POLITECNICO DI TORINO
Corso di Laurea Magistrale in Ingegneria Biomedica
Strumentazione Biomedica

Tesi di Laurea Magistrale

Introduzione delle *linee guida di design del software* nel processo di valutazione dell'usabilità di una cartella clinica elettronica

Relatori:
Prof. Alberto AUDENINO

Candidati:
Desirée MARCHI

Co-relatori:
Ing. Giovanni PUTAME

Relatori esterni:
Prof. Ernesto IADANZA
Ing. Luca RADICE

Anno Accademico 2021/2022

L'ingegno sta nel trasformare il problema in una soluzione,

e la soluzione in un'innovazione.

D. M.

Abstract

Con l'entrata in vigore del nuovo regolamento europeo per i dispositivi medici (MDR 2017/745), i software medici devono essere certificati come dispostivi medici di classe IIA o superiore, salvo quelli finalizzati unicamente ad archiviare, memorizzare e trasmettere dati senza alcuna loro elaborazione, che rientrano in classe I. Per ottenere la certificazione, i dispositivi software devono rispettare i requisiti essenziali imposti dal citato regolamento, al fine di garantirne la sicurezza di utilizzo.

Obiettivo del presente lavoro è verificare l'usabilità di una cartella clinica elettronica qualificata dispositivo medico software stand-alone.

A partire dalla stima dei rischi connessi agli errori di utilizzo del prodotto in esame, ne è stata valutata l'usabilità con analisi euristica, introducendo un *nuovo approccio* che ha aggiunto, ai risultati tradizionali, l'informazione relativa a quale principio di usabilità venga violato a livello di design. Il dispositivo in oggetto presenta funzionalità inerenti attività di reparto, ambulatoriali e amministrative ed è caratterizzato da più moduli operativi, diversi per destinazione d'uso e per profilo utente. L'architettura del software varia per numero di funzioni e per tipo di interazione utente.

Per verificare la rispondenza ai requisiti essenziali è stato applicato il processo di gestione del rischio, con riferimento alla norma ISO 14971. I rischi connessi agli errori di utilizzo sono risultati dipendere in modo critico dall'usabilità; si è dunque proceduto alla sua valutazione applicando la norma 62366-1. L'usabilità dei software medicali è strettamente collegata alle caratteristiche dell'interfaccia utente: quest'ultime sono state valutate con analisi euristica, con riferimento alle note euristiche di Zhang. L'applicazione delle euristiche, sebbene stabilisca il non soddisfacimento dei requisiti di usabilità, non permette di identificare gli elementi da introdurre nel design per garantire i criteri di usabilità del software.

Come soluzione a tale mancanza di informazioni, un *nuovo approccio* si è basato sull'utilizzo di linee guida sul design di un'interfaccia software per confrontare, innanzitutto, se una funzione rispetti o meno tali linee guida e, secondariamente, quali euristiche vengano violate per ogni linea guida non rispettata.

Per condurre l'analisi è stato fatto un elenco di tutte le funzioni con destinazione medica d'uso ed è stata stabilita una scala di gravità di tipo binario da assegnare per ogni violazione, ossia impatto sui pazienti diretto/indiretto. A partire da tale scala e per i due metodi di valutazione usati, linee guida ed euristiche, i risultati relativi al numero di violazioni sono stati separati in base al livello di gravità. Infine, per stimare il livello di accettabilità dei risultati, sono stati considerati: il numero massimo di violazioni con impatto diretto sui pazienti e a quali linee guida ed euristiche corrispondesse. In generale, per entrambi i metodi di valutazione, il numero massimo di violazioni è risultato inferiore al 40% e i risultati con impatto diretto sui pazienti sono risultati sempre inferiori rispetto a quelli indiretti. In base ad essi è possibile affermare che l'usabilità del prodotto non risulta conforme ed esso deve essere sottoposto a successive misure di controllo.

In conclusione, l'efficacia del *nuovo approccio* ha fornito informazioni sufficienti a stabilire quali criteri di usabilità devono essere applicati nel design di un prodotto, da cui partire per le successive misure di controllo.

INDICE

PARTE I

Procedure di conformità di un dispositivo medico software – MDR 2017/745

PARTE II

Gestione del rischio e usabilità di una cartella clinica elettronica

I. Indice delle Figure

II. Indice delle Tabelle

Abbreviazioni

DM	Dispositivo Medico
DMSW	Dispositivo Medico Software
MDD	Medical Device Directive (Direttiva sui dispositivi medici)
MDR	Medical Device Regulation (Regolamento sui dispositivi medici)
MDCG	Medical Device Coordination Group
IEC	International Electrotechnical Commission
ISO	International Standards Organization
TR	Technical Report
IMDRF	International Medical Device Regulators Forum
UDI	Unique Device Identification
FTA	Fault Tree Analysis
FMEA	Failure Mode and Effects Analysis
AFAP	*As Far As Possible*
SOUP	Software Of Unknown Provenance
HFE	Human factor Engineering
HCI	Human Computer Interaction
AAMI	Association for the Advancement of Medical Instrumentation

Introduzione

La tesi è stata sviluppata in due parti. La prima parte è di tipo descrittivo: introduce il nuovo regolamento 2017/745 nei confronti dei dispositivi medici software, evidenziando le novità introdotte rispetto alle precedenti direttive sia nelle regole che nel processo di marcatura CE (necessario a dimostrare la conformità del prodotto al regolamento stesso) sia nelle procedure di conformità ai requisiti applicati a un dispositivo medico software.

Vengono poi descritte dettagliatamente le norme relative a due dei processi necessari a verificare la conformità di un dispositivo medico software: il processo di gestione del rischio (ISO14971) e il processo di usabilità (IEC 62366-1).

La seconda parte applica le norme sopracitate a una cartella clinica elettronica. Dopo una breve descrizione del prodotto in esame, vengono ad esso applicati i processi di gestione del rischio e dell'usabilità, introducendo un nuovo approccio per la valutazione dell'usabilità delle interfacce utente.

PARTE I

Procedure di conformità di un dispositivo medico software

MDR 2017/745

1. Processo per la marcatura CE sui dispositivi medici software ai sensi del MDR 2017/745

1.1 Introduzione

Non è una sorpresa che l'utilizzo del software nel settore sanitario sia letteralmente esploso. Ciò ha comportato la necessità di inquadrare questo sviluppo tumultuoso all'interno della vigente legislazione. E non si è trattato di una valutazione semplice.

Nonostante questo notevole sviluppo, tasso di crescita e download da rete degli utenti sembravano soffrire di un certo rallentamento. Una delle cause di tale apparente decrescita va individuata nel complesso scenario normativo che necessiterebbe di una regolamentazione organica *ad hoc*, idonea a garantire agli utenti la sicurezza e la funzionalità dei servizi informatici in un contesto particolarmente sensibile quale l'ambito medico. Il mercato, infatti, si è scontrato con alcune criticità rilevanti, che riguardano proprio il contesto normativo in cui *mApp* e *medical software* si collocano: è un contesto fortemente regolato se si pensa ai dispositivi medici, ma di difficile interpretazione se si ragiona invece esclusivamente in termini di software, nonostante le diverse linee guida emanate sia a livello nazionale che europeo.

1.1.1 Dalla Direttiva sui Dispositivi Medici MDD/47/CE

La qualificazione del software come dispositivo medico è stata introdotta dalla Direttiva 2007/47/CE (MDD), che modificava la preesistente normativa sui *medical devices* (Direttiva 93/42/CE). L'articolo 1 definisce dispositivo medico:

Qualunque strumento, apparecchio, impianto, software, sostanza o altro prodotto, utilizzato da solo o in combinazione, compresi gli accessori tra cui il software destinato dal fabbricante ad essere impiegato specificamente con finalità diagnostiche e/o terapeutiche e necessario al corretto funzionamento del dispositivo stesso. [1]

Come ogni dispositivo medico, anche il software ha dunque bisogno di essere classificato, per poter procedere alle verifiche di conformità con la Direttiva: se la classe di un software "embedded" viene attribuita alla stessa del dispositivo medico in cui è integrato, diverso è il caso di un Software *stand-alone*. A questo bisogno interviene dunque l'allegato IX, sezione 14, che fa rientrare il Software stand-alone nei dispositivi medici attivi:

Il software stand-alone è considerato un dispositivo medico attivo. [1]

Tali articoli non effettuano, peraltro, alcun criterio di distinzione tra i diversi tipi di software che possono essere utilizzati in ambito medicale, in particolare tra prodotti sviluppati per interagire con un dispositivo medico, i c.d. "software embedded" e "software stand-alone" che operando autonomamente, siano di per sé qualificabili come *medical devices*.

L'unica prescrizione esplicita è data dal punto 12.1bis dell'Allegato I, costituente un Requisito Essenziale nei confronti dei software: esso subordina la convalida del software allo stato dell'arte nel settore di riferimento, tenendo in conto i principi del ciclo di vita dello sviluppo, della gestione dei rischi, della validazione e della verifica:

Per i dispositivi che incorporano software o che sono software medici di per sé, il software deve essere convalidato secondo lo stato dell'arte tenendo conto dei principi del ciclo di vita dello sviluppo, della gestione del rischio, della convalida e della verifica. [1]

Tutte le altre prescrizioni riguardano i dispositivi medici attivi e quindi basati su un gruppo molto più ampio, variegato e sostanzialmente non finalizzato a prodotti immateriali (come è fondamentalmente un software).

L'effetto di questo approccio è stato duplice. Da un lato, i fabbricanti si sono trovati nella difficoltà materiale di capire se il proprio software fosse effettivamente inquadrabile come dispositivo medico, tanto che l'argomento è stato oggetto di una guida apposita, la *MEDDEV 2.1/6*. Dall'altro lato, il soddisfacimento dei Requisiti Essenziali imposti dalla Direttiva si è quasi interamente basato sulle prescrizioni riguardanti i dispositivi medici attivi, per larga parte impropri se applicati ad un software. Addirittura, nessuna regola di classificazione nomina i software, per cui la loro stessa classificazione si è basata su quella dei dispositivi medici attivi (Regole da 9 a 12, Allegato IX).

A cascata è disceso il problema di avere molti software inquadrati in classe I secondo la Regola 12, perché non ricadenti nelle Regole precedenti a classificazione superiore, ma poco idonei o troppo stringenti per la destinazione prevista di un software. Viceversa, il soddisfacimento dei Requisiti Essenziali, considerabile come problema successivo all'inquadramento legale, si è risolto in virtù del punto 12.1bis sulla base dell'applicazione di un sistema di gestione della qualità (basata su ISO 13485), costituente in sé una delle norme armonizzate fondamentali nell'ambito medicale. In più, si è fatto ricorso alla norma armonizzata specifica per i software basata sulla IEC 62304. Entrambe le norme hanno contribuito a bilanciare gli aspetti generali rispetto a quelli specifici, riuscendo anche a complementarsi sugli aspetti non direttamente trattati (su tutti, l'esclusione della validazione e del rilascio finale del software, anche quando costituente un dispositivo medico a se stante, dall'ambito di applicazione della norma 62304).

Più facile è stata la sorte dei software che fanno parte integrante di dispositivi medici attivi, grazie alla norma armonizzata che li riguarda, che recepisce la IEC 60601-1, oltre che al punto 12.1 dell'Allegato I. In questo caso, in virtù del punto 2.3 dell'Allegato IX, il software è classificabile direttamente in base al dispositivo medico attivo su cui opera e le prescrizioni dettagliate della 60601-1 hanno fatto tutto il resto.

1.1.2 Al Regolamento sui Dispositivi Medici (UE) 2017/745 (MDR)

Il nuovo Regolamento (UE) 2017/745 o MDR (Medical Devices Regulation) è il Regolamento Europeo sui dispositivi medici che definisce normative e vincoli che tutti i fabbricanti e distributori devono rispettare, al fine di immettere un Dispositivo Medico (DM) sul mercato Europeo.

Perché?

L'MDR nasce dalla necessità dalle richieste di adeguamento, da parte del sistema legislativo nel settore dei dispositivi medici, alle esigenze di sviluppo, al fine di ottenere un quadro regolamentare conforme ad esse e coordinare il sistema operativo del mercato interno tra gli stati membri dell'Unione Europea.

Vengono di seguito raccolti i principali obiettivi del regolamento:

- Superare i contrasti, all'interno degli Stati membri dell'Unione Europea, relativi ai sistemi legislativi
- Accrescere l'importanza del ruolo degli Organismi Notificati all'interno delle aziende
- Accrescere la sorveglianza post-mercato
- Identificare e migliorare la tracciabilità dei DM
- Far fronte all'immissione nel mercato, sempre più veloce, dei prodotti sempre più all'avanguardia con le nuove tecnologie ibride
- Affrontare la regolamentazione dei software nel settore sanitario in modo più esplicito, diretto e dettagliato.

MDR Vs MDD: Le principali novità

- Dispositivi con destinazione d'uso non medica: vengono introdotti requisiti specifici per questa categoria
- DM ad alta rischiosità: vengono rafforzate le verifiche in fase di pre-commercializzazione e i controlli di gruppi di esperti a livello europeo
- Indagini cliniche e valutazioni cliniche: vengono approfondite le regole relative ad essi
- Dispositivi medici software (DMSW) e nanomateriali: le regole di classificazione diventano più stringenti e vengono introdotte nuove regole
- DM invasivi/destinati a somministrazione: le regole diventano più rigorose e stringenti
- UDI: viene creato un sistema di codifica attraverso un codice unico di identificazione
- Ambito di applicazione dei DM: vengono approfondite le regole relative ad esso
- Sistema regolamentare dei prodotti: viene incrementato il ruolo della Commissione nei confronti dello status regolamentare
- *Reuse* di DM: viene approfondito questo argomento nel settore delle strutture sanitarie sia per la fabbricazione che per l'utilizzo
- Operatori economici: viene approfondito l'argomento con regole sulla responsabilità di queste figure e vengono dati nuovi obblighi verso la protezione di consumatori/pazienti danneggiati
- MDCG: viene istituito un nuovo Gruppo di coordinamento (MDCG)
- EUDAMED: viene istituita una banca dati specifica per i DM e resa pubblica. Viene introdotto in EUDAMED un documento di sintesi sulla sicurezza e prestazioni cliniche di DM impiantabili e DM di classe III disponibile
- Tessera sanitaria: viene creata specificatamente per i pazienti portatori di impianti, contenente tutte le informazioni relative al DM impiantato
- Vigilanza e sorveglianza nel mercato: viene marcata l'importanza di una cooperazione tra gli Stati Membri

Quando?

- 26 maggio 2017: il regolamento entra in vigore e vengono abrogate le Direttive 90/385/CEE (AIMDD) e 93/42/CEE (MDD).
- 26 maggio 2021: data di applicazione a tutti gli effetti dell'MDR 2017/745 (prorogata rispetto all'iniziale 26 maggio 2020, a causa dell'emergenza Coronavirus).
- 27 maggio 2024: perdita di validità dei Certificati MDD/AIMDD ed entrata in vigore dell'MDR 2017/745 per i DM di classe I con necessità di verifica di un Organismo Notificato.
- 27 maggio 2025: divieto di messa in mercato dei dispositivi immessi ai sensi delle MDD e AIMDD.

I principali contenuti

Il Nuovo Regolamento stabilisce un quadro normativo solido, trasparente, prevedibile e sostenibile per i dispositivi medici e garantisce un livello elevato di sicurezza e di salute, sostenendo nel contempo l'innovazione. Al fine di migliorare la salute e la sicurezza, è stato opportuno approfondire alcuni elementi chiave dell'approccio normativo avuto sino ad oggi, quali ad esempio il ruolo degli organismi notificati, le procedure di valutazione della conformità, le indagini cliniche e la valutazione clinica, la vigilanza e la sorveglianza del mercato, e introdurre nel contempo disposizioni che garantiscano la trasparenza e la tracciabilità dei dispositivi. Molti degli obblighi dei fabbricanti, come quelli relativi alla valutazione clinica o alle segnalazioni nel quadro della vigilanza, che nella precedente Direttiva erano definiti solo negli allegati, sono stati integrati nel Regolamento per facilitarne l'attuazione.

Riclassificazione dei prodotti già classificati come dispositivi medici

Le regole per definire le classi di rischio sono contenute all'Allegato VIII. La suddivisione dei dispositivi medici resta invariata in quattro classi di rischio (Classe I, IIa, IIb e III); tuttavia, alcune delle regole contenute nell'Allegato VIII sono cambiate in maniera importante, comportando quindi una possibile ri classificazione di alcuni DM(per lo più in classi di rischio superiori).

Un cambiamento importante del nuovo MDR è l'introduzione di una regola dedicata interamente alla classificazione dei dispositivi medici software: la regola 11. Nella MDD, la maggior parte del software rientrava, infatti, in Classe I; la nuova regola 11 prevede invece requisiti molto più stringenti, che comportano il passaggio di molti software a classi di rischio superiore. Ciò implica il coinvolgimento dell'organismo notificato e l'applicazione di procedure di valutazione della conformità diverse, che rappresentano un onere maggiore per i produttori di software in termini di budget e pianificazione temporale.

1.2 *Fasi del processo*

Introduzione

Il processo di marcatura CE ha il fine ultimo di certificare i dispositivi medici, permettendo la loro commercializzazione all'interno dell'Unione Europea. Tale certificazione dimostra che un dispositivo soddisfa tutti i requisiti imposti dal regolamento e ad esso applicabili.

In questo capitolo si vogliono definire i criteri per il soddisfacimento dei requisiti di un software come dispositivo medico e approfondire alcuni aspetti dell'applicazione del Regolamento (UE) 2017/745 al suddetto software. La guida MDCG 2019-11 fornisce informazioni utili per la qualifica, classificazione e immissione sul mercato dei dispositivi medici software e dei dispositivi medico-diagnostici in vitro ai sensi dell'MDR: tale guida può essere applicata sia ai software embedded, che stand-alone che alle applicazioni installate su un dispositivo mobile, nel cloud o su altre piattaforme.

Ai sensi del nuovo Regolamento, anche il processo di verifica di conformità e marcatura CE vede delle novità: viene dunque di seguito schematizzato il modello a blocchi (Figura 1.1), con le procedure che devono essere seguite sequenzialmente a un qualsiasi software qualificato come dispositivo medico ai fini di poter dimostrare la completa conformità ai vigenti regolamenti e apporre il marchio CE, evidenziando le novità introdotte dal MDR.

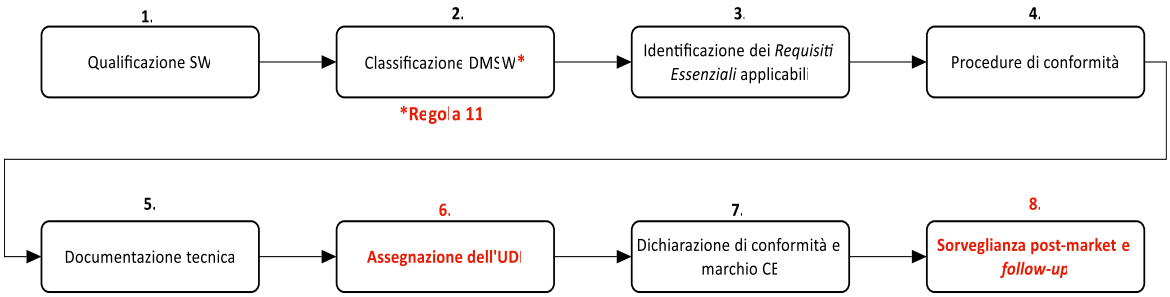


Figura 1.1. Modello a blocchi – Iter procedurale della Marcatura CE sui MDSW ai sensi del MDR

I prossimi paragrafi del presente capitolo saranno dedicati a un'analisi dettagliata della procedure sovra elencate, limitandosi al caso specifico dei Software come dispositivi medici per quanto riguarda i prime quattro steps; al contrario, dallo step 5 in poi le considerazioni valgono per qualsiasi dispositivo medico.

1.3 *Qualificazione*

*Qualunque strumento, apparecchio, apparecchiatura, **software**, impianto, reagente, materiale o altro articolo, destinato dal fabbricante a essere impiegato sull'uomo, **da solo o in combinazione**, per una o più delle seguenti destinazioni d'uso mediche specifiche:*

- *diagnosi, prevenzione, monitoraggio, previsione, prognosi, trattamento o attenuazione di malattie,*
- *diagnosi, monitoraggio, trattamento, attenuazione o compensazione di una lesione o di una disabilità,*

- *studio, sostituzione o modifica dell'anatomia oppure di un processo o stato fisiologico o patologico,*
- *fornire informazioni attraverso l'esame in vitro di campioni provenienti dal corpo umano, inclusi sangue e tessuti donati, e che non esercita nel o sul corpo umano l'azione principale cui è destinato mediante mezzi farmacologici, immunologici o metabolici, ma la cui funzione può essere coadiuvata da tali mezzi.*

Si considerano dispositivi medici anche i seguenti prodotti:

- *dispositivi per il controllo del concepimento o il supporto al concepimento,*
- *i prodotti specificamente destinati alla pulizia, disinfezione o sterilizzazione dei dispositivi di cui all'articolo 1, paragrafo 4, e di quelli di cui al primo comma del presente punto.*

(Art. 2, [2])

1.3.1 Riferimenti normativi

- **MDCG 2019-11:** ***Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR***

La linea guida MDCG 2019-11 ha lo scopo principale di guidare il fabbricante a comprendere *come* applicare il nuovo Regolamento nel caso specifico dei dispositivi medici software.

Il software deve avere uno scopo medico di per sé per essere qualificato come software per dispositivi medici (DMSW). Va notato che lo scopo previsto come descritto dal produttore del software è rilevante per la qualificazione e la classificazione di qualsiasi dispositivo.

Per essere qualificato come software per dispositivi medici, il prodotto deve prima soddisfare la definizione di software secondo questa guida e la definizione di dispositivo medico secondo l'articolo 2 del regolamento (UE) 2017/745 – MDR.

Il software per dispositivi medici è un software destinato a essere utilizzato, da solo o in combinazione, per uno scopo specificato nella definizione di "dispositivo medico" nell'MDR o nell'IVDR, indipendentemente dal fatto che il software sia indipendente o che guidi o influenzi il uso di un dispositivo. [3]

Passi decisionali per la qualificazione del software come DMSW
Vengono di seguito riportati i passi decisionali descritti dalla guida per una corretta qualificazione di un DMSW:

Fase 1: se il prodotto è un software ai sensi della Sezione 2 (Definizioni e abbreviazioni) di questa guida, potrebbe trattarsi di un software per dispositivi medici: passare alla fase 2 della decisione; se il prodotto non è un software secondo la definizione di questa guida, allora non è coperto da questa guida ma potrebbe essere comunque coperto dalle normative sui dispositivi medici.

Fase 2: se il prodotto è un dispositivo MDR dell'allegato XVI, o è un accessorio di un dispositivo medico, o è un software che guida o influenza l'uso di un dispositivo medico, allora deve essere

considerato parte di quel dispositivo nel suo processo normativo o indipendentemente se è un accessorio. In caso contrario, procedere al passaggio 3 della decisione.

Fase 3: se il software esegue un'azione sui dati, o esegue un'azione oltre la memorizzazione, l'archiviazione, la comunicazione, la ricerca semplice, la compressione senza perdita di dati (cioè utilizzando una procedura di compressione che consente la ricostruzione esatta dei dati originali) allora potrebbe essere un software per dispositivi medici procedere al passaggio 4.

Fase 4: l'azione va a beneficio dei singoli pazienti? Esempi di software che non sono considerati a beneficio dei singoli pazienti sono quelli destinati esclusivamente ad aggregare dati di popolazione, fornire percorsi diagnostici o terapeutici generici (non rivolti ai singoli pazienti), letteratura scientifica, atlanti medici, modelli e template come nonché software destinati esclusivamente a studi o registri epidemiologici.

Fase 5: il software per dispositivi medici (DMSW) è conforme alla definizione di questa guida?

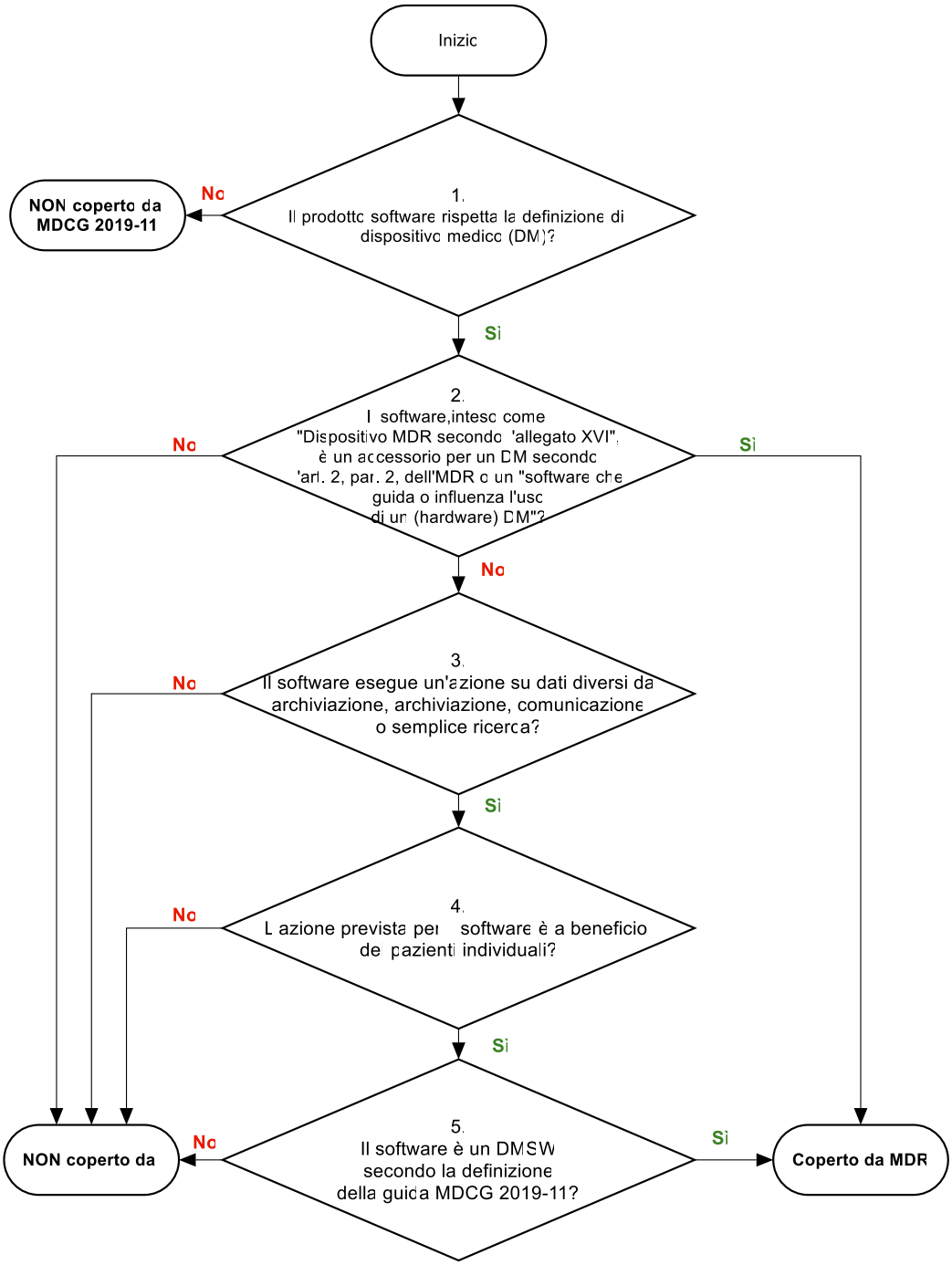
- ***Manual on borderline and classification in the Community Regulatory Framework for medical devices***

  Si definisce dispositivo *borderline* un generico prodotto che per natura non è facilmente riconducibile ad un determinato settore: è dunque difficile definire sotto quale normativa rientri. Nel campo dei dispositivi medici, è stato istituito un gruppo di lavoro *Borderline and Classification medical devices expert group*, presso la Commissione Europea, specifico per la qualificazione di dispositivi borderline: all'interno di tale gruppo partecipano non solo esperti, ma anche le autorità rappresentanti delle aziende.

  Lo scopo del manuale è quello di inserire i prodotti borderline all'interno del corretto contesto legislativo di riferimento, così da assicurare un coordinamento in questo settore tra i paesi dell'Unione Europea.

  Il gruppo, nell'ambito del proprio mandato, ha redatto un manuale, *Manual on borderline and classification in the Community Regulatory Framework for medical devices*, che viene aggiornato periodicamente sulla base dei consensi raggiunti. Pur non avendo forza di legge, rappresenta il punto di vista del gruppo di lavoro e come tale costituisce un utile strumento a disposizione delle Autorità Competenti per le decisioni su prodotti borderline.

Viene riportato il Flowchart 1.1 presente nella guida stessa per determinare se un Software sia qualificabile o meno come dispositivo medico ai sensi del Regolamento 2017/745.



Flowchart 1.1 Qualificazione di un DMSW

1.4 Classificazione

Ogni dispositivo che venga qualificato come dispositivo medico deve essere necessariamente classificato dal fabbricante in una delle classi di rischio stabilite dal regolamento, al fine di attuare le procedure di valutazione della conformità previste specifiche per ciascuna classe.

La classificazione dei software è effettuata conformemente alle regole di applicazione e alle regole di classificazione elencate nell'Allegato VIII del regolamento (UE) 2017/745. I software sono quindi suddivisi nelle classi I, IIa, IIb e III in funzione delle destinazioni d'uso previste e dei rischi che comportano. Tutte le regole di applicazione dell'allegato VIII devono essere considerate, ma quelle di maggiore interesse per l'identificazione della corretta classe di rischio di un software sono le seguenti:

3.3 Il software destinato a far funzionare un dispositivo o a influenzarne l'uso rientra nella stessa classe del dispositivo. Se il software non è connesso con nessun altro dispositivo, è classificato separatamente.
3.5 Se diverse regole o, nell'ambito della stessa regola, più sotto-regole si applicano allo stesso dispositivo in base alla sua destinazione d'uso, si applicano la regola e sotto-regola più rigorose che comportano la classificazione più elevata.

3.7 Si ritiene che un dispositivo consenta una diagnosi diretta quando fornisce esso stesso la diagnosi della malattia o della condizione clinica in questione o quando fornisce informazioni decisive per la diagnosi. [2]

Dalle regole di applicazione emerge che, se un software guida o influenza un altro dispositivo medico e ha anche uno scopo di per sé, allora è la sua destinazione d'uso a determinare la classe in cui rientra, purché la classe di rischio non sia inferiore della classe di rischio del dispositivo guidato o influenzato.

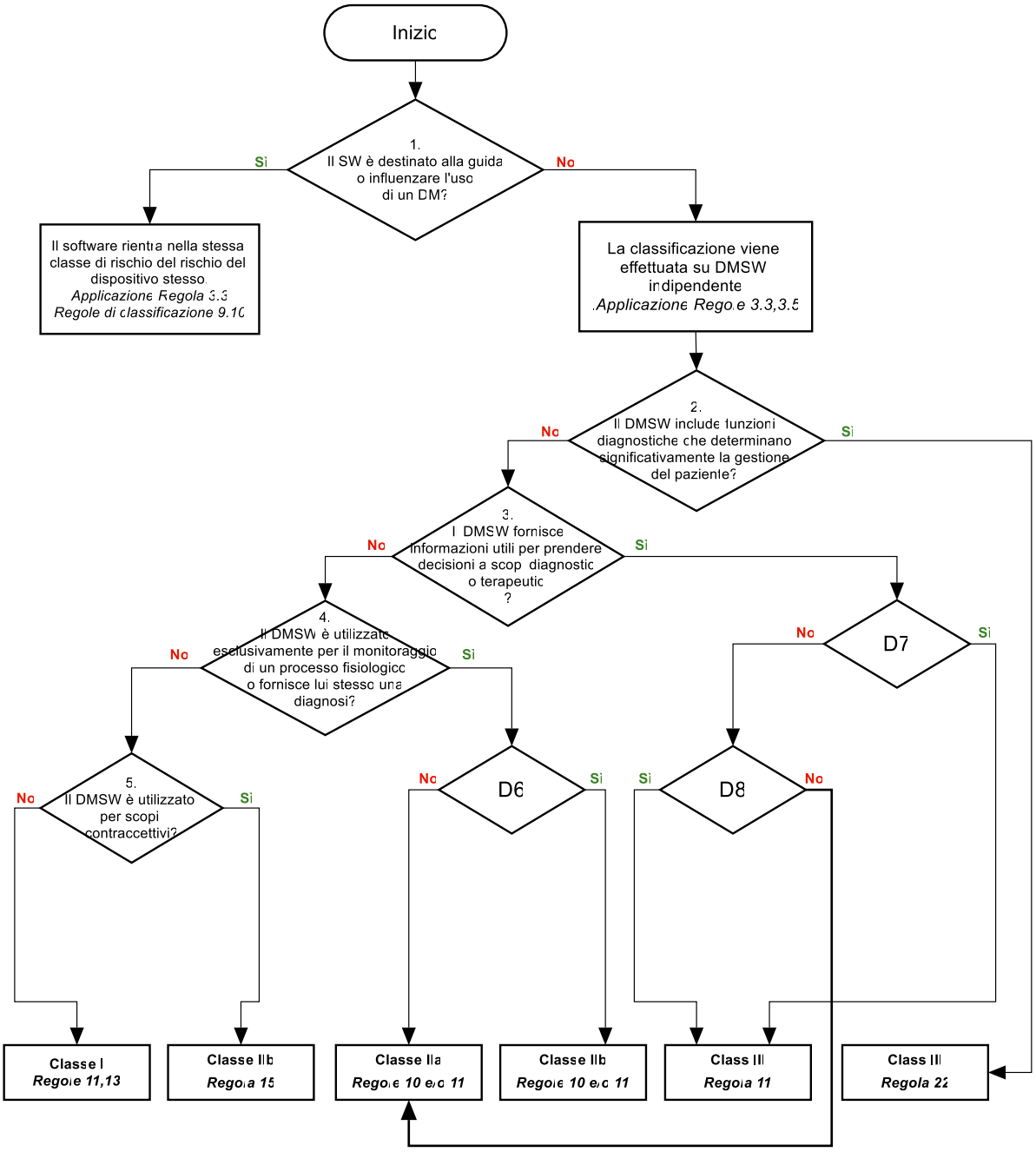
Per ciò che concerne invece le regole di classificazione, in generale dipendono dai seguenti fattori:

- Durata di contatto del DM con il paziente. La durata può essere temporanea, breve termine o lungo termine.
- Invasività del DM. Il livello di invasività si distingue in: DM non invasivo, invasivo negli orifizi del corpo, invasivo chirurgico, impiantabile
- Tipo di funzionamento operativo: un DM può essere considerato non attivo, attivo terapeutico o attivo diagnostico
- Sede anatomica del paziente in cui è previsto l'uso del DM. La distinzione della sede viene fatta su due livelli: sistema circolatorio centrale SCC e sistema nervoso centrale SNC

Nel caso specifico dei software come dispositivi medici, si considerano in primo luogo quelle riferite ai dispositivi medici attivi in quanto in base all'articolo 2 del MDR (UE) 2017/745, il software è considerato rientrante in tale categoria di dispositivi.

Le regole di classificazione applicabili ai software sono riportate di seguito, fornendo anche degli esempi di software a cui possono essere applicate. Nonostante ciò, si consideri che la classificazione finale dei software presi come esempio potrebbe essere diversa nel caso in cui allo stesso software risultassero applicabili anche altre regole, in accordo con la regola di implementazione 3.5.

