ESTRATTO

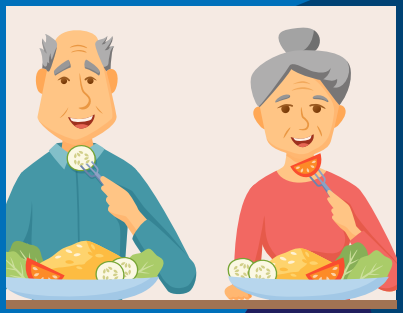
Volume 39 - Numero 3
Marzo 2026
ISSN 0394-9303 (cartaceo)
ISSN 1827-6296 (online)

Notiziario
dell'Istituto Superiore di Sanità

Inquadramento normativo, responsabilità e ruoli, nel controllo/monitoraggio remoto dei device cardiaci impiantabili

F. Censi, M. Bocchino, L. Santini, D. Ricci, F. Ammirati, G. Bisignani



www.iss.it

INQUADRAMENTO NORMATIVO, RESPONSABILITÀ E RUOLI, NEL CONTROLLO/MONITORAGGIO REMOTO DEI DEVICE CARDIACI IMPIANTABILI

Federica Censi[1], Manuela Bocchino[2], Luca Santini[3], Dario Ricci[4], Fabrizio Ammirati[5] e Giovanni Bisignani[6]
[1]*Dipartimento Malattie Cardiovascolari, Dismetaboliche e dell'Invecchiamento, ISS*
[2]*UOC Sviluppo Organizzativo e della Competence Individuale, Direzione Generale, ASL Roma 3, Roma*
[3]*UOC Cardiologia, Presidio Ospedaliero G.B. Grassi, ASL Roma 3, Roma*
[4]*UOC Sistemi Informativi, ASL della Provincia di Bari, Bari*
[5]*ASL Roma 3, Roma*
[6]*UOC Cardiologia-UTIC-Emodinamica, Ospedale Castrovillari, ASP Cosenza, Castrovillari*

RIASSUNTO - Il controllo remoto dei dispositivi cardiaci impiantabili consente la trasmissione automatica dei dati clinici, migliorando l'assistenza e riducendo visite e ricoveri. Introdotto nel 2001, è oggi parte essenziale della telemedicina. Il quadro normativo europeo e le linee guida definiscono ruoli e responsabilità dei diversi attori. Il General Data Protection Regulation (2016/679) tutela i dati personali; il Medical Device Regulation (2017/745) assicura sicurezza, efficacia e corretta destinazione d'uso; l'Artificial Intelligence Act (2024/1689) regola i sistemi di intelligenza artificiale ad alto rischio. Le linee guida Heart Rhythm Society/European Heart Rhythm Association 2023 ed European Society of Cardiology/European Heart Rhythm Association 2020 fissano standard clinici, legali e organizzativi, promuovendo sicurezza e formazione.
Parole chiave: telemedicina; monitoraggio remoto; conformità normativa

SUMMARY (*Regulatory framework, responsibilities and roles in the remote control/monitoring of implantable cardiac devices*) - Remote monitoring of implantable cardiac devices enables the automatic transmission of clinical data, improving care and reducing visits and hospitalizations. Introduced in 2001, it is now an essential part of telemedicine. The European regulatory framework and related guidelines define the roles and responsibilities of all stakeholders. The General Data Protection Regulation (2016/679) protects personal data; the Medical Device Regulation (2017/745) ensures device safety, effectiveness, and proper intended use; and the AI Act (2024/1689) regulates high-risk artificial intelligence systems. The Heart Rhythm Society/European Heart Rhythm Association 2023 and European Society of Cardiology/European Heart Rhythm Association 2020 guidelines establish clinical, legal, and organizational standards, promoting safety, professional training, and structured data management.
Key words: telemedicine; remote monitoring; regulatory compliance
federica.censi@iss.it

Il controllo remoto dei dispositivi impiantabili consente ai medici di ricevere automaticamente, tramite trasmettitori o app, i dati diagnostici e terapeutici registrati dal dispositivo (ritmo cardiaco, batteria, funzionalità, eventuali aritmie). Questo sistema permette di individuare precocemente problemi, ridurre le visite ambulatoriali e i ricoveri non necessari, migliorando l'efficienza delle cure e la qualità di vita del paziente. Introdotto nel 2001, oggi rappresenta un paradigma consolidato della telemedicina che ha rivoluzionato la gestione clinica dei pazienti (1). Dalla sua introduzione, la tecnologia per il controllo remoto si è evoluta con piattaforme più sicure, rapide e semplici da usare, basate su reti cellulari, Internet e Bluetooth (2).

