

Design Control

Il filo rosso che porta dall'idea al Dispositivo Medico

Paolo Gibellini

Commissione Biomedica - Ordine degli Ingegneri della Provincia di Brescia

La diffusione di Dispositivi Medici digitali - dai *software* diagnostici ai sistemi basati su AI - sta trasformando la pratica clinica. La velocità con cui sta avvenendo questa evoluzione spinge a chiedersi quando possiamo considerare davvero sicuro uno strumento digitale utilizzato in sanità. La risposta non risiede in una singola norma, ma in un insieme articolato di processi, controlli e responsabilità condivise.

Il ruolo centrale del Design Control

Alla base dello sviluppo di ogni Dispositivo Medico c'è il *Design Control*, un insieme di metodologie formali e documentate che guida la progettazione e getta le basi per l'intero ciclo di vita del prodotto. È un percorso strutturato che parte dalla definizione dei requisiti clinici e arriva alla validazione prima dell'immissione sul mercato, collegandosi poi al monitoraggio *post-market*.

Il termine nasce nella *regulation* statunitense FDA (21 CFR 820.30) ed è stato adottato dalle norme ISO (v. ISO 13485). In settori regolamentati, come i Dispositivi Medici e i diagnostici in vitro (IVD), il *Design Control* è un requisito obbligatorio, ma resta una buona prassi per qualsiasi attività di sviluppo di *hardware* o *software* complessi.

L'obiettivo non è rallentare l'innovazione, ma garantire che ogni funzione sia giustificata, ogni rischio mitigato e ogni modifica tracciata. È il "filo rosso" che collega l'idea iniziale al dispositivo che entra in reparto.

Il *Design Control* si attiva subito dopo le fasi preliminari di fattibilità e impone al fabbricante di documentare gli aspetti principali del progetto:

- **Intended Use** (Destinazione d'uso), alla base di tutto: il fabbricante definisce lo scopo clinico del dispositivo, i pazienti target, gli utilizzatori e l'ambiente d'uso (sala operatoria, uso domestico, ...).
- Definizione dei **requisiti**: raccolta delle

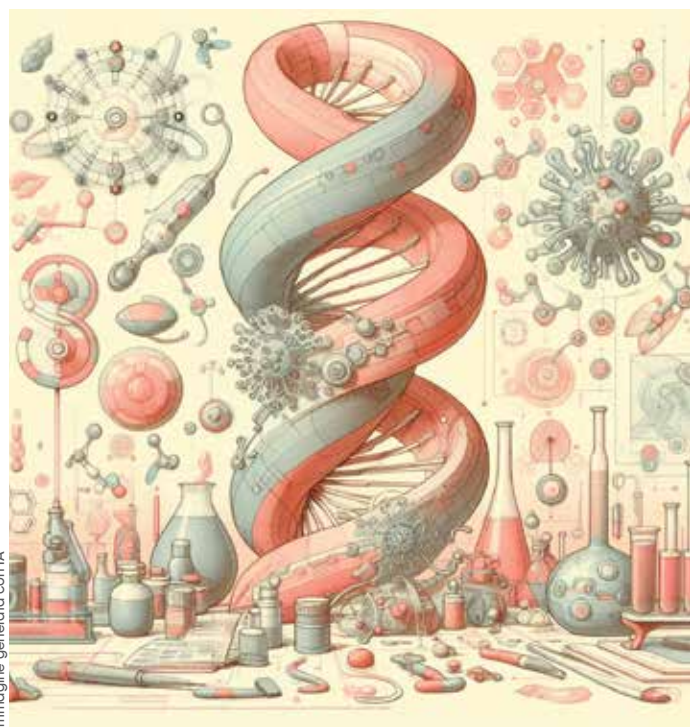


Immagine generata con IA

specifiche funzionali, non funzionali, di prestazione, di interfaccia utente, di sicurezza dell'utente (*safety*) e dei dati (*security*).

- **Gestione dei Rischi**, processo continuo (v. ISO 14971) per identificare pericoli potenziali, proporre mitigazioni adeguate, introdurre requisiti di *safety* e *cybersecurity*.
- **Sviluppo dei requisiti**: processo iterativo che porta al prototipo attraverso una continua **verifica** che ciascun requisito sia stato soddisfatto (*"abbiamo fatto il prodotto nel modo corretto"*).
- **Validazione** del dispositivo, effettuata prima della commercializzazione, attraverso test clinici o in ambienti simulati. Serve a ottenere l'evidenza che il dispositivo risponda alle reali necessità di medici e pazienti e sia idoneo per l'*intended use* (*"abbiamo fatto il prodotto corretto"*).
- **Change Control e Post-Market**: segnalazioni degli utilizzatori, aggiornamenti normativi o minacce informatiche attivano un processo controllato di modifica (**change**) che porta alla revisione dei requisiti e termina con il rilascio di una nuova release del prodotto, al fine di mantenere inalterate affidabilità, sicurezza e conformità del sistema nel tempo.

