging, qualità dei dati e supervisione umana.

Prevedere nel capitolato di appalto che i sistemi di AI siano corredati da DPIA e FRIA magari fatte da soggetti di terze parti volte ad indentificare la effettiva minimizzazione del rischio sia relativamente al trattamento dei dati personali sia relativamente alla tutela dei diritti fondamentali.

Qualità e governance dei dati

Assicurare che i dati usati per addestrare l'IA siano:

- rappresentativi,
- privi di bias,
- accurati,
- provenienti da fonti certificate.

Ridurre i rischi di cybersecurity nell'uso dell'IA in sanità

1.A Definizione delle responsabilità

Serve una governance chiara su:

- responsabilità del produttore,
- Responsabilità del distributore,
- responsabilità dell'utilizzatore professionale
- obblighi di segnalazione e sorveglianza post-market.

Ridurre i rischi di cybersecurity nell'uso dell'IA in sanità

3. Formazione obbligatoria del personale sanitario

Medici, tecnici e operatori devono:

- comprendere come funzionano gli algoritmi,
- riconoscere segnali di errore o bias,
- sapere quando e come intervenire per correggere il sistema.
- Formazione obbligatoria in tema di sicurezza informatica e corretto uso degli strumenti informatici (art. 32 GDPR, e obbligo previsto dall'AI Act, dalla L.132/2025 e dalla NIS 2).

L'IA può potenziare la sanità come mai prima d'ora:
vede prima, supporta decisioni rapide e precise.
Ma da sola non basta.
Può funzionare solo quando è **condivisa e governata insieme** da medici, tecnici, infermieri e sviluppatori.
Non sostituisce il personale: **ne amplifica competenze, valori e capacità di cura.**

GRAZIE PER L'ATTENZIONE