Per integrarlo nei servizi sanitari nazionali è necessario chiarire ruoli e responsabilità di operatori, produttori, autorità e pazienti. Il quadro normativo europeo (Figura) stabilisce regole fondamentali su sicurezza, protezione dei dati ed efficacia, mediante i Regolamenti Medical Device Regulation (MDR, Regolamento sui Dispositivi Medici 2017/745) (3) e General Data Protection Regulation (GDPR, ▶

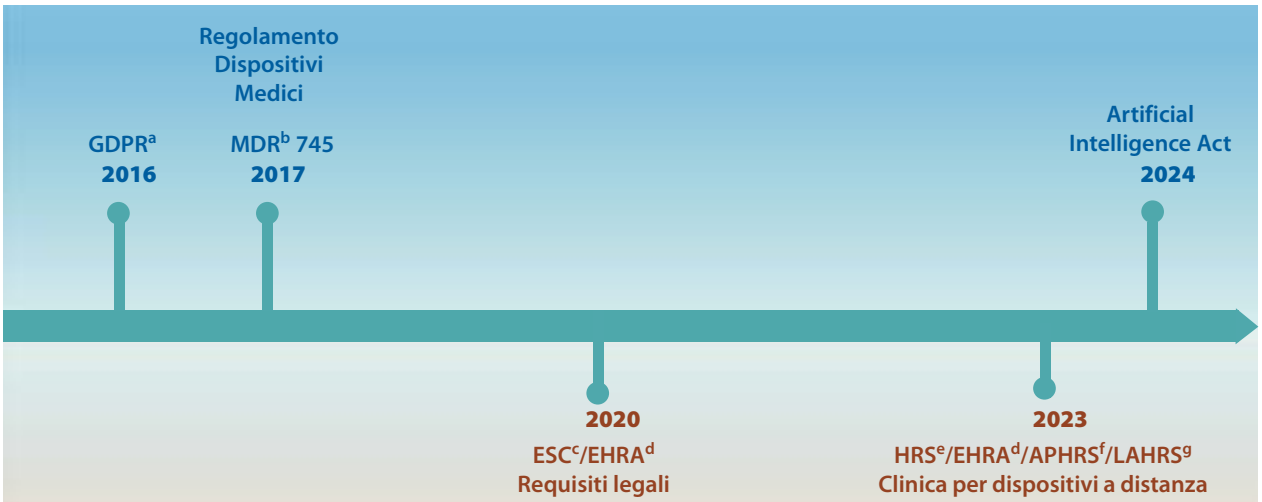


Figura - Quadro normativo e linee guida nel contesto del controllo remoto dei dispositivi cardiaci impiantabili

Regolamento Generale sulla Protezione dei Dati 2016/679) (4), oltre a linee guida internazionali (5) e al Report European Society of Cardiology (ESC)/ European Heart Rhythm Association (EHRA) sui requisiti legali ed etici (6). Poiché i dati raccolti possono alimentare algoritmi di intelligenza artificiale a fini prognostici o terapeutici, è necessario tenere conto dell'applicabilità del Regolamento sull'Artificial Intelligence Act (AI Act) 2024/1689 (7).

In questo articolo verranno analizzate le implicazioni dei Regolamenti e delle linee guida relative a questa tecnologia, con l'obiettivo di facilitare la comprensione dei ruoli e delle responsabilità dei diversi attori coinvolti. In questo contesto, l'Istituto Superiore di Sanità svolge un ruolo chiave, grazie alla conoscenza approfondita dei Regolamenti e alla capacità di considerare tali aspetti nei progetti e nelle attività di ricerca nel settore dei pacemaker e della telemedicina.

