DISPOSITIVI MEDICI

Cybersecurity: una nuova sfida per la sicurezza del paziente

a cura di:
Marisa Testa, Silvia Scarpellini e Sandro Storelli

con la collaborazione di:
Veronica Forcelli e Maria Giovanna della Volpe

Le informazioni contenute in questa pubblicazione sono valide e attuali al momento della scrittura della stessa. Le disposizioni legislative e regolatorie sono soggette a cambiamenti e aggiornamenti da parte degli enti predisposti dello Stato a cui si riferiscono.
Lo scrivente declina ogni responsabilità con riguardo ad informazioni obsolete o eventualmente inesatte contenute in questa pubblicazione.

Coordinamento:
Thema s.r.l.
Via Saragat, 5
40026 Imola (BO)
Tel. 0542 643496
email info@thema-med.com

Novembre 2016

INDICE

Introduzione

Società e cybersecurity

Le sfide della *cybersecurity* investono i campi della tecnologia, dell'economia, della società intera. Per affrontarle, è indispensabile forte sinergia tra i mondi della ricerca, della produzione e del governo. *Cybersecurity* vuol dire prevenzione di accessi non autorizzati, di modifiche o uso improprio delle informazioni che potrebbero intervenire su dispositivi, server o reti, producendo gravi rischi. Uno dei temi più caldi è l'evoluzione continua verso l'Internet delle Cose (*Internet of Things - IoT*). Vi concorrono vari aspetti: la miniaturizzazione e specializzazione dei dispositivi digitali, la loro costante connessione alla rete e la loro pervasiva interazione. Di fatto, i prodotti moderni – dallo spazzolino da denti all'automobile, dall'aereo al dispositivo medico - sono sempre più computerizzati, monitorati e controllati da reti di elaboratori interne ed esterne. Ad esempio, l'automobile connessa a Internet potrà cooperare con l'infrastruttura stradale e con gli altri veicoli. Tuttavia, questo comporta anche che, attraverso le interfacce di comunicazione, gli elaboratori interni dell'auto possono essere infiltrati. I sistemi di bordo critici possono essere attaccati da remoto, magari attraverso uno *smartphone*. Analogamente, il problema si pone per i diversi prodotti e dispositivi, così come per le infrastrutture: le minacce derivanti da attacchi cibernetici si fanno sempre più concrete. Una recente indagine a tappeto per verificare il rispetto della privacy, svolta in 26 Paesi dalle Autorità per la protezione dei dati personali appartenenti al *Global Privacy Enforcement Network*, ha preso in esame oltre 300 dispositivi collegati ad internet, tra cui braccialetti intelligenti, contatori elettronici e dispositivi medici di ultima generazione. Oltre il 60% del campione non ha superato l'esame dei Garanti della privacy. E' risultato che la gran parte dei dispositivi non offre un'informativa adeguata su come i dati personali vengono utilizzati e comunicati a terzi; non fornisce appropriate informazioni sulle modalità di conservazione dei dati; non spiega come cancellare i dati dal dispositivo. Molti dispositivi hanno presentato anche problemi sulla sicurezza dei dati, ad esempio trasmettendo "in chiaro" (mentre per i dati sensibili è obbligatoria la modalità criptata) al medico curante informazioni relative alla salute degli utenti. D'altra parte, il processo di interconnessione è dinamico quanto inevitabile. Basti pensare che la gestione del dispositivo *IoT*, compreso l'aggiornamento del *software* su cui è basato il suo funzionamento, è spesso determinante per la sicurezza. L'aggiornamento del *software* offre di solito maggior usabilità, nuove prestazioni. Spesso però consente anche di risolvere le vulnerabilità di sicurezza attraverso delle *patch*. La prospettiva è quindi di convivere con una miriade di dispositivi connessi miniaturizzati, potenzialmente vulnerabili, ma al contempo sempre più indispensabili. C'è da aggiungere che non sempre i dispositivi vengono progettati tenendo conto della sicurezza come fattore rilevante e ciò, ovviamente, li rende ancor più vulnerabili.

