# CYBERSECURITY

# LEGISLAZIONE DA PRODOTTO
# e
# AI ACT



## Chi sono, Avv. Silvia Stefanelli

**Fondatrice e co-titolare dello Studio Legale Stefanelli&Stefanelli.**
**Presidente della BEST in HEALTH, SPA tra professionisti**
**Socio fondatore della Start up InsideAI , consulenza in materia di Intelligenza Artificiale**
**Esperta di diritto sanitario, con particolare competenza in ambito di sanità digitale, medical device, pubblicità sanitaria, contratti con la PA, protezione dei dati.**
**Consulente svariati progetti di sviluppo innovativi in sanità legati all'uso delle nuove tecnologie.**
**DPO in diverse strutture sanitarie pubbliche e private.**
**componente aal 2022 sono entrata a far parte del team di Individual Expert per l'implementazione di un pool a supporto del EDPB - European Data Protection Board nei gruppi "Technical expertise in new technology and information security" e "Legal expertise in new technologies".**
**Collaboratrice della Fondazione SmithKline su progetti nazionali in ambito di Digital Therapeutics.**
**Team Leader di Clusit su progetti di Intelligenza Artificiale.**
**Membro del Comitato Scientifico dell'Osservatorio di Telemedicina di Altems- Unicatt.**

Il mio profilo

s.stefanelli@studiolegalestefanelli.it

# SITUAZIONE OGGI IN SANITA'

**SOFTWARE MARCATI CE**
**EX DIR 93/42/CEE**

**la direttiva non conteneva nessun requisito specifico per i software**
**(né per la cybersecurity)**

**SOFTWARE DI LIBERA VENDITA**

**DIR 2001/95/ SULLA SICUREZZA GENERALE DEI PRODOTTI**

**nessun requisito specifico per i software**
**(né per la cybersecurity)**



# EVOLUZIONE IN SANITA'

**SOFTWARE MARCATI CE**
**REG. UE 2017/745 (MDR)**

***impiegato sull'uomo a scopo terapeutico***

**ampliamento dei software che rientrno nella nozione di medical device**

**SOFTWARE DI LIBERA VENDITA**

**REGOLAMENTO 2023/988 sulla sicurezza generale dei prodotti**

**13 dicembre 2024**

# EVOLUZIONE IN SANITA'

**SOFTWARE MARCATI CE**
**REG. UE 2017/745 (MDR)**

**REQUISITI SPECIFICI PER SOFTWARE**
**allegato I punto 17.2**

il software è sviluppato e fabbricato conformemente allo stato dell'arte, tenendo conto dei principi del ciclo di vita dello sviluppo, della gestione del rischio, **compresa la sicurezza delle informazioni**, della verifica e della convalida

(ISO 24971 collegata alla 14971
– confidenziale, intergro e disponitibile)

**SOFTWARE DI LIBERA VENDITA**

**REGOLAMENTO 2023/988 sulla sicurezza generale dei prodotti**

**art. 6**

*g) laddove lo imponga la natura del prodotto, **le adeguate caratteristiche di cibersicurezza necessarie per proteggere il prodotto da influenze esterne, compresi terzi malintenzionati,** se tale influenza potrebbe avere un impatto sulla sicurezza del prodotto, compresa la possibile perdita di interconnessione*



# EVOLUZIONE IN SANITA'

**MDCG 2019-16**
**Guidance on Cybersecurity for medical devices**
**December 2019**

Bruxelles, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020

(Testo rilevante ai fini del SEE)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