Regolamenti europei

GDPR: titolarità e responsabilità del trattamento dei dati

Il controllo remoto dei Dispositivi Cardiaci Impiantabili (DCI) comporta la raccolta, l'elaborazione e la trasmissione di dati personali, rendendo centrale il rispetto del GDPR - Regolamento UE 2016/679 (4). In questo contesto, è fondamentale stabilire la titolarità e le responsabilità del trattamento dei dati personali. Secondo il GDPR, il titolare del trattamento è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati Membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati Membri". Il GDPR definisce il responsabile del trattamento come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".

Sulla base di queste definizioni, come anche riportato nel report della task force ESC/EHRA, il fabbricante dei DCI non può non essere considerato titolare del trattamento dati, in quanto, nell'ambito della destinazione d'uso del controllo remoto definisce le finalità e i mezzi del trattamento. La responsabilità del trattamento dei dati può invece essere attribuita anche a terze parti. Questi aspetti verranno approfonditamente trattati nel paragrafo relativo al report della task force ESC/EHRA.

Per quanto riguarda i diritti del paziente, il GDPR garantisce ai pazienti il diritto di accesso, rettifica e cancellazione dei propri dati, oltre alla trasparenza sull'uso e sulla conservazione delle informazioni raccolte dai dispositivi. Questi aspetti devono essere

necessariamente considerati nel consenso informato, che rappresenta l'atto con cui i pazienti vengono informati relativamente al trattamento dei loro dati.

Infine, la conformità al GDPR impone l'adozione di misure di sicurezza avanzate, tra cui la crittografia e la pseudonimizzazione, per prevenire accessi non autorizzati e garantire l'integrità delle informazioni trasmesse.

MDR: destinazione d'uso e responsabilità del fabbricante e dell'utilizzatore

L'MDR (Regolamento UE 2017/745) (3) disciplina l'immissione sul mercato e l'utilizzo dei dispositivi medici, inclusi i DCI dotati di funzionalità di monitoraggio remoto. L'MDR assicura che i dispositivi medici immessi sul mercato o messi in servizio rispettino rigorosi requisiti di sicurezza e prestazione, in modo da tutelare la salute di pazienti e operatori. Inoltre, richiede che l'utilizzo del dispositivo comporti un beneficio clinico documentato, superiore ai rischi connessi. La conformità al Regolamento è attestata attraverso il rilascio della marcatura CE.

I DCI e i relativi sistemi di monitoraggio remoto rientrano pienamente nella definizione di dispositivo medico secondo l'MDR. Considerata la loro elevata classe di rischio, la valutazione di conformità deve essere eseguita da un organismo notificato, ovvero un ente designato dall'autorità competente per verificare il rispetto di tutti i requisiti normativi da parte del fabbricante.

Una specificità dei sistemi di monitoraggio remoto è che il loro funzionamento fino all'invio dei dati al server è interamente sotto la responsabilità del fabbricante. L'accesso ai dati da parte delle strutture sanitarie, invece, è escluso da tale responsabilità. Questo aspetto è regolato dall'MDR attraverso la definizione della destinazione d'uso, che è stabilita dal fabbricante.

Nel contesto del monitoraggio remoto, la destinazione d'uso - con formulazioni che possono variare tra produttori - viene generalmente descritta come strumento per la sorveglianza a distanza da parte del medico, a supporto della diagnosi nei pazienti portatori di DCI, ma non per l'uso in situazioni di emergenza.

Infatti, l'accesso ai dati trasmessi avviene spesso tramite reti di comunicazione non controllate direttamente dal fabbricante (ad esempio, connessioni Internet delle strutture sanitarie). Di conseguenza, non è garantita la continuità e la sicurezza della trasmissione dei dati, e non è possibile attribuire in modo univoco eventuali responsabilità in caso di disservizi. Per questo motivo, tali sistemi non sono considerati idonei alla gestione di situazioni di emergenza o urgenza.

Va, infine, sottolineato che un utilizzo del dispositivo difforme, rispetto alla destinazione d'uso definita dal fabbricante, comporta lo spostamento della responsabilità dal fabbricante stesso all'utilizzatore.