Sebbene, a partire dall'11 settembre 2001, la protezione da attacchi informatici abbia acquisito un'elevatissima priorità per i governi, a partire da Stati Uniti e Stati membri dell'Unione Europea, le infrastrutture critiche sono soggette ad attacchi informatici sempre più frequenti e sempre più sofisticati. Per una loro efficace protezione sono necessari interventi sul piano tecnico-scientifico e su quello normativo. Ad esempio, occorre imporre che i sistemi finali, in fase di utilizzo, garantiscano livelli prestabiliti di sicurezza, senza cedere a logiche di mercato e di riduzione dei costi. E' evidente che le soluzioni tecnologiche non possono da sole assicurare la sicurezza di un sistema, ma per evitare comportamenti inappropriati va sviluppata una cultura della sicurezza informatica. Tutto questo per evidenziare quanto sarebbe importante, per il Sistema Paese, una struttura in grado di fornire analisi, valutazioni, misure dei livelli di sicurezza, nonché consulenze e certificazioni nella gestione di tutte le fasi del ciclo di vita di *software* e *hardware*, per dispositivi ed infrastrutture.

La rete Internet

Internet un tempo serviva, per lo più, per svago o ricerca. Oggi è indispensabile per qualunque servizio informativo. Purtroppo il progetto di Internet anteponeva la funzionalità alla sicurezza. Quindi, insita nella rete stessa, vi è una insicurezza di base. Internet resta un'astrazione logica: nella realtà, i dati vengono trasmessi tra reti adiacenti con accordi specifici per inoltrare il traffico verso una certa o una tal altra destinazione. La politica *cyber* sta diventando sempre più importante, nell'architettura del sistema competitivo a livello internazionale, dove la digitalizzazione costituisce un rilevante fattore di crescita economica. Tra gli obiettivi strategici, ormai fondamentale è quello di garantire il mimino rischio di furto di informazioni digitali e la massima sicurezza nelle transazioni on-line. L'Italia dovrebbe muoversi in modo deciso, sull'onda di quanto già predisposto da alcuni paesi, incentivando l'introduzione di *framework* nazionali di sicurezza *cyber* e tenendo conto della specificità del settore produttivo formato da piccole e medie imprese. Ciò risulta essenziale anche per adeguate politiche e normative per migliorare la *Supply Chain* del Sistema Paese.

Cybersecurity nel settore sanitario

Il settore sanitario è alle prese con formidabili minacce alla sicurezza informatica. In ogni parte del mondo, attacchi informatici hanno preso di mira le organizzazioni della salute. Sono, naturalmente, aumentate le azioni di contrasto e di miglioramento delle protezioni di sicurezza informatica. La *Food and Drug Administration* (FDA) ha tenuto all'inizio di quest'anno un workshop dal titolo

"Moving Forward: collaborative approach to Medical Device Cybersecurity" mirato a fornire indicazioni circa la gestione della sicurezza informatica per i dispositivi medici, *pre* e *post market*. I dispositivi medici sono sempre più connessi a internet. Viene stimato che, entro il 2020, dovrebbero essere immessi sul mercato prodotti per la salute connessi a Internet per 300 miliardi di dollari. La sicurezza *cyber* è una questione di business, prima che di tecnologia: per questo, occorre un approccio olistico. Come è evidenziato da varie ricerche, gran parte delle organizzazioni sanitarie hanno sperimentato violazioni dei dati e incidenti significativi di sicurezza informatica. Il fenomeno del furto di dati sanitari personali è purtroppo in rapida ascesa. Non solo: il fatto che tali informazioni vengano gestite da società non attive direttamente nel medicale, rende vulnerabile l'intero ecosistema di raccolta e gestione. I dati sulla salute sono preziosi e le informazioni personali del paziente possono avere quotazioni alte al mercato nero. In Europa, la direttiva *Network and Information Security (NIS)*, approvata nel maggio 2016 dal Consiglio dell'Unione Europea, attende di passare al Parlamento per l'approvazione in seconda lettura, per diventare definitiva. Ma, di fatto, ad oggi non esiste una soluzione per la sicurezza informatica. Solo l'integrazione di un programma di sicurezza informatica in una più ampia attività di gestione del rischio d'impresa può far sì che l'organizzazione sia ben attrezzata per la sicurezza informatica e per soddisfare gli obblighi di legge per la tutela dei dati sanitari. Anche i *software* dispositivi medici sono suscettibili a violazioni, che potenzialmente impattano sulla sicurezza e l'efficacia del dispositivo e, di conseguenza, sulla sicurezza del paziente. Questa vulnerabilità aumenta in quanto i dispositivi medici sono sempre più connessi a Internet, reti ospedaliere, altri dispositivi medici. Nei fatti, ogni dispositivo medico è soggetto ad un certo livello di rischio. D'altra parte, mentre il maggiore uso della tecnologia *wireless* e *software* in dispositivi medici aumenta le potenziali minacce di sicurezza informatica, le stesse caratteristiche migliorano anche l'assistenza sanitaria e la capacità di cura dei pazienti e poiché le minacce di sicurezza informatica non possono essere del tutto eliminate, occorre gestirle. Bisogna dunque saper integrare i fattori della sicurezza del paziente, dello sviluppo di tecnologie innovative e di migliori prestazioni del dispositivo.