Sulla base delle regole di applicazione e di classificazione è proposto il Flowchart 1.2 per facilitare l'identificazione della classe di rischio di un dispositivo medico software. I vari step decisionali sono stati identificati in modo tale che i software che hanno più destinazioni d'uso e per i quali sarebbe quindi possibile applicare più regole di classificazione siano associati alla classe di rischio più alta, in accordo con la regola di applicazione 3.5.



D6: Monitora parametri fisiologici vitali e la natura delle variazioni di detti parametri può creare un pericolo immediato per il paziente (Regole 10 e 11) o effettua diagnosi in situazioni cliniche in cui il paziente si trova in pericolo immediato (Regola 10)?

D7: Le decisioni prese hanno effetti tali da poter causare il decesso o il deterioramento irreversibile delle condizioni di salute di una persona (Regola 11)?

D8: Le decisioni prese hanno effetti tali da poter causare un grave deterioramento delle condizioni di salute di una persona o un intervento chirurgico (Regola 11) o sono effettuate in situazioni cliniche in cui il paziente si trovi in pericolo immediato (Regola 10)?

Flowchart 1.2 Classificazione di un DMSW

Vengono di seguito riportati degli esempi di DM classificati diversamente in base alle regole di classificazione di appartenenza; rispetto alla regola 11, insieme agli esempi viene riportata la citazione stessa del MDR.

- Regola 9:

  Esempio: il software facente parte di un sistema di ventilazione respiratoria ambulatoriale destinato ad un uso a lungo termine (e.g. a casa) che segnala all'operatore qualsiasi disconnessione o deviazione dal volume respiratorio programmato deve essere classificato nella classe IIb.

- Regola 10:

  Esempio: i dispositivi attivi, quali i termometri e gli stetoscopi elettronici, che comprendono un software destinato alla diagnosi diretta, possono essere classificati nella classe IIa poiché la temperatura corporea e la frequenza cardiaca sono considerate informazioni decisive ai fini della diagnosi (regola di implementazione 3.7), qualora la natura delle variazioni di tali parametri non può provocare un pericolo immediato per il paziente.

- **Regola 11:**

  *I software destinati a **fornire informazioni utilizzate per prendere decisioni a fini diagnostici o terapeutici rientra nella classe IIa**, a meno che tali decisioni abbiano effetti tali da poter causare:*

  — il decesso o un deterioramento irreversibile delle condizioni di salute di una persona, nel qual caso rientra nella classe III, o

  — un grave deterioramento delle condizioni di salute di una persona o un intervento chirurgico, nel qual caso rientra nella classe IIb.

  Il software destinato a monitorare i processi fisiologici rientra nella classe IIa, a meno che sia destinato a monitorare i parametri fisiologici vitali, ove la natura delle variazioni di detti parametri sia tale da poter creare un pericolo immediato per il paziente, nel qual caso rientra nella classe IIb. Tutti gli altri software rientrano in classe I. [2]

  Un DMSW, nella maggior parte dei casi, non è correlato in modo diretto ai rischi; è connesso invece alle conseguenze del danno indiretto, derivante dalla mancanza di informazioni corrette fornite dal dispositivo.

  Pertanto, in linea con il considerando 5 del regolamento sui dispositivi medici e la guida internazionale dell'IMDRF (International Medical Device Regulators Forum), la regola 11 è stata introdotta nell'MDR ed è intesa ad affrontare i rischi relativi alle informazioni fornite da un dispositivo attivo, come DMSW. La Regola 11, in particolare, descrive e classifica il significato delle informazioni fornite dal dispositivo attivo per la decisione sanitaria (gestione del paziente) in combinazione con la situazione sanitaria (condizione del paziente).

  Il testo della Regola 11 può essere suddiviso in quelle che sono essenzialmente tre sotto regole, che vengono applicate a seconda dell'uso/scopo previsto del DMSW:

- 11a: (3 commi primi della Regola 11) destinati a fornire informazioni utili al supporto di decisioni con finalità diagnostiche o terapeutiche;
- 11b: (comma 4 della Regola 11) destinati a monitorare processi o parametri fisiologici;
- 11c: (comma 5 della regola 11) tutti gli altri usi.

La regola 11 è stata introdotta anche per rispecchiare le linee guida regolamentari sviluppate a livello internazionale e in particolare nel contesto dell'International Medical Device Regulators Forum (IMDRF). Il framework IMDRF per la categorizzazione del rischio del software come dispositivo medico (SaMD) ("IMDRF Risk Framework") classifica il rischio del software in base alla combinazione del significato delle informazioni fornite dal software per la decisione sanitaria e la situazione sanitaria o condizione del paziente.

IMDRF ha anche sviluppato una tabella per assistere gli operatori nell'identificazione della categoria di rischio appropriata per il proprio prodotto.

Tale tabella (Tabella 1) potrebbe fornire agli operatori che immettono DMSW sul mercato UE alcune utili indicazioni sulla classe di rischio applicabile ai loro prodotti a seguito dell'applicazione della Regola 11 del MDR.

Tabella 1. Guida di classificazione di un DMSW secondo la regola 11 del MDR

		Significance of Information provided by the MDSW to a healthcare situation related to diagnosis/therapy		
State of Healthcare situation or patient condition		**High** Treat or diagnose *~ IMDRF 5.1.1*	**Medium** Drives clinical management *~ IMDRF 5.1.2*	**Low** Informs clinical management *(everything else)*
	Critical situation or patient condition *~ IMDRF 5.2.1*	**Class III** *Category IV.i*	**Class IIb** *Category III.i*	**Class IIa** *Category II.i*
	Serious situation or patient condition *~ IMDRF 5.2.2*	**Class IIb** *Category III.ii*	**Class IIa** *Category II.ii*	**Class IIa** *Category I.ii*
	Non-serious situation or patient condition *(everything else)*	**Class IIa** *Category II.iii*	**Class IIa** *Category I.iii*	**Class IIa** *Category I.i*

Esempio 1: un DMSW destinato ad eseguire la diagnosi mediante analisi delle immagini per decidere il trattamento in pazienti con ictus acuto deve essere classificato nella classe III ai sensi del primo paragrafo.

Esempio 2: Un'applicazione mobile destinata ad analizzare il battito cardiaco di un utente, rilevare anomalie e di conseguenza informare un medico dovrebbe essere classificato come classe IIb per il primo paragrafo se le informazioni fornite dal software sono utilizzate per guidare il medico nella diagnosi.

Esempio 3: i DMSW destinati ad essere utilizzati per la sorveglianza continua dei processi fisiologici vitali in anestesia, terapia intensiva o in emergenza devono essere classificati nella classe IIb ai sensi del secondo paragrafo. Al contrario, i DMSW destinati a monitorare i processi fisiologici che non sono considerati vitali, e quelli destinati ad essere utilizzati per ottenere letture di segnali fisiologici vitali nei controlli di routine, compreso il monitoraggio a domicilio, dovrebbero essere classificati nella classe IIa ai sensi dello stesso paragrafo.

- Regola 13:

  Esempio: DMSW destinato a sostenere il concepimento calcolando lo stato di fertilità dell'utente sulla base di un algoritmo statistico convalidato. Tale software prevede che l'utente immetta i dati sul suo stato di salute, quali la temperatura corporea basale e i giorni mestruali per monitorare e prevedere l'ovulazione.

  […] Oltre alle regole di classificazione specifiche per i dispositivi attivi, anche alcune delle regole speciali sono applicabili. In particolare:

- Regola 15:

  Esempio: DMSW destinato ad evitare il concepimento sulla base di dati immessi dall'utente sul suo stato di salute, quali la temperatura corporea basale e i giorni mestruali.

- Regola 22:

  Esempio: software che include una funzione diagnostica, sulla base della quale il software adatta il trattamento della depressione, è classificato nella classe III per tale regola.

1.5 Identificazione dei requisiti essenziali applicabili

Al fine di poter apporre la marcatura CE, di fondamentale importanza è la corretta identificazione dei requisiti essenziali: essi devono essere infatti soddisfatti per assicurare la conformità del proprio software al Regolamento.

I suddetti requisiti prescrivono che il software debba garantire prestazioni in linea con la destinazione d'uso, essere sicuro, efficace e conforme allo stato dell'arte, oltre che compatibile e interoperabile con i dispositivi con cui viene utilizzato. Il software deve inoltre essere sviluppato e fabbricato tenendo conto dei principi del ciclo di vita dello sviluppo, della gestione del rischio, della verifica e della convalida.

Aspetto fondamentale è la necessità di implementare un sistema di gestione del rischio che abbia lo scopo di minimizzare i rischi noti e prevedibili che si possono verificare durante l'uso previsto e durante l'uso scorretto. In particolare, bisogna porre attenzione ai rischi associati alle caratteristiche ergonomiche del software, così come considerare la capacità, istruzione, esperienza e condizione medica dei diversi utilizzatori, oltre che valutare le informazioni derivanti dalla sorveglianza post-commercializzazione.

Lo stesso sistema di gestione del rischio deve considerare gli aspetti legati alla cyber-sicurezza, allo scopo di garantire la confidenzialità delle informazioni a riposo, in uso e in movimento, l'autenticità e l'accuratezza dei dati e la disponibilità dei sistemi connessi e di ridurre i rischi legati alla probabilità che il software interagisca negativamente con l'ambiente tecnologico in cui opera e in cui si interconnette. Gli aspetti legati alla cyber-sicurezza devono essere valutati durante tutto il processo di vita del software, dalla progettazione alle attività di post-commercializzazione, tenendo anche in considerazione l'ambiente tecnologico in cui il software lavora.

I fabbricanti devono infatti indicare i requisiti minimi a livello hardware, le misure della sicurezza informatica, inclusa la protezione contro accessi non autorizzati, e le caratteristiche delle reti informatiche IT: tutti questi aspetti sono necessari a far funzionare il software secondo la sua destinazione d'uso.

In ultimo, i requisiti prescrivono che i fabbricanti devono fornire tutte le informazioni legate alla sicurezza e alla prestazione del proprio dispositivo, oltre che alla sua identificazione e comprensione per un corretto utilizzo, e.g. le precauzioni da adottare, le contro-indicazioni, effetti collaterali, i rischi residui e le avvertenze.

1.5.1 Rispondenza ai requisiti

Rispondere ai requisiti essenziali del MDR significa dimostrare la sicurezza del DM prodotto, e per dimostrare ciò è obbligatorio applicare il processo di gestione del rischio e le procedure dettate dalle norme ad esso correlate a qualsiasi DM. Ogni procedura deve essere tracciata e quindi documentata in un fascicolo tecnico; in base alla classe di rischio del DM, a tale documentazione si deve aggiungere anche l'attestazione di conformità.

Tra le procedure gestionali, le principali sono le seguenti:

- Procedura di qualità (la norma di riferimento è la ISO 13485): guida il fabbricante durante il design e lo sviluppo del DM
- Procedura gestionale che per la sorveglianza del mercato, il piano di azioni correttive e di rintracciabilità
- Procedura per la rintracciabilità e segnalazioni di incidenti

La norma tecnica armonizzata ISO 14971 guida il fabbricante nel condurre correttamente e in modo completo il processo di gestione del rischio.

Viene di seguito riportato un diagramma a blocchi in cui vengono riassunti gli strumenti necessari affinché un DM possa essere considerato conforme ai requisiti essenziali (Figura 1.2)

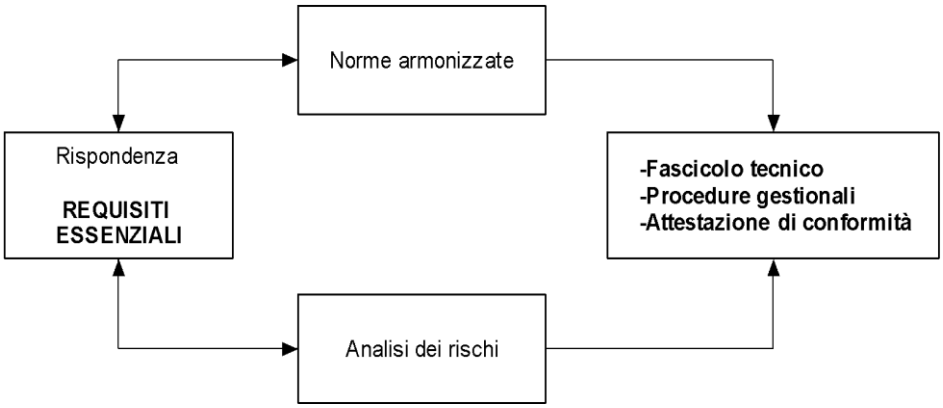


Figura 1.2. Diagramma a blocchi: Rispondenza ai requisiti

1.6 Procedure di conformità

Per verificare la conformità ai requisiti essenziali di un DM, vengono applicate le procedure di conformità ai requisiti stessi: esse variano di complessità a seconda della classe di rischio in cui cade il DM, aumentando all'aumentare di quest'ultima.

Nella Figura 1.3 di seguito riportata, sono riassunte le procedure per la valutazione di conformità adottabili per ciascuna classe di rischio. Fondamentale è che ogni valutazione della conformità sia preceduta dalla stesura della documentazione tecnica e seguita dalla redazione della dichiarazione di conformità in accordo con l'allegato IV, oltre che dalla marcatura del dispositivo con il marchio CE di cui allegato V.

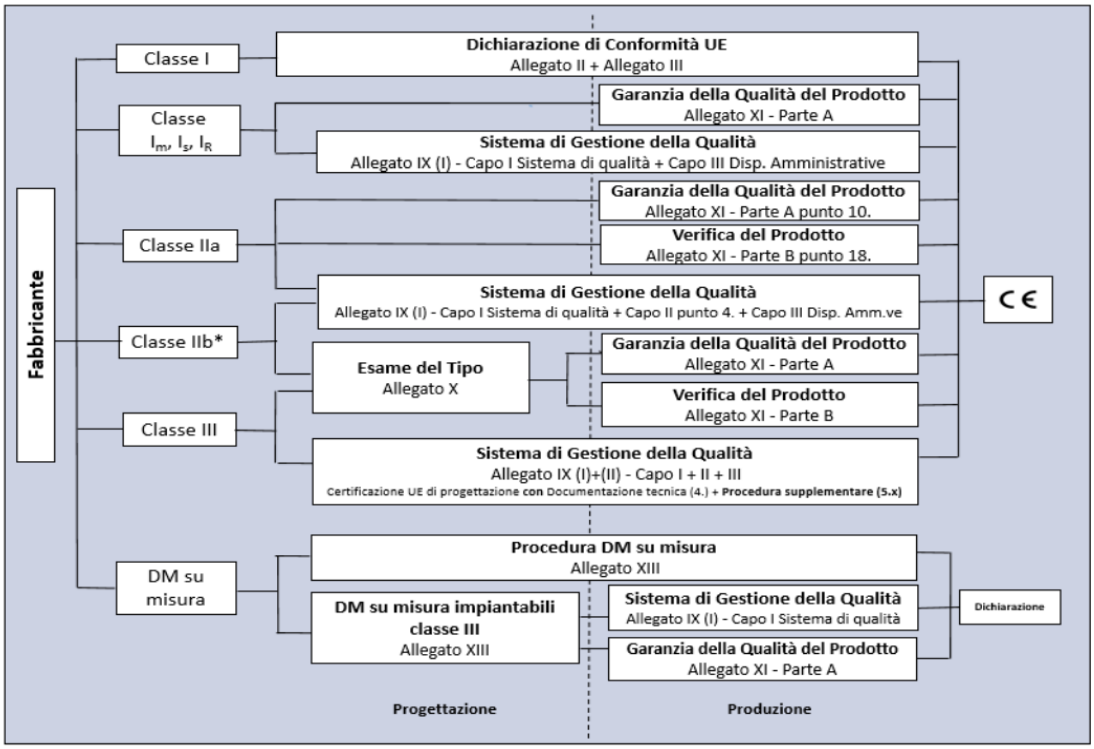


Figura 1.3. Procedure di valutazione di Conformità di un DM

1.7 Documentazione tecnica

Al termine delle procedure di conformità di un DMSW, i risultati vengono raccolti in un fascicolo tecnico. Di seguito vengono elencati i contenuti minimi che deve avere qualsiasi fascicolo tecnico di un dispositivo medico, citati dal Ministero della Salute nel documento relativo agli *Aspetti regolatori e operativi* dei Dispositivi Medici: [4]

STRUTTURA MINIMA DI UN FASCICOLO TECNICO

1. Descrizione del prodotto
2. Schemi di progettazione e metodi di fabbricazione
3. Risultati dell'analisi del rischio
4. Norme tecniche applicate
5. Tabella di rispondenza ai requisiti essenziali
6. Relazioni di prova e, ove necessario, i dati clinici di cui all'Allegato X del MDR 2017/745
7. Progetto di etichettatura ed, eventualmente, di istruzioni d'uso

1.8 Attribuzione e apposizione dell'UDI

Lo UDI, *Unique Device Identification*, è un sistema di codifica per identificare in maniera univoca tutti i dispositivi medici e diagnostici in vitro in Europa, Stati Uniti e altri paesi: si tratta di un codice alfanumerico.
L'attribuzione e l'apposizione dell'UDI ad un software medicale deve essere effettuata conformemente all'articolo 6.5 dell'allegato VI del MDR.

1.9 Dichiarazione di conformità e Marchio CE

Dichiarazione di conformità

La dichiarazione di conformità è il documento con il quale un fabbricante garantisce e dichiara che il proprio DM è conforme al Regolamento.
Le informazioni da riportare sulla dichiarazione di conformità sono indicate all'interno della norma tecnica 45014. Inoltre, sulla *Guida all'attuazione delle direttive fondate sul nuovo approccio e sull'approccio globale,* sono riportate le seguenti informazioni minime che la dichiarazione di conformità dovrebbe fornire:

- Dati identificativi del fabbricante o dell'organismo notificato (nel caso di DM a classe superiore alla I);
- Caratteristiche identificative del DM: nome e informazioni legate al modello
- Requisiti che sono stati considerati e i risultati relativi al loro soddisfacimento; Tutte le disposizioni del caso che sono state soddisfatte;
- Riferimenti normativi applicati;
- Informazioni supplementari come classe e categoria;
- Data di rilascio della dichiarazione;
- Firma dell'ente notificato o marchio equivalente;
- Dichiarazione del fabbricante e dell'ente notificato in cui attestino la responsabilità dei processi avvenuti;
- Dati identificativi del responsabile della gestione documentale.

Certificato CE

Il certificato CE è un documento redatto da un soggetto di terza parte, l'ente notificato, con il quale viene attestato di aver svolto un processo di valutazione e di essere conformi al Regolamento di riferimento.

Marcatura CE

Indipendentemente dalla classe di rischio del DMSW e dunque delle procedure che sono state svolte per dichiarare la conformità al MDR, il simbolo associato a tale certificato è il marchio CE (Figura 1.4).

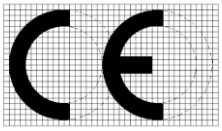


Figura 1.4. Marchio CE

1.10 Post-commercializzazione

Una delle variazioni più significative del Regolamento rispetto alla Direttiva è il rafforzamento del sistema di vigilanza e sorveglianza post-commercializzazione. Inoltre, il Regolamento prevede un aumento delle responsabilità dei fabbricanti nell'assicurare la conformità del dispositivo ai requisiti di sicurezza e prestazione dopo l'immissione in commercio e la messa in servizio dello stesso. Le prescrizioni relative al sistema di vigilanza, al sistema di sorveglianza post-commercializzazione e quelle relative alla sorveglianza del mercato sono descritte nel *capo VII – Sorveglianza post-commercializzazione, vigilanza e sorveglianza di mercato* del Regolamento e, a decorrere dalla data di applicazione dell'MDR, dovranno essere applicate anche ai dispositivi immessi sul mercato ai sensi della direttiva 93/42/CEE.

1.10.1 Sorveglianza post-commercializzazione

La sorveglianza post-commercializzazione, descritta nella sezione 1 del capo III, riguarda:

Tutte le attività svolte dal fabbricante in collaborazione con altri operatori economici volte a istituire e tenere aggiornata una procedura sistematica per raccogliere e analizzare in modo proattivo l'esperienza acquisita sui dispositivi che immettono sul mercato, che mettono a disposizione sul mercato o che mettono in servizio, al fine di identificare eventuali necessità di procedere immediatamente a eventuali azioni correttive o preventive. (art. 2, [2]).

La sorveglianza post-commercializzazione deve essere svolta sulla base di un piano i cui requisiti sono descritti nell'allegato III dell'MDR. Tale piano riguarda la raccolta e l'utilizzo delle informazioni disponibili dopo la messa in commercio e comprende, tra le altre cose, i metodi e i processi per raccogliere ed analizzare le suddette informazioni, gli indicatori da utilizzare nel riesame dell'analisi dei rischi e dei benefici, le procedure per individuare ed avviare le azioni correttive, i protocolli per comunicare con le autorità competenti e il piano di follow-up clinico post-commercializzazione (PMCF). Di conseguenza, le informazioni che vengono raccolte sono utilizzate ad esempio per aggiornare la valutazione dei rischi e dei benefici, aggiornare la valutazione clinica, identificare le azioni preventive e correttive necessarie, aggiornare le istruzioni per l'uso o migliorare l'usabilità.

Le comunicazioni previste dal sistema di sorveglianza sono proporzionate alla classe di rischio e alla tipologia di dispositivo: per i dispositivi di classe I deve essere stilato un rapporto sulla sorveglianza post-commercializzazione solo ove necessario e messo a disposizione delle autorità competenti su richiesta; al contrario, per i dispositivi di classe IIa, IIb e III deve essere stilato un rapporto periodico di aggiornamento sulla sicurezza (PSUR) che deve essere messo a disposizione delle autorità competenti tramite il sistema elettronico. Entrambi i rapporti fanno parte della documentazione tecnica di cui agli allegati II e III e sintetizzano i risultati e le conclusioni dell'analisi dei dati raccolti. Inoltre, il rapporto periodico di aggiornamento della sicurezza indica anche le conclusioni da utilizzare nella valutazione dei rischi e dei benefici, i risultati del PMCF e le stime sulle vendite e sull'utilizzo del dispositivo.

1.10.2 Vigilanza post-commercializzazione

La vigilanza viene invece trattata nella sezione 2 del capo III.

Essa riguarda da una parte l'identificazione e la segnalazione di incidenti gravi e dall'altra l'adozione di azioni correttive di sicurezza. Il sistema richiede che il fabbricante segnali alle autorità competenti gli incidenti gravi in maniera tanto più tempestiva quanto più è alta la serietà dell'incidente (2 giorni dalla venuta a conoscenza in caso di grave minaccia per la salute pubblica, 10 in caso di decesso o grave deterioramento delle condizioni di salute, altrimenti 15 giorni) e provveda a svolgere le indagini necessarie per mettere eventualmente in atto le azioni correttive necessarie per garantire la salute e la sicurezza.

Il sistema di vigilanza richiede la cooperazione diretta ed efficace tra le istituzioni, gli operatori sanitari, i fabbricanti, gli organismi notificati e le autorità nazionali competenti per i dispositivi medici. In particolare, le autorità competenti informano i fabbricanti degli incidenti gravi di cui ricevono notizia, assicurano il monitoraggio delle indagini e valutano i rischi derivanti dagli incidenti e le eventuali azioni correttive messe in atto.

Sia il sistema di vigilanza che quello di sorveglianza post-commercializzazione sono supportati da uno stesso sistema elettronico. Questo raccoglie ad esempio le segnalazioni dei fabbricanti relative agli incidenti gravi e alle azioni correttive intraprese, i PSUR, le relazioni dei fabbricanti sulle tendenze, le informazioni scambiate tra le autorità competenti e i link alla banca dati UDI.

1.10.3 Sorveglianza del mercato

In ultimo, la *sezione* 3 del capo III descrive l'attività di sorveglianza del mercato.

Questa, compito delle autorità competenti, si basa su prestabiliti piani di sorveglianza annuali attuati al fine di garantire che tutti i dispositivi non sicuri vengano ritirati dal mercato. In particolare, la sorveglianza prevede ispezioni dei locali degli operatori economici eventualmente senza preavviso, la verifica della documentazione e verifiche fisiche o di laboratorio, oltre che l'utilizzo di determinate procedure nel caso venisse riscontrata la presenza di un rischio inaccettabile per la salute e la sicurezza dei pazienti o altre non conformità.

Così come il sistema di vigilanza e quello di sorveglianza post-commercializzazione anche il sistema di sorveglianza del mercato è supportato da un sistema elettronico per la raccolta e il trattamento di tutte le informazioni, quali ad esempio la sintesi dei risultati dell'attività di sorveglianza, i rapporti di ispezione, le non conformità riscontrate e le informazioni relative ai dispositivi che presentano rischi inaccettabili per la salute e la sicurezza.

2. Ciclo di vita e Gestione del rischio di dispositivi medici software

I fabbricanti stabiliscono, implementano, documentano e mantengono un sistema di gestione del rischio. La gestione del rischio è intesa come un processo iterativo continuo durante l'intero ciclo di vita di un dispositivo, che richiede un costante e sistematico aggiornamento.

(Allegato I, art. 3 [2])

Introduzione

Le complessità dei rischi della sicurezza informatica crescono con l'avanzamento della tecnologia.

I fabbricanti di dispositivi sono chiamati a intraprendere una valutazione della sicurezza informatica, per identificare e dare priorità alle aree in cui si è reso evidente un miglioramento.

Si deve includere la sicurezza del ciclo di vita del prodotto, prevista in schemi di valutazione dei rischi e di controllo.

Di fronte a tale obiettivi e al requisito generale del nuovo MDR, con cui è stato introdotto il presente capitolo, vengono di seguito elencate le principali norme armonizzate, atte a definire i metodi con cui raggiungere tali obiettivi:

- IEC 62304:2006 + A1:2015, *Medical Device Software – Software lifecycle processes,* [5]
- ISO 14971:2019, *Medical devices — Application of risk management to medical devices.*[6]

In riferimento a quest'ultima, è stato sviluppato un report tecnico per guidare il fabbricante nel caso specifico in cui il dispositivo medico in questione sia di tipo software:

  - TR 80002 - 1, *Guidance on the application of ISO 14971 to medical device software.* [7]

2.1 Processo del ciclo di vita

Il processo del ciclo di vita dei dispositivi medici software include diversi requisiti di sicurezza. Lo standard IEC 62304 descrive una strategia di prove per soddisfare tali requisiti: analisi dei requisiti del software, piano di sviluppo, implementazione e verifica, gestione dei rischi, integrazione e test, rilascio e manutenzione del software.

2.1.1 Riferimenti normativi: IEC 62304

Introduzione

La norma fornisce un framework per i processi del ciclo di vita di un dispositivo medico software, definendo in particolare le *activities*[1] e i *tasks*[2] necessari per le attività di sviluppo e manutenzione di un software altamente affidabile e *safe*[3].

Tale software può essere sia integrato o parte di un dispositivo medico, sia un dispositivo a sé stante. La suddetta norma si basa sul presupposto che sia implementato un sistema di qualità, certificato o meno, e un sistema di gestione del rischio conformemente alla norma ISO 14971: *Medical Devices – Application of risk management to medical devices*.

In aggiunta a questi due processi, nella norma vengono definiti altri processi considerati essenziali per l'ottenimento di un software *safe*, ovvero il processo di sviluppo, manutenzione, configurazione e quello di risoluzione dei problemi, di seguito analizzati.

Definizioni ricorrenti [5]

Termine	Descrizione
Modello software (del ciclo di vita di sviluppo)	Struttura concettuale che abbraccia la vita del software dalla definizione dei suoi requisiti al suo rilascio, che: ha identificato il processo, le attività e i compiti coinvolti nello sviluppo del software per dispositivi medici; descrive la sequenza e la dipendenza tra attività e compiti, e identifica le pietre miliari in corrispondenza delle quali viene verificata la completezza dei risultati finali specificati.
Sistema software	Raccolta integrata di elementi software organizzati per svolgere una specifica funzione o insieme di funzioni.
Elemento software	Qualsiasi parte identificabile di un programma per computer, ad esempio codice sorgente, codice oggetto, codice di controllo, dati di controllo o una raccolta di questi elementi.
Unità software	Articolo software non suddiviso in altri articoli.
SOUP	Software di provenienza sconosciuta: Articolo software già sviluppato e generalmente disponibile e che non è stato sviluppato allo scopo di essere incorporato nel dispositivo medico (noto anche come "software standard) o software elemento precedentemente sviluppato per il quale non sono disponibili registrazioni adeguate dei processi di sviluppo.

[1] *Activities*: a set of one or more interrelated or interacting tasks
[2] *Tasks:* a single piece of work that needs to be done
[3] *Safety:* freedom from unacceptable risk

I. Classi di sicurezza di un DMSW

Considerando il rischio di possibili danni a pazienti o altri utenti a seguito di situazioni pericolose derivanti dall'uso di un software, vengono definite tre classi di sicurezza per un DMSW:

- **Classe A**
  Comprende i software che non contribuiscono al verificarsi di situazioni pericolose: le misure di controllo esterne al software (e.g. procedure sanitarie) sono sufficienti per garantire un rischio accettabile.

- **Classe B**
  Comprende i software che contribuiscono al verificarsi di situazioni pericolose: le misure di controllo non sono sufficienti a garantire un rischio accettabile e la possibile lesione NON è seria.

- **Classe C**
  Comprende i software che contribuiscono al verificarsi di situazioni pericolose: le misure di controllo non sono sufficienti a garantire un rischio accettabile e la possibile lesione È SERIA.

II. Processo di sviluppo di un DMSW

Il processo di sviluppo del software prevede una serie di *activities*, che sono le seguenti:

1. Pianificazione dello sviluppo

L'obiettivo di questa activity è di pianificare i tasks da svolgere, necessari a ridurre i potenziali rischi causati dal software, comunicare al team di sviluppo le procedure e gli obiettivi ed assicurarsi che siano soddisfatti i requisiti di qualità.
Il piano di sviluppo deve essere sufficientemente dettagliato da permettere il corretto svolgimento del processo di sviluppo, considerando che il livello di dettaglio necessario è proporzionale al rischio associato al software, e dunque alla sua classe di sicurezza.
L'output di questa fase è quindi un piano di sviluppo che, oltre a definire il modello del ciclo di vita da usare, definisce i processi da utilizzare durante lo sviluppo, i risultati e gli output attesi a seguito di ciascuna activity o task, il rapporto tra i requisiti del sistema, i requisiti del software, i test del sistema e le misure di controllo del rischio.

Inoltre, il piano di sviluppo comprende o fa riferimento al piano di manutenzione, al piano di integrazione e testing, a quello di gestione del rischio e alla documentazione da produrre durante il ciclo di vita del software.

2. Definizione dei requisiti software

Questa activity ha come obiettivo la definizione e la verifica dei requisiti software, a partire dai requisiti di sistema precedentemente definiti (il processo di definizione dei requisiti di sistema non è oggetto di questa norma).
I requisiti software comprendono, ad esempio, le caratteristiche fisiche (e.g. piattaforma, sistema operativo e linguaggio di programmazione), le caratteristiche dell'ambiente

informatico in cui il software opera (e.g. hardware, memoria, unità di processamento, infrastruttura di rete), i requisiti delle interfacce utente, gli input e gli output del software (e.g. caratteristiche dei dati, range), i requisiti necessari per garantire la security[4] e i requisiti di interoperabilità.

3. **Progettazione dell'architettura**

   Tale activity, prevista solo per i software di classe B e C, consiste principalmente nella definizione e verifica dell'architettura a partire dai requisiti software. Ciò consiste nella definizione della struttura del software, identificandone le *componenti principali*, le *interfacce* tra esse e quelle con componenti esterne.

4. **Progettazione di dettaglio**

   La progettazione di dettaglio richiede, ai fabbricanti di software di classe B o C, di suddividere le componenti del software, identificate nella fase precedente, in *unità* software.
   Inoltre, esclusivamente per i software di classe C, è richiesta la progettazione e la verifica dettagliata delle unità software e delle rispettive interfacce: la progettazione deve specificare gli algoritmi, la rappresentazione dei dati e le interfacce interne ed esterne delle unità, mentre la verifica deve assicurarsi che la progettazione implementi l'architettura del software e che non presenti contraddizioni con essa.

5. **Implementazione e verifica delle unità**

   Tale activity richiede al fabbricante di scrivere il codice delle unità software. Per i software di classe B e C, il codice deve essere verificato utilizzando strategie, metodi e procedure ben definite, al fine di controllare che implementi la progettazione in modo corretto.
   I criteri di accettazione sono stabiliti in modo generale dal fabbricante, ma per i software di classe C devono riguardare almeno determinati aspetti elencati nella norma.

6. **Integrazione moduli e test di integrazione**

   Questa attività, prevista per i software di classe B e C, richiede di eseguire, in accordo con il piano di integrazione e testing, l'integrazione in componenti delle unità software e verificare che tali componenti funzionino come previsto, concentrandosi in particolare sul trasferimento dei dati e sul controllo delle interfacce interne ed esterne (interfacce esterne sono ad esempio quelle con altri software). Eventuali anomalie riscontrate durante questa attività sono input del processo di risoluzione di un problema.

7. **Test del sistema**

   Il test del sistema prevede la definizione e l'utilizzo di procedure codificate e di criteri di accettazione per verificare che tutti i requisiti software siano stati correttamente

[4] *Security*: Protection of information and data so that unauthorized people or systems cannot read or modify them and so that authorized persons or systems are not denied access to them. [ISO/IEC 12207:1995 definition 3.25]

implementati. Eventuali anomalie riscontrate durante questa attività sono input del processo di risoluzione di un problema.

8. Rilascio del software

L'attività di rilascio richiede al fabbricante di dichiarare la versione del software, l'ambiente e le procedure usate per crearla, di controllare che la verifica sia stata completata, che eventuali anomalie residue siano documentate e valutate e che tutte le attività del processo di sviluppo siano state effettuate.

III. Processo di manutenzione

Il processo di manutenzione del software è un processo molto simile a quello di sviluppo, ma permette ai fabbricanti di implementare facilmente modifiche al software, in risposta a problemi urgenti di sicurezza o di non conformità, preservandone l'integrità.

Le activities previste sono la definizione di un piano di manutenzione, l'analisi delle modifiche e dei problemi e l'implementazione delle modifiche utilizzando il processo di sviluppo.

I fabbricanti devono pianificare come svolgere l'attività di manutenzione, specificando in un piano le procedure da seguire, i criteri per determinare se un feedback deve essere considerato un problema e le modalità d'uso dei processi di gestione del rischio, di risoluzione di un problema e di gestione della configurazione. In merito all'analisi delle modifiche, i fabbricanti devono valutare i feedback ricevuti dopo il rilascio del software, per identificare eventuali problemi.
In seguito, gli stessi fabbricanti devono utilizzare il processo di risoluzione di un problema, analizzare ed approvare la richiesta di modifica e avvisare gli utenti e le autorità dei problemi riscontrati e la natura delle modifiche.

L'implementazione delle modifiche deve avvenire identificando ed eseguendo le activities, proprie del processo di sviluppo, che devono essere ripetute a seguito delle modifiche, compreso il rilascio del software modificato.

IV. Processo di gestione del rischio

Come già accennato, il processo di gestione del rischio, per un software previsto in questa norma, richiede l'uso di quello per un dispositivo medico conformemente alla norma ISO 14971: una sezione della ISO 14971 riguarda il controllo dei rischi associati a ciascun pericolo identificato durante l'analisi del rischio; la norma EN 62304:2006+A1:2015 è invece utilizzata per fornire ulteriori requisiti per il controllo dei rischi associati sia al software, identificati durante l'analisi dei rischi come potenzialmente contribuente ad una situazione pericolosa, sia al software utilizzato per controllare i rischi associati al dispositivo medico .