La documentazione viene raccolta nel **Design History File** (DHF), mostrato durante le verifiche ispettive e tenuto periodicamente aggiornato.

L'ingegnere non può progettare senza il medico

Il Design Control si nutre dell'esperienza clinica, il contributo del medico è indispensabile in tre fasi cruciali:

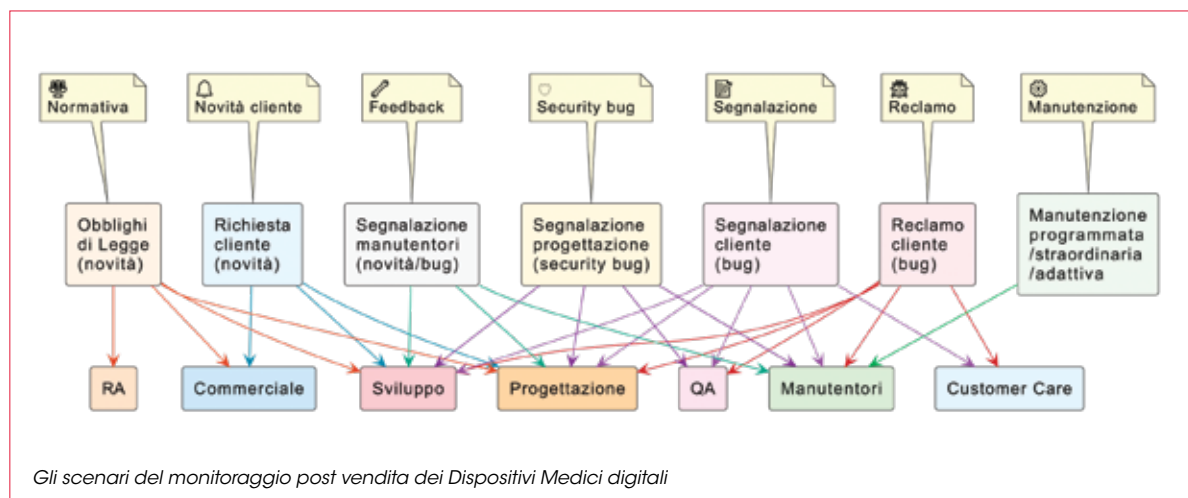
- **Definizione degli URS** (requisiti utente): all'inizio del percorso, il medico definisce le specifiche d'uso e i requisiti di usabilità in reparto, evitando strumenti tecnologicamente perfetti ma inutilizzabili sul campo.
- **Validazione Clinica**: nelle fasi finali, i clinici testano i prototipi (in simulazione o studi clinici) per confermare che il dispositivo risolva il problema del paziente e si integri nei flussi ospedalieri.
- **Sorveglianza Post-Market**: una volta che il dispositivo è in reparto, le segnalazioni di anomalie ed i suggerimenti dei medici alimentano il miglioramento continuo del prodotto.

Il quadro normativo: MDR, IVDR, GDPR e AI Act

Su questa base metodologica si innestano i regolamenti europei: **MDR** per i Dispositivi Medici, **IVDR** per gli IVD, **GDPR** per la gestione dei dati personali. Quando un dispositivo integra algoritmi di AI, entra in gioco l'**AI Act**, che introduce requisiti aggiuntivi: qualità dei *dataset*, assenza di *bias*, trasparenza del funzionamento, supervisione umana, permettendo al medico di comprendere come il sistema elabori un responso. Grazie al pacchetto europeo *Omnibus AI*, si potranno assorbire i requisiti dell'**AI Act** nei controlli di conformità previsti da MDR ed IVDR, semplificando il processo.

Esempi concreti dal mondo clinico

- Un *software* basato su AI che analizza immagini radiologiche deve dimostrare non solo accuratezza, ma anche stabilità delle prestazioni su popolazioni diverse da quelle usate per addestrarlo.