E-health, app della salute e privacy

Il mercato delle applicazioni dedicate alla salute è ormai in crescita esponenziale. Le *app* possono consentire diagnosi da remoto, aiutare gli stessi pazienti a gestire meglio la salute, dando accesso a informazioni vitali. Come evidenziato da una recente ricerca dell'Osservatorio del Politecnico di Milano, se da un lato la sanità elettronica pubblica si sviluppa in modo discontinuo, dall'altro si registra un boom nell'utilizzo di servizi sanitari online. Il 53% dei medici di base utilizza *WhatsApp*, che "consente uno scambio efficace di dati, immagini e informazioni, permettendo di evitare una visita". Pazienti e medici di base comunicano sempre più attraverso canali digitali. Purtroppo,

come emerge da un'indagine del Garante italiano sulla Privacy su questo fronte, gli utenti non sono adeguatamente tutelati. C'è ben di più: la Commissione Europea, dopo una consultazione sulla *Mobile Health*, ha pubblicato il "Green Paper on Mobile Health" (Libro Verde sulle app sanitarie mobili). Risulta dalle indagini che, su oltre 1.200 *app* prese in esame, solo il 15% risulta dotato di un'informativa privacy adeguata e chiara sull'uso delle informazioni.

Implicazioni su mercato: la posta in gioco

Stante l'aumento, la diffusione e i relativi danni delle violazioni della sicurezza, quella della *cybersecurity* è ora acquisita come questione strategica, nelle politiche industriali. L'attenzione e l'attività regolatoria verso la *cybersecurity* sono quindi destinate a svilupparsi sempre più, a livello nazionale ed internazionale. Ciò impone ai fabbricanti di dispositivi medici e ai fornitori di servizi sanitari di adottare le opportune azioni preventive per garantire la sicurezza dei dispositivi e delle tecnologie mediche e per prevenire le violazioni che potrebbero causare un danno al paziente. La posta in gioco è molto alta per i sistemi sanitari e per i fabbricanti di dispositivi medici, ai quali è richiesto sempre più un atteggiamento proattivo. Nel fattore della sicurezza rientra, naturalmente, anche la garanzia della *privacy on-line*. Le imprese sono quindi chiamate a condurre valutazioni di sicurezza di routine per minimizzare le vulnerabilità dei dispositivi. Occorre definire buone pratiche di settore, eventualmente anche mutuandole da settori maggiormente avanzati sugli aspetti della sicurezza cyber, come ad esempio quello bancario. La segmentazione e la gestione dei dispositivi, in ogni caso, diventano sempre più cruciali. I dispositivi vanno necessariamente tenuti aggiornati, protetti da *firewall*, predisposti con reti separate per dati medici e sensibili e accessibili attraverso *password.* Tutto questo deve essere oggi una preoccupazione fondamentale.

1. Il Software Dispositivo Medico

Le applicazioni del software nella pratica clinica, e le conseguenti implicazioni per la sicurezza e protezione dei dati informatici, non possono prescindere da ciò che il legislatore europeo ha disciplinato in materia di software all'interno delle Direttive sui dispositivi medici e sui dispositivi medico-diagnostici in vitro.
In tale direzione, il presente capitolo offre una panoramica su ciò che può (o non può) essere definito software in ambito medicale, sulle regole di classificazione del software (paragrafo 1.2), volgendo infine lo sguardo verso ciò che ci attenderà in un futuro prossimo. I nuovi regolamenti europei sono destinati a ridefinire l'intera materia dei dispositivi medici e dei dispositivi medico-diagnostici in vitro, considerando, ovviamente, anche il software.

