

Indice

- p. 11 Introduzione di Raffaele Oriani
- 13 Capitolo 1
Lo scenario clinico e le criticità delle reti attuali: l'imperativo del tempo
1.1. Le sindromi coronariche acute: la sfida diagnostica sul campo, 13
1.2. L'organizzazione della riperfusione: il modello Hub & Spoke, 18
1.3. Le vulnerabilità del sistema attuale: tra frammentazione informativa e stress decisionale, 19
- 21 Capitolo 2
Il cuore dell'innovazione: un nuovo percorso assistenziale
2.1. Ridefinire il triage preospedaliero: dal soccorso statico al routing dinamico, 22
2.2. Validazione clinica, sostenibilità e il paradigma "human-on-the-loop", 24
2.3. Azioni prioritarie, 25
2.4. Cronoprogramma (12 mesi), 26
- 29 Capitolo 3
L'ecosistema intelligente: infrastruttura digitale e telecardiologia
3.1. Applicazioni alla rete IMA: dall'acquisizione del segnale alla trasmissione remota, 30
3.2. L'intelligenza artificiale: il motore algoritmico della rete IMA, 35
- 43 Capitolo 4
La continuità delle cure: la riabilitazione predittiva
4.1. Il superamento della stratificazione statica, 44
4.2. L'ospedale a domicilio e i "biomarcatori digitali", 44
4.3. L'alleanza terapeutica digitale: comunicazione e psicologia, 46
4.4. Una rete orientata alla sostenibilità globale, 47

- p. 49 Capitolo 5
La cornice regolatoria: sicurezza, responsabilità e valore pubblico
5.1. Conformità del progetto alla normativa sulle reti tempo-dipendenti, 50
5.2. Valutazioni di programmazione sanitaria, clinical governance, HTA e sostenibilità finanziaria, 52
5.3. Inquadramento del sistema degli acquisti pubblici in sanità, 53
5.4. La scelta del medical device: normativa, tutela contrattuale e responsabilità, 55
5.5. Data protection nei dispositivi medici integrati con IA, 57
5.6. Risk management, 59
- 63 Capitolo 6
Architettura della rete IA: governance, interoperabilità e indipendenza tecnologica
6.1. Il problema architetturale: dalla monolitica al paradigma agnostico, 63
6.2. Architettura a livelli e standard di interoperabilità, 65
6.3. Indipendenza dal modello di IA: orchestrazione e meta-modello, 68
6.4. Validazione continua e vigilanza algoritmica sul territorio, 69
6.5. Sovranità dei dati e governance contrattuale dei fornitori, 71
6.6. Resilienza operativa e architettura edge-cloud, 72
6.7. Cybersecurity by design e gestione degli incidenti, 73
6.8. Sintesi e prospettive, 74
- 77 Bibliografia