AI Act: applicazioni sanitarie ad alto rischio e conformità

L'AI Act (2024/1689) (7) definisce regole armonizzate per lo sviluppo e l'uso sicuro dell'intelligenza artificiale nel mercato europeo. Pur avendo un ambito generale, richiama esplicitamente le applicazioni rientranti nell'MDR. Dall'analisi congiunta dei due Regolamenti emerge che i sistemi di controllo remoto con AI rientrano tra quelli ad alto rischio. Tali applicazioni richiedono una valutazione di conformità simile a quella dell'MDR, con marchio CE a garanzia. Entrambi i Regolamenti impongono una documentazione tecnica completa; per il software, l'MDR richiede descrizione, architettura, gestione dei dati e analisi dei rischi, mentre l'AI Act aggiunge requisiti di trasparenza e responsabilità, comprese valutazioni dei rischi, governance dei dati e test di prestazioni. Questa documentazione può essere integrata in quella prevista dall'MDR. Entrambi i Regolamenti adottano un approccio basato sul ciclo di vita. L'MDR assicura sicurezza e prestazioni dei dispositivi, mentre l'AI Act rafforza tale prospettiva con revisione continua, monitoraggio post-commercializzazione e supervisione umana dei sistemi ad alto rischio. È richiesto un sistema di gestione del rischio continuo, aggiornato con i dati provenienti dall'uso clinico.

Per i dispositivi dotati di AI che continuano ad apprendere dopo l'immissione in commercio, il monitoraggio post-market è essenziale per mantenere sicurezza e conformità, identificare tempestivamente nuovi rischi e comunicare aggiornamenti a pazienti, professionisti e organismi notificati.

Linee guida

Le linee guida in ambito medico rappresentano il riferimento fondamentale per la gestione clinica. Basate su evidenze scientifiche e consenso degli esperti, forniscono indicazioni aggiornate e validate a livello internazionale, garantendo che le pratiche adottate siano sicure, efficaci e conformi agli standard scientifici e normativi. Seguire le linee guida consente: ▶

- un approccio uniforme e standardizzato alla gestione dei pazienti, riducendo la variabilità clinica;
- una maggiore sicurezza e qualità dell'assistenza attraverso protocolli convalidati;
- l'adeguamento alle normative europee e internazionali, evitando criticità legali o etiche.

Linee guida HRS/EHRA 2023 sul controllo remoto

Le linee guida HRS/EHRA 2023 (5) definiscono il monitoraggio remoto dei DCI come standard di cura (Classe I, livello A), supportato da evidenze che dimostrano la capacità di rilevare precocemente eventi clinicamente rilevanti (aritmie, disfunzioni, scompenso), ridurre le visite in presenza, migliorare il rispetto da parte del paziente delle indicazioni terapeutiche e delle raccomandazioni cliniche, quindi potenzialmente la sopravvivenza.

Tra i principali benefici, il documento sottolinea la connettività continua, cioè l'acquisizione e la trasmissione frequente e automatica dei dati. Tale modello consente una sorveglianza costante e un intervento precoce, contribuendo alla riduzione delle ospedalizzazioni e, in alcuni studi, della mortalità. Condizione essenziale è una connessione stabile e duratura. L'efficacia dei programmi dipende dall'organizzazione clinica che le linee guida raccomandano che sia dedicata con team multidisciplinari con compiti definiti, workflow strutturati e dotazione adeguata di personale (almeno 3 unità di personale full-time equivalente ogni 1.000 pazienti). Centrale è l'ottimizzazione della gestione degli alert, che va personalizzata e supportata da strumenti digitali e algoritmi per garantire tempestività e contenere il carico di lavoro.

L'arruolamento del paziente dovrebbe avvenire prima della dimissione, soprattutto nei portatori di *loop recorder*. Il successo del primo collegamento è indice di corretta attivazione e devono esistere protocolli per il rapido ripristino della connettività. Paziente e caregiver vanno coinvolti con formazione personalizzata già nella fase pre-impianto, al fine di migliorare consapevolezza, aspettative e aderenza a lungo termine.

Dal punto di vista tecnologico, le soluzioni di controllo remoto differiscono per modalità e frequenza di trasmissione; l'affidabilità e la sicurezza restano imprescindibili, così come la consapevolezza che il sistema non sostituisce quello di emergenza. È raccomandata una formazione specifica del personale clinico e la realizzazione di *audit* periodici di qualità.