1.1 Definizione

La definizione di software in ambito medicale è stata ridefinita dalla Direttiva 2007/47/CE di emendamento alla Direttiva 90/385/CEE sui dispositivi medici impiantabili attivi e alla Direttiva 93/42/CEE sui dispositivi medici.
La Direttiva 2007/47/CE ha infatti modificato la definizione di dispositivo medico di cui all'art.1, paragrafo 2, lettera a) come segue:

"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****, destinato dal fabbricante ad essere impiegato sull'uomo a fini di:*

- *diagnosi, prevenzione, controllo, trattamento o attenuazione di malattie,*
- *diagnosi, controllo, trattamento, attenuazione o compensazione di una ferita o di un handicap,*
- *studio, sostituzione o modifica dell'anatomia oppure di un processo fisiologico,*
- *controllo del concepimento,*

che non eserciti nel o sul corpo umano l'azione principale cui è destinato con mezzi farmacologici, immunologici o mediante processi metabolici, ma la cui funzione possa essere coadiuvata da tali mezzi.

Dalla definizione di cui sopra discende che il software, destinato dal Fabbricante ad essere impiegato per gli scopi di cui all'art.1, lettera a) sopra citato, rientra legittimamente nella definizione di dispositivo medico.

La Direttiva 2007/47/CE non ha invece emendato la Direttiva 98/79/CE sui dispositivi medico-diagnostici in vitro. La definizione di dispositivo IVD quindi non include ad oggi alcun riferimento specifico al software.
Tuttavia, la MEDDEV 2.1/6:2012 (Linea Guida sulla classificazione del software stand-alone) specifica che il software stand-alone, ovvero il software non incorporato in un dispositivo, nel momento della sua immissione in commercio o della sua messa in servizio, può essere qualificato come dispositivo medico-diagnostico in vitro, a condizione che esso soddisfi la definizione di dispositivo IVD come fornita dall'art.1, paragrafo 2, lettera b) della Direttiva 98/79/CE. Inoltre, la MEDDEV sopra citata fornisce criteri per qualificare il software come dispositivo medico-diagnostico in vitro, sulla base delle informazioni fornite dal software stesso; in particolare:

- Se le informazioni fornite dal software si basano solo su dati ottenuti da un dispositivo IVD, il software è un dispositivo IVD e ricade nella disciplina della Direttiva 98/79/CE;
- Se le informazioni fornite dal software si basano solo su dati ottenuti da un dispositivo medico, il software è un dispositivo medico e ricade nella disciplina della Direttiva 93/42/CEE e s.m.i.;
- Se le informazioni fornite dal software si basano sia su dati ottenuti da un dispositivo medico che da un dispositivo IVD, il software è un dispositivo IVD e ricade nella disciplina della Direttiva 98/79/CE.

Infine, se il software ricade nella definizione di **accessorio** del dispositivo medico, ed è quindi qualificabile come prodotto che, pur non essendo un dispositivo, è destinato in modo specifico dal Fabbricante ad essere utilizzato con un dispositivo per consentirne l'utilizzazione prevista dal Fabbricante stesso, allora il software non è di per sé un dispositivo medico, bensì un accessorio del dispositivo medico ai sensi dell'art. 1, paragrafo 2, lettera b) della Direttiva 93/42/CEE.
Ugualmente, se il software soddisfa la definizione di accessorio di un dispositivo medico-diagnostico in vitro come fornita dall'art.1, paragrafo 2, lettera c) della Direttiva 98/79/CE, allora sarà qualificabile come accessorio di un dispositivo IVD.

La Direttiva 2007/47/CE evidenzia ulteriori criteri di qualifica del software come dispositivo medico al punto (6): *Occorre chiarire che un software è di per sé un dispositivo medico quando è specificamente destinato dal fabbricante ad essere impiegato per una o più delle finalità mediche stabilite nella definizione di dispositivo medico. Anche se utilizzato in un contesto sanitario, il software generico non è un dispositivo medico*.

Dall'ultima disposizione deriva, pertanto, che un software creato per scopi non medici (ad esempio per funzionalità amministrative e finanziarie) nel settore sanitario non rientra nella fattispecie di dispositivo medico e non ricade nella normativa sui dispositivi medici.