Il processo di gestione del rischio per un software prevede:

- l'analisi delle sue componenti e la definizione delle misure di controllo del rischio

- l'analisi di eventuali modifiche apportate, per individuare quelle che possono avere un impatto sulla *safety* del dispositivo.

In particolare, l'analisi delle componenti e la definizione di misure di controllo del rischio sono richieste solo per i software di classe B e C, mentre per i software di classe A è prescritta solo l'analisi di eventuali modifiche. Per i software di classe A l'assicurazione di safety ed efficacia è infatti principalmente raggiunta tramite il processo di validazione ed attraverso semplici controlli durante il ciclo di vita del software; modifiche apportate al software potrebbero invece causare un aumento della classe di rischio e di conseguenza determinare la necessità di misure di controllo.

Analisi dei componenti software

Nel dettaglio, analizzando i componenti software, è necessario identificare quelli che possono contribuire al verificarsi di situazioni pericolose e successivamente, identificando, implementando e verificando le misure di controllo del rischio, ci si aspetta di ridurre ad un livello accettabile la probabilità e/o severità di tali situazioni.

Nella norma viene specificato che non tutte le situazioni pericolose associate ad un software possono essere identificate prima della definizione della sua architettura.
Nella suddetta fase è quindi opportuno riesaminare l'analisi di rischio, per includere le eventuali nuove situazioni pericolose derivanti dal software (e.g. situazioni pericolose legate a fattori umani), le rispettive misure di controllo del rischio e quelle revisionate alla luce della valutazione della loro praticità, considerando l'architettura del software.

Analisi delle modifiche apportate al software

L'activity di gestione del rischio delle modifiche apportate al software prevede invece che il fabbricante analizzi nel dettaglio i cambiamenti, per determinare se sono state introdotte nuove potenziali cause che contribuiscono al verificarsi di situazioni pericolose e la necessità di nuove misure di controllo del rischio.

Sulla base di tale analisi, il fabbricante deve eventualmente ripetere l'analisi delle componenti software e la definizione delle misure di controllo del rischio.

V. Processo di gestione della configurazione

Il processo di gestione della configurazione del software prevede di applicare una serie di procedure amministrative e tecniche durante tutto il ciclo di vita del software, al fine di identificare e definire le componenti software in un sistema, compresa la documentazione, di documentare le modifiche e i rilasci delle varie versioni e di documentare la necessità di effettuare dei cambiamenti a seguito del processo di risoluzione dei problemi.

La gestione della configurazione del software è quindi necessaria per individuare le parti costitutive del software e per fornire una storia delle modifiche che gli sono state apportate: le activities previste sono infatti l'identificazione della configurazione, il controllo delle modifiche e la registrazione della storia delle configurazioni.

VI. Processo di risoluzione di un problema

Il processo di risoluzione di un problema è quello utilizzato per documentare, analizzare e stabilire come risolvere i problemi (incluse le non conformità) che vengono alla luce durante tutte le fasi del ciclo di vita del software, incluse lo sviluppo e la manutenzione.

L'obiettivo è quindi quello di fornire uno strumento per garantire che i problemi che hanno un impatto sulla safety siano trattati in modo strutturato.

Tale processo prevede ad esempio che per ogni problema riscontrato, il fabbricante prepari una segnalazione di problema (*problem report*), valuti l'impatto del problema sulla *safety* del software utilizzando il processo di gestione del rischio e prepari una richiesta di modifica (*change request*) contenente le modifiche necessarie per correggere il problema o, in alternativa, documenti le motivazioni per cui non sono necessari cambiamenti nel caso in cui il problema non influisca sulla *safety*.

2.2 Processo di gestione del rischio

Concetto di rischio

Il rischio è ogni evento potenziale che possa influenzare negativamente il raggiungimento degli obiettivi di processo e come tale richiede il massimo di attenzione da parte del management. Nel valutarlo, si deve tenere conto dell'impatto e della probabilità dell'avvenimento negativo.

La combinazione di questi due aspetti determina la rilevanza del rischio per il dispositivo. La gestione del rischio è il processo mediante il quale si misura o si stima il rischio e successivamente si sviluppano strategie per governarlo. [8]

Introduzione

Nel tempo, questi concetti hanno subìto una forte evoluzione e trovato applicazione anche all'interno del settore sanitario, in particolare nello sviluppo di dispositivi medici.

Condizione necessaria per la certificazione di un dispositivo medico, e dunque di un software come dispositivo medico, è proprio la gestione dei rischi.

È compito del fabbricante dare il suo giudizio sulla sicurezza del dispositivo medico, per quanto riguarda la destinazione d'uso dichiarata, in base all'accettabilità del rischio e allo stato dell'arte generalmente accettato.

Il software di per sé non è un pericolo, ma può contribuire a situazione pericolose, per cui la maggior parte delle attività di gestione del rischio per i software consistono nell'identificare quelle serie di eventi che possono contribuire a situazioni pericolose e quei punti in cui la serie può essere interrotta, prevenendo un danno o riducendone la probabilità.

Le serie di eventi che possono portare a situazioni pericolose possono rientrare in due categorie:

1. Errori nelle specifiche del software
2. Errori nell'implementazione del software

Dal momento che è molto difficile stimare la probabilità del verificarsi di un'anomalia software che possa contribuire a situazioni pericolose; inoltre, poiché il software non è soggetto a rottura o usura, l'analisi dei rischi applicata a un DMSW consiste nell'andare a identificare funzionalità che possano condurre a situazioni pericolose.

2.2.1 Riferimenti normativi: TR 80002-1

Perché?

L'utilizzo errato di un generico dispositivo medico, compreso un dispositivo medico software, può comportare un rischio *in primis* per la sicurezza del paziente, ma anche dell'utilizzatore e delle altre persone ed attrezzature presenti *in loco*.

TR 80002-1 è un report tecnico: applica la norma ISO 14971 per condurre il processo di gestione dei rischi a un dispositivo medico software.

A chi si rivolge la norma?

- Fabbricante. È il primo responsabile nella gestione del rischio. Si occupa dei seguenti aspetti: determinazione di un rischio accettabile, approvvigionamento di risorse adeguate e personale qualificato, verifica periodica dell'efficacia del processo di gestione del rischio.
- Organizzazione responsabile. È il responsabile della corretta esecuzione delle indicazioni fornite dal fabbricante riguardo le procedure della gestione del rischio; è inoltre responsabile della gestione del rischio residuo.
- Operatore sanitario. È il responsabile del corretto utilizzo del dispositivo in base al rapporto rischi benefici.

Quando applicare la norma?

La norma deve essere applicata durante il ciclo di vita di un dispositivo medico: installazione, collaudo, funzionamento operativo, manutenzione e dismissione. E dopo ogni modifica significativa.

Scopo e contenuti principali della norma

Il fabbricante deve stabilire, documentare e mantenere per tutto il ciclo di vita del dispositivo un processo per identificare i pericoli associati al dispositivo medico, stimando e valutando tali rischi e monitorando l'efficacia dei controlli.

(Allegato I, [2])

RISK MANAGEMENT PLAN

Il processo di gestione del rischio deve essere innanzitutto pianificato; è compito del fabbricante stabilire e successivamente documentare un piano conforme al processo di gestione del rischio, che deve inserire in un file specifico (file di gestione del rischio) e successivamente nel fascicolo tecnico, insieme agli altri documenti di valutazione del dispositivo medico. Di seguito viene

riportato un elenco dei minimi elementi che devono essere contenuto nel piano di gestione del rischio. [6]

Il piano di gestione del rischio deve includere:

1. Scopo e campo di applicazione del processo, identificando e descrivendo il DM e le fasi del ciclo di vita per cui il piano è applicabile
2. Identificazione delle responsabilità
3. Le attività di verifica
4. Le attività relative alla raccolta e revisione di informazioni di produzione e post-produzione

Se il software è parte integrante del dispositivo medico bisogna includere anche:

5. Un documento che certifica lo sviluppo del software in accordo con la IEC 62304
6. Descrizione del dispositivo medico e funzionalità del software
7. Aspetti di sviluppo del software che fanno riferimento alla gestione del rischio.
8. Criteri di accettabilità del rischio (inclusi criteri per l'accettabilità dei rischi quando la probabilità che si verifichi un danno non può essere stimata).
9. Attività relative alla raccolta e revisione di informazioni di produzione e post produzione.

Poiché gli standard internazionali non danno indicazioni specifiche, è compito del fabbricante scegliere appropriati criteri di accettabilità del rischio.

RISK MANAGEMENT PROCESS

Il processo deve includere le seguenti attività:

1. Analisi dei rischi
2. Valutazione dei rischi
3. Trattamento dei rischi
   3.1. Controllo dei rischi
4. Valutazione dei rischi residui
5. Informazioni di produzione e post-produzione.

La seguente Figura 2.1 mostra lo schema del processo di gestione del rischio.

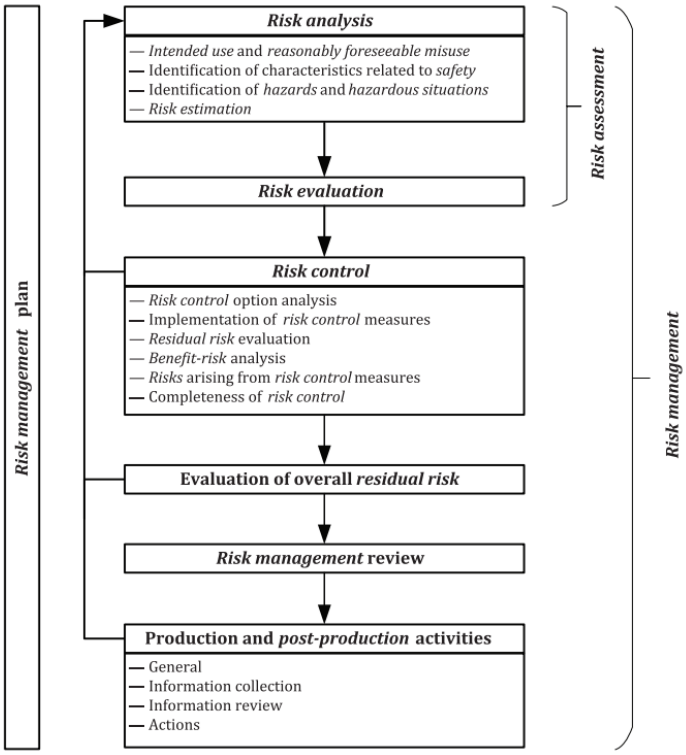


Figura 2.1. Rappresentazione schematica del processo di gestione del rischio

È opportuno precisare che per ogni termine legato alla gestione del rischio esiste una definizione precisa, che deve essere ben compresa e rispettata durante tutte le attività coinvolte nel processo.

Definizioni ricorrenti [6]

Termine	Descrizione
Danno	Lesione fisica o danno alla salute delle persone alle proprietà o all'ambiente.
Pericolo	Potenziale fonte di danno.
Situazione pericolosa	Circostanza in cui le persone, la proprietà o l'ambiente sono esposti a uno o più pericoli.
Rischio	Combinazione della probabilità del verificarsi di un danno e gravità di tali danni.
Gravità	Misura delle possibili conseguenze di un pericolo.

Come verificare la conformità alla norma?

RISK MANAGEMENT FILE

La conformità alla normativa è verificata ispezionando il file di gestione del rischio. Il file deve fornire la tracciabilità per ciascuno pericolo identificato in tutte le fasi del processo; dovrebbe inoltre contenere almeno riferimenti a tutta la documentazione richiesta.

La norma NON prevede

La norma non viene applicata a decisioni cliniche, che possono essere prese solo da personale sanitario qualificato che conosca lo stato di salute di un paziente e l'opinione del paziente stesso; inoltre non specifica i livelli di rischio accettabili, che devono essere stabiliti dal fabbricante specificatamente per il prodotto analizzato.

I prossimi paragrafi sono dedicati a un'analisi dettagliata delle quattro fasi del processo di gestione del rischio applicata ai software dispositivi medici.

2.2.2 Fasi del processo

I. Analisi dei rischi

L'analisi dei rischi comprende tre diverse attività:

a. Identificazione della destinazione d'uso e i prevedibili ed (eventuali) usi impropri:

Nella prima fase dell'analisi del rischio di un DMSW, devono essere identificati la sua destinazione d'uso, tutti gli usi impropri prevedibili e tutte le caratteristiche, qualitative e quantitative, legate alla sua sicurezza.
Il software non è considerato una causa diretta di un danno, ma un suo utilizzo errato aumenta la probabilità di errore nell'utilizzo del dispositivo medico (se software embedded) o del software stesso (software stand-alone). Le cause connesse a questo tipo di errore possono riguardare la complessità del dispositivo medico con conseguente difficoltà nell'essere padroneggiato o compreso dall'operatore, o le insufficienti limitazioni nelle funzionalità del software con conseguente eccessivo affidamento da parte dell'operatore, o ancora l'eccessiva complessità dell'interfaccia utente con conseguente incomprensione da parte di chi la utilizza.
Nel caso specifico dei software embedded, un altro motivo di errato utilizzo del software riguarda la mancanza o insufficienza di restrizioni nelle intercomunicazioni e interconnessioni tra dispositivi medici e non; ciò è una potenziale causa di abusi del software da parte di chi lo utilizza, abusi non facilmente identificabili a priori da fabbricante.

b. Identificazione dei pericoli noti o prevedibili (e loro cause):

La fase di identificazione dei pericoli è obbligatoria per comprendere tutti i rischi prevedibili del DMSW, al fine di pianificare e attuare opportune misure di controllo

nella fase successiva. Come già anticipato, il software non è per natura un pericolo, ma *può contribuire a situazioni pericolose*. Guasti software infatti aumentano la probabilità che un pericolo si trasformi in una situazione pericolosa.

In questa fase devono essere considerati sia i danni derivanti dalla natura del software che i danni da pericoli relativi all'uso del software.
Situazioni pericolose di un software possono verificarsi sia quando esso è la *causa iniziale della sequenza* degli eventi che hanno portato a tali situazioni, sia quando esso stesso è un elemento interno a tale *sequenza* (es. software destinati a rilevare mal funzionamenti hardware).

Per quanto riguarda le anomalie del software, va tenuto in conto che, se presenti in una particolare versione del software, saranno presenti in tutte le copie di quel software. Tuttavia, la probabilità che un'anomalia del software porti a un guasto del software stesso è molto difficile da stimare, a causa della natura *casuale* degli input a ciascuna copia separata del software.

Il software potrebbe poi includere un componente SOUP o il riutilizzo di un componente precedentemente sviluppato.

Nei pericoli connessi all'utilizzo del software devono essere considerati quelli legati al corretto utilizzo e quelli relativi alle anomalie software: mentre il primo caso vede l'utilizzatore come responsabile di tale rischio, il secondo coinvolge principalmente il fabbricante.

Per condurre l'identificazione dei pericoli la norma richiede il coinvolgimento di personale qualificato e multidisciplinare e di condurre l'analisi al livello globale di sistema (e non in modo isolato).

c. Stima dei rischi per ogni situazione pericolosa

La stima di ciascun rischio è il risultato del prodotto della probabilità del danno e della gravità delle conseguenze legate a ciascuna situazione pericolosa individuata per tale danno. Poiché è molto difficile stimare la probabilità di danni derivanti da un'anomalia del software, stimare i rischi di un DMSW consiste nel valutare la probabilità che situazioni pericolose possano verificarsi ed evolvere.

Probabilità

La probabilità che un'anomalia del software porti ad un guasto del software è molto difficile da stimare, a causa della natura casuale degli input per ciascuna copia separata del Software.

Per trovare una soluzione a tale difficoltà, la norma suggerisce di considerare il caso peggiore, ponendo il livello di probabilità associata a quel guasto pari a 1.

In questi casi dunque, la valutazione del rischio di un *software dispositivo medico viene fatta solo sulla base della gravità del danno derivante da situazioni pericolose*.

Severità

Considerando che spetta al fabbricante definire i criteri e i livelli di gravità, ai fini di valutazione del rischio secondo la ISO 14971, è utile stabilire questi livelli di gravità in modo che esista una relazione con la classificazione di sicurezza del software di IEC 62304, altrimenti potrebbe essere necessario classificare i livelli di gravità due volte, una volta per la valutazione del rischio necessaria per la complessiva processo di gestione del rischio e una per la determinazione della classe di sicurezza del software secondo IEC 62304.

Tecniche per la stima del rischio

Tra i metodi usati per identificare il ruolo del software all'interno di una situazione pericolosa, le principali sono le seguenti:

i. Fault Tree Analysis (FTA):

"L'FTA è un metodo tradizionale dall'alto verso il basso, spesso utilizzato a partire dal dispositivo medico nel suo insieme. FTA viene utilizzato principalmente per analizzare le cause del danno. Esso parte dalla postulazione che si verifichi un danno e utilizza la logica booleana per identificare gli eventi o le condizioni che devono essere presenti affinché si verifichi tale danno.

Gli eventi o le condizioni vengono analizzati in modo sempre più dettagliato fino a raggiungere un punto in cui è possibile identificare una o più misure di controllo del rischio che prevengano il danno.

FTA può essere utilizzato per identificare gli elementi software coinvolti in una sequenza di eventi che si traduce in una situazione pericolosa; viene utilizzato nell'analisi del rischio come strumento per fornire una stima delle probabilità di guasto e per identificare guasti singoli e guasti di causa comune che provocano situazioni pericolose". [7]

ii. Failure Modes and Effect Analysis (FMEA):

"La modalità di errore e l'analisi degli effetti (FMEA) è un approccio bottom-up che inizia con un componente o un sottosistema (per il software questo è un articolo software in IEC 62304) e pone la domanda: se questo elemento si guasta, quali sarebbero le conseguenze?

Data la difficoltà di anticipare quali difetti software saranno presenti in ciascun articolo software, il punto di partenza per FMEA sarebbe elencare i requisiti relativi alla sicurezza di ciascun articolo software e considerare la domanda: se questo requisito non è soddisfatto, quali potrebbero essere le conseguenze?

Ciò porta all'identificazione degli articoli software il cui guasto potrebbe causare danni e all'identificazione di quali tipi di guasto devono essere prevenuti.

Quando si identificano sequenze o combinazioni di eventi che possono determinare una situazione pericolosa, è più facile concentrarsi sul software direttamente correlato

alle prestazioni essenziali del dispositivo medico (ad esempio un algoritmo che calcola i livelli di glucosio nel sangue) e le cause specifiche dei pericoli correlati . È anche importante considerare le cause del software che potrebbero causare modalità di errore impercettibili e quindi causare uno o più pericoli del dispositivo medico.

NOTA Cause specifiche sono difetti del software la cui funzionalità è chiaramente correlata alla funzionalità clinica del dispositivo e comportano uno dei PERICOLI del dispositivo. Un esempio è un difetto in un algoritmo per il calcolo del risultato di un test.

Sebbene sia difficile prevedere esattamente cosa potrebbe non funzionare in un articolo software, è possibile identificare categorie di difetti, ognuno dei quali ha misure ben note di controllo dei rischi. Ad esempio, la corruzione dei dati è una classe di errore che può essere rilevata e prevenuta utilizzando una procedura di *checksum*. I produttori dovrebbero mantenere i propri elenchi di categorie di difetti del software rilevanti per i propri prodotti." [9]

Metodi per la stima del rischio

In generale, è opportuno effettuare una stima del rischio di tipo quantitativo, tuttavia là dove le informazioni a disposizione sono insufficienti a garantirne l'attendibilità è accettabile e anzi da preferire una stima qualitativa.

Un'altra distinzione va fatta sui fattori coinvolti nel calcolo matematico stesso: indipendentemente dal tipo di stima adottata, il rischio può essere calcolato come il prodotto dei due fattori sopra descritti (probabilità, severità) ma può essere calcolato anche con un terzo fattore di moltiplicazione, per aumentare l'affidabilità dei risultati attesi; quest'ultimo prende il nome dalla tecnica da cui deriva, "calcolo FMEA".

Di seguito vengono descritti entrambi i tipi di calcolo (PxG e FMEA) per entrambe le tipologia di stime, qualitativa e quantitativa:

1. **Calcolo PxG**

$$\boldsymbol{Rischio} = \boldsymbol{Probabilit}\grave{\mathrm{a}} \times \boldsymbol{Gravit}\grave{\mathrm{a}}$$

   a. **Matrice del rischio qualitativa 3x3**

Livello di gravità	***Descrizione***
Serio	Morte o perdita di funzione o struttura
Moderato	Lesioni reversibili o lievi
Trascurabile	Non causerà lesioni o ferirà leggermente
Livello di probabilità	***Descrizione***
Alto	È probabile che accada, spesso, frequente
Medio	Può succedere, ma non di frequente
Basso	Improbabile che accada, raro, remoto

	Severità		
Probabilità	**Trascurabile**	**Moderato**	**Serio**
Alto			
Medio			
Basso			

b. Matrice del rischio quantitativa 5x5

Livello di gravità	***G*[5]**
Catastrofico	10^7
Critico	10^6
Serio	10^5
Minore	10^4
Trascurabile	10^3
Livello di probabilità	***P*[6]**
Frequente	10^{-1}
Probabile	10^{-2}
Occasionale	10^{-3}
Remoto	10^{-4}
Improbabile	10^{-5}

	Gravità				
Probabilità	**Trascurabile**	**Minore**	**Serio**	**Critico**	**Catastrofico**
Frequente					
Probabile					
Occasionale					
Remoto					
Improbabile					

Il calcolo della stima dei rischi PxG presenta alcuni limiti, di seguito sintetizzati:

- Non è facile distinguere i risultati che hanno lo stesso valore pur con calcoli opposti (4x1 e 1x4)
- Non permette di distinguere se la valutazione sia riferita alle misure di prevenzione già attuate o ancora da attuare

2. Calcolo FMEA PxGxE

$$\boldsymbol{Rischio} = \boldsymbol{Probabilit}\text{à} \times \boldsymbol{Gravit}\text{à} \times \boldsymbol{Efficacia}$$

[5] G = indice di gravità associata al verificarsi del danno

[6] P = indice legato alla probabilità che l'evento pericoloso si verifichi e causi un danno

Tale approccio, derivato dalla relativa tecnica di analisi dei rischi, aggiunge un terzo parametro alla stima del rischio, l'efficacia, senza cambiarne la procedura di calcolo:

Come anticipato, la procedura di calcolo non cambia ma viene aggiunto un terzo fattore. Anche questo attributo è sostanzialmente un *ranking number,* "Efficacia", che identifica la probabilità di rilevare un fallimento o le sue cause.

Per entrambe le matrici, non cambia il modo di calcolare stima del rischio (prodotto tra fattori) ma cambia l'interpretazione del risultato finale, in cui viene ora considerato l'effetto di tale fattore in base al livello attribuito. Di seguito vengono descritti i livelli di efficacia sia in una matrice di tipo qualitativo sia in una di tipo quantitativo:

a. Esempio di Matrice del rischio qualitativa 3x3

Livello di efficacia	***Descrizione***
Alto	Pericolo rilevabile automaticamente, con segnalazione all'utilizzatore
Medio	Pericolo rilevabile verificando la soluzione, manuale/diretta, da parte dell'utilizzatore
Basso	Criticità non rilevabile o difficilmente rilevabile prima del suo verificarsi

b. Esempio di Matrice del rischio quantitativa 5x5

Livello di efficacia	***E*[7]**
Alto	10^{1}
Medio	10^{0}
Basso	10^{-1}

II. Valutazione dei rischi

A partire dai criteri di accettabilità del rischio stabiliti nel piano di gestione del rischio, per ogni situazione di pericolo identificata il fabbricante deve decidere quanto vale il rischio, garantendo di aver considerato i rischi derivanti da *tutte* le possibili situazioni di pericolo.
Lo standard ISO 14971 non specifica quale sia il livello di rischio accettabile, in quanto tale decisione viene lasciata al fabbricante.

Di seguito vengono riportati i principali (ma non unici) metodi per assegnare il livello di accettabilità di un rischio, seguendo le evidenze dello stato dell'arte del software al momento della sua progettazione:

- Riferimento a standard che contengano requisiti per il raggiungimento dell'accettabilità del rischio, riguardo particolari tipi di DM o rischi particolari;

[7] E = indice legato alla capacità di rilevare l'esistenza di criticità e individuare la problematica

- Confronto dei livelli di rischio dei dispositivi medici già in uso;
- Valutazione dei dati degli studi clinici, specialmente per le nuove tecnologie.

Indipendentemente dal metodo scelto è opportuno ricordare che la stima del rischio determinata empiricamente spesso è diversa dalla percezione del rischio; quest'ultima viene valutata da parte di un'ampia sezione trasversale di *stakeholders*.

Livelli di accettabilità del rischio

Qualsiasi sia il metodo scelto per valutare un rischio, i livelli di accettabilità si distinguono in tre classi:

- **Rischio NON accettabile**: devono essere necessariamente individuate misure di controllo che riducano il rischio entro i limiti di accettabilità o nelle regioni AFAP: in caso negativo, quella soluzione NON è realizzabile.
- **AFAP**[8] (*As Far As Possible*): i rischi non sono elevati ma devono essere ugualmente trattati e per essere ridotti *quanto più possibilmente*. Viene dunque applicato il processo di riduzione del rischio.

- **Rischio accettabile**: il rischio rientra nei limiti di accettabilità previsti. Non sono necessarie misure di riduzione.

A partire dalle strutture di matrice sopra descritti, le stesse vengono ora riprese complete dei livelli di accettabilità di rischio e secondi i due criteri di calcolo del rischio stesso, qualitativo e quantitativo:

Esempio di Matrice del rischio *qualitativa 3x3*

	Severità		
Probabilità	**Trascurabile**	**Moderato**	**Serio**
Alto			
Medio			
Basso			

Esempio di Matrice del rischio *quantitativa 5x5*

	Severità				
Probabilità	**Trascurabile**	**Minore**	**Serio**	**Critico**	**Catastrofico**
Frequente	10^2	10^3	10^4	10^5	10^6
Probabile	10^1	10^2	10^3	10^4	10^5
Occasionale	10^0	10^1	10^2	10^3	10^4
Remoto	10^{-1}	10^0	10^1	10^2	10^3
Improbabile	10^{-2}	10^{-1}	10^0	10^1	10^2

[8] MDR 2017/745 *Requisiti generali – Requisiti Generali di sicurezza e prestazione*, Art.2. Da non confondere con la definizione precedente, ALARP (*As Low As Reasonably Practicable*), relativa alla vecchia Direttiva Dispositivi Medici, la quale specificava di ridurre il rischio *quanto più ragionevolmente possibile*

Legenda	
	Rischio NON accettabile
	AFAP
	Rischio accettabile

III. Trattamento dei rischi

La fase di trattamento dei rischi consiste nell'elaborazione di programmi per la gestione dei rischi identificati e valutati nelle fasi precedenti.
Emerge qui l'importanza di una definizione delle azioni necessarie per fronteggiare e dunque *trattare* tali rischi. Gli approcci possibili sono quattro:

- *Evitare*: è l'approccio necessario nel caso la valutazione del rischio cada nel livello "rischio NON accettabile". Consiste nell'andare a eliminare qualsiasi attività legata agli eventi che possono generare il rischio; tale approccio prevede la non accettazione del rischio.

- *Trasferire*: è l'approccio necessario nel caso la valutazione del rischio cada nel livello "rischio NON accettabile". Consiste nel trasferire le conseguenze negative di un evento a terze parti; in particolare, consiste nel trasferire il rischio da un dispositivo in cui l'effetto sia dannoso a un altro il cui effetto non lo sia.

- *Accettare*: è l'approccio necessario nel caso la valutazione del rischio cada nel livello "rischio accettabile". Accettare un rischio comporta la non necessità di pianificare attività di controllo sulle sue conseguenze sfavorevoli; viene però effettuato un piano, cosiddetto di emergenza, che predispone tutte le azioni che devono essere svolte in caso si manifesti un rischio identificato.

- ***Ridurre*:** è l'approccio necessario nel caso la valutazione del rischio cada nel livello "AFAP". Ridurre il rischio comprende azioni intraprese ad abbassare la probabilità che un evento negativo, e dunque le conseguenze dannose ad esso correlate, si verifichi.
  Tale approccio può essere condotto in due modi:
  - *Prevenzione e controllo delle perdite associate al rischio in oggetto;*
  - Un approccio basato sulla cosiddetta "legge dei grandi numeri": maggiore è il numero di unità esposte a uno stesso rischio, minore è l'impatto che una perdita può avere sul singolo rispetto all'esposizione totale.

  L'approccio descritto nella norma è il primo, il controllo del rischio, analizzato nel prossimo sotto-paragrafo.

III.1. Riduzione del rischio (o Controllo del rischio)

Se la stima del rischio ricade nel livello AFAP, devono essere effettuate delle attività di controllo per ridurre la gravità del danno, per ridurre la probabilità che il danno si verifichi o entrambe.

Tipi di misure di controllo

Esistono tre principali misure di controllo, di cui il fabbricante può utilizzarne una o più nei confronti di un DM; vengono di seguito elencate e descritte, in ordine di priorità:

- **Sicurezza intrinseca di progettazione (*Safety by Design*)**

  La progettazione di un qualsiasi software è spesso soggetta a un eccessivo numero di interazioni da parte delle componenti al suo interno; ciò può portare a inaspettate situazioni pericolose. Attuando misure di controllo sin dalle prime fasi di progettazione è possibile evitare tali situazioni, pur soddisfacendo le esigenze della maggior parte dei clienti.

  La sicurezza intrinseca sin dalla fase di design del software porta i seguenti vantaggi:
  - Elimina funzionalità che non sono ritenute in sicurezza
  - Modifica l'architettura del DMSW, così che sequenze di eventi legate a situazioni pericolose siano eliminate
  - Semplifica l'interfaccia utente, andando così a ridurre la probabilità di errori umani durante l'utilizzo
  - Definisce regole di progettazione software volte a evitare la presenza di anomalie

- **Misure di protezione**

  Le misure protettive vengono implementate nel dispositivo stesso o nel processo produttivo e a fine sviluppo del prodotto e riguardano sia il lato hardware (software embedded) che software (software embedded/ software stand-alone).

  Tali misure devono essere *indipendenti* da qualsiasi funzione ad esse correlata: ciò è verificato nei casi in cui le misure protettive di un software siano applicate a livello hardware e viceversa.

  Per capire quali misure protettive adottare, implementare e applicare al software, innanzitutto è necessario eliminare o ridurre la possibilità che siano presenti più guasti derivanti da una stessa causa.

- **Informazioni per la sicurezza**

  La misura di controllo tramite informazioni per la sicurezza prevede modifiche a livello di interfaccia software, al fine di renderlo più semplice e intuitivo e, di conseguenza, diminuire la complessità e la mole del manuale utente.

Elementi software in cui implementare le misure di controllo

Gli elementi software in cui è possibile applicare le misure di controllo sono i seguenti tre:

- *Input*
  È opportuno limitare il range di input nel software, al fine di prevenire output non sicuri e di ridurre la probabilità di danno a livello di input stesso dovuto a un'anomalia software.

Esempi:

- A livello software: soglie di controllo degli input
- A livello hardware

- *Output*
  Applicare misure di controllo agli output permette di controllare il rispetto delle soglie di tali valori entro un range prefissato, così che siano prevenuti danni.

  Esempi:

  - A livello software: soglie di controllo nei valori di output
  - A livello hardware: soglia limite all'energia applicata al paziente
  - Sistemi di avviso (alert e interruttore): quest'ultima presuppone che l'operatore sia in grado di riconoscere una situazione pericolosa verso il paziente

- *Interfacce interne tra moduli software:*
  Sono misure applicate a livello di input o output di componenti software.

Qualora non sia possibile identificare un singolo range di parametri che garantisca la sicurezza del dispositivo durante il funzionamento operativo, è possibile specificare un "*safe operating envelope*".

Esistono altri casi, invece, in cui i valori di *input* e *output* sono noti solo al personale clinico e quindi non è possibile stabilire un range di valori di sicurezza, in fase di sviluppo; in questi casi è possibile solo trovare incongruenze tra valori di input e output, senza agire in modo diretto con misure di controllo software/hardware.

Applicazione delle misure di controllo

Indipendentemente dal tipo di misura scelta, per aumentare l'efficacia di tali misure è utile considerare i seguenti fattori:

- Ciclo di vita del software: per effettuare la scelta di una misura di controllo devono essere prima valutati i vantaggi e gli svantaggi in tutte le fasi di vita del software; una stessa misura di controllo può avere un costo maggiore se applicata nelle prime fasi di sviluppo piuttosto che nelle successive
- Classificazione dei componenti software in base i livelli di sicurezza: assegnare classi di sicurezza in fase di pianificazione delle misure da adottare aiuta a discriminare i componenti software in base al livello di criticità. Tale classificazione non è tuttavia statica ma può cambiare durante il ciclo di vita del prodotto e a seguito dell'implementazione di misure di controllo.

  Di seguito vengono riportati tre tipi di implementazione delle misure di controllo di rischio di un software:

- **Architettura software**

  Alcuni danni possono essere evitati agendo a livello dell'architettura di un dispositivo medico software, sia dal lato hardware che software stesso.

In particolare, le misure di controllo per una *progettazione intrinsecamente sicura (misura safety by design)* prevedono un'architettura cosiddetta "fault tolerant": è un'architettura che garantisce il funzionamento operativo in caso di primo guasto delle funzioni di sicurezza e delle segregazioni di componenti software legate alla sicurezza.

Qualora non sia possibile eliminare un rischio a livello progettuale si ricorre alle *misure protettive*. In un'architettura software tali misure possono intervenire in modo diretto per eliminare o almeno limitare i danni, oppure possono intervenire indirettamente andando a generare un allarme di avviso.

Le misure protettive per un software sono due e in entrambi i casi la loro applicazione comporta il raggiungimento della sicurezza del software a spese della sua operatività:

- *Fail-safe* a livello di architettura. Tale misura preserva la sicurezza di paziente e operatore a scapito della perdita di funzione del sistema o del componente malfunzionanti
- *Fail-operational* a livello di sistema. Tale misura permette la continuità operativa del software ma con performance ridotte.

- **Anomalie software**

Per quanto un design possa essere fatto con attenzione, i software possono presentare anomalie non facilmente prevedibili: per ridurre la presenza di anomalie è necessario agire con opportune misure di controllo.

In questi casi le misure di controllo dovrebbero essere applicate a livello dell'architettura software e in particolare nelle parti in cui è più probabile che si verifichi un'anomalia: in tal modo viene garantitala sicurezza del software anche senza conoscere tutte le anomalie possibili.

Esistono anche anomalie che *generano sequenze di eventi che portano a un danno non evitabile*: in questi casi le misure di controllo non sono sufficienti ed è necessario eliminare l'anomalia stessa.

- **Componenti ad alta integrità**

I componenti software sono definiti ad alta integrità se viene garantita, dal produttore, la sicurezza e affidabilità delle funzionalità interne e se viene garantita l'operabilità in totale assenza di errori. Per ottenere un componente ad alta integrità il fabbricante deve sviluppare il software seguendo rigorosamente la norma relativa al suo sviluppo, IEC 62304. Il processo di sviluppo di componenti ad alta integrità ha lo scopo di ridurre la probabilità di anomalie software.

- ***Software of Unknown Provenance* o SOUP**

L'utilizzo di *Software of Unknown Provenance* (SOUP) viene spesso rilevato in fase di progettazione del sistema. Maggiore è il potenziale rischio del dispositivo medico, più dettagliate dovrebbero essere le analisi delle potenziali modalità di guasto di SOUP, e maggiori le misure di controllo del rischio da implementare.