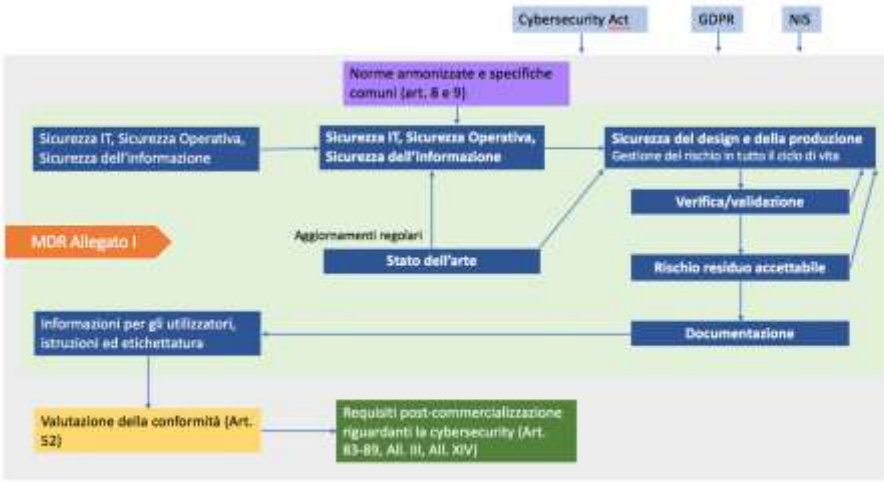



**Figura 2:** Requisiti di sicurezza informatica nell'MDR; l'applicazione di altre normative UE pertinenti,



# Qualificazione giuridica – dispositivo medico

**2. Concetti di base della cybersecurity**
- 2.1. Sicurezza IT, sicurezza delle informazioni, sicurezza delle operazioni
- 2.2. Sicurezza, protezione ed efficacia
- 2.3. Uso previsto e ambiente operativo previsto di utilizzo
- 2.4. Uso scorretto ragionevolmente prevedibile[7]
- 2.5. Ambiente operativo
- 2.6. **Responsabilità congiunta - Aspettative specifiche da parte di altri stakehold**

**3. Progettazione e fabbricazione sicura**
- 3.1. "Sicurezza by design"
- 3.2. Gestione dei rischi per la sicurezza
- 3.3. Capacità di sicurezza
- 3.4. Valutazione dei rischi per la sicurezza
- 3.5. Analisi del rapporto beneficio-rischio per la sicurezza
- 3.6. Requisiti minimi IT
- 3.7. Verifica/Validazione
- 3.8. Aspetti del ciclo di vita

**4. Documentazione e istruzioni per l'uso**
- **4.1. Documentazione**
- **4.2. Istruzioni per l'uso**
- **4.3. Informazioni da fornire agli operatori sanitari**

**5. Sorveglianza e vigilanza post-commercializzazione**
- 5.1. Sistema di sorveglianza post-market
- 5.2. Vigilanza

AI ACT

STEFANELLI & STEFANELLI STUDIO LEGALE

# art. 15

**Accuratezza, robustezza e cibersicurezza**

*I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da conseguire un adeguato livello di accuratezza, robustezza e cibersicurezza e da operare in modo coerente con tali aspetti durante tutto il loro ciclo di vita.*

*I sistemi di IA ad alto rischio sono **il più** resilienti **possibile** per quanto riguarda errori, guasti o incongruenze che possono verificarsi all'interno del sistema o nell'ambiente in cui esso opera, in particolare a causa della loro interazione con persone fisiche o altri sistemi.*
***A tale riguardo sono adottate misure tecniche e organizzative.***



AI ACT

STEFANELLI & STEFANELLI STUDIO LEGALE

art. 15

Accuratezza, robustezza e cibersicurezza

*I sistemi di IA ad alto rischio che proseguono il loro apprendimento dopo essere stati immessi sul mercato o messi in servizio sono sviluppati in modo tale da **eliminare o ridurre il più possibile il rischio di output potenzialmente distorti che influenzano** gli input per operazioni future (feedback loops, ossia "circuiti di feedback") e garantire che tali circuiti di feedback siano oggetto di adeguate misure di attenuazione.*

*I sistemi di IA ad alto rischio sono resilienti ai tentativi di terzi non autorizzati di modificarne l'uso**, gli output** o le prestazioni sfruttando le vulnerabilità del sistema.*

.

# AI ACT

## art. 15

**Accuratezza, robustezza e cibersicurezza**

*Le soluzioni tecniche finalizzate ad affrontare le vulnerabilità specifiche dell'IA includono, ove opportuno, misure volte a prevenire**, accertare, rispondere, risolvere** e controllare gli attacchi che cercano di manipolare il set di dati di addestramento (data poisoning, ossia "avvelenamento dei dati") **o i componenti preaddestrati utilizzati nell'addestramento (model poisoning, ossia "avvelenamento dei modelli"),** gli input progettati in modo da far sì che il modello di IA commetta un errore (adversarial examples, ossia "esempi antagonistici"**, o model evasion, ossia "evasione dal modello"), gli attacchi alla riservatezza** o i difetti del modello.*



11




12

**LE NOSTRE RISORSE ONLINE:**

www.studiolegalestefanelli.it


https://privacygdpr.it/


https://www.medicaldevicenews.eu/


Osservatorio europeo della privacy


Osservatorio sanzioni privacy


Rubrica ricerca scientifica e privacy


Rubrica e raccolta fonti normative sull'IA


Rubrica DM in collaborazione con Aboutpharma


Osservatorio europeo DM

13

GRAZIE DELL' ATTENZIONE!

Restiamo a Vostra disposizione
contattateci su:
info@studiolegalestefanelli.it
O su
Linkedin