Numerosi studi dimostrano il rapporto costo-efficacia del controllo remoto rispetto al follow-up in presenza, grazie alla riduzione di visite, ospedalizzazioni e costi indiretti. Tuttavia, la mancanza di un rimborso uniforme limita la diffusione, con forti disomogeneità regionali. L'Accordo Stato-Regioni 2020 ha riconosciuto la telemedicina come prestazione del Servizio Sanitario Nazionale, ma solo alcune Regioni hanno introdotto codici dedicati (Piemonte, Liguria, Veneto, Trento, Friuli Venezia Giulia, Toscana, Puglia), altre la consentono genericamente (Valle d'Aosta, Sardegna, Campania), mentre Emilia-Romagna e Lazio ne permettono l'integrazione con la televisita.

Il *Consensus* raccomanda modelli di rimborso che riflettano i costi reali e garantiscano accesso, equità e sostenibilità. Sottolinea, inoltre, l'importanza di una collaborazione strutturata tra clinici, produttori di dispositivi e fornitori di servizi, per assicurare aggiornamenti, supporto tecnico, formazione e gestione condivisa degli alert di sicurezza.

Linee guida ESC/EHRA 2020 sui requisiti legali e il GDPR

Le linee guida ESC/EHRA 2020 (6) definiscono i requisiti legali del controllo remoto, in collegamento con il GDPR (UE 2016/679) (4). I punti centrali riguardano ruoli di titolare e responsabile del trattamento, cybersecurity e consenso informato.

I fabbricanti di DCI e sistemi di monitoraggio, stabilendo finalità e mezzi del trattamento, sono titolari ai sensi del GDPR, così come le strutture sanitarie, poiché selezionano e gestiscono i dati necessari al monitoraggio. Serve, quindi, un accordo contrattuale tra fabbricante e struttura, soprattutto in caso di trasferimento dati extra-UE. All'interno delle strutture sanitarie i medici possono essere considerati titolari del trattamento dati solo se liberi professionisti. In generale, fabbricante e struttura dovrebbero configurarsi come co-titolari, con eventuali fornitori esterni nel ruolo di responsabili del trattamento.

Relativamente alla sicurezza dei dati, i DCI attuali utilizzano interfacce radio per comunicare in modalità wireless con dispositivi esterni, permettendo la telemetria dei dati e la riprogrammazione non invasiva. Questi vantaggi si accompagnano a nuove vulnerabilità in termini di cybersicurezza, poiché l'aumento di software e interfacce estende la "superficie d'attacco" dei dispositivi.

Studi recenti dimostrano che attacchi possono essere condotti sia tramite l'interfaccia wireless sia, in casi limitati, tramite l'interfaccia analogica

(sensori e attuatori interni) (8-10). Le minacce wireless sono più rilevanti, perché più facili da eseguire anche a distanza, mentre gli attacchi analogici richiedono condizioni difficili da realizzare. L'uso di protocolli proprietari non offre protezione adeguata: si raccomanda l'adozione di robusti protocolli crittografati, validati e aperti, abbandonando soluzioni obsolete.

Quanto al consenso informato, il GDPR richiede che sia libero, specifico, informato e chiaro. Nella pratica, però, studi su 72 moduli provenienti da 16 Paesi hanno rilevato incoerenze e carenze, come l'assenza di informazioni su localizzazione e accesso ai dati (6). Molti pazienti ricevono meno dettagli di quanto si aspettino. Per questo la task force ha elaborato un modulo informativo e un esempio di consenso, con il contributo dei pazienti, per migliorarne chiarezza e accessibilità.

Discussione

Responsabilità delle strutture sanitarie

Le strutture sanitarie che gestiscono il controllo remoto, insieme ai fabbricanti dei dispositivi, possono assumere la qualifica di co-titolari (*joint controllers*) del trattamento dei dati secondo il GDPR. In questa veste, hanno la responsabilità condivisa di proteggere le informazioni cliniche raccolte dai dispositivi e di supervisionare eventuali trasferimenti verso fornitori esterni responsabili del trattamento dei dati (*data processor*), nel rispetto delle normative nazionali ed europee. Devono informare i pazienti in modo chiaro sull'uso di servizi di terze parti, sui rischi di sicurezza e sulle modalità di trattamento dei dati, così da ottenere un consenso consapevole e valido.