Un SOUP generalmente non può essere modificato per incorporare nuove misure di controllo del rischio, necessarie a monitorarlo o isolarlo al fine di evitare che contribuisca a pericoli o situazioni pericolose, in caso di guasto. Né ci sono adeguate informazioni di progettazione interna, disponibili a identificare tutti i potenziali pericoli causati da SOUP.

Pertanto, le misure di controllo necessarie a monitorare o isolare un SOUP in caso di guasto dovrebbero essere implementate *a livello del sistema e dell'architettura del software*, così da evitare che diventi una causa di pericolo.

Dopo aver identificato e selezionato le misure di controllo del rischio più appropriate, la fase successiva è la loro implementazione e la verifica della loro efficacia.

Per verificare l'efficacia di una misura di controllo adottata, i principali aspetti da considerare sono i seguenti:

- Tracciabilità: devono essere identificati tutti i componenti di un DMSW e devono essere specificate le sue funzionalità legate alla sicurezza, in modo che possano essere successivamente implementate e testate nel software e nelle sue versioni varianti possibili

- Il range di condizioni di utilizzo durante l'esecuzione dei test

- Test di regressione: devono essere effettuati in un DMSW per verificare le sue funzionalità legate alla sicurezza; devono essere ripetuti ogni volta che viene apportata una modifica ad esse

IV. Valutazione del rischio residuo

Al termine della fase di misure di controllo segue la valutazione del rischio residuo del DMSW: per condurre questa fase viene fatto riferimento ai criteri che sono stati stabiliti nel piano di gestione del rischio.

A partire dai risultati ottenuti dalle misure di controllo, viene valutata l'accettabilità del rischio residuo del DMSW. Qualora il rischio residuo fosse *non* accettabile e *non* fosse possibile agire con ulteriori controlli relativi al rischio, deve essere fatta una valutazione rischio/beneficio del paziente da parte del fabbricante: se il beneficio supera il rischio complessivo, devono essere adottate le misure di controllo del rischio tramite informazioni di sicurezza, da parte del fabbricante, nei confronti del rischio residuo stesso; in caso fosse il rischio residuo a superare il rapporto, tale rischio viene considerato inaccettabile. Tutti i risultati delle attività di test devono essere valutati facendo riferimento ai criteri di accettabilità.

Revisione periodica delle misure di controllo

Per evitare che le misure di controllo, implementate in un software, possano aver creato nuovi pericoli o situazioni pericolose, è necessaria una revisione periodica di tali misure.

Revisioni delle misure di controllo devono essere fatte sia al termine della progettazione del DMSW sia dopo le verifiche di sistema.

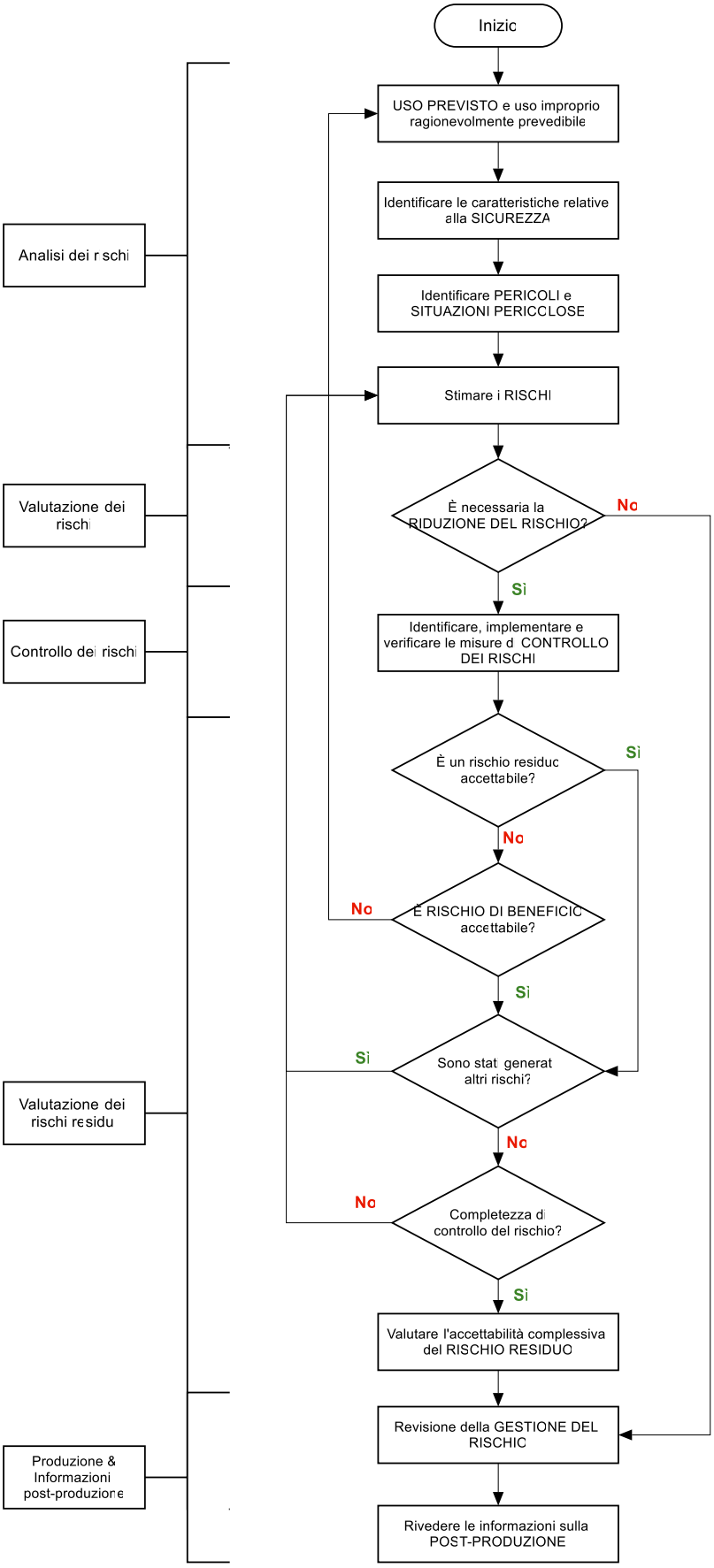
V. Informazioni di produzione e post produzione

Per quanto l'affidabilità della stima dei rischi aumenti con il rispetto delle indicazioni fornite dalle norme, nessuna di queste rende la stima affidabile quanto una valutazione post commercializzazione, in cui è l'utilizzatore stesso a rilevare i rischi durante l'uso effettivo. È dunque di estrema importanza la sorveglianza post commercializzazione delle informazioni sugli aspetti connessi ai rischi, da parte del fabbricante.

Come già accennato, la gestione del rischio è un processo iterativo durante l'intero ciclo di vita del dispositivo: tale gestione, in un'azienda, è responsabilità dell'ingegnere clinico e dell'organizzazione responsabile (cioè i dirigenti dell'azienda).

Il fabbricante garantisce la sicurezza e l'efficacia del proprio dispositivo all'Azienda sanitaria di riferimento, ma dato il numero di dispositivi sempre crescente, così come il grado di informazioni che lo stesso dispositivo scambia con altri dispositivi medicali e attraverso reti IT (ambienti altamente dinamici), non è possibile prevedere tutti i possibili cambiamenti e quindi assicurare il corretto funzionamento del dispositivo in tutte le situazioni possibili. È responsabilità dunque dell'Azienda avere al suo interno una struttura specifica alla gestione del rischio, al fine di essere sempre informata sull'evoluzione informativa e sull'impatto che essa può avere nella gestione dei dispositivi.

A conclusione di quanto analizzato viene di seguito riportato un flowchart riassuntivo delle fasi costituenti l'intero processo di Gestione dei Rischi per un dispositivo medico software, da applicare durante tutte le fasi del suo ciclo di vita.



Flowchart 2.1 Processo di Gestione dei rischi di DMSW

3. Usabilità di dispositivi medici software

Per eliminare o ridurre i rischi connessi agli errori d'uso i fabbricanti devono:

a) ridurre, per quanto possibile, i rischi connessi alle caratteristiche ergonomiche del dispositivo e all'ambiente in cui è previsto che quest'ultimo sia usato (progettazione per la sicurezza del paziente);
b) considerare il livello di conoscenza tecnica, esperienza, istruzione, formazione e ambiente d'uso, e, ove possibile, le condizioni mediche e fisiche degli utilizzatori previsti (progettazione per utilizzatori profani, professionali, disabili o altri).

(Allegato I, art. 5, [2])

[…] Ogni scala di misura, di controllo o di indicazione è progettata e fabbricata sulla base di principi ergonomici tenendo conto della destinazione d'uso, degli utilizzatori previsti e delle condizioni ambientali in cui i dispositivi sono destinati a essere utilizzati.

(Allegato I, art. 14.6, [2])

Introduzione

L'utilizzo di un DM è considerato uno dei fattori principali del *recall* post commercializzazione, e il motivo è strettamente legato a problematiche relative alla difficoltà dell'utilizzo del prodotto.

L'allegato I del MDR rafforza il concetto di corretto utilizzo e i fattori che lo influenzano come requisito essenziale per garantire sicurezza ed efficacia dei DM.

Una delle caratteristiche principali dell'utilizzo di un prodotto è l'usabilità, che è strettamente connesso al concetto più generale di Fattore Umano.

Nel settore dei Dispositivi Medici Software sono molte le pubblicazioni, norme o linee guida, che trattano questo argomento. Fra quelle più importanti possiamo ricordare:

- Wickens Lee, Liu Gordon-Becker, *An Introduction to Human Factors Engineering*
  Viene fatto riferimento ad esso per descrivere il concetto di Ingegneria dei Fattori Umani, e in particolare per descrivere l'interazione uomo-computer. [10]

- IEC 62366-1: 2015 + A1:2020, *Medical devices : Application of usability engineering to medical devices*
  Viene fatto riferimento per descrivere come applicare l'ingegneria dei fattori umani a dispositivi medici. [11]

3.1 Concetto di usabilità

L'ingegneria dei fattori umani (HFE) è l'applicazione della conoscenza delle capacità umane (fisiche, sensoriali, emotive e intellettuali) e delle limitazioni umane alla progettazione e allo sviluppo di strumenti, dispositivi, sistemi, ambienti e organizzazioni. HFE potrebbe anche essere chiamato fattori umani, ergonomia, ingegneria umana, ingegneria dell'usabilità o interazione uomo-computer (HCI).

L'HFE prevede l'uso di scienze comportamentali e metodologie ingegneristiche a supporto della progettazione e della valutazione.

3.1.1 Interazione uomo – macchina

Il lavoro dei fattori umani relativo ai computer può essere approssimativamente suddiviso in argomenti relativi alla progettazione dell'hardware, alla funzionalità del software e alla progettazione dell'interfaccia del software. [10]

- *Funzionalità* si riferisce a ciò che l'utente può fare con il software e come supporta o sostituisce le attività umane.

- ***Interfaccia software o interazione uomo-computer HCI*** si riferisce alle informazioni fornite dal computer che vediamo o ascoltiamo e ai meccanismi di controllo per l'immissione di informazioni nel computer. Attualmente, per la maggior parte dei computer, ciò significa schermo, tastiera e mouse. I software che aumentano la produttività devono essere utili (fornire le funzionalità appropriate) e utilizzabili (disporre di un'interfaccia che possa essere utilizzata facilmente). Un'interfaccia ben progettata non garantisce un prodotto utile.

- Per quanto riguarda l'*hardware*, le workstation informatiche dovrebbero essere progettate per massimizzare le prestazioni delle attività e ridurre al minimo i problemi oi rischi ergonomici, come i disturbi da trauma cumulativo.

Una buona progettazione dell'interfaccia software deve tenere conto delle capacità cognitive e percettive degli esseri umani. La progettazione dell'interfaccia richiede anche l'applicazione dei principi di visualizzazione e controllo. Infine, il processo di interazione uomo-computer (HCI) influenzerà e/o sarà influenzato da altri fattori come affaticamento, carico di lavoro mentale, stress e ansia.

3.1.2 Riferimenti normativi per i dispositivi medici

Il successo dello sviluppo di dispositivi e sistemi medici sicuri e utilizzabili richiede l'applicazione dei principi e dei processi HFE durante tutto il ciclo di progettazione del prodotto. Ciò può aiutare a ridurre l'errore di utilizzo, migliorare la sicurezza del paziente e dell'utente, migliorare l'usabilità e l'efficienza del prodotto e aumentare la soddisfazione dell'utente. La relazione tra HFE e gestione del rischio nella riduzione dell'errore d'uso è trattata nella Commissione elettrotecnica internazionale (IEC) 62366-1:2015, Dispositivi medici – Applicazione dell'ingegneria dell'usabilità ai dispositivi medici.

La gestione del rischio è un processo decisionale per determinare il rischio accettabile, mentre l'ingegneria dell'usabilità è un processo di progettazione e sviluppo dell'interfaccia utente per ridurre la possibilità di errori di utilizzo che potrebbero causare danni.

3.2 Processo di usabilità

USABILITÀ è la caratteristica dell'interfaccia utente che ne facilita l'uso e quindi stabilisce l'efficacia, l'efficienza e la soddisfazione dell'utente nell'ambiente di utilizzo previsto.

NOTA 1 all'ingresso: tutti gli aspetti dell'usabilità, inclusi EFFICACIA, EFFICIENZA E SODDISFAZIONE DELL'UTENTE, possono aumentare o diminuire la SICUREZZA.

(3.23 *Usability*, [11])

3.2.1 Riferimenti normativi: IEC 62366-1

Introduzione

Il processo di ingegneria dell'usabilità ha lo scopo di identificare e ridurre al minimo gli errori d'uso e quindi ridurre i rischi associati all'uso. Alcune, ma non tutte, le forme di uso scorretto sono idonee al controllo da parte del produttore. Il processo di ingegneria dell'usabilità è correlato al processo di gestione del rischio.

IEC 62366-1 è uno standard internazionale che descrive un processo di ingegneria dell'usabilità per fornire un rischio accettabile correlato all'usabilità di un dispositivo medico. Questo standard si concentra rigorosamente sull'applicazione del processo di ingegneria dell'usabilità per ottimizzare l'usabilità dei dispositivi medici in relazione alla sicurezza.
La relazione tecnica complementare (IEC 62366-2) è completa e ha un focus più ampio. Si concentra non solo sull'usabilità in relazione alla sicurezza, ma anche su come l'usabilità si riferisce ad attributi come accuratezza, completezza ed efficienza dell'attività e soddisfazione dell'utente.

Perché?

Lo scopo della norma è quello di fornire, tramite l'uso del processo dell'ingegneria dell'usabilità, gli strumenti per valutare e mitigare i rischi associati all'uso normale di un dispositivo medico.

In generale il processo dell'ingegneria dell'usabilità permette di identificare i rischi associati anche all'uso anomalo del dispositivo ma non prevede la loro valutazione e mitigazione.

In particolare, l'obiettivo della norma è quello di minimizzare la possibilità che un errore d'uso, che dipende da una scarsa progettazione delle interfacce utente, possa causare il verificarsi di una situazione pericolosa.

Metodi di uso di un dispositivo medico

Al fine di chiarire lo scopo della norma è utile definire prima i metodi di uso di un dispositivo medico (le seguenti definizioni sono prese direttamente dalla norma). L'uso di un dispositivo medico si suddivide in:

- USO NORMALE: funzionamento, comprese le ispezioni e le regolazioni di routine da parte di qualsiasi utilizzatore, e stand-by, secondo le istruzioni per l'uso o secondo la prassi generalmente accettata per quei dispositivi medici forniti senza istruzioni per l'uso.

  L'uso normale si suddivide a sua volta in:
  - UTILIZZO CORRETTO: utilizzo normale senza errori d'uso

  - ERRORE D'USO: azione dell'utente o mancata azione dell'utente durante l'utilizzo del dispositivo medico che porta ad un risultato diverso da quello previsto dal produttore o previsto dall'utente

- UTILIZZO ANOMALO: atto consapevole, deliberato o omissione deliberata di un atto contrario o che violi il normale utilizzo e che esula anche da ogni ulteriore ragionevole mezzo di controllo del rischio relativo all'interfaccia utente da parte del produttore.

Lo schema seguente (Figura 3.1) mostra la correlazione tra i concetti sopra definiti.

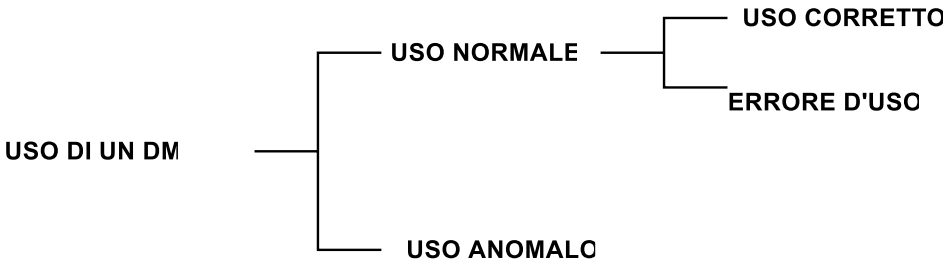


Figura 3.1. Schema dei metodi di utilizzo di un DM

Errore d'uso

È bene chiarire che, in base alla definizione sopra citata, sono considerati errori d'uso solo gli errori che avvengono nella fase di azione del ciclo di interazione tra software e utente, come rappresentato nella Figura 3.2 di seguito estratta dalla norma.

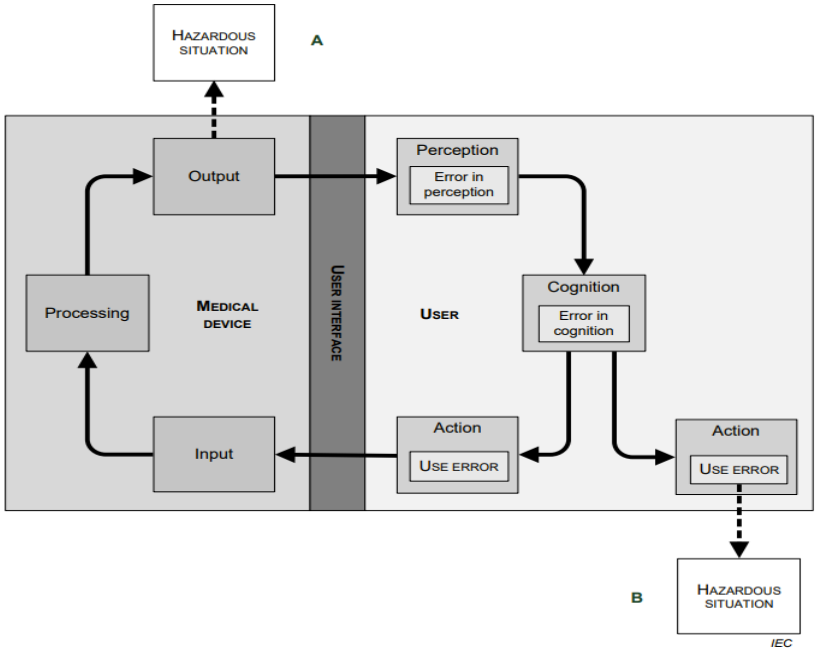


Figura 3.2. Modello di interazione utente-dispositivo medico ed errore di utilizzo correlato al pericolo

Un errore d'uso può causare due tipologie di situazioni pericolose:

- *la situazione pericolosa causata dalla risposta del dispositivo medico*: l'errore d'uso consiste in un input errato al dispositivo che a sua volta produce un output che conduce direttamente alla situazione pericolosa (caso A);

- *la situazione pericolosa causata da un'azione dell'utente o mancanza di azione* (sul paziente o con un diverso dispositivo medico) basata sulle informazioni ottenute dal dispositivo: l'errore d'uso si verifica nell'ambiente d'uso e non all'interfaccia con il dispositivo (caso B)

In generale, un utente percepisce le informazioni (e.g. legge le informazioni sul display), trasforma cognitivamente queste informazioni (e.g. interpreta le informazioni sul display) e decide di compiere un'azione (e.g. premere un bottone sull'interfaccia).

Pertanto, gli errori causati da un problema di percezione (e.g. errore di lettura) oppure di interpretazione delle informazioni non sono considerati errori d'uso ma piuttosto eventi che concorrono ad esso.

Si precisa inoltre che un errore d'uso non comporta necessariamente il verificarsi di una situazione pericolosa e che una situazione pericolosa non determina necessariamente un danno: lo stesso errore d'uso può causare un danno in una situazione e non essere dannoso in un'altra.

Sulla base di ciò, tutti gli errori d'uso che possono causare una situazione pericolosa sono soggetti al processo dell'ingegneria dell'usabilità.

3.2.2 Fasi del processo

Il processo dell'ingegneria dell'usabilità descritto in questa norma è un processo di sviluppo delle interfacce che prevede lo studio iniziale, la progettazione, l'implementazione e la verifica finale di esse, facendo in parte anche riferimento alla norma ISO 14971 sulla gestione del rischio. In particolare, le attività previste dalla norma sono:

I. Identificazione delle specifiche d'uso

Il processo inizia con l'identificazione delle caratteristiche più importanti del dispositivo associate al suo uso quali, ad esempio, l'indicazione medica, gli utenti previsti, l'ambiente di utilizzo e il principio di funzionamento, fondamentali per identificare le caratteristiche delle interfacce utente correlate alla sicurezza e i potenziali errori d'uso associati che possono verificarsi.

II. Identificazione delle caratteristiche delle interfacce utente correlate alla sicurezza e a potenziali errori d'uso

III. Identificazione dei pericoli e situazioni pericolose conosciuti e prevedibili

L'identificazione delle caratteristiche delle interfacce utente correlate alla sicurezza deve essere parte dell'analisi del rischio effettuata conformemente alla norma ISO 14971, così come quella dei danni e delle situazioni pericolose conosciute e prevedibili.

IV. Identificazione e descrizione degli scenari d'uso connessi ai pericoli

Gli scenari d'uso connessi ai pericoli sono definiti come la serie di azioni condotte da uno specifico utente in uno specifico ambiente e la conseguente risposta del dispositivo medico che possono condurre ad una situazione pericolosa.
La descrizione di tali scenari deve includere tutte le azioni previste e la loro sequenza, oltre la severità del danno che possono causare. Inoltre, nell'identificare gli scenari d'uso il fabbricante deve esaminare non solo le azioni che intende far eseguire dall'utente, ma anche quelle che non intende far eseguire ma che sono ragionevolmente prevedibili.

V. Selezione degli scenari d'uso connessi ai pericoli per cui svolgere una valutazione sommativa

La selezione degli scenari d'uso connessi ai pericoli, per i quali bisogna svolgere una valutazione sommativa al termine del processo di progettazione, implementazione e valutazione formativa delle interfacce, dovrebbe avvenire sulla base del rischio (*severità del pericolo x probabilità del pericolo*). Specialmente per i nuovi dispositivi, di cui non si hanno dati derivanti dalla post-commercializzazione, la probabilità, componente del rischio, è spesso difficile da valutare per cui è possibile considerare esclusivamente la gravità che le possibili conseguenze di un pericolo possono comportare per la valutazione del rischio.

VI. Definizione delle specifiche delle interfacce utente

Le specifiche delle interfacce utente devono essere definite sulla base delle specifiche d'uso, gli errori d'uso e scenari d'uso connessi ai pericoli identificati e devono garantire che i rischi, associati all'usabilità del dispositivo, siano accettabili.

VII. Creazione di un piano di valutazione delle interfacce utente

Il piano di valutazione deve comprendere la pianificazione della valutazione formativa, della valutazione sommativa e, se del caso, le informazioni riguardanti i test di usabilità.

VIII. Progettazione, implementazione e valutazione formativa delle interfacce utente

La valutazione formativa è una valutazione condotta iterativamente *durante* il processo di progettazione e sviluppo delle interfacce, al fine di identificare i punti di forza del dispositivo, le debolezze e gli errori d'uso precedentemente non previsti.

Essa consiste nel sottoporre il dispositivo alla valutazione di un gruppo di utenti e la sua pianificazione deve documentare l'obiettivo e definire sia i metodi che vengono adottati sia quale parte delle interfacce valutare.

In generale, l'obiettivo della valutazione formativa è quello di iterare la progettazione delle interfacce utente, fintanto che non sia raggiunto il livello di qualità sufficiente, che si pensi garantisca il soddisfacimento del criterio di accettazione finale della valutazione sommativa.

IX. Progettazione, implementazione e valutazione sommativa dell'usabilità delle interfacce utente

A differenza della valutazione formativa, la valutazione sommativa prevede un criterio formale di accettazione finale, come può essere l'assenza di errori d'uso che comportano un danno, o l'assenza di errori d'uso che comportano un rischio inaccettabile di danno.

La valutazione sommativa è infatti una valutazione condotta *alla fine* dello sviluppo delle interfacce utente, allo scopo di ottenere delle evidenze oggettive della sicurezza del dispositivo in relazione alla sua usabilità.

Obiettivo della valutazione sommativa è simulare un uso realistico del dispositivo, per valutare se utenti reali riescono a completare le attività previste in uno scenario d'uso connesso a pericoli. Per essere realistica, gli utenti sottoposti al test di usabilità devono quindi ricevere la formazione necessaria e la documentazione di accompagnamento, quale ad esempio le istruzioni per l'uso.

La pianificazione della valutazione sommativa deve specificare i metodi che vengono adottati e le motivazioni per cui essi si reputano sufficienti per ottenere le evidenze oggettive, le informazioni specifiche relative il test di usabilità, le parti delle interfacce da valutare, la documentazione di accompagnamento e l'attività di formazione degli utenti necessaria.

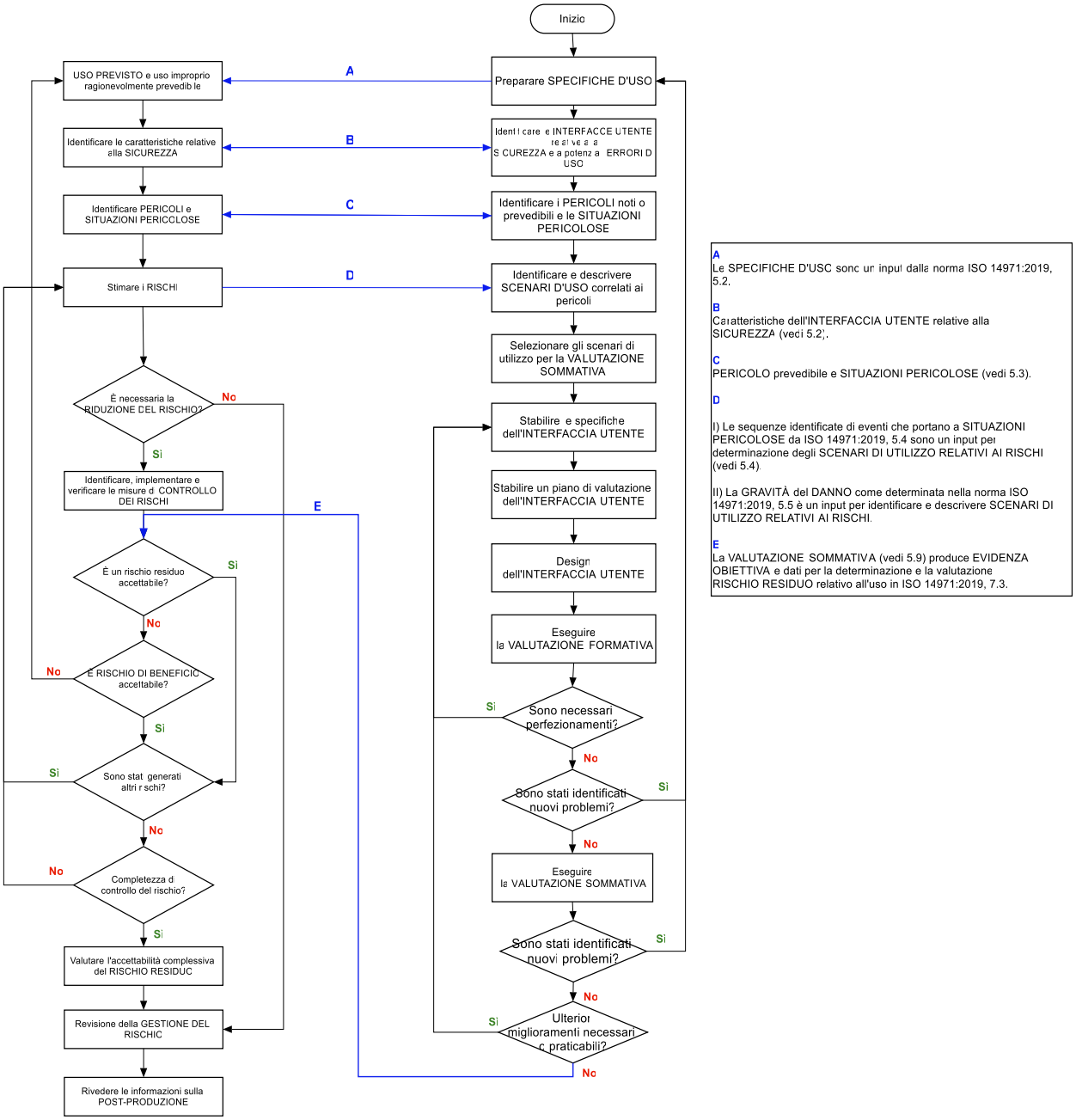
Del test di usabilità condotto si devono specificare l'ambiente e le condizioni d'uso, nonché i metodi da usare per ottenere i dati necessari per una successiva valutazione degli errori d'uso. Oltre a questi, sono da valutare anche le difficoltà riscontrate dagli utenti durante l'uso del dispositivo: in differenti condizioni e per diversi utenti la stessa difficoltà potrebbe causare o meno un errore d'uso.

La valutazione sommativa è quindi la fase finale del processo dell'ingegneria dell'usabilità e consiste sostanzialmente nella validazione degli aspetti di sicurezza associati all'uso delle interfacce utente.

Conclusioni

Se a seguito di tale valutazione non sono identificati nuovi errori d'uso, pericoli, situazioni pericolose o scenari d'uso associati a pericoli e non sono possibili ulteriori miglioramenti delle interfacce utente, il processo può considerarsi concluso se sono stati valutati anche i rischi residui in accordo con la norma ISO 14971.

Il flowchart di seguito riporta le attività previste dalla norma e appena descritte, per una visione schematica del processo.



Flowchart 3.1 Processo di Usabilità di DMSW: relazione con il processo di gestione dei rischi

3.3 Metodi di valutazione dell'usabilità delle interfacce utente

Valutazione dell'interfaccia utente: processo mediante il quale il produttore esplora o valuta le interazioni dell'utente con l'interfaccia utente.

*NOTA 1 alla voce: una valutazione dell'interfaccia utente può consistere in una o più delle seguenti tecniche, tra le altre, **test di usabilità**, revisioni di esperti, **analisi euristiche**, audit di progettazione o un percorso cognitivo.*

NOTA 2 alla voce: la valutazione dell'interfaccia utente viene spesso eseguita in modo iterativo durante il processo di progettazione e sviluppo (questa è valutazione formativa).

NOTA 3 all'ingresso: la valutazione dell'interfaccia utente è una parte delle attività coinvolte nella verifica e valida della progettazione complessiva del dispositivo medico (questa è valutazione sommativa).

(3.27 *User interface evaluation*, [11])

I principali metodi di valutazione di un'interfaccia software sono l'analisi euristica e i test di usabilità.

Di seguito vengono descritte le principali caratteristiche e gli iter procedurali di entrambi i metodi sopracitati.

3.3.1 Analisi euristica

L'aggettivo *euristico* si usa, in matematica, per denotare un procedimento non rigoroso che consente di prevedere o rendere plausibile un determinato risultato, che in un secondo tempo dovrà essere controllato e convalidato con metodi rigorosi. Nell'ingegneria dell'usabilità, si chiamano euristiche quelle valutazioni di usabilità effettuate da esperti, analizzando il comportamento di un sistema e verificandone la conformità a specifiche "regole d'oro" (chiamate, appunto, euristiche), derivanti da principi o linee guida generalmente accettati. In pratica, per eseguire una valutazione euristica, l'esperto di usabilità dovrebbe considerare una regola euristica alla volta, ed esaminare dettagliatamente le funzioni del sistema, per verificarne la conformità.

Le euristiche impiegate sono diverse. In letteratura se ne trovano alcune costituite da centinaia di regole dettagliate. È evidente che valutare un sistema in base a una tale quantità di regole risulta impraticabile. Si preferisce quindi, più spesso, utilizzare euristiche costituite da pochi principi guida generali. Fra queste, sono molto note le euristiche di Nielsen e Schneiderman, costituite da dieci regole che, sebbene molto generali, permettono al valutatore di inquadrare i problemi rilevati in categorie bene individuate.

Una guida consolidata per la progettazione di buone interfacce utente è stata sviluppata da due importanti esperti, Nielsen, con le *sue 10 usability heuristics for User Interface Design* e Schneiderman con le *sue Eight Golden Rules of Interface Design*. Più recentemente, Zhang ha combinato e adattato questi principi di progettazione in 14 euristiche di usabilità per facilitare l'analisi euristica dei dispositivi medici. Durante l'analisi, vengono identificate le caratteristiche

di progettazione che violano una o più euristiche. Per ogni violazione, i valutatori identificano quali problemi di utilizzo probabilmente sorgeranno a seguito della violazione e il potenziale impatto di ciascun problema di utilizzo.

Fasi dell'analisi

I. Identificazione dei valutatori

Questa tecnica richiede che tre o più valutatori applichino in modo indipendente una serie di euristiche di usabilità o linee guida di progettazione dell'interfaccia utente a un prodotto, identifichino le violazioni dell'euristica e valutino la gravità di ciascuna violazione.

Esempi di euristica di usabilità e linee guida di progettazione sono descritti nelle sezioni successive.

II. Stesura di un elenco di tutte le attività svolte con l'interfaccia utente ("Task list")

Utilizzando qualsiasi osservazione della tecnologia e qualsiasi dato di intervista, viene prima creato un elenco passo-passo o una descrizione delle attività svolte con la tecnologia. Le attività devono includere tutte le attività eseguite da tutti i gruppi di utenti, in particolare le attività critiche per la sicurezza o lo scenario peggiore. Si raccomanda di condurre osservazioni a sostegno dello sviluppo dell'elenco delle attività.
Questo elenco di attività verrà utilizzato per guidare ogni valutatore passo dopo passo attraverso la loro analisi euristica. È importante considerare l'intera gamma di compiti nell'analisi euristica poiché è molto più facile farlo con questo metodo rispetto ad altri metodi di valutazione dei fattori umani come i test di usabilità.

III. Pianificazione di una scala di gravità

L'obiettivo della valutazione è identificare i problemi di progettazione che hanno il potenziale di causare problemi di sicurezza e usabilità. Prima di identificare qualsiasi problema di sicurezza e usabilità, è necessario assegnare un livello di gravità per assegnare i problemi ad alta priorità e per facilitare un confronto tra i prodotti, se l'analisi viene eseguita per supportare una valutazione comparativa. La Tabella 2 mostra una scala di valutazione della gravità che è stata adattata in base al lavoro di Zhang et al.