1.2 Classificazione

Una prima classificazione per ciò che concerne i software a scopo medico, può essere operata distinguendo tra:

- **Software embedded** (o integrato);
- **Software stand-alone**.

Il software embedded o integrato costituisce una parte del dispositivo medico; il software stand-alone, invece, è esso stesso un dispositivo medico.

A differenza del software embedded o integrato, il software stand-alone è un dispositivo medico a sé stante che può:

- Fornire mezzi e suggerimenti per la mitigazione di una malattia;
- Fornire informazioni per determinare la compatibilità, la rilevazione, la diagnosi, il monitoraggio o trattamento di stati fisiologici, di stati di salute, di malattie o di malformazioni congenite;
- Essere un aiuto nella diagnosi, nello screening, nel monitoraggio, nella prognosi, nella previsione e nella determinazione dello stato fisiologico.

Il software stand-alone dotato di uno scopo medico, come indicato nei punti precedenti, è considerato, ai fini della sua classificazione ai sensi dell'Allegato IX della Direttiva 93/42/CEE e s.m.i., come **dispositivo medico attivo**, cioè come dispositivo dipendente, per il suo funzionamento, da una fonte di energia elettrica o di altro tipo di energia, diversa da quella generata direttamente dal corpo umano o dalla gravità e che agisce convertendo tale energia (rif. Dir. 93/42/CEE, Allegato IX, sez. 1.4).

Ai dispositivi medici attivi sono applicabili le Regole 9, 10, 11 e 12 dell'Allegato IX, e sulla base dell'applicazione di tali regole, è possibile effettuare un'ulteriore classificazione, in particolare:

- (Regola 9) **Software con funzione terapeutica**: si tratta di un software collegato attraverso la rete ad un dispositivo terapeutico. Esempi: software contenuto in uno stimolatore muscolare/un incubatore/un laser, apparecchiature fisioterapiche per il monitoraggio a distanza, sistema di pianificazione di radioterapia usata per calcolare la dose di radiazioni ionizzanti da somministrare al paziente, pianificazione del dosaggio dell'insulina tramite software stand-alone.

- (Regola 10) **Software con funzione diagnostica**: si tratta di un software collegato attraverso la rete (cablata o wireless) ad un dispositivo medico diagnostico. Esempi: software contenuto in qualsiasi scanner (ultrasuoni, raggi X, risonanza magnetica), un termometro elettronico, software per archiviazione immagini e sistema di comunicazione. Inoltre, può trattarsi di un software stand alone di elaborazione dati dei pazienti per consentire la diagnostica diretta (es. un'App utilizzata per calcolare i dati diagnostici).

- (Regola 11) **Software con funzione di somministrazione/sottrazione**: si tratta di un software collegato attraverso la rete (cablata o wireless) ad un dispositivo di somministrazione o di sottrazione di un farmaco, di un liquido corporeo o altre sostanze dal corpo. Esempi: software incluso in pompe di infusione, ventilatori, nebulizzatori, pompe di aspirazione, apparecchiature per dialisi.

- (Regola 12) **Altri software stand-alone**. si tratta dei software che non rientrano nell'ambito di applicazione delle regole 9, 10, 11 dell'Allegato IX. Esempi: software utilizzato per un letto d'ospedale, software utilizzato per monitorare o controllare un dispositivo di classe I, software stand alone per l'elaborazione dei dati per la diagnosi (es. un'App utilizzata per calcolare un valore).

In Europa, lo standard EN IEC 62304 costituisce norma armonizzata ed è relativa alla gestione del ciclo di vita del software. I requisiti per la validazione del software sono da applicarsi in funzione del rischio correlato al software stesso, sulla base della seguente classificazione:
- **classe A**: il software non è suscettibile di produrre alcuna lesione o danno alla salute;
- **classe B**: il software è suscettibile di causare lesioni non gravi;
- **classe C**: il software è suscettibile di causare morte o lesioni gravi.