Dal punto di vista operativo, le strutture devono garantire personale formato, risorse tecnologiche e procedure adeguate per il corretto funzionamento dell'organizzazione del personale addetto al monitoraggio. Anche in caso di esternalizzazione di attività (*triage*, raccolta dati, report), restano responsabili della supervisione, verificando qualifiche dei fornitori, tracciabilità e conformità etica e normativa. Una gestione inadeguata può generare rischi clinici, economici e legali a carico dell'istituzione. Infine, è essenziale integrare i dati del monitoraggio remoto nei sistemi informativi sanitari, per garantire continuità di cura, disponibilità delle informazioni a tutti gli operatori e protezione dei diritti del paziente.

Responsabilità del fabbricante

I fabbricanti dei dispositivi medici impiantabili assumono sempre il ruolo di titolari del trattamento dei dati secondo il GDPR, in quanto determinano quali dati raccogliere, il loro formato e le finalità del trattamento.

I fabbricanti hanno un ruolo chiave nello sviluppo dei DCI e nella garanzia di sicurezza ed efficacia. Devono comunicare tempestivamente con clinici e pazienti in caso di interruzioni, richiami o avvisi di sicurezza, ma senza sostituirsi al personale sanitario nella cura o nella gestione dei dati. Devono garantire il corretto funzionamento dei sistemi di monitoraggio remoto in diverse aree geografiche, affrontando problemi di connettività e compatibilità internazionale. Poiché i dati risiedono su server gestiti dai fabbricanti, è essenziale assicurarne sicurezza, crittografia e conformità alle norme sulla privacy. Tali dati sono utili non solo al miglioramento dei dispositivi, ma anche alla ricerca scientifica.

La connettività costante è fondamentale per la sicurezza del paziente. I fabbricanti devono fornire supporto formativo e tecnico, soluzioni alternative per chi ha scarsa connettività o competenze digitali, e garantire compatibilità con diversi smartphone. I sistemi di monitoraggio remoto devono avvisare chiaramente in caso di disconnessione e fornire istruzioni semplici per il ripristino, coinvolgendo i pazienti nella gestione autonoma dei problemi per ridurre il carico sulle cliniche.

Con l'aumento dei richiami e degli avvisi di sicurezza, la comunicazione con le cliniche deve essere immediata, multipla e aggiornata fino a conferma della ricezione. La collaborazione con autorità e comunità clinica è cruciale per mantenere fiducia e sicurezza.

Infine, le differenze tra i vari fabbricanti in termini di interfacce, algoritmi e frequenza di trasmissione dei dati richiedono supporto costante al personale sanitario, soprattutto dopo l'impianto, per ottimizzare la programmazione ed evitare falsi allarmi. La scelta del sistema deve considerare anche la capacità del paziente di utilizzarlo efficacemente, per garantire il successo del monitoraggio nel tempo.

Responsabilità del personale sanitario e tecnico

Un elemento centrale per l'efficacia del controllo remoto è l'adozione di un modello organizzativo multidisciplinare, supportato da procedure condivise che definiscano formalmente i compiti di medici, infermieri, tecnici e personale amministrativo. Le linee guida internazionali raccomandano questo approccio, poi- ▶

ché una struttura operativa chiara favorisce una gestione ottimale delle attività. Il personale clinico che revisiona e interpreta le trasmissioni deve possedere competenze certificate, acquisite tramite formazione o percorsi specifici. La qualificazione professionale è essenziale per garantire qualità e aderenza alle evidenze scientifiche. A tale scopo, sono raccomandati *audit* periodici e programmi di miglioramento continuo.

Le responsabilità operative sono distribuite in base alle funzioni: medici, infermieri specializzati e tecnici gestiscono trasmissioni, alert, comunicazione con i pazienti e programmazione dei dispositivi; il personale non sanitario supporta attività amministrative e logistiche, arruolamento, connettività, aggiornamento piattaforme e, se previsto, *triage* dei dati.