Tabella 2. Scala di gravità secondo Zhang

Livello di gravità	Descrizione
0	Non è un problema di usabilità. *Nessuna correzione richiesta.*
1	Problema solamente estetico. *Non deve essere risolto a meno che non sia disponibile tempo extra.*
2	Problema di usabilità minore. *La risoluzione di questo problema dovrebbe avere una priorità bassa.*
3	Problema di usabilità Maggiore. *Risolvere questo problema è importante e dovrebbe avere la massima priorità.*
4	Problema di usabilità catastrofico. *La correzione di questo è fondamentale e deve essere eseguita prima che il prodotto possa essere rilasciato.*

IV. Confronto dell'elenco delle attività con l'euristica dell'usabilità

Questo è il nucleo della valutazione euristica. In primo luogo, vengono identificati i principi di progettazione dell'interfaccia più rilevanti, che affrontano i compiti del prodotto. Il secondo passo consiste nell'applicare le linee guida, i principi e l'euristica selezionati all'elenco delle attività del prodotto. I potenziali problemi di usabilità vengono identificati quando l'interfaccia viola una o più euristiche.

V. Identificazione e quantificazione di qualsiasi euristica violata

Eventuali violazioni dei principi o osservazioni sulla tecnologia devono essere registrate su una scheda di raccolta dati dal valutatore.
Quando si descrive la conseguenza di una violazione o di un problema, è importante farlo in relazione agli obiettivi o allo scopo della tecnologia.
Descrivere le conseguenze in termini di obiettivi o scopo del sistema rende più facile assegnare i livelli di gravità poiché il livello di gravità dovrebbe essere lo stesso per tutti i problemi con le stesse conseguenze.

VI. Selezione delle violazioni più critiche e assegnazione di raccomandazioni o azioni proposte

Una volta determinati i livelli di gravità per ogni problema di usabilità, il foglio di calcolo della raccolta dati deve essere organizzato in modo da evidenziare le violazioni più gravi. Generare un elenco di raccomandazioni o azioni proposte per affrontare ogni grave violazione può essere utile a seconda del contesto dell'analisi euristica. Se possibile, le violazioni ritenute gravi dovrebbero essere affrontate immediatamente in base alle azioni raccomandate identificate.

Tipi di euristiche

- **Nielsen e Shneiderman**

  Nielsen e Shneiderman sono i primi ad aver raggruppato alcune linee guida sull'usabilità, che potevano essere più predittive delle difficoltà comuni degli utenti rispetto ad altre, in un piccolo numero di fattori di usabilità: *10 Usability Heuristics for User Interface Design* (Nielsen) e *Eight Golden Rules of Interface Design* (Shneiderman). Vengono di seguito esplicitate le euristiche di entrambi in un'unica tabella (Tabella 3):

Tabella 3. Euristiche di Nielsen e Shneiderman

Nielsen: ***10 euristiche di usabilità per il design di un'interfaccia utente***	**Shneiderman:** ***8 regole d'oro per il design di un'interfaccia* (software)**
1. Visibiltà dello stato di sistema	**1.** Cercare la coerenza
2. Corrispondenza tra il Sistema e il mondo reale	**2.** Consentire agli utenti frequenti di utilizzare le scorciatoie
3. Controllo e libertà all'utente	**3.** Offrire feedback informativi
4. Consistenza e standard	**4.** Progettare forme di dialogo per chiudere il sistema
5. Prevenire errori, riconoscerli e correggerli	**5.** Offrire una semplice gestione degli errori
6. Riconoscere piuttosto che richiamare	**6.** Consentire una facile inversione delle azioni
7. Flessibilità ed efficienza d'uso	**7.** Supportare il luogo di controllo interno
8. Estetica e minimalismo nel design	**8.** Ridurre il carico di memoria a breve termine
9. Aiutare gli utenti a riconoscere, analizzare e imparare dagli errori	
10. Aiuto e documentazione	

- **Zhang**

  Jiajie Zhang ha combinato e adattato questi principi di progettazione in 14 euristiche di usabilità per facilitare l'analisi euristica dei dispositivi medici (Tabella 4).

Tabella 4. Le 14 Euristiche di Nielsen–Shneiderman, (o Euristiche di Zhang)

Zhang ***14 Euristiche di usabilità Nielsen – Shneiderman*** [12]	
Euristica	**Descrizione**
1. Consistenza e standard *[Consistenza]*	Gli utenti non dovrebbero chiedersi se parole, situazioni o azioni diverse significhino la stessa cosa. Gli standard e le convenzioni nella progettazione del prodotto dovrebbero essere seguiti:Sequences of actions (skill acquisition); – Colore (categorizzazione); – Layout e posizione (coerenza spaziale); – Carattere, maiuscolo (livelli di organizzazione); – Terminologia (cancella, cancella, rimuovi, rm) e lingua (parole, frasi); – Standard (ad es. testo sottolineato in blu per collegamenti ipertestuali non visitati).
2. Visibilità dello stato di sistema *[Visibilità]*	Gli utenti dovrebbero essere informati su cosa sta succedendo con il sistema attraverso un feedback appropriato e la visualizzazione di informazioni: - Qual è lo stato attuale del sistema? - Cosa si può fare allo stato attuale? - Dove possono andare gli utenti? - - Quale modifica viene apportata dopo un'azione?
3. Corrispondenza tra Sistema e mondo reale *[Corrispondenza]*	L'immagine del sistema percepita dagli utenti dovrebbe corrispondere al modello che gli utenti hanno sul sistema: User model matches system image; - Le azioni fornite dal sistema devono corrispondere alle azioni eseguite dagli utenti; - Gli oggetti nel sistema devono corrispondere agli oggetti dell'attività.
4. Minimalista *[Minimalista]*	Qualsiasi informazione estranea è una distrazione e un rallentamento: - Meno è meglio; - Semplice non equivale ad astratto e generale; - Semplice è efficiente; - - Livelli di dettaglio progressivi.
5. Minimizzare il carico di memoria *[Memoria]*	Agli utenti non dovrebbe essere richiesto di memorizzare molte informazioni per svolgere attività. Il carico di memoria riduce la capacità degli utenti di svolgere le attività principali: - Riconoscimento vs. richiamo (es. menu vs. comandi); - Esternalizzare le informazioni attraverso la visualizzazione; - Procedure percettive; - Struttura gerarchica; - Valori standard; - Esempi concreti (GG/MM/AA, es. 20/10/99);

	- - Regole e azioni generiche (ad es. trascinare oggetti).
6. Feedback informativo *[Feedback]*	Gli utenti dovrebbero ricevere un feedback tempestivo e informativo sulle loro azioni: - Informazioni che possono essere percepite, interpretate e valutate direttamente; - Livelli di feedback (principiante ed esperto); - Concreti e specifici, non astratti e generali; - Tempo di risposta; o un. 0,1 s per reazione istantanea; o B. 1,0 s per un flusso di pensiero ininterrotto; o C. 10 s per il limite di attenzione.
7. Flessibilità ed efficienza *[Flessibilità]*	Gli utenti imparano sempre e gli utenti sono sempre diversi. Offri agli utenti la flessibilità di creare personalizzazioni e scorciatoie per accelerare le loro prestazioni: - Scorciatoie per utenti esperti; - Scorciatoie o macro per operazioni di uso frequente; - Acquisizione di abilità tramite chunking; Esempi: abbreviazioni, tasti funzione, tasti di scelta rapida, tasti di comando, macro, alias, modelli, type-ahead, segnalibri, hot link, cronologia, valori predefiniti, ecc.
8. Messaggi d'errori efficaci *[Messaggio]*	I messaggi dovrebbero essere sufficientemente informativi in modo che gli utenti possano comprendere la natura degli errori, imparare dagli errori e recuperare dagli errori: - Formulato in un linguaggio chiaro, evita codici oscuri. - Esempio di codice oscuro: ''sistema bloccato, codice di errore 147.''; - Preciso, non vago o generico. Esempio di commento generale: ''Impossibile aprire il documento.''; - Costruttivo; - Educato. Esempi di messaggio scortese: ''azione utente illegale'', ''lavoro interrotto'', ''sistema bloccato'', ''errore irreversibile'', ecc.
9. Prevenire errori *[Errore]*	È sempre meglio progettare interfacce che impediscano il verificarsi di errori nel file primo posto: - Interfacce che rendono impossibili gli errori; - Evita le modalità o utilizza feedback informativi, ad es. suoni diversi; - Errore di esecuzione vs. errore di valutazione; - Vari tipi di lapsus ed errori.
10. Chiusura chiara *[Chiusura]*	Ogni compito ha un inizio e una fine. Gli utenti dovrebbero essere chiaramente informati del completamento di un'attività: - Cancella inizio, metà e fine; - Completa 7 fasi di azioni.

	- Feedback chiaro per indicare che gli obiettivi sono stati raggiunti e possono essere rilasciati gli attuali stack di obiettivi. Esempi di buone chiusure includono molti dialoghi.
11. Azioni reversibili *[Reversibilità]*	Gli utenti dovrebbero essere autorizzati a recuperare dagli errori. Le azioni reversibili incoraggiano anche l'apprendimento esplorativo: - A diversi livelli: una singola azione, un sottocompito o un compito completo; - Più passaggi.
12. Usare il linguaggio dell'utente *[Linguaggio]*	La lingua deve essere sempre presentata in una forma comprensibile agli utenti previsti: - Usa i significati standard delle parole; - Linguaggio specialistico per gruppo specializzato; - Alias definiti dall'utente; - Prospettiva degli utenti. Esempio: "abbiamo comprato quattro biglietti per te" (non valido) vs. "hai comprato quattro biglietti" (buono).
13. Utenti al controllo *[Controllo]*	Non dare agli utenti l'impressione di essere controllati dai sistemi: - Gli utenti sono artefici delle azioni, non rispondenti alle azioni; - Evita azioni sorprendenti, risultati inaspettati, noiose sequenze di azioni, ecc.
14. Aiuto e documentazione *[Documentazione]*	Fornisci sempre aiuto quando necessario: - Guida sensibile al contesto; - Quattro tipi di aiuto; - Un compito orientato; o in ordine alfabetico; o semanticamente organizzato; o ricerca. - Guida incorporata nei contenuti.

3.3.2 Test di usabilità

"Le teorie di design forniscono un quadro generale per i progettisti per concettualizzare il loro problema e discuterne, utilizzando un linguaggio indipendente dall'applicazione. I modelli possono fornire risposte più specifiche su come le persone potrebbero rispondere al sistema. Una teoria e un modello possono aiutare i progettisti a sviluppare un'idea generale delle capacità dell'utente, inclusa una descrizione dei tipi di attività cognitive che si svolgono durante l'uso del software". [10]

Anche un sistema attentamente progettato che utilizza le migliori teorie deve essere valutato nei test di usabilità.

I test di usabilità coinvolgono utenti tipici che utilizzano il sistema in situazioni realistiche. Le difficoltà e le frustrazioni che incontrano vengono registrate per identificare le opportunità per migliorare il software.

Fasi del test

I. **Elenco di tutte le attività di usabilità, individuate preliminarmente dal team di progettazione.**

II. **Definizione di tutti gli scenari di attività, al fine di svolgere come utenti reali coinvolti sarebbe in circostanze normali.**

III. **Osservazione, registrazione video e cronometraggio degli utenti, durante l'utilizzo del software per eseguire attività.**

Prototipi tipicamente utilizzati nei test di usabilità:

- Modelli a bassa fedeltà: nelle prime fasi del processo di progettazione,
  - Esempio: schede, adesivi, disegni su carta e penna e storyboard.
- Modelli ad alta fedeltà in fase finale,
  - Esempio: schermi completamente interattivi con l'aspetto grafico.

IV. **Valutazione del compito svolto**

Le metriche di usabilità tendono a cambiare natura e ambito man mano che il progetto va avanti.

- Valutazione qualitativa, per i modelli a bassa fedeltà:
  Sono pochi gli utenti coinvolti e la valutazione qualitativa dell'usabilità generale e della soddisfazione degli utenti viene valutata semplicemente parlando con loro.
  Esempio di valutazione qualitativa: se il compito può essere svolto anche utilizzando il sistema

- Metriche di usabilità, per modelli ad alta fedeltà:
  Tutti gli utenti sono coinvolti e la misurazione quantitativa viene valutata, osservandoli.
  La valutazione quantitativa viene applicata per misurare l'efficacia, l'efficienza e la soddisfazione degli utenti, come quella mostrata nella Tabella 5 (da Mayhew, 1992; Nielson, 1993), assegnando una scala di valutazione per ciascuna metrica.

  Scala di valutazione che va da 1 = estremamente difficile da usare a 9 = estremamente facile da usare.

  Esempio di misure: tempo, tassi di errore, soddisfazione soggettiva.

Tabella 5. Metriche di usabilità

Efficacia	***Efficienza***	***Soddisfazione dell'utente***
- Punteggio di successo - N° di errori - Tasso di occorrenza degli errori (EOR)	- Tempo di attività - Efficienza basata sul tempo	- Domanda di facilità singola (SEQ) - Scala di usabilità del sistema (SUS)

V. Relazione su cosa è stato osservato e perché tale comportamento è stato osservato

Un test di usabilità efficace non deve, e forse non dovrebbe contenere prescrizioni su come risolvere il problema di usabilità.

PARTE II

Gestione del rischio e usabilità

di una Cartella Clinica Elettronica

4. Gestione del rischio di una cartella clinica elettronica

4.1 Introduzione

Con l'entrata in vigore del nuovo regolamento europeo UE 2017/745, i software medici devono essere certificati come dispostivi medici (DM) **classe IIA**, salvo quelli finalizzati unicamente ad archiviare, memorizzare e trasmettere dati senza effettuare alcuna elaborazione dei dati stessi.

Oggetto del lavoro svolto è stato il dispositivo medico software stand-alone prodotto, per uso interno, da una Azienda Ospedaliero-Universitaria.

4.2 Descrizione del dispositivo medico software

Caratteristiche del prodotto

Il dispositivo medico software in esame è una cartella clinica elettronica con funzionalità riguardanti attività ospedaliere inerenti agli aspetti di cura, assistenza e tracciabilità delle attività clinico-assistenziali ed amministrative. Esso mette a disposizione al suo interno anche numerose funzionalità riguardanti l'attività quotidiana di reparto, ambulatorio e attività amministrative.

Destinazione d'uso e classificazione

Il software analizzato è un dispositivo medico, utilizzato per la gestione organica e strutturata dei dati riferiti alla storia clinica di un paziente, garantendo il supporto dei processi clinici (diagnostico-terapeutici) e assistenziali nei singoli episodi di cura e favorendo la continuità di cura del paziente tra diversi episodi di cura afferenti alla stessa struttura ospedaliera mediante la condivisione e il recupero dei documenti clinici in essi registrati.

Il supporto dei processi clinici, nel dispositivo, è fornito dalle soglie degli allarmi per la memorizzazione dei parametri di trattamento e dei valori di taratura. Esempi:

Parametri di trattamento: presenza di allergie, prescrizioni terapeutiche e procedure cliniche di un paziente.

Valori di taratura: soglie inferiori e superiori per l'inserimento di dati clinici di un paziente.

Ai sensi del MDR 2017/745 e della Regola 11 (vedi citazione e descrizione della regola nel cap. 1, par.1.4 *Classificazione di dispositivi medici*), il dispositivo medico software rientra dunque in classe IIa.

Funzionalità principali

Viene proposto un elenco, anche se parzialmente esaustivo, delle funzionalità a disposizione delle SOD, degli ambulatori e dei servizi amministrativi.

- Strutture Organizzative Dipartimentali (SOD)

  Il sistema gestisce il paziente nei vari passaggi:

  1. Ammissione in reparto, con recupero dei dati anagrafici dall'anagrafe Centrale, e disbrigo della parte burocratica compreso l'aggiornamento automatico ADT, gestione Osservazione Breve, e stampa dei vari *barcode*
  2. Recupero dello storico del paziente sia locale che aziendale
  3. Compilazione dell'anamnesi da parte del Medico accettante con accesso automatico allo storico anamnestico
  4. Compilazione e stampa delle varie richieste di consulenze ed esami strumentali
  5. Compilazione della terapia con accesso automatico all'archivio della farmacia aziendale
  6. Gestione del magazzino farmaci
  7. Compilazione della cartella infermieristica
  8. Gestione dei trasferimenti sia interni che negli altri reparti con aggiornamento ADT
  9. Interrogazione e recupero automatico dei risultati degli esami di laboratorio
  10. Gestione quotidiana della terapia e dei parametri vitali con possibilità di elaborazione dati e con sistema di allarmi vari delle scadenze
  11. Compilazione automatizzata e stampa dei certificati vari
  12. Compilazione automatizzata e stampa della SDO e della dimissione
  13. Compilazione automatizzata e stampa della relazione di degenza con stampa automatica delle ricette per i farmaci prescritti sui vari tipi di ricettario (aziendale, regionale, ecc)
  14. Stampa istantanea della cartella clinica
  15. Possibilità di salvataggio sia della cartella medica che infermieristica in formato PDF per RMA digitale
  16. Statistiche in tempo reale
  17. Gestione dell'archivio generale cartelle cartacee con tracciabilità delle stesse
  18. Trasmissione dei flussi regionali, in caso di OB, in maniera automatica
  19. Ricerche avanzate con possibilità di esportazione sia in formato XML che Excel

- Ambulatorio
  1. Gli appuntamenti nelle varie stanze
  2. Liste di attesa
  3. L'anamnesi dei pazienti
  4. Gli esami analitici e strumentali
  5. L'eventuale terapia compilazione e stampa automatizzata delle ricette
  6. La trasmissione dei flussi regionali in maniera automatica
  7. Statistiche in tempo reale
  8. Ricerche avanzate

- Utilities

  Il sistema mette a disposizione molte funzionalità utili nell'attività quotidiana del personale sanitario ed amministrativo di cui se ne propone un elenco parziale.

1. Sistema di posta interna e di consegne interpersonali
2. Agenda di impegni personali esportabile in iCal
3. Client e-mail integrato
4. Prontuario on line sia regionale che aziendale
5. Sistema ICD con i codici diagnosi e procedure
6. Calcolatrice con conversioni varie e calcolo dei flussi
7. gestione dell'orario medici, specializzandi ed infermieri

Interfaccia software

Il dispositivo è caratterizzato da più moduli operativi, diversi a seconda della destinazione d'uso del software. L'architettura del software è costituita da più interfacce software, diverse in funzione del profilo utente abilitato all'uso: cambiano sia il tipo di funzioni presenti nell'interfaccia di un profilo utente, sia il tipo di interazione di una stessa funzione tra utenti con destinazione d'uso diversa.

L'interfaccia software è caratterizzata da tre parti:

- Testata, in alto della pagina
- Menu laterale, a sinistra della pagina
- Schermata principale, al centro della pagina

Di seguito viene riportato un esempio per mostrare tale differenza, prendendo come riferimento il numero di funzioni presenti nella testata e nel menu laterale di interfacce di più profili utente con uguale destinazione d'uso: medica:

1. Medico

- Testata dell'interfaccia software

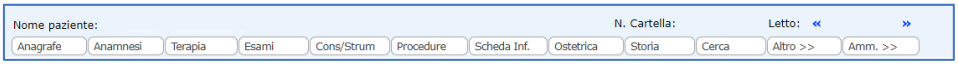


Figura 4.1. Testata dell'interfaccia software di un profilo medico

- Menu laterale dell'interfaccia software

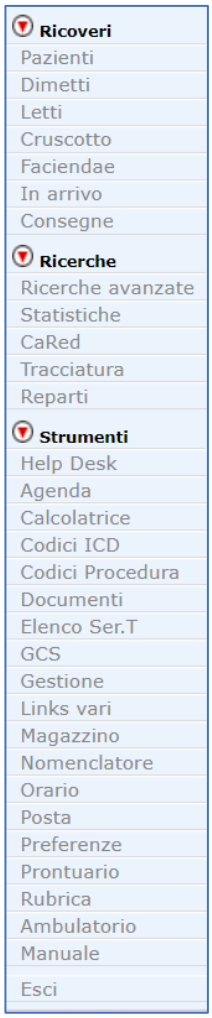


Figura 4.2. Menu laterale dell'interfaccia software di un profilo medico

2. Infermiere, OSS

- Testata dell'interfaccia software

Figura 4.3. Testata dell'interfaccia software di profili infermieri e OSS

- Menu laterale dell'interfaccia software

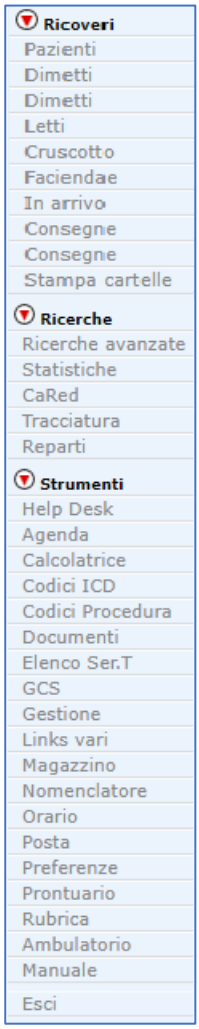


Figura 4.4. Menu laterale dell'interfaccia software di profili infermieri e OSS

3. Trasporto dei pazienti

- Testata dell'interfaccia software

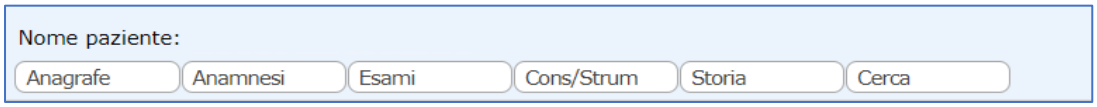


Figura 4.5. Testata di un profilo trasporto dei pazienti

- Menu laterale dell'interfaccia software

Figura 4.6. Menu laterale di un profilo trasporto dei pazienti

Tale differenza risulta sia nell'interfaccia software tra profili utente con destinazioni d'uso diverse (es. medica/amministrativa), sia la stessa destinazione d'uso ma con competenze professionali diverse(medico/infermiere/OSS): nel primo caso la differenza si verifica nel numero e tipologia di funzioni, nel secondo caso si verifica nel tipo di interazione di una stessa funzione.

Di seguito viene mostrato un esempio per mostrare tale differenza, prendendo di riferimento la schermata principale di un modulo operativo comune a tre profili utente con uguale destinazione d'uso ma con interfaccia software diversa.

- Destinazione d'uso: **Medica**
  - Profili utente: medico, infermiere, OSS

- Modulo operativo di riferimento: **Terapia**

1. Medico

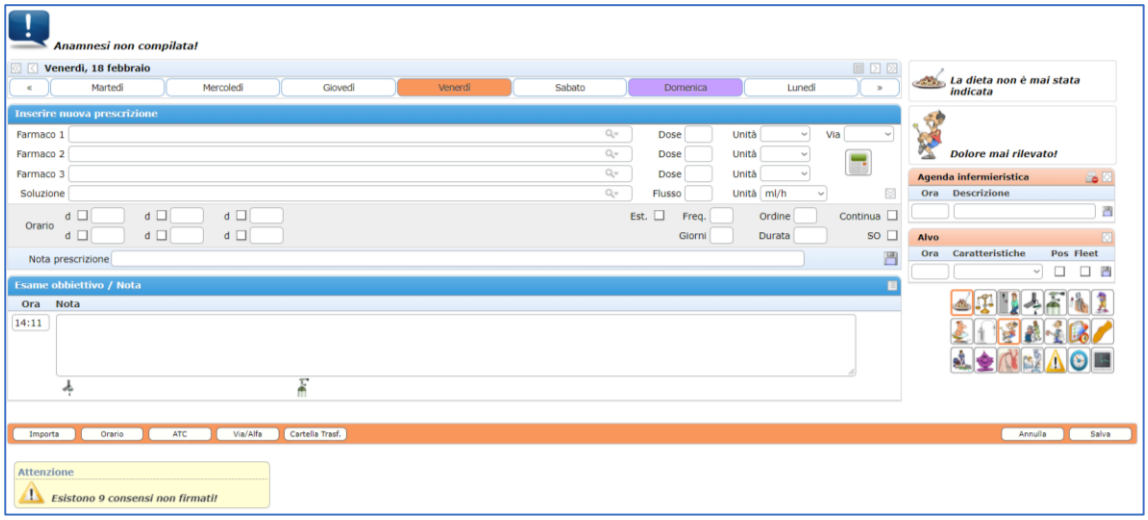


Figura 4.7. Schermata principale di un profilo medico

2. Infermiere

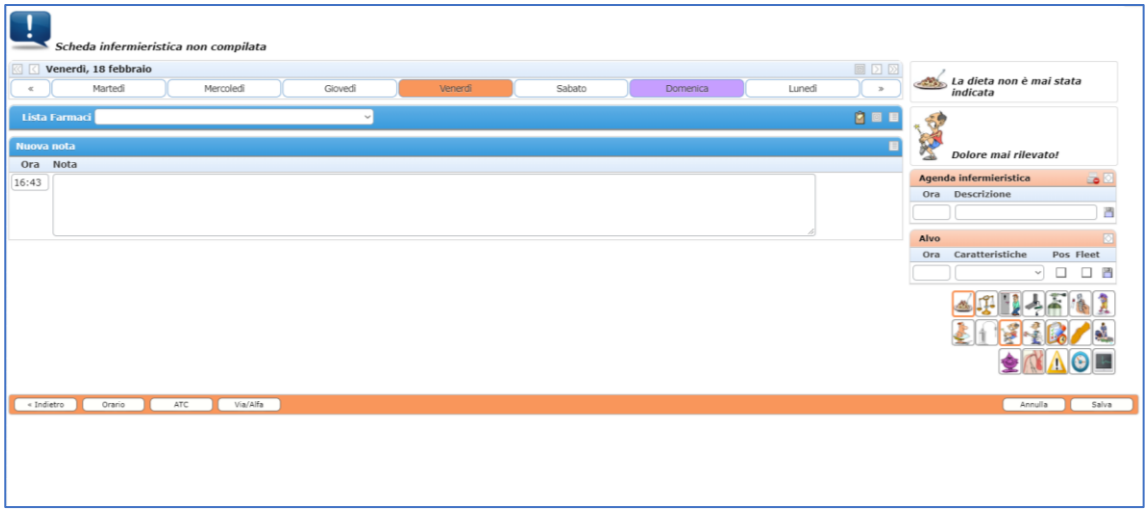


Figura 4.8. Schermata principale di un profilo infermiere

3. OSS

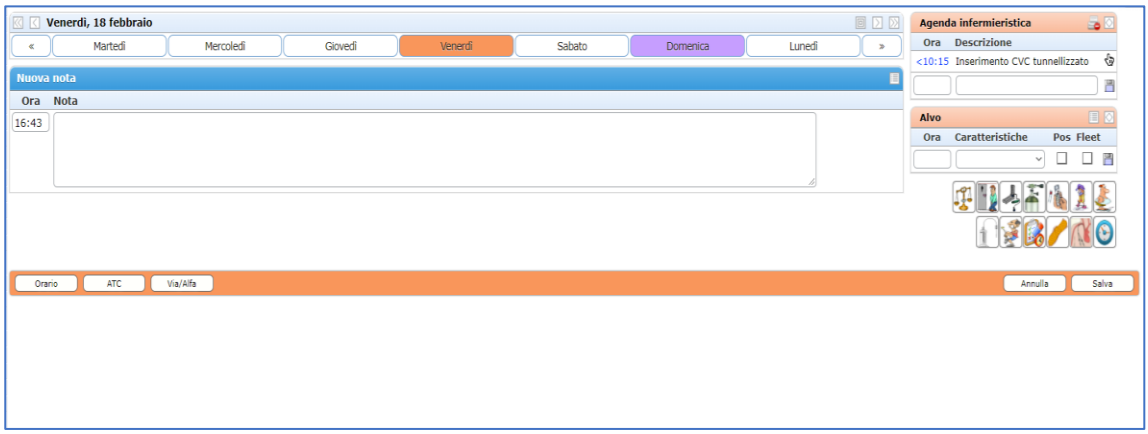


Figura 4.9. Schermata principale di un profilo OSS

Riferimenti normativi

Per ottenere la certificazione, i prodotti software devono rispettare i requisiti essenziali imposti dal regolamento: per rispettare i requisiti essenziali devono essere applicate le opportune procedure di conformità.

Per verificare la rispondenza del prodotto ai requisiti essenziali del regolamento è stato condotto il processo di gestione dei rischi durante tutte le fasi del ciclo di vita del prodotto.

Per condurre l'analisi sono state applicate le seguenti norme:

- IEC 62304:2006 - Medical device software — Software life-cycle processes [5]
- ISO 14971:2019 - Medical devices — Application of risk management to medical devices [6]

I prossimi paragrafi descrivono le fasi del processo che sono state applicate al prodotto; per ogni fase sono stati descritti i metodi utilizzati e i risultati ottenuti.

4.3 Identificazione della destinazione d'uso e i prevedibili usi impropri

Riferimenti normativi

Per definire la destinazione d'uso del dispositivo medico software sono stati considerati i seguenti riferimenti normativi:

- MDCG 2019-11 Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR [3]
- Manual on borderline and classification in the Community regulatory framework for medical devices, *Classificazione dei software per la gestione delle informazioni e il monitoraggio dei pazienti* [13]

Per identificare gli usi impropri sono stati dapprima identificati gli utilizzatori finali del prodotto e i loro profili, con particolare attenzione alle competenze informatiche richieste per l'utilizzo del prodotto (la descrizione dettagliata degli utenti e dei loro profili è descritta nel *paragrafo Identificazione delle specifiche d'uso* all'interno del capitolo successivo, P*rocesso di usabilità di una cartella clinica elettronica*).

4.3.1 Risultati

La destinazione d'uso del dispositivo medico software viene così definita:

- MDCG 2019-11, Annex I, *Qualification Electronic Patient Record Systems Software*:

  Cartella clinica elettronica di reparto (CCE), con lo scopo di archiviare e trasferire le cartelle cliniche elettroniche. Archivia tutti i tipi di documenti e dati relativi a un paziente specifico.

  Strumento digitale per la gestione organica e strutturata dei dati riferiti alla storia clinica di un paziente, garantendo il supporto dei processi clinici (diagnostico-terapeutici) e assistenziali nei singoli episodi di cura e favorendo la continuità di cura del paziente tra diversi episodi di cura afferenti alla stessa struttura ospedaliera mediante la condivisione e il recupero dei documenti clinici in essi registrati. [3]

- Manual on borderline and classification in the Community regulatory framework for medical devices, *Classificazione dei software per la gestione delle informazioni e il monitoraggio dei pazient*i:

  Sistema basato su software che include una gestione informatica e piattaforma di monitoraggio del paziente.

Per gestione informatica si intende la destinazione d'uso clinica di instradare e memorizzare i dati dei dispositivi medici e le informazioni diagnostiche sui dispositivi, trasferendoli dai dispositive supportati al posto letto alla cartella clinica elettronica e al sistema informativo clinico.

Per monitoraggio del paziente si intende la destinazione d'uso clinica di consentire agli operatori sanitari a distanza di consultare lo stato di un paziente e rivedere, in remoto e quasi in tempo reale, altri dati clinici dei pazienti, standard o critici che siano, forme d'onda e allarmi, al fine di utilizzare queste informazioni per supportare le decisioni cliniche e fornire assistenza al paziente in modo tempestivo. [13]

L'uso del dispositivo richiede una abilitazione specifica all'uso che può essere rilasciata solo dal fabbricante o da personale esplicitamente autorizzato dal fabbricante stesso.

4.4 Identificazione dei pericoli noti o prevedibili e loro cause

Riferimenti normativi

Per l'identificazione dei pericoli sono stati considerati i seguenti riferimenti normativi:

- TR 80002-1 - Guidance on the application of ISO 14971 to medical device software [7]

  Allegato B: è una tabella di pericoli associati a tutte le aree funzionali del software, e definisce sia pericoli associati a guasti software, anomalie software, SOUP e casi di errato utilizzo; sono stati presi dunque solo questi ultimi per l'identificazione degli errori di utilizzo, mentre è stata utilizzata l'intera tabella per determinare i pericoli associati alle attività.

Per ogni pericolo individuato, è stato specificato se fosse applicabile o meno al prodotto in analisi.

4.4.1 Risultati

I risultati sono riportati in forma tabellare (Tabella 6).