Gli scenari del monitoraggio post vendita dei Dispositivi Medici digitali

- Un algoritmo predittivo per il rischio di sepsi deve permettere al medico di comprendere perché un allarme viene generato, evitando il rischio di “scatole nere” incontrollabili.
- Un’app per il monitoraggio domiciliare deve garantire che un aggiornamento automatico non modifichi il comportamento clinico senza un nuovo ciclo di verifica e validazione.

Safety, security e affidabilità nel mondo reale

Un sistema può definirsi sicuro solo se è in grado di soddisfare contemporaneamente questi requisiti: produrre risultati clinici affidabili nel contesto reale d’uso, proteggere l’integrità dei dati, limitare gli errori d’uso prevedibili e mantenere saldamente il professionista al centro del processo decisionale. La sicurezza non è più un concetto esclusivamente io-medico, è anche cibernetica e comportamentale. La *cybersecurity* è oggi una criticità globale: secondo il Rapporto Clusit 2025, l’Italia è tra i paesi più colpiti da attacchi informatici, con un incremento significativo nel settore sanitario. Gli attaccanti stanno abbandonando i *ransomware* “rumorosi” per tecniche silenziose, installando componenti che restano invisibili e quiescenti fino al momento opportuno. Questo riguarda anche i Dispositivi Medici connessi (IoMT - *Internet of Medical Things*), come pompe infusionali, monitor multiparametrici o sensori indossabili. Un *malware* silente può alterare i dati clinici o bloccare un intero reparto durante un’emergenza.

Accanto alla sicurezza tecnica c’è la sicurezza del dato. Ogni informazione sanitaria, anche apparentemente banale, diventa preziosa quando può essere collegata a una persona. Non solo per i criminali informatici, ma anche per le grandi piattaforme digitali che offrono servizi gratuiti in cambio di una “sbirciatina” sui contenuti scambiati. L’uso improprio di *chat*, *app* o browser non conformi può portare alla trasmissione involontaria di dati sensibili tra medico e paziente, configurando violazioni gravi e non giustificabili (ed esponendo i professionisti a pesanti sanzioni).

Infine, l’AI, che tanto velocemente è entrata nel nostro vivere quotidiano, impone un cambio di paradigma: la tecnologia va indirizzata e mai subita. Per sfruttarla al meglio, il medico deve avere idee estremamente chiare sugli obiettivi clinici ed imparare a fornire al sistema istruzioni e contesti precisi, così da ottenere risposte molto più accurate e prive di allucinazioni *software*. Deve essere anche consapevole dei limiti intrinseci degli algoritmi per evitare il cosiddetto *automation bias* - ovvero la tendenza

La transizione digitale della medicina richiede una nuova cultura della responsabilità.

psicologica ad adagiarsi passivamente sul responso della macchina. Dobbiamo sapere cosa aspettarci ed essere un passo avanti rispetto questa tecnologia per mantenerne il controllo e non adagiarcisi.

Il contesto italiano

In Italia, il quadro si arricchisce di norme nazionali e regionali: sistemi informativi clinici, Fascicolo Sanitario Elettronico, anagrafi vaccinali, interoperabilità e responsabilità di chi inserisce e utilizza il dato. La qualità dell’informazione non è solo un requisito tecnico, ma un elemento essenziale per la sicurezza del paziente, vanno quindi previsti robusti metodi organizzativi.

Il dialogo tra produttori e sanità è sostenuto da reti come Confindustria Dispositivi Medici, Agenas e le società scientifiche, che contribuiscono alla definizione di standard e buone pratiche. Le idee per nuovi strumenti nascono spesso dai clinici: il medico è il primo osservatore dei bisogni reali e un attore fondamentale nella definizione dei requisiti utente.

Responsabilità condivise e governance del rischio

Sul piano operativo, le responsabilità sono distribuite:

- Il **Medico** deve conoscere limiti e indicazioni d’uso del dispositivo.
- La **struttura sanitaria** deve garantire valutazione, integrazione, *cybersecurity* e formazione.
- Gli **operatori** devono seguire procedure e istruzioni del fabbricante.
- Il **caregiver** può utilizzare le tecnologie domiciliari solo entro limiti chiari e tracciabili.

In conclusione, la transizione digitale della medicina non si riduce ad avere nuovi *software* o macchinari in reparto, ma richiede una nuova cultura della responsabilità. Solo un ecosistema coordinato - produttori, clinici, ingegneri, strutture ed autorità regolatorie - può assicurare che l’innovazione tecnologica mantenga la sua promessa originaria: rimanere clinicamente affidabile, ciberneticamente sicura e profondamente centrata sul paziente.