La crescente mole di trasmissioni programmate e non programmate richiede un adeguamento delle risorse: la gestione di 1.000 pazienti necessita di almeno 3 Full-Time Equivalent (FTE, Equivalente a Tempo Pieno) clinici e amministrativi, con variazioni legate al tipo di device e alla quota di trasmissioni non programmate, spesso associate a necessità di interventi tempestivi. La gestione dei dati include sorveglianza dei parametri, valutazione di eventi clinici, comunicazione con il team curante, documentazione e rendicontazione, attività che devono seguire un workflow strutturato e tracciabile. Un controllo remoto efficace richiede una risposta rapida e organizzata agli alert, che possono indicare eventi clinici o problemi tecnici: la tempestività nella loro gestione è direttamente collegata agli esiti dei pazienti e rappresenta una responsabilità centrale del team. ■

Dichiarazione sui conflitti di interesse

Gli autori dichiarano che non esiste alcun potenziale conflitto di interesse o alcuna relazione di natura finanziaria o personale con persone o con organizzazioni, che possano influenzare in modo inappropriato lo svolgimento e i risultati di questo lavoro.

Riferimenti bibliografici

1. Vandenberk B, Raj SR. Remote Patient Monitoring: What Have We Learned and Where Are We Going? *Curr Cardiovasc Risk Rep* 2023;17(6):103-15 (doi: 10.1007/s12170-023-00720-7).
2. Tan VH, See Tow HX, Fong KY, *et al*. Remote monitoring of cardiac implantable electronic devices using smart device interface versus radiofrequency-based interface: A systematic review. *J Arrhythm* 2024;40(3):596-604 (doi: 10.1002/joa3.13054).
3. Unione Europea. Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio. *Gazzetta Ufficiale dell'Unione Europea* L 117, 5 maggio 2017.
4. Unione Europea. Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (regolamento generale sulla protezione dei dati). *Gazzetta Ufficiale dell'Unione Europea* L 119/1, 4 maggio 2026.
5. Ferrick AM, Raj SR, Deneke T, *et al*. 2023 HRS/EHRA/APHRS/LAHRS Expert Consensus Statement on Practical Management of the Remote Device Clinic. *Europace* 2023;25(5):euad123 (doi: 10.1093/europace/euad123).
6. Nielsen JC, Kautzner J, Casado-Arroyo R, *et al*. Remote monitoring of cardiac implanted electronic devices: legal requirements and ethical principles - ESC Regulatory Affairs Committee/EHRA joint task force report. *Europace* 2020;22(11):1742-58 (doi: 10.1093/europace/euaa168). *Erratum* in: Europace 2021;23(6):843 (doi: 10.1093/europace/euab053).
7. Unione Europea. Regolamento (UE) 2024/1689 del Parlamento europeo e del consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale). *Gazzetta Ufficiale dell'Unione Europea* L 2024/1689, 12 luglio 2024.
8. Rios B, Butts J. *Security evaluation of the implantable cardiac device ecosystem architecture and implementation interdependencies*. WhiteScope; 2017 (https://a51.nl/sites/default/files/pdf/Pacemaker%20Ecosystem%20Evaluation.pdf).
9. US Food and Drug Administration. *Cybersecurity vulnerabilities affecting Medtronic implantable cardiac devices, programmers, and home monitors*. FDA safety communication; 2019 (https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity).
10. Pycroft L, Aziz TZ. Security of implantable medical devices with wireless connections: the dangers of cyber-attacks. *Exp Rev Med Dev* 2018;15 (6):403-6 (doi: 10.1080/17434440.2018.1483235).

TAKE HOME MESSAGES

- Il monitoraggio remoto dei dispositivi cardiaci impiantabili migliora la qualità dell'assistenza, riducendo visite e ricoveri attraverso una sorveglianza continua e tempestiva.
- Il rispetto dei Regolamenti europei (GDPR, MDR, AI Act) è fondamentale per garantire sicurezza, privacy e responsabilità nella gestione dei dati e dei DCI.
- L'organizzazione clinica e la formazione del personale sono essenziali per un uso efficace e sicuro della telemedicina, assicurando standard di cura uniformi e sostenibili.