Tabella 6. Risultati relativi ai pericoli noti o prevedibili

Potenziale errore di utilizzo	*Pericoli associati*	*Applicabile*	
1. Segnalazioni per l'utente e avvisi		Sì	No
1.1. Priorità	1. Le segnalazioni a basso livello di priorità mascherano il display o l'audio delle segnalazioni ad alto livello di priorità	X	

	2. La segnalazione ad alto livello di priorità non persiste	X	
1.2. Azioni protettive	1. Le azioni protettive verso le condizioni di segnalazione o delle loro categorie non sono chiare	X	
	2. Una volta disattivata la segnalazione, non viene specificato come rimuovere l'azione protettiva	X	
1.3. Spegnimento/modalità provvisoria/recupero	1. Le azioni in modalità provvisoria non sono adeguate	X	
	2. Le azioni in modalità provvisoria creano nuovi pericoli	X	
1.4. Interfaccia Utente	1. L'interfaccia utente "affollata" o "vuota" maschera la reale condizione della segnalazione	X	
	2. Le azioni da intraprendere in risposta alla segnalazione non sono chiare	X	
1.5. Log	1. È presente un errore persistente che sta segnalando un guasto rimasto in sospeso	X	
	2. Le segnalazioni sono associate al paziente sbagliato	X	
1.6. Sistema Audio	1. La presenza di rumore di fondo copre l'audio della segnalazione		X
	2. Il volume della segnalazione è così alto che gli utenti trovano mezzi alternativi per disabilitarla		X
	3. Il sistema audio non funziona e l'utente è inconsapevole del guasto		X

2. Stati critici del ciclo di alimentazione		Sì	No
2.1 Integrità dei dati	1. Scrittura “non-volatile” in corso durante lo spegnimento del computer	X	
	2. I parametri critici non sono conservati per riprendere il trattamento dopo il ciclo di accensione del programma	X	
	3. I parametri critici sono inavvertitamente sovrascritti dalla presenza di un’anomalia latente, presente nel software durante l'operazione corrente	X	
2.2 Ripristino	1. Mancata sincronizzazione con le componenti del programma dopo un ripristino imprevisto	X	
	2. Non vengono rilevati i ripristini persistenti che potrebbero segnalare un guasto in sospeso	X	
2.3 Recupero	1. Il dispositivo medico non è disponibile per l’uso previsto durante le procedure di inizializzazione del sistema in fase di avvio	X	
	2. Guasti “non-volatili” presenti all’avvio: *Cosa fai*?	X	
	3. L'utente non è consapevole che l'impostazione critica è ripristinata alle impostazioni di fabbrica	X	
2.4 Modalità di alimentazione	1. Sistemi audio o altre funzioni UI di segnalazione non sono disponibili durante le condizioni di basso stato di potenza	X	
	2. Quando il software passa allo stato di basso consumo viene disabilitato inavvertitamente il comando di interruzione d’emergenza	X	

3. Comandi critici / Usabilità		Sì	No
3.1 Regolazione / Navigazione / Selezione	Il software permette la modifica dei valori nella UI, ma il processo di controllo non li riceve mai	X	
3.2 Inserimento dati	1. I valori di input sono fuori dell'intervallo ammissibile	X	
	2. I valori di input rientrano nell'intervallo ammissibile ma non corrispondono ai valori previsti dall'utente	X	
3.3 Accessibilità	1. Controllo di spegnimento nascosto	X	
	2. I controlli del *touch screen* non funzionano con l'uso di guanti chirurgici	X	
3.4 Modifiche dello schermo	La segnalazione cambia "automaticamente" la schermata del display	X	
3.5 Progettazione dell'interfaccia utente	1. Uso dei colori senza riguardo nei confronti delle forme comuni di daltonismo	X	
	2. L'utente non è in grado di determinare quale sia la causa della segnalazione in corso	X	
4. Display		**Sì**	**No**
4.1 Immagini diagnostiche	1. Ribaltamento delle immagini		X
	2. Associazione errata del paziente		X
4.2 Forme d'onda diagnostiche	1. Filtro del display inappropriate		X
	2. *Aliasing*, distorsione, errore di scalatura, errori del *timebase*, perdita della		X

	compressione del segnale		
5. Controllo di componenti Hardware		Sì	No
5.1 Algoritmi di Controllo del motore	*Windup* integrale, perdita di informazioni, sincronizzazione, eccesso nel flusso di lavoro, errore di porta (porta seriale/porta parallela)	X	
5.2 Energia applicata	1. Non vengono controllate tutte le porte né in fase di inizio né durante lo svolgimento di una terapia	X	
	2. Il sistema di sicurezza non funziona ma l'utente non ne è consapevole	X	
5.3 Discretizzazione	1. Blocco di *bit*	X	
	2. Le variazioni di *bit* non vengono rilevate a causa dell'interruzione temporanea del sistema dovuta al *Polling* (esecuzione del test di verifica di corretto funzionamento dei bit stessi)	X	
5.4 Calibrazione / Autotest / Controlli dell'intervallo / Calibrazione del dosaggio (Calibrazione specifica del software)	1. Insufficienti istruzioni per l'uso fanno sì che l'utente calibri erroneamente il dispositivo medico collegato	X	
	2. Operazione di auto-azzeramento eseguita con un segnale diverso da zero, come ad esempio la pressione imprevista nel bracciale o in linea, o la forza sul trasduttore	X	
5.5 Rilevazione di guasti relativi ai componenti Hardware	1. L'errore hardware è rilevabile ma mai segnalato all'utente	X	
	2. Il dispositivo medico continua ad essere utilizzato in questa condizione	X	
	3. L'errore hardware si verifica dopo	X	

	l'accensione		
	4. Il software controlla i guasti hardware solo in fase di accensione	X	
5.6 Auto-pulizia	L'utente interrompe il sistema di pulizia o di disinfezione a metà ciclo del processo	X	
5.7 Erogazione di fluidi	1. Rilevamento improprio di una calibrazione	X	
	2. Non vengono controllate tutte le porte del fluido né in fase di inizio né durante lo svolgimento di una terapia	X	
5.8 Supporto vitale	1. Non viene mai definito il livello dello stato di sicurezza	X	
	2. Tra i diversi metodi di arresto, uno non disattiva le interruzioni	X	
	3. Nessun *backup* per le funzioni di supporto vitale	X	
6. Monitoraggio		**Sì**	**No**
6.1 Processo decisionale	1. Errore di "Modo Comune" nel sistema di monitoraggio del software	X	
	2. Condizioni affrettate possono causare risultati errati	X	
6.2 Sistema di disattivazione	1. Il sistema di controllo è ignaro che il sistema di monitoraggio abbia spento il sottosistema	X	
	2. Il parametro di registrazione del sistema di rete è disattivato sul dispositivo medico	X	
6.3 Display	1. Il valore visualizzato non viene aggiornato	X	

	ma l'utente non ne è a conoscenza		
	2. Le scritte nel display vengono eseguite a due o più livelli di priorità	X	
6.4 Misurazione	Errati tempi di acquisizione dati o frequenza di campionamento dei dati inseriti	X	
7. Interfacce		**Sì**	**No**
7.1 Trasmissione di informazioni	1. La funzione trasmette un valore in *microlitri* ma l'utente si aspetta un valore in *millilitri*	X	
	2. Viene trasmesso il puntatore errato	X	
	3. Il puntatore viene trasmesso alla memoria "volatile" e i valori vengono persi prima della loro elaborazione	X	
7.2 Sistema di rete	1. Il software entra in un ciclo infinito in attesa di risposta del sistema *host* del computer	X	
	2. I dispositivi medici in rete vengono assegnati al software con nomi identici, con conseguente perdita di dati	X	
	3. L'elaborazione in rete dei dati controlla i cicli della CPU privi delle funzioni di sicurezza o delle funzioni previste nella destinazione d'uso	X	
8. Dati		**Sì**	**No**
8.1 Informazioni cliniche	1. Il sistema accede all'archivio del paziente errato e l'errore non appare nel display	X	
	2. Il sistema memorizza i dati del paziente in un archivio errato	X	

8.2 *Reports*	Il report fornisce dati errati o li identifica nella sequenza sbagliata o li identifica senza unità	X	
8.3 *Database*	Corruzione dei dati a causa di eventi avversi causati da guasti a livello di sistema o da *Software di Provenienza Sconosciuta* (SOUP)	X	
9. Diagnostica		**Sì**	**No**
9.1 Processo decisionale	L'indicazione di rilevamento degli artefatti sopprime l'indicazione di asistolia sul display	X	
9.2 Conversione dei dati	1. Gli errori di precisione aritmetica risultano non validi	X	
	2. L'algoritmo utilizza o mostra a display unità errate	X	
9.3 Manutenzione preventiva automatizzata	1. La diagnostica in *background* modifica i dati temporaneamente, mentre il codice del programma sta recuperando i dati per l'uso corrente	X	
	2. La diagnostica in *background* interferisce con la corretta sincronizzazione		
10. Security (Protezione dati)		**Sì**	**No**
10.1 Opzioni di configurazione	Nessuna o inadeguata protezione dell'accesso a parametri o dati di configurazione critici	X	
10.2 Accesso funzionale	Nessuna o inadeguata protezione dell'accesso a controlli della terapia o di operazioni che si servano di strumenti	X	
10.3 Accesso all'interfaccia	Assenza o inadeguatezza del sistema di *Protezione dati* e dei comandi inviati tramite interfacce o reti di comunicazione	X	

11. Prestazione		Sì	No
11.1 Capacità / Caricamento / tempo di risposta	1. La sincronizzazione dati diventa critica quando il caricamento dati raggiunge il picco	X	
	2. La sequenza di trasmissione/input/output dei dati viene è alterata o i dati vengono persi quando il caricamento dati raggiunge il picco	X	
	3. Il controllo del motore è alterato quando caricamenti di sistema raggiungono i loro picchi	X	

4.5 Stima dei rischi per ogni situazione pericolosa

Introduzione

Per individuare una situazione pericolosa è necessario prima individuare gli scenari di utilizzo del prodotto in tutte le sue fasi di vita; dopo averli individuati, è necessario individuare i potenziali pericoli che si possono verificare. La stima dei rischi viene fatta per ciascun pericolo individuato, sulla base della politica di accettazione del rischio stabilita in una fase preliminare dell'analisi.

Riferimenti normativi

Sono stati considerati i seguenti riferimenti normativi:

- TR 80002-1 - Guidance on the application of ISO 14971 to medical device software [7]

  Allegato C: è una tabella che elenca i principali pericoli nelle fasi del ciclo di vita del software; ho preso questa per definire le attività e i pericoli in fase di rilascio e manutenzione.

4.5.1 Determinazione della politica di accettabilità del rischio

La politica del fabbricante per la determinazione del rischio accettabile è stata definita attraverso la matrice di valutazione e accettabilità dei rischi. [14]

Conseguenze, probabilità e rischio sono quantificate sulla base dell'esperienza diretta maturata dal personale del fabbricante e della bibliografia conosciuta.

La zona bianca indica il livello di rischio accettabile.

Come richiesto dal regolamento, sono gestiti tutti i rischi identificabili, anche quelli trascurabili, sulla base del rapporto rischio/beneficio.

Non sono esclusi dalla gestione i rischi definiti accettabili in base ai criteri di accettabilità stabiliti dal fabbricante.

La riduzione dei rischi identificati è fatta nella misura del possibile, senza lasciare spazio a principi di carattere economico. L'eventuale applicazione della zona AFAP non è fatta per principi di carattere economico.

L'analisi rischio/beneficio è svolta per ogni rischio identificato e a livello complessivo sul prodotto.

Alle informazioni per l'utilizzatore non si attribuisce carattere di riduzione del rischio, ma di informazione relativa al rischio residuo.

4.5.1.1 Risultati

Sono stati assegnati sei livelli di gravità del danno e probabilità e a ciascun livello è stata assegnata una categoria, come descritto di seguito: [15]

- **Livelli di gravità:**

1. NULLA
   Nessun danno a cose o persone

2. MINORE
   Danno reversibile: si risolve spontaneamente senza ulteriori conseguenze

3. MAGGIORE
   Danno reversibile: per la risoluzione si prevede un intervento terapeutico non invasivo e un tempo relativamente breve per la sua scomparsa

4. GRAVE
   Danno reversibile: per la risoluzione si prevede un intervento terapeutico invasivo per prevenire una menomazione di una funzione del corpo o una lesione di una struttura e/o un tempo alquanto lungo per la sua scomparsa e/o il prolungamento della degenza

5. MOLTO GRAVE
   Danno irreversibile senza pericolo di vita: per la risoluzione si prevede un intervento terapeutico con compromissione della funzione, della struttura, della vita di relazione (disabilità permanente) ma senza pericolo di vita

6. LETALE
   Danno può pregiudicare la vita delle persone
   (paziente/terapista/medico/assistente

- **Livelli di probabilità:**

1. NULLA
   Evento mai riscontrato

2. MOLTO BASSA
   La situazione di pericolo è improbabile durante l'intero ciclo di vita del dispositivo

3. BASSA
   La situazione di pericolo si verifica non più di una volta all'anno

4. MEDIA
   La situazione di pericolo si può verificare una/due volte in un anno

5. ALTA
   La situazione di pericolo si può verificare fino a dieci volte in un anno

6. MOLTO ALTA
   La situazione di pericolo si può verificare più di dieci volte in un anno

La matrice di valutazione dei rischi (Tabella 7) è stata costruita sulla base di tali livelli, così come i criteri di accettabilità del rischio:

Tabella 7. Matrice di valutazione dei rischi

Gravità / Probabilità	Nulla	Minore	Maggiore	Grave	Molto Grave	Letale
Molto Alta	**ACC**	**N. ACC**	**N. ACC**	**N. ACC**	**N. ACC**	**N. ACC**
Alta	**ACC**	**AFAP**	**N. ACC**	**N. ACC**	**N. ACC**	**N. ACC**
Media	**ACC**	**AFAP**	**AFAP**	**N. ACC**	**N. ACC**	**N. ACC**
Bassa	**ACC**	**ACC**	**AFAP**	**AFAP**	**N. ACC**	**N. ACC**
Molto Bassa	**ACC**	**ACC**	**ACC**	**ACC**	**AFAP**	**N. ACC**
Nulla	**ACC**	**ACC**	**ACC**	**ACC**	**ACC**	**ACC**

ACC	Accettabile. Rischio trascurabile.
AFAP	Per quanto possibile. Regione di tollerabilità, il rischio è considerato accettabile rispetto al beneficio. La tollerabilità non è correlata ai costi di riduzione del rischio.
N. ACC	Non accettabile. Il rischio non può essere giustificato se non in circostanze eccezionali

4.5.2 Identificazione degli scenari di utilizzo

Per prima cosa sono stati identificati gli scenari di utilizzo nelle seguenti fasi del ciclo di vita del prodotto:

a. Addestramento all'uso
b. Rilascio
c. Primo avvio
d. Funzionamento operativo
e. Manutenzione
f. Dismissione

Per ciascuna fase, lo scenario di utilizzo è stato identificato considerando le seguenti informazioni:

- Ambienti di utilizzo
- Attività svolte, prendendo di riferimento una guida relativa alla progettazione di una cartella clinica elettronica [16]
- Utenti coinvolti

4.5.2.1 Risultati

I risultati sono riportati in forma tabellare (Tabelle 8 -13), suddivise per fase di vita del DMSW analizzata.

a. Addestramento all'uso

Tabella 8. Risultati relativi agli scenari di utilizzo: addestramento all'uso

Ambienti di utilizzo	*Attività*	*Utenti*
Aula informatica	Formazione teorica	– Tutor – Personale medico / infermieristico / sanitario – Personale amministrativo
Ambienti di utilizzo reale	Affiancamento pratico	– Tutor – Personale medico / sanitario/infermieristico Personale amministrativo

b. Rilascio

Tabella 9. Risultati relativi agli scenari di utilizzo: rilascio

Ambienti di utilizzo	*Attività*	*Utenti*
Uffici - logistica	1. Dichiarazione della versione del software, l'ambiente e delle procedure usate per crearla 2. Valutazione e documentazione di eventuali anomalie residue	Categoria I Sviluppatori

c. Primo avvio

Tabella 10. Risultati relativi agli scenari di utilizzo: primo avvio

Ambienti di utilizzo	*Attività*	*Utenti*
Uffici - logistica	1. Verifica della connessione Internet della struttura ospedaliera e del corretto avviamento del software tramite inserimento del sito Web a un qualsiasi browser Internet; 2. Verifica dell'integrazione e dell'interoperabilità del software con gli altri sistemi informativi.	Categoria I Sviluppatori

d. Funzionamento operativo

Tabella 11. Risultati relativi agli scenari di utilizzo: funzionamento operativo

Ambienti di utilizzo	*Attività*	*Utenti*
1. Ambulatori	1. Ammissione 2. Assessment medico 3. Assistenza infermieristica e di altre professioni sanitarie	Categoria A Personale medico
		Categoria B Personale infermieristico

	4. Ciclo del farmaco ambulatoriale 5. Referto ambulatoriale e certificazioni	
		Categoria C Professioni tecniche sanitarie e della riabilitazione
		Categoria D OSS
		Categoria E Professioni tecnico sanitarie e della riabilitazione Assistenti sociali Psicologi
		Categoria H Studenti medicina
2. **Degenze**	1. Ammissione/ Dimissione/ Trasferimenti 2. Assessment medico (anamnesi) 3. Assessment infermieristico (parametri vitali) 4. Attività diagnostico – assistenziali (procedure) 5. Attività di order entry (Richieste prestazioni/esami/servizi) 6. Gestione consulenze / esami	**Categoria A** Personale medico
		Categoria A bis Anestesisti
		Categoria B Personale infermieristico e ostetrico
		Categoria C Professioni tecnico sanitarie e della riabilitazione
		Categoria E Professioni tecnico sanitarie e della riabilitazione Assistenti sociali Psicologi

		Categoria H Studenti medicina Ausiliari
	7. Ciclo del farmaco a) Prescrizione terapia	**Categoria A** Personale medico
	Ciclo del farmaco b) Somministrazione terapia	**Categoria A bis** Anestesisti
		Categoria B Personale infermieristico
3. **Farmacia ospedaliera**	Ciclo del farmaco c) Preparazione e distribuzione del farmaco	**Categoria F** Personale farmaceutico
4. **Laboratori**	1. Gestione esami / servizi 2. Trasmissione esiti degli esami	**Categoria A** Personale medico
		Categoria C Professioni tecnico sanitarie
		Categoria E Biologi
5. **Studi ambulatoriali MMG**	Gestione del *follow-up* clinico	**Categoria H** MMG
6. **Uffici – accettazione amministrativa**	Amissione / Dimissione / Trasferimenti	**Categoria G** Personale amministrativo
7. **Uffici – amministrazione**	1. Amministrazione del personale e affari generali	**Categoria G** Personale amministrativo

	2. Attività amministrativa a supporto delle attività sanitarie 3. Contabilità generale e finanza	
8. Uffici – direzione	1. Pianificazione e analisi periodica delle attività e dei costi 2. Redditività per DRG (*Diagnosis Related Groups*)	Categoria A Direzione SOD
		Categoria H RID / RAD Direzione medico / infermieristica
9. Uffici – nascite	1. Produzione e archivio dei certificati di nascita 2. Trasmissione dati	Categoria G Personale amministrativo
10. Altro – Smart working	Consultazione dati	Personale medico / infermieristico/tecnico sanitario

e. Manutenzione

Tabella 12. Risultati relativi agli scenari di utilizzo: manutenzione

Ambienti di utilizzo	*Attività*	*Utenti*
Uffici - logistica	1. Definizione di un piano di manutenzione 2. Analisi delle modifiche e dei problemi 3. Implementazione delle modifiche	Categoria I Sviluppatori

f. Dismissione

Tabella 13. Risultati relativi agli scenari di utilizzo: dismissione

Ambienti di utilizzo	*Attività*	*Utenti*
	1. Verifica della sicurezza e	Categoria I

Uffici – logistica	dell'integrità dei dati durante il trasferimento dati da un sistema software a uno nuovo 2. Verifica del mantenimento delle prestazioni del prodotto e della continuità del servizio 3. Procedure di eliminazione del software	Sviluppatori

4.5.3 Identificazione delle situazioni pericolose

Al termine dell'identificazione degli scenari di utilizzo, sono state identificate le situazioni pericolose per ciascuna attività svolta in ciascuna ambiente di utilizzo e l'analisi è stata ripetuta per ogni fase di vita del software.

Per identificare le situazioni pericolose, sono stati considerati i pericoli, per ogni attività svolta, individuati al passo precedente e sono stati identificati i pericoli applicabili da quelli non.

4.5.3.1 Risultati

I risultati sono riportati in forma tabellare (Tabelle 14 -19), suddivisi per fase di vita del DMSW analizzata.

a. Addestramento all'uso

Tabella 14. Risultati relativi alle situazioni pericolose: addestramento all'uso

Aula informatica			
Attività	Aree funzionali software dei *Pericoli associati*	*Applicabile*	
		Sì	No
Formazione teorica	1. Segnalazioni per l'utente e avvisi		X
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità		X
	4. Controllo di componenti Hardware		X
	5. Monitoraggio		X

	6. Interfacce	X	
	7. Dati		X
	8. Diagnostica		X
	9. Security		X
	10. Prestazioni		X
Ambienti di utilizzo reale			
Attività	Aree funzionali software dei *Pericoli associati*	*Applicabile*	
		Sì	No
Affiancamento pratico	a. Segnalazioni per l'utente e avvisi		X
	b. Stati critici del ciclo di alimentazione	X	
	c. Comandi critici / Usabilità	X	
	d. Controllo di componenti Hardware		X
	e. Monitoraggio		X
	f. Interfacce	X	
	g. Dati		X
	h. Diagnostica		X
	i. Security		X
	j. Prestazioni	X	

b. Rilascio

Tabella 15. Risultati relativi alle situazioni pericolose: rilascio

Uffici – logistica	
Attività	*Pericoli associati* [8]
1. Dichiarazione della versione del software, dell'ambiente e delle	1. La mancata messa in accordo della versione della documentazione rilasciata con il software rilasciato può fuorviare il team di sviluppo e test sulle future versioni del prodotto. Una documentazione imprecisa e la tracciabilità potrebbero portare alla perdita di collegamenti e portare a trascurare i pericoli e le loro cause, a perdere le misure di

procedure usate per crearla	controllo dei rischi o a non verificare adeguatamente il software relativo alla sicurezza.
	2. Tralasciare il fatto che, una volta che una terza parte non distribuisce più una specifica versione SOUP, tali versioni non saranno disponibili per le indagini sui guasti e le correzioni sul campo.
	3. Poiché uno strumento e una versione specifici dello strumento non sono stati archiviati (come un compilatore), la possibilità di creare la versione specifica del software viene persa.
	4. La vita del dispositivo medico potrebbe essere più lunga della vita dei mezzi d'archivio attuali.
2. Valutazione e documentazione di eventuali anomalie software residue	1. Mancato coinvolgimento di persone con adeguate conoscenze cliniche nella valutazione delle anomalie residue.
	2. Valutazione della significatività delle anomalie residue basata unicamente sul sintomo funzionale rilevato piuttosto che su una completa analisi delle cause per determinare tutti i potenziali effetti collaterali in una gamma di condizioni.

c. Primo avvio

Tabella 16. Risultati relativi alle situazioni pericolose: primo avvio

Uffici – logistica			
Attività	Aree funzionali software dei *Pericoli associati*	*Applicabile*	
		Sì	No
1. Verifica della connessione Internet della struttura ospedaliera e del corretto avviamento del software tramite inserimento del sito Web a un qualsiasi browser	1. Segnalazioni per l'utente e avvisi		X
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità		X
	4. Controllo di componenti Hardware		X
	5. Monitoraggio		X
	6. Interfacce		X
	7. Dati		X

Internet	8. Diagnostica		X
	9. Security		X
	10. Prestazioni	X	
2. Verifica dell'interoperabilità del software con gli altri sistemi informativi.	1. Segnalazioni per l'utente e avvisi		X
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità		X
	4. Controllo di componenti Hardware		X
	5. Monitoraggio		X
	6. Interfacce		X
	7. Dati		X
	8. Diagnostica		X
	9. Security	X	
	10. Prestazioni	X	

d. Funzionamento operativo

Tabella 17. Risultati relativi alle situazioni pericolose: funzionamento operativo

Ambulatori			
Attività	Aree funzionali software dei *Pericoli associati*	*Applicabile*	
		Sì	No
1. Ammissione	1. Segnalazioni per l'utente e avvisi		X
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità	X	
	4. Controllo di componenti Hardware		X
	5. Monitoraggio	X	
	6. Interfacce	X	
	7. Dati	X	

	8. Diagnostica	X	
	9. Security	X	
	10. Prestazioni	X	
2. Attività cliniche	1. Segnalazioni per l'utente e avvisi	X	
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità	X	
	4. Controllo di componenti Hardware		X
	5. Monitoraggio	X	
	6. Interfacce	X	
	7. Dati	X	
	8. Diagnostica		X
	9. Security	X	
	10. Prestazioni	X	
3. Assistenza infermieristica e di altre professioni sanitarie	1. Segnalazioni per l'utente e avvisi	X	
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità	X	
	4. Controllo di componenti Hardware		X
	5. Monitoraggio	X	
	6. Interfacce	X	
	7. Dati	X	
	8. Diagnostica	X	
	9. Security	X	
	10. Prestazioni	X	
4. Ciclo del farmaco ambulatoriale	1. Segnalazioni per l'utente e avvisi	X	
	2. Stati critici del ciclo di alimentazione	X	

	3. Comandi critici / Usabilità	X	
	4. Controllo di componenti Hardware	X	
	5. Monitoraggio	X	
	6. Interfacce	X	
	7. Dati	X	
	8. Diagnostica	X	
	9. Security	X	
	10. Prestazioni	X	
5. Referto ambulatoriale e certificazioni	1. Segnalazioni per l'utente e avvisi		X
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità	X	
	4. Controllo di componenti Hardware		X
	5. Monitoraggio	X	
	6. Interfacce	X	
	7. Dati	X	
	8. Diagnostica		X
	9. Security	X	
	10. Prestazioni	X	
Degenze			
Attività	Aree funzionali software dei *Pericoli associati*	*Applicabile* Sì	No
1. Ammissione/Dimissione/Trasferimenti	1. Segnalazioni per l'utente e avvisi		X
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità	X	
	4. Controllo di componenti Hardware		X

	5. Monitoraggio	X	
	6. Interfacce	X	
	7. Dati	X	
	8. Diagnostica	X	
	9. Security	X	
	10. Prestazioni	X	
2. Assessment medico	1. Segnalazioni per l'utente e avvisi	X	
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità	X	
	4. Controllo di componenti Hardware		X
	5. Monitoraggio		X
	6. Interfacce	X	
	7. Dati	X	
	8. Diagnostica		X
	9. Security	X	
	10. Prestazioni	X	
3. Assessment infermieristico	1. Segnalazioni per l'utente e avvisi	X	
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità	X	
	4. Controllo di componenti Hardware		X
	5. Monitoraggio		X
	6. Interfacce	X	
	7. Dati	X	
	8. Diagnostica	X	
	9. Security	X	

	10. Prestazioni	X	
4. Attività diagnostico – assistenziali	1. Segnalazioni per l'utente e avvisi	X	
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità	X	
	4. Controllo di componenti Hardware		X
	5. Monitoraggio	X	
	6. Interfacce	X	
	7. Dati	X	
	8. Diagnostica	X	
	9. Security	X	
	10. Prestazioni	X	
5. Attività di order entry	1. Segnalazioni per l'utente e avvisi		X
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità	X	
	4. Controllo di componenti Hardware		X
	5. Monitoraggio		X
	6. Interfacce	X	
	7. Dati	X	
	8. Diagnostica		X
	9. Security		X
	10. Prestazioni	X	
6. Gestione consulenze / esami	1. Segnalazioni per l'utente e avvisi		X
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità	X	
	4. Controllo di componenti Hardware		X

	5. Monitoraggio		X
	6. Interfacce	X	
	7. Dati	X	
	8. Diagnostica		X
	9. Security	X	
	10. Prestazioni	X	
7. Ciclo del farmaco a) Prescrizione terapia	1. Segnalazioni per l'utente e avvisi	X	
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità	X	
	4. Controllo di componenti Hardware		X
	5. Monitoraggio		X
	6. Interfacce	X	
	7. Dati	X	
	8. Diagnostica		X
	9. Security	X	
	10. Prestazioni	X	
Ciclo del farmaco b) Somministrazione terapia	1. Segnalazioni per l'utente e avvisi	X	
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità	X	
	4. Controllo di componenti Hardware	X	
	5. Monitoraggio	X	
	6. Interfacce	X	
	7. Dati	X	
	8. Diagnostica	X	
	9. Security	X	

	10. Prestazioni	X	
Farmacia ospedaliera			
Attività	Aree funzionali software dei *Pericoli associati*	*Applicabile*	
		Sì	No
Ciclo del farmaco c) Preparazione e distribuzione del farmaco	1. Segnalazioni per l'utente e avvisi		X
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità	X	
	4. Controllo di componenti Hardware		X
	5. Monitoraggio	X	
	6. Interfacce	X	
	7. Dati	X	
	8. Diagnostica	X	
	9. Security	X	
	10. Prestazioni	X	
Laboratori			
Attività	Aree funzionali software dei *Pericoli associati*	*Applicabile*	
		Sì	No
1. Gestione esami / servizi	1. Segnalazioni per l'utente e avvisi		X
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità	X	
	4. Controllo di componenti Hardware		X
	5. Monitoraggio		X
	6. Interfacce	X	
	7. Dati	X	
	8. Diagnostica		X
	9. Security		X

	10. Prestazioni	X	
2. Trasmissione esiti degli esami	1. Segnalazioni per l'utente e avvisi		X
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità	X	
	4. Controllo di componenti Hardware		X
	5. Monitoraggio		X
	6. Interfacce	X	
	7. Dati	X	
	8. Diagnostica		X
	9. Security	X	
	10. Prestazioni	X	
Studi ambulatoriali MMG			
Attività	Aree funzionali software dei *Pericoli associati*	*Applicabile* Sì	No
Gestione del *follow-up* clinico	1. Segnalazioni per l'utente e avvisi		X
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità	X	
	4. Controllo di componenti Hardware		X
	5. Monitoraggio	X	
	6. Interfacce	X	
	7. Dati	X	
	8. Diagnostica	X	
	9. Security	X	
	10. Prestazioni	X	
Uffici – accettazione amministrativa			
Attività	Aree funzionali software dei	*Applicabile*	

	Pericoli associati	Sì	No
1. Amissione / Dimissione / Trasferimenti	1. Segnalazioni per l'utente e avvisi		X
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità	X	
	4. Controllo di componenti Hardware		X
	5. Monitoraggio	X	
	6. Interfacce	X	
	7. Dati	X	
	8. Diagnostica	X	
	9. Security	X	
	10. Prestazioni	X	
Uffici – amministrazione			
Attività	Aree funzionali software dei *Pericoli associati*	*Applicabile* Sì	No
1. Amministrazione del personale e affari generali	1. Segnalazioni per l'utente e avvisi		X
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità	X	
	4. Controllo di componenti Hardware		X
	5. Monitoraggio		X
	6. Interfacce	X	
	7. Dati	X	
	8. Diagnostica		X
	9. Security		X
	10. Prestazioni	X	
2. Attività	1. Segnalazioni per l'utente e avvisi		X

amministrativa a supporto delle attività sanitarie	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità	X	
	4. Controllo di componenti Hardware		X
	5. Monitoraggio		X
	6. Interfacce	X	
	7. Dati	X	
	8. Diagnostica		X
	9. Security	X	
	10. Prestazioni	X	
3. Contabilità generale e finanza	1. Segnalazioni per l'utente e avvisi		X
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità	X	
	4. Controllo di componenti Hardware		X
	5. Monitoraggio		X
	6. Interfacce	X	
	7. Dati	X	
	8. Diagnostica		X
	9. Security		X
	10. Prestazioni	X	
Uffici – direzione			
Attività	Aree funzionali software dei *Pericoli associati*	*Applicabile* Sì	No
1. Analisi periodica delle attività e dei costi	1. Segnalazioni per l'utente e avvisi		X
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità		X

	4. Controllo di componenti Hardware		X
	5. Monitoraggio		X
	6. Interfacce	X	
	7. Dati	X	
	8. Diagnostica		X
	9. Security		X
	10. Prestazioni	X	
2. Redditività per DRG (*Diagnosis Related Groups*)	1. Segnalazioni per l'utente e avvisi		X
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità		X
	4. Controllo di componenti Hardware		X
	5. Monitoraggio		X
	6. Interfacce	X	
	7. Dati	X	
	8. Diagnostica		X
	9. Security		X
	10. Prestazioni	X	
Uffici – nascite			
Attività	Aree funzionali software dei *Pericoli associati*	*Applicabile* Sì	*Applicabile* No
1. Produzione e archivio dei certificati di nascita	1. Segnalazioni per l'utente e avvisi	X	
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità	X	
	4. Controllo di componenti Hardware		X
	5. Monitoraggio	X	

	6. Interfacce	X	
	7. Dati	X	
	8. Diagnostica	X	
	9. Security	X	
	10. Prestazioni	X	
2. Trasmissione dati	1. Segnalazioni per l'utente e avvisi		X
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità	X	
	4. Controllo di componenti Hardware		X
	5. Monitoraggio		X
	6. Interfacce	X	
	7. Dati	X	
	8. Diagnostica		X
	9. Security	X	
	10. Prestazioni	X	
Altro – smart working			
Attività	Aree funzionali software dei *Pericoli associati*	*Applicabile* Sì	No
Consultazione dati	1. Segnalazioni per l'utente e avvisi	X	
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità	X	
	4. Controllo di componenti Hardware		X
	5. Monitoraggio	X	
	6. Interfacce	X	
	7. Dati	X	

	8. Diagnostica	X	
	9. Security	X	
	10. Prestazioni		X

e. Manutenzione

Tabella 18. Risultati relativi alle situazioni pericolose: manutenzione

Uffici – logistica	
Attività	*Pericoli associati* [7]
1. Definizione di un piano di manutenzione	1. Stabilire un piano di manutenzione che non abbia un approccio chiaro al processo di gestione del rischio di eventuali modifiche
	2. Stabilire un processo di gestione del rischio per le modifiche che riguardano solo la funzionalità prevista della specifica modifica, non le componenti interessate ad essa e i relativi rischi associati.
2. Analisi delle modifiche e dei problemi 3. Implementazione delle modifiche	1. Presupporre che un piccolo cambiamento funzionale non possa influire sulla sicurezza.
	2. Estendere l'uso del dispositivo medico a nuove "popolazioni bersaglio", nuove indicazioni di malattie, nuovi tipi di utenti (ad es. infermieri anziché chirurghi) o nuove piattaforme senza aver prima riesaminato le misure di controllo del rischio esistenti e l'adeguatezza dell'interfaccia utente.
	3. Definire le priorità delle risorse per la risoluzione dei problemi in base alle segnalazioni dei problemi sul campo, senza determinare la causa principale e i potenziali effetti collaterali.
	4. Il software, progettato per scopi non clinici (ad es. fatturazione), contiene dati che vengono successivamente trasmessi a scopi clinici, senza un'adeguata gestione del rischio.

f. Dismissione

Tabella 19. Risultati relativi alle situazioni pericolose: dismissione

Uffici – logistica			
Attività	Aree funzionali software dei *Pericoli associati*	*Applicabile*	
		Sì	No
1. Verifica della sicurezza e dell'integrità dei dati durante il trasferimento dati dal sistema software in uso a uno nuovo	1. Segnalazioni per l'utente e avvisi		X
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità		X
	4. Controllo di componenti Hardware		X
	5. Monitoraggio	X	
	6. Interfacce		X
	7. Dati	X	
	8. Diagnostica	X	
	9. Security	X	
	10. Prestazioni		X
2. Verifica del mantenimento delle prestazioni del prodotto e della continuità del servizio	1. Segnalazioni per l'utente e avvisi		X
	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità		X
	4. Controllo di componenti Hardware		X
	5. Monitoraggio		X
	6. Interfacce		X
	7. Dati		X
	8. Diagnostica		X
	9. Security	X	
	10. Prestazioni	X	
3. Procedure di	1. Segnalazioni per l'utente e avvisi		X

eliminazione del software	2. Stati critici del ciclo di alimentazione	X	
	3. Comandi critici / Usabilità		X
	4. Controllo di componenti Hardware		X
	5. Monitoraggio		X
	6. Interfacce		X
	7. Dati		X
	8. Diagnostica		X
	9. Security	X	
	10. Prestazioni	X	

4.5.4 Stima dei rischi

Sulla base della politica di accettabilità del rischio, sono stati riportati in una tabella tutti i pericoli identificati ai passi precedenti e per ogni pericolo sono state assegnate le seguenti informazioni:

- Articoli del regolamento di riferimento (ove presenti)
- Sicurezza fondamentale associata (sì/no)
- Prestazioni essenziali di riferimento (ove presenti)
- Cause del pericolo
- Elementi del sistema collegati al pericolo (ove presenti)
- Fasi del processo in cui il pericolo può verificarsi
- Livello di gravità
- Livello di probabilità

Per assegnare i livelli di gravità e probabilità sono stati considerati, oltre all'esperienza diretta del fabbricante del prodotto software, i risultati ottenuti da una precedente analisi [16] svolta da FDA riguardo all'analisi dei rischi di una cartella clinica elettronica nelle aziende sanitarie.

4.5.4.1 Risultati

La Tabella 20 della stima dei rischi è stata dunque strutturata come mostrato di seguito:

Tabella 20. Struttura relativa alla stima dei rischi

Identificazione del pericolo	MDR	Sicurezza Fondamentale	Prest. Ess.	Cause	Elementi del Sistema	Fasi dei processi di progetto, produzione, uso e manutenzione	Gravità	Probabilità

Tra i pericoli stimati sono stati considerati quelli connessi agli errori umani. Le informazioni richieste per la stima dei rischi associati sono state raccolte nella seguente Tabella 21:

Tabella 21. Risultati relativi alla stima dei rischi

Pericolo: Errori d'uso	
Identificazione del pericolo	Danno da errore umano: sospensione o allungamento del tempo di terapia/diagnosi/trattamento
MDR	NA
Sicurezza fondamentale	NA
Prestazioni essenziali	Sì
Cause	– Errori basati su procedure – Errore di strategia – Violazione di procedure – Perdita di attenzione dell'assistente – Perdita di efficienza dovuta indicazione dello stato macchina errata o confusiva – **Disposizione dei comandi confusiva o di difficile utilizzo – Usabilità**
Elementi del sistema	Possibili elementi hardware: – Touchscreen – Connettori – Hard disk Possibili – Elementi software: – Interfaccia utente
Fasi del processo	Funzionamento operativo
Gravità [20]	**Letale**
Probabilità [20]	**Media**

4.6 Conclusioni

Dalle informazioni ottenute, una delle potenziali cause degli errori di utilizzo è l'usabilità del prodotto.

Dalla matrice di valutazione di riferimento, la stima del rischio associata ai pericoli connessi agli errori umani risulta dunque essere **NON ACCETTABILE**.

Si può dunque concludere che è necessario verificare l'usabilità del dispositivo medico software.

5. Usabilità di una cartella clinica elettronica

5.1 Introduzione

Dalla stima dei rischi, quelli connessi agli errori di utilizzo sono risultati dipendere in modo critico dall'usabilità. È stato dunque necessario verificare l'usabilità del dispositivo medico software. Per verificare l'usabilità del prodotto è stata verificata la conformità alla norma 62366-1.

I prossimi paragrafi descrivono le fasi del processo che sono state applicate al prodotto; per ogni fase sono stati descritti i metodi utilizzati e i risultati ottenuti.

5.2 Identificazione delle specifiche d'uso

Le specifiche d'uso devono comprendere le seguenti informazioni:

- Indicazioni per l'uso
- Pazienti di riferimento
- Eventuali tipi di contatto tra il dispositivo medico, i pazienti e gli utilizzatori
- Gli utenti e i loro profili
- Ambienti di utilizzo
- Principio operativo

Per identificare le indicazioni per l'uso è stata considerata la Destinazione d'uso del prodotto.
Per stabilire la destinazione d'uso del prodotto sono state considerate le seguenti guide:

- MDCG 2019-11, Annex I, Qualification Electronic Patient Record Systems Software [3]
- *Manual on borderline and classification in the Community regulatory framework for medical devices, Classificazione dei software per la gestione delle informazioni e il monitoraggio dei pazienti* [13]

Di seguito vengono riportate le difinizioni di cartella clinica elettronica con riferimento alle guide sopra ripotate:

- MDCG 2019-11, Annex I, Qualification Electronic Patient Record Systems Software:

  Strumento digitale per la gestione organica e strutturata dei dati riferiti alla storia clinica di un paziente, garantendo il supporto dei processi clinici (diagnostico-terapeutici) e assistenziali nei singoli episodi di cura e favorendo la continuità di cura del paziente tra diversi episodi di cura afferenti alla stessa struttura ospedaliera mediante la condivisione e il recupero dei documenti clinici in essi registrati. [3]

- *Manual on borderline and classification in the Community regulatory framework for medical devices, Classificazione dei software per la gestione delle informazioni e il monitoraggio dei pazienti:*

  Sistema basato su software che include una gestione informatica e piattaforma di monitoraggio del paziente.

  - *Per gestione informatica si intende la destinazione d'uso clinica di instradare e memorizzare i dati dei dispositivi medici e le informazioni diagnostiche sui dispositivi, trasferendoli dai dispositivi supportati al posto letto alla cartella clinica elettronica e al sistema informativo clinico.*
  - *Per monitoraggio del paziente si intende la destinazione d'uso clinica di consentire agli operatori sanitari a distanza di consultare lo stato di un paziente e rivedere, in remoto e quasi in tempo reale, altri dati clinici dei pazienti, standard o critici che siano, forme d'onda e allarmi, al fine di utilizzare queste informazioni per supportare le decisioni cliniche e fornire assistenza al paziente in modo tempestivo.* [13]

Per identificare i pazienti di riferimento, gli utenti del prodotto, gli ambienti di utilizzo e il principio operativo sono state svolte interviste al fabbricante del prodotto e al personale dell'azienda ospedaliera in cui il dispositivo opera.

Per individuare i profili degli utenti sono state utilizzate le informazioni ricavate dalle interviste e dalla letteratura.

5.2.1 Risultati

I. Indicazioni per l'uso

Supporto a diagnosi, terapia, monitoraggio e cura di tutte le tipologie di patologie afferenti ad ambulatori e a qualsiasi reparto di degenza dell'Azienda Ospedaliero Universitaria Careggi.

II. Pazienti di riferimento

- Fascia d'età : *Da neonatale a geriatrica.*
- Peso: *DATO NON SIGNIFICATIVO.*
- Genere: *DATO NON SIGNIFICATIVO.*
- Gruppo etnico: *DATO NON SIGNIFICATIVO.*
- Condizioni limitanti: *DATO NON SIGNIFICATIVO.*
- Altri dati significativi: *DATO NON SIGNIFICATIVO.*

III. Contatto tra dispositivo medico, pazienti e utilizzatori

- Il dispositivo NON è in contatto DIRETTO né INDIRETTO con pazienti e nemmeno con l'utilizzatore.
- Tipo di contatto: *nessuno*.
  - Durata del contatto: *DATO NON SIGNIFICATIVO*.

IV. Profilo degli utenti

I risultati sono riportati in forma tabellare (Tabella 22).

Tabella 22. Risultati relativi ai profili utenti

Utente	*Profilo utente* [17] *Per ciascuna educazione in cui sia prevista una laurea specialistica è prevista anche l'iscrizione all'Albo della relativa professione	
Area medico / infermieristica		
1. Personale medico	***Età***	*DATO NON SIGNIFICATIVO.*
	Genere	*DATO NON SIGNIFICATIVO.*
	Educazione*	Specializzazione post laurea.
	Comprensione linguistica	Italiana, inglese.
	Conoscenze professionali	– Saper riconoscere gli strumenti essenziali per esercitare, creando la propria borsa del medico – Saper utilizzare i software, i siti internet, i portali, le password per accedere ai servizi essenziali di ogni medico – Saper gestire la propria contabilità, la propria corrispondenza, la propria previdenza – Imparare le abilità di volta in volta richieste, a seconda dell'incarico svolto – Saper utilizzare gli strumenti di pianificazione del lavoro
	Esperienza informatica	Competenze di informatica necessaria per la comunicazione e la gestione dell'attività professionale .
	Invalidità / limitazioni	Uso del software escluso ai portatori di handicap legati alla vista e alle articolazioni delle mani.
2. Medici di Medicina Generale (MMG)	***Età***	*DATO NON SIGNIFICATIVO.*
	Genere	*DATO NON SIGNIFICATIVO.*
	Educazione	Specializzazione post laurea (Diploma di formazione specifico).
		Italiana, inglese.

	Comprensione linguistica	
	Conoscenze professionali	– Conoscenze per la gestione delle patologie croniche e le sindromi ad esse collegate di più comune riscontro nella pratica della Medicina Generale – Conoscenze per la gestione dei sintomi e manifestazioni patologiche acute di più comune riscontro nella pratica della Medicina Generale – Conoscenze per gestire situazioni complesse
	Esperienza informatica	Competenze di informatica applicata.
	Invalidità / limitazioni	Uso del software escluso ai portatori di handicap legati alla vista e alle articolazioni delle mani.
3. Direzione SOD 4. Direzione medico-infermieristica	***Età***	*DATO NON SIGNIFICATIVO.*
	Genere	*DATO NON SIGNIFICATIVO.*
	Educazione*	Specializzazione post laurea
	Comprensione linguistica	Italiana, lingua straniera.
	Conoscenze professionali	Organizzazione tecnico-sanitaria della struttura sotto il profilo igienico ed organizzativo essendone responsabile nei confronti della titolarità e dell'autorità sanitaria competente.
	Esperienza informatica	Competenze di informatica di base.
	Invalidità / limitazioni	Uso del software escluso ai portatori di handicap legati alla vista e alle articolazioni delle mani.
Studenti di Medicina	***Età***	*DATO NON SIGNIFICATIVO.*
	Genere	*DATO NON SIGNIFICATIVO.*
	Educazione	Licenza media superiore.

	Comprensione linguistica	Italiana, inglese.
	Conoscenze professionali	*Vedi Medico.*
	Esperienza informatica	Competenze di informatica di base.
	Invalidità / limitazioni	Uso del software escluso ai portatori di handicap legati alla vista e alle articolazioni delle mani.
5. Anestesisti	***Età***	*DATO NON SIGNIFICATIVO.*
	Genere	*DATO NON SIGNIFICATIVO.*
	Educazione*	Specializzazione post laurea.
	Comprensione linguistica	Italiana.
	Conoscenze professionali	– Abilità in ambito scientifico – Biologia – Anatomia – Fisiologia – Conoscenze specifiche in farmacologia, fisica e chimica
	Esperienza informatica	Competenze di informatica per la comunicazione e la gestione dell'attività professionale.
	Invalidità / limitazioni	Uso del software escluso ai portatori di handicap legati alla vista e alle articolazioni delle mani.
Area sanitaria		
6. Assistenti sociali	***Età***	*DATO NON SIGNIFICATIVO.*
	Genere	*DATO NON SIGNIFICATIVO.*
	Educazione	Laurea breve.
	Comprensione linguistica	Italiana.
		– Normativa in materia sanitaria

	Conoscenze professionali	– Elementi di politica sociale – Modelli organizzativi dei Servizi sociali – Metodi e tecniche del servizio sociale – Principi e fondamenti del servizio sociale – Codice deontologico – Rete territoriale dei servizi sociali – Metodologie di valutazione interventi in area sociale – Teorie e tecniche di comunicazione interpersonale (ruoli, dimensioni e fattori coinvolti)
	Esperienza informatica	Competenze di tecniche e programmi informatici per il trattamento delle informazioni.
	Invalidità / limitazioni	Uso del software escluso ai portatori di handicap legati alla vista e alle articolazioni delle mani.
7. Ausiliari	***Età***	*DATO NON SIGNIFICATIVO.*
	Genere	*DATO NON SIGNIFICATIVO.*
	Educazione	Fino alla scuola dell'obbligo.
	Comprensione linguistica	Italiana.
	Conoscenze professionali	– Utilizzo di macchinari e attrezzature specifici – Pulizia e riordino degli ambienti interni ed esterni – Tutte le operazioni inerenti al trasporto di materiali in uso nell'ambito dei settori o servizi di assegnazione – Operazioni elementari e di supporto richieste, necessarie al funzionamento dell'unità operativa.
	Esperienza informatica	Conoscenze di informatica di base.
	Invalidità / limitazioni	Uso del software escluso ai portatori di handicap legati alla vista e alle articolazioni delle mani.
	Età	*DATO NON SIGNIFICATIVO.*

8. Biologi	***Genere***	*DATO NON SIGNIFICATIVO.*
	Educazione	Laurea.
	Comprensione linguistica	Italiana, lingua straniera (livello tecnico scientifico).
	Conoscenze professionali	– Chimica organica, Chimica analitica e Chimica Biologica Metabolica – Tossicologia – Biomatematica – Biomonitoraggio – Ecologia – Fisica e Fisica dell'atmosfera – Igiene ambientale e del lavoro – Economia applicata al territorio – Ergonomia – Medicina del lavoro – Epidemiologia – Elementi di comunicazione nella valutazione del rischio – Patologia ambientale – Elementi di legislazione del lavoro – Specializzazione nei sistemi acquatici – Chemodinamica ambientale – Tecniche di analisi inorganiche e Tecniche di analisi di superficie – Fondamenti di Chemiometria – Trattamento dei rifiuti – Impianti di trattamento dei reflui – Impianti e processi di produzione industriale – Elementi di Economia e organizzazione aziendale – Impatto ambientale e certificazione – Conservazione e trattamento dei materiali
	Esperienza informatica	Competenze di informatica di base.
	Invalidità / limitazioni	Uso del software escluso ai portatori di handicap legati alla vista e alle articolazioni delle mani.
9. Personale	***Età***	*DATO NON SIGNIFICATIVO.*
	Genere	*DATO NON SIGNIFICATIVO.*

farmaceutico	***Educazione***	Laurea.
	Comprensione linguistica	Italiana, straniera.
	Conoscenze professionali	Discipline biologiche e farmacologiche: – Farmacoterapia – Fitoterapia, omeopatia e altre medicine non convenzionali – Tossicologia – Metodologie applicate nella sperimentazione biochimica (impostazione dell'esperimento e raccolta dei dati) Discipline chimico-farmaceutiche e tecnologiche: – Tecnologia farmaceutica – Legislazione farmaceutica – Conoscenze necessarie alla formulazione, allestimento, controllo e confezionamento di prodotti galenici – Conoscenza dell'uso dei diversi prodotti della salute – Elementi di farmacocinetica – Elementi di progettazione, identificazione e sintesi di sostanze biologicamente attive
	Esperienza informatica	– Conoscenza di alcuni software di utilità quotidiana (word processor e foglio elettronico) – Conoscenza di specifici applicativi
	Invalidità / limitazioni	Uso del software escluso ai portatori di handicap legati alla vista e alle articolazioni delle mani.
10. Personale infermieristico	***Età***	*DATO NON SIGNIFICATIVO.*
	Genere	*DATO NON SIGNIFICATIVO.*
	Educazione	Laurea breve.
	Comprensione linguistica	Italiana.

	Conoscenze professionali	– Principi di infermieristica generale e clinica – Metodologia infermieristica – Metodologia infermieristica basata sulle prove di evidenza (EBM) – Chirurgia generale, oncologica e d'urgenza – Infermieristica cardiovascolare e respiratoria – Infermieristica oncologica – Infermieristica psichiatrica – Medicina e infermieristica d'urgenza e intensiva – Medicina e infermieristica fisica e riabilitativa – Elementi di geriatria – Elementi di neurologia – Anestesiologia e rianimazione – Discipline specialistiche legate ai diversi problemi di salute (dermatologia, gastroenterologia, endocrinologia, reumatologia, ecc.) – Infermieristica pediatrica, ginecologia e ostetricia
	Esperienza informatica	Competenze di informatica di base.
	Invalidità / limitazioni	Uso del software escluso ai portatori di handicap legati alla vista e alle articolazioni delle mani.
11. OSS	***Età***	*DATO NON SIGNIFICATIVO.*
	Genere	*DATO NON SIGNIFICATIVO.*
	Educazione	Fino alla scuola dell'obbligo.
	Comprensione linguistica	Italiana.
	Conoscenze professionali	– Aiuto per l'igiene personale – Somministrazione pasti – Cambio medicazioni e fasciature – Prevenzione di piaghe da decubito – Controllo della corretta postura – Rilevazione dei parametri vitali; – Verifica dell'esatta assunzione dei medicinali previsti dal piano terapeutico – Supporto alle attività infermieristiche

		– Attività ricreative e sociali
	Esperienza informatica	Competenze di informatica di base.
	Invalidità / limitazioni	Uso del software escluso ai portatori di handicap legati alla vista e alle articolazioni delle mani.
12. Personale ostetrico	***Età***	*DATO NON SIGNIFICATIVO.*
	Genere	*DATO NON SIGNIFICATIVO.*
	Educazione	Laurea breve.
	Comprensione linguistica	Italiana, inglese.
	Conoscenze professionali	– Istologia e embriologia – Genetica – Anatomia e fisiologia generale e dell'apparato riproduttivo, del feto e degli annessi – Principi di fisica ed ecografia – Ginecologia e ostetricia – Fisiopatologia della riproduzione umana – Medicina dell'età prenatale – Ginecologia urologica, ginecologia oncologica, senologia – Colpocitologia – Neonatologia – Neuropsichiatria infantile – Elementi di scienza dell'alimentazione e nutrizione clinica – Malattie a trasmissione sessuale
	Esperienza informatica	Competenze di informatica di base.
	Invalidità / limitazioni	Uso del software escluso ai portatori di handicap legati alla vista e alle articolazioni delle mani.
13. Professioni sanitarie della riabilitazione	***Età***	*DATO NON SIGNIFICATIVO.*
	Genere	*DATO NON SIGNIFICATIVO.*
		Laurea breve.

	Educazione	
	Comprensione linguistica	Italiana.
	Conoscenze professionali	– Saper utilizzare tecniche e metodologie proprie della riabilitazione psichiatrica – Saper definire e applicare criteri e sistemi di valutazione dei risultati raggiunti – Saper applicare tecniche di comunicazione efficace – Saper applicare i fondamenti delle dinamiche relazionali
	Esperienza informatica	Competenze di informatica di base.
	Invalidità / limitazioni	Uso del software escluso ai portatori di handicap legati alla vista e alle articolazioni delle mani.
14. Professioni tecnico sanitarie	***Età***	*DATO NON SIGNIFICATIVO.*
	Genere	*DATO NON SIGNIFICATIVO.*
	Educazione*	Laurea breve.
	Comprensione linguistica	Italiana, inglese.
	Conoscenze professionali	– Tecniche diagnostiche di istocitopatologia – Tecniche diagnostiche di microbiologia – Tecniche diagnostiche di biochimica e genetica – Tecniche diagnostiche di medicina di laboratorio – Tecniche diagnostiche di biologia e citogenetica molecolare – Sistemi di elaborazione delle informazioni – Scienze e tecniche diagnostiche e farmacologiche – Elementi di etica e organizzazione della professione
	Esperienza informatica	Conoscenza degli elementi d informatica.

	Invalidità / limitazioni	Uso del software escluso ai portatori di handicap legati alla vista e alle articolazioni delle mani.
15. Psicologi	***Età***	*DATO NON SIGNIFICATIVO.*
	Genere	*DATO NON SIGNIFICATIVO.*
	Educazione*	Specializzazione post laurea.
	Comprensione linguistica	Italiana, inglese.
	Conoscenze professionali	– Psicologia cognitiva – Psicologia criminologica – Psicologia dei gruppi – Psicologia dell'orientamento – Psicologia della comunicazione – Psicologia dello sport – Psicologia dello sviluppo e della vita familiare – Psicopatologia – Metodi di intervento clinico – Metodi di intervento psicologico per i servizi alla persona e alla comunità – Metodologie del counseling psicologico – Neuroscienze cognitive – Tecniche di valutazione psicologica – Terapia e consulenza psicologica
	Esperienza informatica	Competenze di informatica di base.
	Invalidità / limitazioni	Uso del software escluso ai portatori di handicap legati alla vista e alle articolazioni delle mani.
16. RAD / RID (Responsabile Area Dipartimentale/ Responsabile Infermieristico Dipartimentale)	***Età***	*DATO NON SIGNIFICATIVO.*
	Genere	*DATO NON SIGNIFICATIVO.*
	Educazione	Laurea breve.
	Comprensione linguistica	Italiana, inglese.
	Conoscenze professionali	Direzionali: – Partecipazione al raggiungimento degli obiettivi assegnati al Dipartimento e alla

		DPS – Conoscenza, utilizzo e promozione di strumenti operativi per l'analisi del contesto organizzativo e per il governo dei processi – Elaborazione e implementazione di progetti organizzativi – Pianificazione attività per lo sviluppo, la gestione e il controllo dei processi operativi
	Esperienza informatica	Competenze di informatica di base.
	Invalidità / limitazioni	Uso del software escluso ai portatori di handicap legati alla vista e alle articolazioni delle mani.
Area amministrativa		
17. Assistenti amministrativi	***Età***	*DATO NON SIGNIFICATIVO.*
	Genere	*DATO NON SIGNIFICATIVO.*
	Educazione	Fino alla scuola dell'obbligo.
	Comprensione linguistica	Italiana.
	Conoscenze professionali	*DATO NON SIGNIFICATIVO.*
	Esperienza informatica	Competenze informatiche necessarie per usare fogli elettronici, elaborare testi al computer, gestire archivi e database e altre applicazioni (ad esempio software gestionali).
	Invalidità / limitazioni	Uso del software escluso ai portatori di handicap legati alla vista e alle articolazioni delle mani.
18. Personale amministrativo (impiegati)	***Età***	*DATO NON SIGNIFICATIVO.*
	Genere	*DATO NON SIGNIFICATIVO.*
	Educazione	Licenza media superiore.
	Comprensione linguistica	Italiana.

	Conoscenze professionali	– Contabilità generale e fiscale – Diritto commerciale – Diritto privato – Bilancio d'esercizio – Contabilità analitica – Budgeting
	Esperienza informatica	Competenze di informatica di base.
	Invalidità / limitazioni	Uso del software escluso ai portatori di handicap legati alla vista e alle articolazioni delle mani.
Area tecnica		
19. Sviluppatori	***Età***	*DATO NON SIGNIFICATIVO.*
	Genere	*DATO NON SIGNIFICATIVO.*
	Educazione	Licenza media superiore.
	Comprensione linguistica	Italiana, inglese.
	Conoscenze professionali	– Ambienti di sviluppo e strumenti (CASE e IDE) – Applicazioni critiche e distribuite – Basi di Dati – Linguaggi e metodi di programmazione – Componenti hardware e software – Elementi di networking e comunicazioni – Disegno dei sistemi e implementazione – Ingegneria dei requisiti – Principi di programmazione sicura – Elementi di sicurezza informatica – Progettazione, sviluppo e utilizzo di applicazioni web – Strategie organizzative e sistemi ITC correlati – Regole per il collaudo di sistema – Principi di testing
	Esperienza informatica	Competenze di informatica applicata.
	Invalidità / limitazioni	Uso del software escluso ai portatori di handicap legati alla vista e alle articolazioni delle mani.

V. *Principio operativo*

I risultati sono riportati in forma tabellare (Tabella 23).

Tabella 23. Risultati relativi ai profili utenti

Utente	*Interazioni attese*
1. Rilascio	
Categoria I	
Sviluppatori	Procedura tecnica
2. Primo avvio	
Categoria I	
Sviluppatori	Procedura tecnica
3. Funzionamento operativo	
Categoria A	
Personale medico	Terapia Ammissione Richieste di consulenze / esami strumentali Risposte di consulenze / esami strumentali Procedura sanitaria
Direzione SOD	
Categoria A bis	
Anestesisti	Terapia Richieste di consulenze / esami strumentali Risposte di consulenze / esami strumentali Procedura sanitaria
Categoria B	
Personale infermieristico e ostetrico	Terapia Ammissione Procedura sanitaria
Categoria C	
Professioni tecnico sanitarie e della riabilitazione (fisioterapisti)	Solo lettura Risposte di consulenze / esami strumentali Procedura sanitaria
Categoria D	
OSS	Ammissione Procedura sanitaria

Categoria E	
Biologi	Solo lettura Risposte di consulenze / esami strumentali
Professioni tecnico sanitarie (dietisti) e della riabilitazione	
Assistenti sociali	
Psicologi	
Categoria F	
Personale farmaceutico	Terapia
Categoria G	
Personale amministrativo	Procedura amministrativa Ammissione
Categoria G bis	
Assistenti amministrativi	Ammissione
Categoria H	
Studenti medicina	Solo lettura
RAD (Responsabile Area Dipartimentale) / RID	
Direzione sanitaria	
Trasporto pazienti	
MMG (Medici Medicina Generale)	
4. Manutenzione	
Categoria I	
Sviluppatori	Procedura tecnica
5. Dismissione	
Categoria I	
Sviluppatori	Procedura tecnica

VI. *Ambienti di utilizzo*

1. Gli ambienti di utilizzo riguardano tutte le Unità Operative (U.O.) dei presidi Ospedalieri Aziendali di:

A. Addestramento all'uso
   a. Aula informatica
   b. Ambienti di utilizzo reale

B. Rilascio
   a. Uffici – logistica

C. Primo avvio
   a. Uffici – logistica

D. Funzionamento operativo
   a. Ambulatori
   b. Ambulatori MMG
   c. Degenze
   d. Farmacia ospedaliera
   e. Laboratori
   f. Uffici
   g. Altro (SMART WORKING)

E. Manutenzione
   a. Uffici – logistica

F. Dismissione
   a. Uffici – logistica

2. Visibilità:

2.1 Luminosità :

Tabella 24. Risultati relativi alla luminosità degli ambienti di utilizzo

Ambienti di utilizzo	***Luminosità media (E_m)*** [18]
2.1 Ambulatori 2.2 Ambulatori MMG	Em : 500 lx
2.3 Aula informatica	Em : 200 lx
2.4 Degenze	Em : 500 lx
2.5 Farmacia ospedaliera	Em : 500 lx
2.6 Laboratori	Em : 300 lx

2.7 Uffici	Em : 200 lx
2.8 Altro (SMART WORKING)	*DATO NON SIGNIFICATIVO.*

2.2 Distanza di visualizzazione: [19]

Tabella 25. Risultati relativi alla distanza di visualizzazione

Uso da scrivania	da 50 cm a 75 cm
Dispositivi touch screen	

2.3 Angolo di visualizzazione del monitor: da 10° a 30° (rispetto a un'asse orizzontale).

5.3 Identificazione delle specifiche delle interfacce utente

Le specifiche delle interfacce utente devono comprendere le seguenti informazioni:

- *I requisiti tecnici, compresi i requisiti per le parti dell'INTERFACCIA UTENTE associate alle misure di CONTROLLO DEI RISCHI selezionate;*
- *Indicazioni sulla necessità di una documentazione di accompagnamento e/o formazione specifica*

Per identificare le specifiche delle interfacce utente sono stati considerati i seguenti fattori:

- *Specifiche d'uso*
- *Errori d'uso noti o prevedibili*
- *Scenari d'uso connessi ai pericoli*

(5.7, *Establish user interface specification*, [11])

5.3.1 Risultati

Le interfacce utente devono essere valutate considerando i seguenti fattori:

- Dispositivi di comando,
- Codici colore,
- Indicatori,
- Simbologia,
- Ergonomia,
- Disposizione dei comandi,
- Gerarchia delle operazioni,
- Menu software,
- Visibilità degli avvisi,
- Udibilità degli avvisi.

Le indicazioni sulla necessità di una documentazione di accompagnamento e/o formazione specifiche risultano essere le seguenti:

Tabella 26. Risultati relativi alle specifiche delle interfacce utente

Fasi di utilizzo del software	*Necessità di:*	
	Corso di formazione*	Manuale d'uso
1. Rilascio	/	/
2. Primo avvio		X
3. Funzionamento operativo	X	X
4. Manutenzione	X	X
5. Dismissione		X

***** Corso di formazione e affiancamento organizzato da tutor interni all'Ospedale e della durata di circa una settimana, con l'obiettivo di far acquisire all'utente autonomia nella manutenzione e nella realizzazione di nuove funzioni.

5.4 Valutazione dell'usabilità delle interfacce utente: nuovo approccio

5.4.1 Analisi euristica

Tra i metodi principali di valutazione dell'usabilità delle interfacce utente proposti dalla norma, i più comuni risultano essere l'analisi euristica e il test di usabilità. Viene di seguito riportata una tabella (Tabella 27) in cui vengono messi a confronto questi due metodi, evidenziando anche gli svantaggi e i vantaggi di entrambi.

Tabella 27. Confronto tra caratteristiche connesse all'analisi euristica e al test di usabilità

Analisi euristica Vs Test di Usabilità	
Analisi euristica	**Test di usabilità**
Scopo	
Focus sulla progettazione dell'interfaccia software. Per andare a valutare quanto bene la progettazione dell'interfaccia del software in esame aderisca alle linee guida, ai principi o all'euristica dell'interfaccia (regole per la progettazione dell'interfaccia che generalmente, ma non sempre, funzionano).	Focus sugli utenti finali. [...] Per trovare un prototipo che piace agli utenti: si impara facilmente e può essere utilizzato per eseguire correttamente le attività (efficacia, efficienza, soddisfazione dell'utente).
Persone coinvolte	
3-5 Specialisti. È probabile che diversi esperti di HCI scoprano una serie diversa di problemi. Per questo motivo, è importante che da due a quattro esperti valutino il sistema in modo indipendente.	– 5-6 Utenti tipici, – Team di design Gli sviluppatori fanno meglio a eseguire un test di usabilità con sei persone, apportare modifiche e quindi eseguire un altro test sul software rivisto piuttosto che eseguire un singolo test di usabilità con altri sei partecipanti.
Ambiente	
Nessun requisito	Ambiente reale. […] L'ambiente attentamente controllato limita i fattori estranei che potrebbero influenzare le prestazioni. […] Per alcuni prodotti, problemi critici possono emergere solo in ambienti più realistici.
Vantaggi	

– Velocità ed efficacia. – È un metodo più economico di altri. – Non richiede il coinvolgimento degli utenti finali. – Comprende lo stato attuale del prodotto. – Identifica i problemi di base che possono essere evitati se si tratta di una riprogettazione. – Propone anche soluzioni per risolverli, sulla base dell'esperienza dei valutatori.	– La comunicazione è diretta con il target di riferimento. – Puoi rispondere a domande sul prodotto attraverso un'analisi. – Valuta come gli utenti rispondono a diverse alternative. I potenziali problemi vengono rilevati prima del rilascio del prodotto. – Gli utenti possono raggiungere i propri obiettivi, assicurandosi che l'azienda raggiunga i propri obiettivi.
Svantaggi	
– È possibile ottenere errori fasulli che non sono associati a problemi di usabilità. – Non specifica in modo semplice o chiaro quale sia la soluzione per le caratteristiche individuate.	– I test non sono rappresentativi al 100% dello scenario della vita reale. – È un metodo qualitativo. Ciò significa che non fornisce grandi campioni di commenti.

A partire dalle specifiche sopra definite e dai rischi connessi agli errori di utilizzo, è stata utilizzata l'analisi euristica per valutare l'interfaccia software del prodotto, facendo riferimento alle note euristiche di Zhang.

5.4.2 Definizione del problema

È stato proposto un nuovo approccio per risolvere i seguenti problemi:

1 Analisi basata su regole generali

2 Il focus è sull'utente: l'analisi viene fatta a partire dalla difficoltà che l'utente riscontra nell'utilizzo di una funzione

3 Le violazioni delle euristiche rispondono alla domanda *Cosa non ha per essere usabile?* ma non contengono informazioni sufficienti a stabilire *Come dovrebbe essere per essere usabile?* se non raccomandazioni basate solo sull'esperienza del valutatore e di conseguenza soggettive.

4 L'analisi euristica non è un metodo sistematico ed è limitata, in quanto i soli problemi di usabilità che verranno rilevati sono quelli incapsulati dalle stesse euristiche. Se un particolare problema di progettazione del dispositivo non rientra nelle 14 euristiche, è improbabile che esso sia individuato attraverso un'analisi euristica. Inoltre, assegnare un punteggio di gravità a ciascun problema di usabilità è un esercizio soggettivo. Per questi motivi, un'analisi euristica è generalmente considerato un metodo di valutazione informale.

5 La dipendenza dell'analisi dall'esperienza del valutatore fa sì che questo metodo debba essere svolto per lo più da esperti di usabilità, come i professionisti dei fattori umani, in quanto

addestrati a vedere i problemi che violano i principi delle migliori pratiche nella progettazione. Inoltre, dovrebbero essere inclusi esperti in materia (ad es. clinici) per la loro conoscenza dei processi che verranno intrapresi con il DMSW valutato. È possibile abbinare un esperto di usabilità e un esperto in materia per ogni valutazione, al fine di identificare una gamma più ampia di problemi da ciascuna valutazione. Se invece vengono coinvolti esperti di non usabilità, una raccomandazione consueta è quello di dedicare del tempo a familiarizzare e ad esercitarsi con l'interfaccia utente, applicando le euristiche a dispositivi diversi prima di intraprendere la valutazione euristica. Per i valutatori meno esperti, la raccomandazione è quella di coinvolgere di più valutatori in un'unica valutazione, al fine di aumentare la probabilità di scoprire problemi di usabilità.

Gli svantaggi relativi all'approccio standard dell'analisi euristica rendono il metodo SOGGETTIVO

Esempio: struttura per un'analisi euristica standard (Tabella 28)

Tabella 28. Struttura per analisi euristica standard

	Nome del valutatore **Dispositivo**
Scala di gravità	**Descrizione**
0	Non è un problema di usabilità. *Nessuna correzione richiesta.*
1	Problema solamente estetico. *Non deve essere risolto a meno che non sia disponibile tempo extra.*
2	Problema di usabilità minore. *La risoluzione di questo problema dovrebbe avere una priorità bassa.*
3	Problema di usabilità Maggiore. *Risolvere questo problema è importante e dovrebbe avere la massima priorità.*
4	Problema di usabilità catastrofico. *La correzione di questo è fondamentale e deve essere eseguita prima che il prodotto possa essere rilasciato.*

14 Euristiche di Zhang	
1. [Consistenza] *Consistenza e standard*	**2. [Visibilità]** *Visibilità dello stato di sistema*
3. [Corrispondenza] *Corrispondenza tra Sistema e mondo reale*	**4. [Minimalista]** *Minimalista*
5. [Memoria] *Minimizzare il carico di memoria*	**6. [Feedback]** *Feedback informativo*
7. [Flessibilità] *Flessibilità ed efficienza*	**8. [Messaggio]** *Messaggi d'errore efficacy*
9. [Errore] *Prevenire errori*	**10. [Chiusura]** *Chiusura chiara*
11. [Reversibilità] *Azioni reversibili*	**12. [Languaggio]** *Usare il linguaggio dell'utente*
13. [Controllo] *Utenti al controllo*	**14. [Documentazione]** *Aiuto e documentazione*

POSIZIONE DEL PROBLEMA	**DESCRIZIONE DEL PROBLEMA**	**RACCOMANDAZIONI**	**EURISTICHE VIOLATE** **SCALA di GRAVITà**
			0 1 2 3 4

5.4.3 Soluzioni proposte

Scopo del lavoro: Introduzione di criteri oggettivi di usabilità nell'analisi euristica

Soluzione proposta:

Nuovo approccio: Introduzione delle linee guida di design

A partire da questa considerazione, è stato proposto di valutare l'usabilità delle funzioni considerando il problema non solo a livello delle euristiche violate, ma sin dalla sicurezza intrinseca nel design.
Per valutare tale aspetto sono state applicate le linee guida AAMI HE75 *Human factors engineering – Design of medical devices* andando a confrontare *prima* se la funzione in analisi rispetti o meno le linee guide e *poi* quali euristiche vengono violate se quelle stesse raccomandazioni non vengono rispettate, e andando infine a sostituire le raccomandazioni soggettive del valutatore con criteri oggettivi di usabilità forniti dalle stesse linee guida. Le stesse raccomandazioni fornite al termine di un'analisi euristica divengono in tal modo lo strumento da cui partire per la fase successiva all'analisi: misure di controllo a livello di design (safety by design).

Di seguito vengono riportati i riferimenti utilizzati per la violazione delle euristiche e per la violazione delle linee guida di design / raccomandazioni per le euristiche violate:

a) **Riferimenti per le violazioni euristiche: 14 Euristiche di Zhang** [12]

b) **Riferimenti per le violazioni di usabilità nel design/ criteri di usabilità: ANSI/AAMI HE75:2009, Human factors engineering – Design of medical devices** [21]

Questa pratica raccomandata è stata prodotta da *Association for the Advancement of Medical Instrumentation* (AAMI) e copre i principi generali dell'ingegneria dei fattori umani (HFE), i principi HFE specifici orientati verso determinati attributi dell'interfaccia utente e le applicazioni speciali dell'HFE (ad es. connettori, controlli, display visivi, automazione, interfacce software-utente, utensili manuali, workstation , dispositivi medici mobili, dispositivi sanitari domiciliari.

"Le interfacce software-utente di tutti i tipi di dispositivi medici dovrebbero facilitare le attività degli utenti, prevenire errori di utilizzo e soddisfare le esigenze degli utenti. Sfortunatamente, molti errori di utilizzo relativi al dispositivo e lamentele degli utenti derivano da carenze nelle interfacce software-utente. […] Questi problemi di usabilità sono evitabili. L'applicazione delle pratiche di progettazione dell'interfaccia utente-software consigliate qui (Tabella 29) produrrà soluzioni che hanno maggiori probabilità di soddisfare le esigenze degli utenti e di ridurre gli errori di utilizzo." [21]

Tabella 29. Linee guida di usabilità nel design di un'interfaccia software

Linee guida AAMI HE75 (Categorie)	Descrizione
1. Modello concettuale	Fornire un costrutto generale su come gli utenti penseranno a un'interfaccia utente. *(vale a dire, l'immagine mentale che gli utenti formano su come funziona l'interfaccia utente-software)*
2. Struttura dell'interfaccia utente	Posizionare i singoli schermi in una gerarchia logica che integri il modo in cui le persone preferiscono affrontare attività frequenti, urgenti e critiche.
3. Stile di interazione	Stabilire un modello di interazione tra l'utente e l'applicazione software che faciliti le attività e soddisfi le capacità degli utenti.
4. Layout della schermata	Organizzare le informazioni nello schermo in modo che gli utenti possano individuare rapidamente elementi specifici e creare associazioni appropriate.
5. Leggibilità	Presentare le informazioni testuali e grafiche in modo chiaro in modo che gli utenti possano leggerle e discriminare i dettagli importanti.
6. Estetica	Presentare le informazioni in modo visivamente gradevole in modo che l'interfaccia utente non intimidisca i nuovi utenti e influenzi positivamente le prestazioni delle attività.
7. Inserimento dati	Stabilire regole su come gli utenti inseriscono i dati o effettuano le selezioni tramite l'interfaccia software-utente.
8. Colore	Usare il colore in modo tale da contribuire alla chiarezza delle informazioni in modi significativi e attirare l'attenzione sulle informazioni più importanti.
9. Display dinamici	Utilizzare elementi grafici e testuali attivi per trasmettere le informazioni in modo più convincente di quanto sia possibile utilizzando display statici.
10. Meccanismi di interazione speciali	Fornire informazioni relative a meccanismi di controllo meno comuni, come interfacce utente con tasti funzione, rotellina di controllo e touchscreen e tastiere su schermo.

11. Supporto utente	Fornire agli utenti le informazioni al momento giusto e nel formato corretto, per aiutarli a svolgere le attività in modo sicuro, rapido ed efficace.
12. Consistenza	Cercare di fornire lo stesso tipo di controlli quando possibile.

5.4.4 Metodi

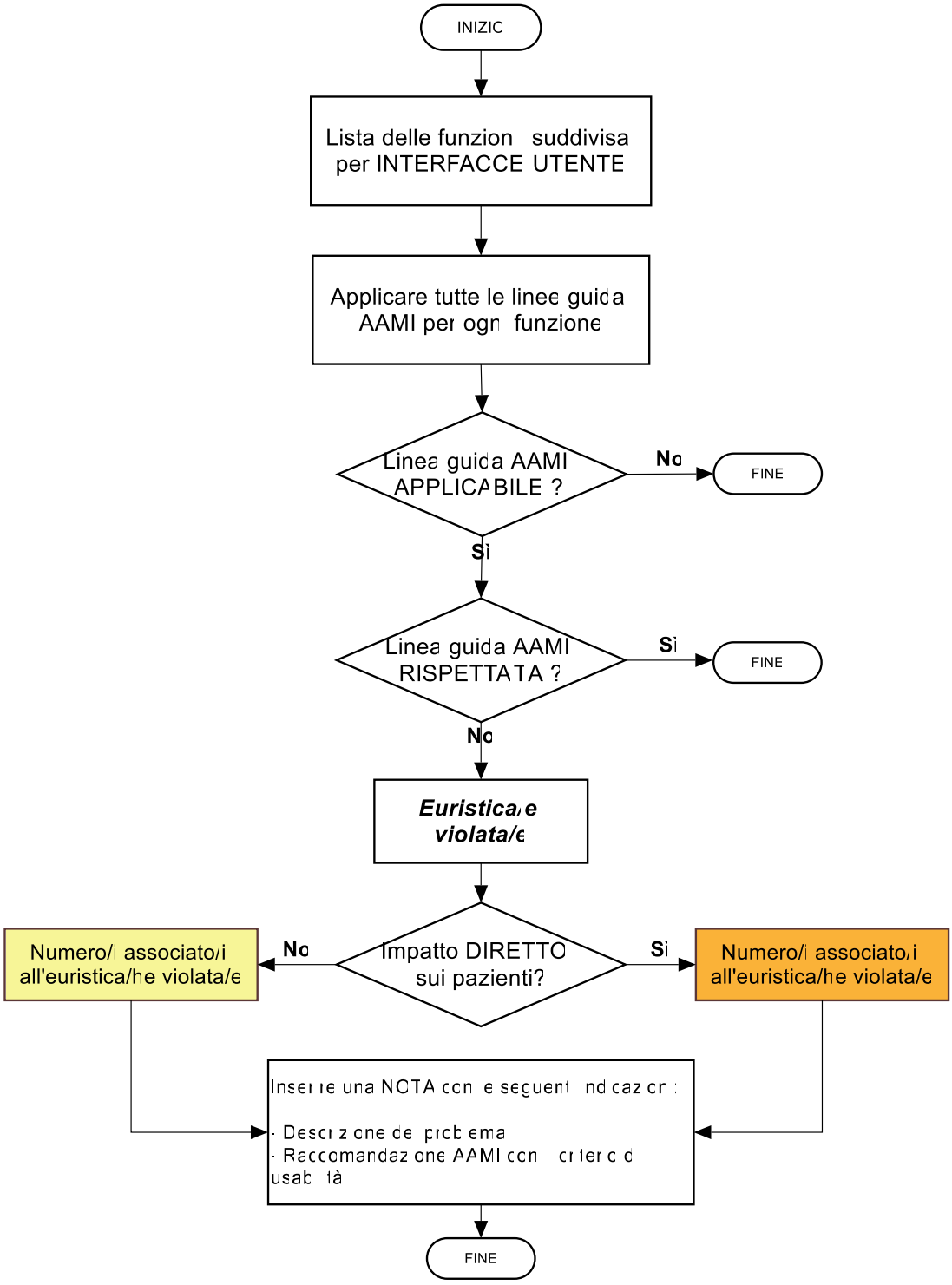
L'analisi euristica è stata pianificata come segue:

- Sono state dapprima selezionate le interfacce utente il cui utilizzo fosse a scopo medico (sono stati considerati sia i profili utente corrispondenti sia gli ambienti di utilizzo)
- Per ciascuna interfaccia utente, è stato fatto un elenco di tutte le funzioni
- Essendo le interfacce del prodotto (e dunque le funzioni) diverse a seconda del profilo utente considerato, le interfacce selezionate al punto precedente sono state ulteriormente suddivise in funzione dei profili utente il cui uso del prodotto fosse a scopo medico e ad impatto diretto sul paziente, e sono state analizzate separatamente.
- Per valutare il rispetto dei princìpi di buon design sono state applicate le raccomandazioni AAMI HE75.
- Per valutare la violazione delle euristiche sono state applicate le 14 euristiche di Zhang.
- La scala di gravità da assegnare alle violazioni delle euristiche è stata imposta di tipo binario: impatto diretto/indiretto sui pazienti della funzione analizzata.

A partire dalla pianificazione sopra definita, l'analisi euristica è stata condotta come segue:

I. È stato fatto un elenco delle funzioni del prodotto, ed è stato ripetuto per tutti gli utenti selezionati nella pianificazione dell'analisi
II. Per ogni funzione di ogni interfaccia utente sono state applicate le raccomandazioni AAMI HE75
III. Se la raccomandazione non era applicabile, la valutazione euristica è stata interrotta
IV. Se la raccomandazione era applicabile, è stato valutato se fosse rispettata dalla funzione in analisi
V. Se la funzione rispettava la raccomandazione, la valutazione euristica è stata interrotta
VI. Se la funzione NON rispettava la raccomandazione, è stato valutato se la funzione andasse a violare una o più delle euristiche
VII. Per ogni euristica relativa a ciascuna raccomandazione, è stata indicata quale fosse stata violata ed è stata aggiunta una nota con la descrizione del problema e lo status attuale della funzione
VIII. È stata infine assegnata una scala di gravità in base all'impatto diretto o meno sui pazienti da parte delle funzione analizzata

Di seguito viene riportato il Flowchart 5.1 che rappresenta l'iter procedurale appena descritto:



Flowchart 5.1 Analisi euristica con il *nuovo approccio*

5.4.5 Risultati

- **Utenti e interazioni software con destinazione medica d'uso**

Le interfacce software con destinazione d'uso medica sono risultate essere quelle relative ai seguenti profili utente (identificati nelle specifiche d'uso):

1. Medico: ambiente di utilizzo in reparto
2. Medico: ambiente di utilizzo in ambulatorio
3. Infermiere: ambiente di utilizzo in reparto
4. Infermiere: ambiente di utilizzo in ambulatorio
5. OSS: ambiente di utilizzo in reparto
6. Trasporto pazienti: ambiente di utilizzo in reparto

Le interazioni dei profili utente con destinazione medica d'uso sono riportate nella seguente Tabella 30:

Tabella 30. Risultati relativi alle interazioni software

Utente	*Interazioni software*
Funzionamento operativo	
Personale medico	Terapia Ammissione Richieste di consulenze / esami strumentali Risposte di consulenze / esami strumentali Procedura sanitaria
Personale infermieristico	Terapia Richieste di consulenze / esami strumentali Risposte di consulenze / esami strumentali Procedura sanitaria
OSS	Solo lettura Risposte di consulenze / esami strumentali Procedura sanitaria
Trasporto pazienti	Solo lettura

- **Struttura del metodo**

Il nuovo approccio ha portato risultati nuovi sin dalla struttura stessa del metodo di valutazione. Di seguito vengono riportate a confronto le strutture rispettivamente dell'approccio standard per l'analisi euristica e del nuovo approccio:

a) Analisi euristica: approccio standard (Tabella 31)

Tabella 31. Risultati relativi alla struttura dell'analisi euristica standard

POSIZIONE DEL PROBLEMA	DESCRIZIONE DEL PROBLEMA	RACCOMANDAZIONI	EURISTICHE VIOLATE SCALA di GRAVITà
PAZIENTE *Funzione*			
Visualizzazione dei messaggi pop-up	1)La dimensione della finestra di messaggio è molto piccola e la visualizzazione dei messaggi viene confusa con il colore della barra superiore. 2)I colori di prova/sfondo molto simili non consentono una lettura immediata.	Coerenza con la visualizzazione e il design della finestra di messaggio e del display LETTI.	*5 [Memoria]* *7 [Flessibilità ed Efficienza]* 0 | 1 | 2 | 3 | 4

b) Analisi euristica: nuovo approccio (Tabella 32)

Tabella 32. Risultati relativi alla struttura dell'analisi euristica con il nuovo approccio

Profilo utente: MEDICO	Interfaccia UI			
Funzioni	**Linea guida violata**	**Euristiche violate**	**Descrizione problema**	**Criteri di usabilità**
Pazienti Home Page	1) Messaggi pop-up 2) Contrasto testo sfondo	**5) Memoria** **7) Flessibilità ed efficienza**	Visibilità degli alerts variabile nel tempo e nello spazio: non esiste una posizione fissa non esiste un "periodo" di tempo fisso in cui restano visibili.	1) Numero di messaggi pop-up: minimo necessario Posizione dei popup: tale da non sovrapporre informazioni importanti su altre schermate. Contenuto informativo: sufficiente per essere compreso dall'utente. L'azione del pop up deve essere reversibile. 2) Contrasti suggeriti per le informazioni critiche:

				testo bianco su sfondo nero o testo nero su sfondo bianco. Contrasti da evitare: caratteri rossi saturi su uno sfondo blu altrettanto saturo.

- **Numero di violazioni per ogni interfaccia software**

  A partire dai due metodi di valutazione, è stato utilizzato lo stesso approccio per analizzare i risultati e renderli confrontabili tra di loro. A partire dalla scala di gravità prestabilita, e per entrambi i metodi di valutazione, sono stati analizzati i risultati relativi alle violazioni delle interfacce utente di ciascun profilo con destinazione medica d'uso analizzata; i risultati sono stati separati in base al livello di gravità stesso e, per ciascuno dei due livelli, sono stati poi riportati separatamente in funzione sia delle linee guida che delle 14 euristiche.

a) Numero di violazioni Linee guida AAMI HE75 per ogni interfaccia software

Interfacce software relative ai profili utente con destinazione medica d'uso: (Figure 5.1 e 5.2)

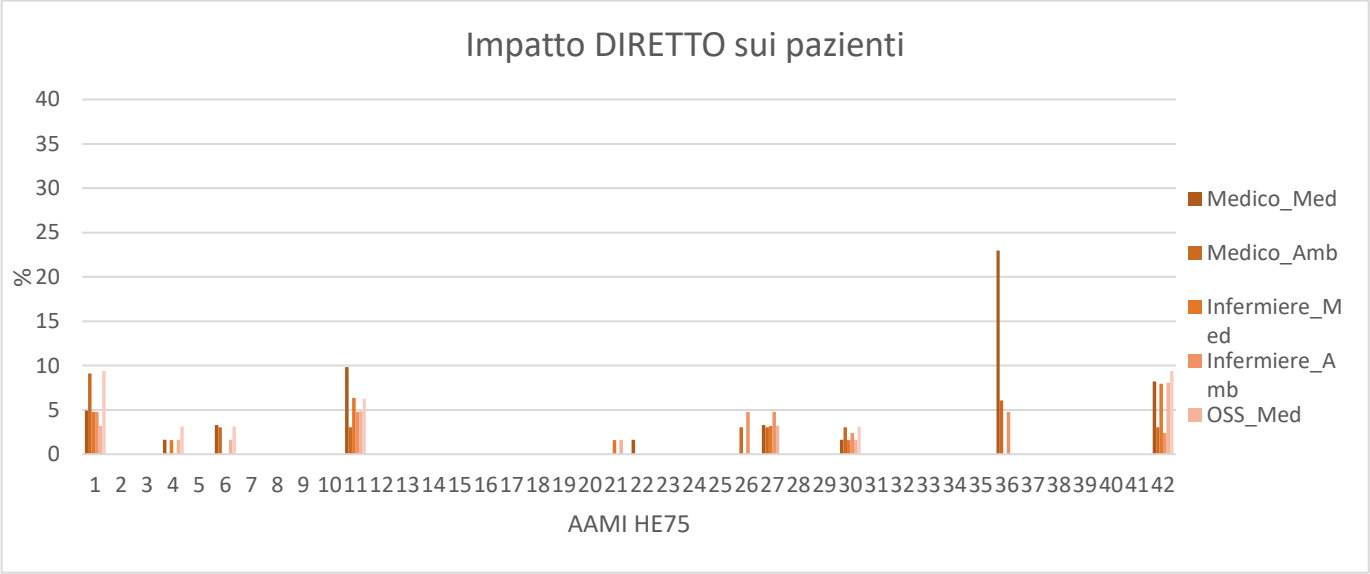


Figura 5.1. Risultati relativi al numero di violazioni delle linee guida: impatto diretto sui pazienti

Tabella 33. Risultati relativi al numero di violazioni delle linee guida: impatto diretto sui pazienti

Livello di gravità	AAMI HE75 violata	N° max di violazioni (%)	Profilo utente (ambiente di utilizzo)
Impatto DIRETTO sui pazienti	36) Messaggi pop-up	22.9 %	Medico (reparto)

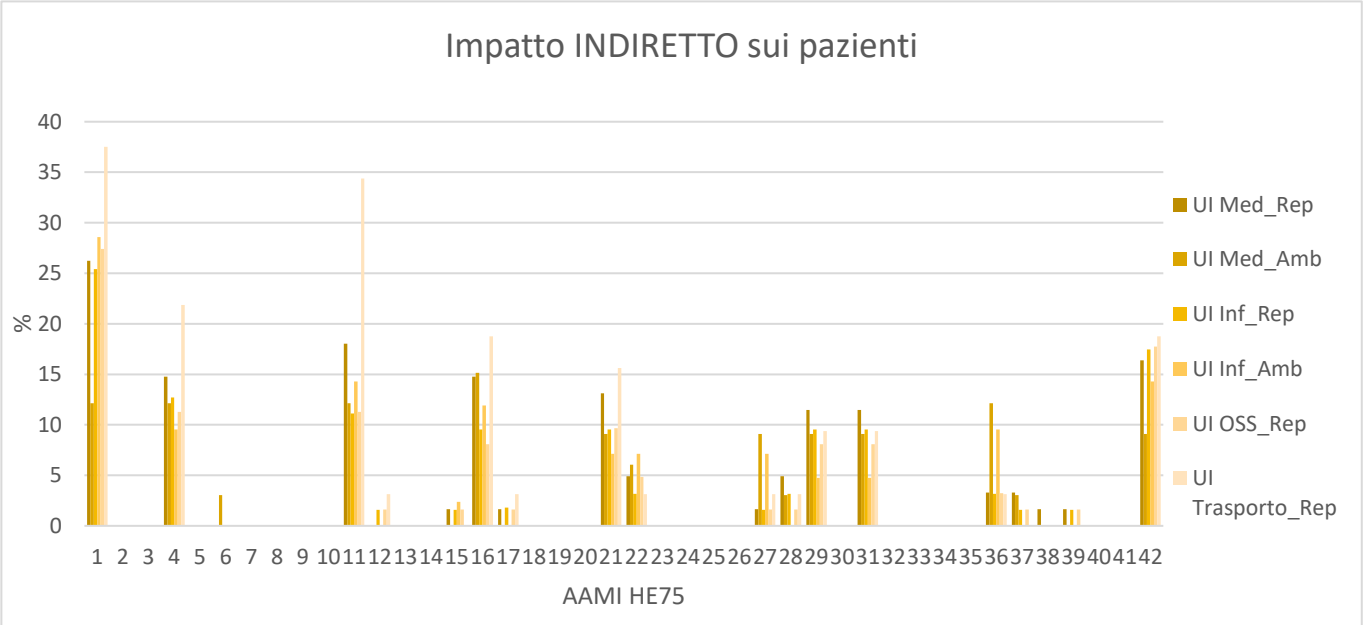


Figura 5.2. Risultati relativi al numero di violazioni delle linee guida: impatto indiretto sui pazienti

Tabella 34. Risultati relativi al numero di violazioni delle linee guida: impatto indiretto sui pazienti

Livello di gravità	AAMI HE75 violata	N° max di violazioni (%)	Profilo utente (ambiente di utilizzo)
Impatto INDIRETTO sui pazienti	1) Ritmo delle attività	37.5%	Medico (reparto)

LEGENDA

n° MAX violazioni	Impatto DIRETTO sui pazienti
n° MAX violazioni	Impatto INDIRETTO sui pazienti

ETICHETTA ASCISSA	LINEA GUIDA AAMI HE75
1	**Ritmo delle attività** (Profilo sanitario: trasporto pazienti)
2	Compatibilità del dispositivo di puntamento
3	Coerenza dello stile di interazione
4	Griglia di allineamento
5	Gerarchia dei contenuti
6	Distribuzione dei contenuti
7	Margini e Spazi bianchi
8	Stile del testo
9	Dimensione del testo
10	Contrasto testo-sfondo
11	Maiuscole del testo
12	Spaziatura interlinea
13	Giustificazione del testo
14	Lunghezza della stringa
15	Icone (simboli)
16	Uso del colore
17	Uso della grafica
18	Densità dello schermo
19	Branding
20	Campi di immissione dati
21	Uso di etichette e unità di misura
22	Posizionamento e aspetto dell'etichetta
23	Giustificazione dei dati
24	Array di dati
25	Riempimento automatico
26	Convalida e controllo dei dati
27	Numero di colori
28	Non fare affidamento sul colore
29	Combinazione di colori
30	Associazioni di colori
31	Personalizzazione del colore
32	Utilizzo del colore per delimitare o indicare lo stato
33	Trend
34	Forme d'onda
35	Valori numerici
36	**Messaggi pop-up** (Profilo: medico, reparto)
37	Concisione
38	Differenziazione
39	Stile
40	Grafica
41	Animazioni
42	Consistenza

b) Numero di violazioni 14 Euristiche di Zhang per ogni interfaccia software

Interfacce software relative ai profili utente con destinazione medica d'uso; i risultati sono separati per livello di gravità:

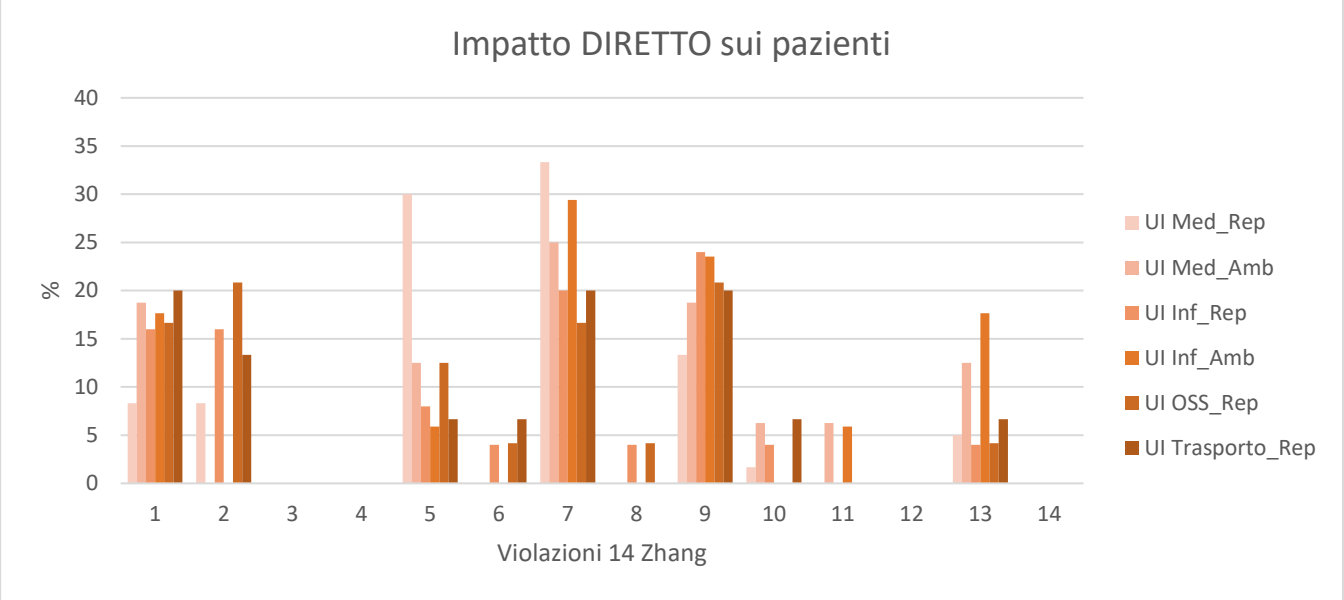


Figura 5.3. Risultati relativi al numero di violazioni delle euristiche: impatto diretto sui pazienti

Tabella 35. Risultati relativi al numero di violazioni delle euristiche: impatto diretto sui pazienti

Livello di gravità	**Euristica violata**	**N° max di violazioni (%)**	**Profilo utente (ambiente di utilizzo)**
Impatto DIRETTO sui pazienti	7) Flessibilità ed efficienza	33.3 %	Medico (reparto)

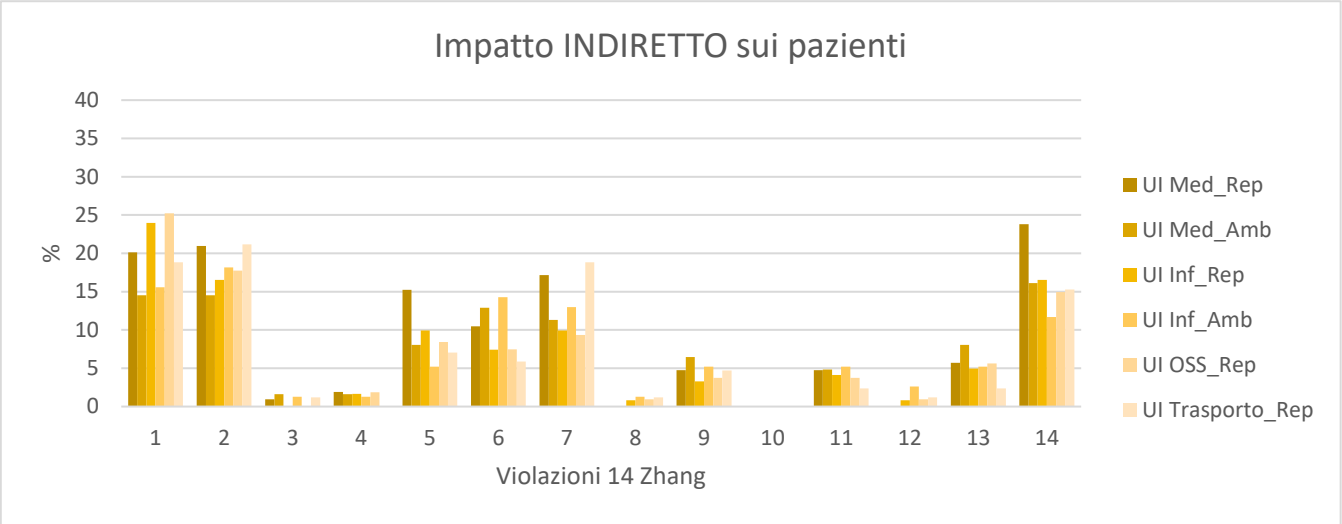


Figura 5.4. Risultati relativi al numero di violazioni delle euristiche: impatto indiretto sui pazienti

Tabella 36. Risultati relativi al numero di violazioni delle euristiche: impatto indiretto sui pazienti

Livello di gravità	**Euristica violata**	**N° max di violazioni (%)**	**Profilo utente (ambiente di utilizzo)**
Impatto INDIRETTO sui pazienti	1) Consistenza e standard	25.2 %	Medico (reparto)

LEGENDA

n° MAX violazioni	Impatto DIRETTO sui pazienti
n° MAX violazioni	Impatto INDIRETTO sui pazienti
ETICHETTA ASCISSA	**14 EURISTICHE DI ZHANG**
1	**Consistenza e standard** (Profilo: OSS)
2	Visibilità dello stato del sistema
3	Corrispondenza tra sistema e mondo
4	Minimalista
5	Minimizzare il carico di memoria
6	Feedback informativo
7	**Flessibilità ed efficienza** (Profilo: medico, reparto)
8	Messaggi di errore esaustivi
9	Prevenire errori
10	Chiusura chiara delle azioni
11	Azioni reversibili
12	Uso del linguaggio dell'utente
13	Controllo in mano all'utente
14	Aiuto e documentazione

È stato possibile analizzare i risultati sia da un punto di vista quantitativo (numero di violazioni ad impatto diretto/indiretto) sia di tipo qualitativo (tipologia di linea guida/euristica con il maggior numero di violazioni raggiunto).

Sia per il metodo di valutazione delle euristiche che per il metodo di valutazione delle linee guida, il numero delle violazioni di ciascuna interfaccia utente è risultato inferiore del 40 % rispetto a entrambi i livelli di gravità. Inoltre, per entrambi i metodi, il numero delle violazioni con impatto diretto sui pazienti è risultato essere inferiore rispetto a quello con impatto indiretto.

In particolare, rispetto alla **valutazione delle linee guida,** il maggior numero di violazioni ad impatto diretto è stato verificato nell'interfaccia utente del profilo medico (22.9%), e la corrispondente linea guida è risultata essere nel design dei *messaggi pop-up*; il maggior numero di violazioni ad impatto indiretto è stato invece verificato nell'interfaccia utente del profilo sanitario dei trasporti (37.5%) e la corrispondente linea guida è risultata nel design sul *ritmo delle attività*.

Rispetto alla **valutazione delle euristiche di Zhang**, invece, il maggior numero di violazioni ad impatto diretto sui pazienti è stato verificato nell'interfaccia utente del profilo medico (33.3%) e la corrispondente euristica è risultata essere *flessibilità ed efficienza*; il maggior numero di violazioni ad impatto indiretto è stato invece verificato nell'interfaccia utente del profilo OSS (25.2%) e la corrispondente euristica è risultata essere *consistenza e standard*.

5.5 Discussione e conclusioni

5.5.1 Discussione

Il dispositivo medico software in esame è stato soggetto al processo di gestione dei rischi per la valutazione di conformità ai requisiti del regolamento MDR 2017/745.

I rischi connessi agli errori di utilizzo sono risultati dipendere in modo critico dall'usabilità. È stata dunque verificata la conformità del dispositivo all'usabilità con riferimento alla norma 62366-1.

Nella fase di valutazione delle interfacce utente è stato introdotto un nuovo approccio: alla tradizionale analisi euristica è stata aggiunta una valutazione sul rispetto delle linee guida nel design dell'interfaccia.

In base ai risultati ottenuti è possibile affermare che l'usabilità del prodotto non risulta conforme; dunque quest'ultimo dovrà essere sottoposto a successive misure di controllo.

L'introduzione del nuovo approccio nell'analisi euristica ha aggiunto informazioni che prima mancavano e ha sostituito informazioni soggettive con criteri oggettivi.

Innanzitutto con il nuovo approccio è possibile valutare sia quale euristica viene violata sia quale principio di usabilità a livello di design viene violato; ciò ha permesso di aggiungere un elemento informativo nell'analisi: l'euristica violata identifica il problema che l'utente riscontra durante l'uso dell'interfaccia software (focus utente); la linea guida violata identifica il problema insito nell'interfaccia stesso (focus software). Tale elemento informativo dell'interfaccia software evidenzia al contempo sia il problema che la relativa soluzione, necessaria anche alla successiva misura di controllo *safety by design*.

Un'altra novità vede la sostituzione delle raccomandazioni soggettive con i criteri di usabilità oggettivi. Non sono più necessarie raccomandazioni basate sull'esperienza del valutatore, bensì criteri di usabilità oggettivi e universali, insiti nelle stesse linee guida che sono state violate; il focus non è più dunque sul valutatore e sulla sua esperienza (con conseguente vincolo della necessità di avere un numero ampio di valutatori e valutatori esperti), bensì sulla scelta di linee guida di design conformi al dispositivo in questione.

Quest'ultima osservazione porta all'ultima conclusione: l'introduzione del nuovo approccio nell'analisi euristica non è limitato al campo di esperienza del valutatore e di conseguenza ai dispositivi di cui ne conosce meglio i princìpi di usabilità, ma è *estendibile* a qualsiasi tipo di dispositivo, a condizione che ne esistano linee guida che ne descrivono il design seguendo i princìpi di usabilità.

Vengono di seguito riportate, in una tabella (Tabella 37), le soluzioni che il nuovo approccio ha apportato per ogni problema rilevato nell'approccio standard:

Tabella 37. Analisi euristica: confronto tra approccio standard e nuovo approccio

Problemi con: **Approccio standard**	**Obiettivi raggiunti con il:** **Nuovo approccio**
1. Analisi basata su regole euristiche.	1. Analisi basata su regole euristiche *e* linee guida di design.
2. Il focus dell'analisi è sull'utente.	2. Il focus del nuovo approccio è stato ampliato: è *sia* sull'utente *sia* sul design dell'interfaccia software.
3. Non specifica in modo semplice o chiaro quale sia la soluzione per le caratteristiche individuate.	3. Per ogni problema di usabilità la soluzione è già insita nella linea guida violata.
4. Metodo di valutazione informale.	4. Metodo di valutazione basato sia su euristiche che su linee guida universali, che rendono il metodo *più oggettivo*. Tuttavia, resta un compito del valutatore e della sua esperienza capire quali linee guida e quali euristiche vengono violate.
5. Sono necessari più valutatori.	5. Il focus del metodo è stato *spostato* dall'esperienza del valutatore alle linee guida. Non è necessario coinvolgere più valutatori per ottenere risultati affidabili.
6. Dovrebbero essere coinvolti valutatori esperti	6. Il focus del metodo è stato *spostato* dall'esperienza del valutatore alle linee guida nella sostituzione delle raccomandazioni con i criteri di usabilità. Tuttavia, la scala di gravità, per ogni violazione riscontrata, resta un compito del valutatore e della sua esperienza.
7. Analisi limitata al campo di esperienza del valutatore.	7. Analisi estendibile a qualsiasi tipo di dispositivo.

Limiti

I punti 4 e 7 delle soluzioni del nuovo approccio (Tabella 37 della pagina precedente) evidenziano la soggettività del metodo nella scelta di quali euristiche e quali linee guida vengono violate per ogni interfaccia software, scelta che resta del valutatore e che dipende di conseguenza dalla sua esperienza; stesso limite resta nella soggettività di assegnare una scala di gravità per ogni violazione individuata. Ciò porta a definire il nuovo approccio come *parzialmente oggettivo*, senza risolvere i problemi legati al coinvolgimento di valutatori esperti per ottenere risultati più attendibili sulla base della loro esperienza.

Sviluppi futuri

Dai risultati ottenuti, gli sviluppi futuri riguardano innanzitutto l'attuazione delle misure di controllo alla cartella clinica elettronica, tramite l'implementazione dei criteri di usabilità rilevati con il nuovo approccio (per quanto riguarda le misure *safety by design*), al fine di dichiarare la conformità all'usabilità del dispositivo medico software analizzato.

A partire dal nuovo approccio è inoltre opportuno trovare soluzioni future atte a rendere il metodo di valutazione dell'usabilità *pienamente oggettivo*.

5.5.2 Conclusioni

In conclusione, l'efficacia del nuovo approccio nell'analisi euristica ne ha ampliato il contenuto informativo, fornendo informazioni sufficienti a stabilire quali criteri di usabilità devono essere applicati nel design di un prodotto e ha sostituito la soggettività delle raccomandazioni con l'oggettività dei criteri stessi. Tale approccio è infine estendibile a qualsiasi tipo di dispositivo medico di cui ne esistano le linee guida di usabilità del design.

6. Bibliografia e Sitografia

[1] DIRETTIVA 2007/47/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 5 settembre 2007 che modifica la direttiva 90/385/CEE del Consiglio per il ravvicinamento delle legislazioni degli Stati membri relative ai dispositivi medici impiantabili attivi, la direttiva 93/42/CEE del Consiglio concernente i dispositivi medici, e la direttiva 98/8/CE relativa all'immissione sul mercato dei biocidi

[2] 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

[3] MDCG 2019-11, Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR October 2019

[4] Ministero della Salute*, Il Regolamento 2017/745: novità e sfide per istituzioni e aziende, 24 marzo 2021*

[5] EN 62304:2006+A1:2015, Medical Device Software - Software life-cycle processes

[6] EN ISO 14971:2019, Medical devices — Application of risk management to medical devices

[7] TR 80002-1, Guidance on the application of EN ISO 14971 to medical device software

[8] Alongi Rosetta Fiorella, *Risk Management e Risk Assessment, Master post laurea in Auditing e controllo interno*

[9] EN IEC 60812:2018, Failure modes and effects analysis (FMEA and FMECA)

[10] Wickens Lee, Liu Gordon-Becker, *An Introduction to Human Factors Engineering*

[11] EN 62366-1:2015+A1:2020, Medical devices : Application of usability engineering to medical devices

[12] J. Zhang et al. / Journal of Biomedical Informatics, *Using usability heuristics to evaluate patient safety of medical devices*

[13] Manual on borderline and classification in the Community regulatory framework for medical devices, *Classificazione dei software per la gestione delle informazioni e il monitoraggio dei pazienti*

[14]EN IEC 31010:2019, *Risk management – Risk assessment techniques*

[15] EN 61508-5:201, *Functional safety of electrical/ electronic/programmable electronic safety related systems,* Part 5: Examples of methods for the determination of safety integrity levels

[16] CARTELLA CLINICA ELETTRONICA OSPEDALIERA Indicazioni per un progetto sostenibile

[17] https://www.gazzettaufficiale.it

[18] IE 102, *Illuminazione ambienti ospedalieri*, ottobre 2016

[19] Testo unico sulla salute e la sicurezza sul lavoro (D.Lgs. 81/2008)

[20] Journal of the American Medical Informatics Association, Using FDA reports to inform a classification for health information technology safety problems, September 2011

[21] ANSI/AAMI HE75:2009, Human factors engineering – Design of medical devices