1.3 Verso i nuovi Regolamenti europei

Le attuali Direttive saranno a breve sostituite da due nuovi Regolamenti di definitiva applicazione nel 2019 (MD) e nel 2021 (IVD).
In materia di software, anche il nuovo Regolamento sui dispositivi medici ha incluso nel proprio campo di applicazione il software e i relativi impieghi nel settore sanitario.
In particolare, sul software viene definito quanto segue: *"Occorre chiarire che il software a sé stante, quando specificamente destinato dal fabbricante ad essere impiegato per una o più delle finalità mediche stabilite nella definizione di dispositivo medico, è qualificato come un dispositivo medico, mentre il software per usi generici, anche quando viene utilizzato in un contesto sanitario,*

o il software per applicazioni associate allo stile di vita e al benessere, non è un dispositivo medico. La qualifica di software, sia come dispositivo sia come accessorio, è indipendente dalla sua ubicazione o dal tipo di interconnessione tra il software ed un dispositivo."

Ovviamente la definizione di dispositivo medico presente nel nuovo Regolamento include anche il software, qualificandolo come *dispositivo attivo* (art. 2, punto 4, Definizioni).

L'applicazione di software associato allo stile di vita e al benessere viene esplicitamente esclusa dalla disciplina relativa ai dispositivi medici.

Ancora, il software può essere qualificato come dispositivo medico o come accessorio, indipendentemente dalla sua ubicazione o dal tipo di interconnessione tra il software e il dispositivo. Da ciò discende che la qualifica del software come dispositivo medico o come accessorio è subordinata esclusivamente al fatto che il software ricada nella definizione di dispositivo medico o di accessorio.

A differenza della Direttiva 98/79/CE, il nuovo Regolamento sui dispositivi IVD include nella definizione di dispositivo medico-diagnostico in vitro anche il software (art.2, paragrafo 2):

Qualsiasi dispositivo medico composto da un reagente, un prodotto reattivo, un calibratore, un materiale di controllo, un kit, uno strumento, un apparecchio, un'attrezzatura, un ***software*** *o un sistema,* ***utilizzato da solo o in combinazione****,* ***destinato dal fabbricante ad essere impiegato in vitro per l'esame di campioni provenienti dal corpo umano, inclusi sangue e tessuti donati****, unicamente o principalmente al fine di fornire informazioni:*

- *su uno stato fisiologico o patologico,*
- *su un'anomalia congenita,*
- *sulla predisposizione a una condizione morbosa o a una malattia,*
- *che consentano di determinare la sicurezza e la compatibilità con potenziali soggetti riceventi,*
- *che consentano di prevedere la risposta o le reazioni a un trattamento,*
- *che consentano di definire o controllare le misure terapeutiche.*

Nel nuovo Regolamento IVD sono poi presenti tutti gli elementi già inseriti nel Regolamento dispositivi medici.

2. Il software nella pratica clinica: rischi e benefici

Lo stato dell'arte della tecnologia software offre oggi grandi possibilità di applicazione dei software medicali nei più diversi ambiti clinici. Questo comporta da un lato importanti benefici per i pazienti e operatori sanitari, ma dall'altro lato anche rischi derivanti da possibili minacce informatiche provenienti dalla rete interna ma anche dall'esterno, soprattutto nelle tecnologie wireless.
Nei paragrafi che seguono vengono quindi delineati alcuni tra i possibili ambiti di applicazione dei software medicali, stand-alone o embedded, cercando di evidenziare i potenziali rischi a fronte dei benefici apportati.

2.1 La chirurgia software-guided

2.1.1 Sistemi di imaging diagnostico intraoperatorio

Il software di apparecchiature di imaging come TC (Tomografia Computerizzata) e RM (Risonanza Magnetica), impiegato normalmente per l'acquisizione di immagini digitali a scopo diagnostico, gioca un ruolo ancora più importante se tali apparecchiature vengono impiegate in fase intraoperatoria, ossia per l'esecuzione di interventi chirurgici guidati dalle immagini.
Negli ultimi due decenni, infatti, medici e ingegneri hanno collaborato nello sviluppo e realizzazione di sistemi di imaging intraoperatorio finalizzati al perfezionamento degli interventi chirurgici. In particolare, immagini TC e RM sono particolarmente importanti per interventi di neurochirurgia. Ecco perché i più importanti ospedali neurochirurgici sempre più spesso oggi sono dotati di sale operatorie polifunzionali che incorporano scanner RM e TC multistrato per fornire ai chirurghi immagini ed informazioni in tempo reale durante la procedura chirurgica (Figura 2.1.1).

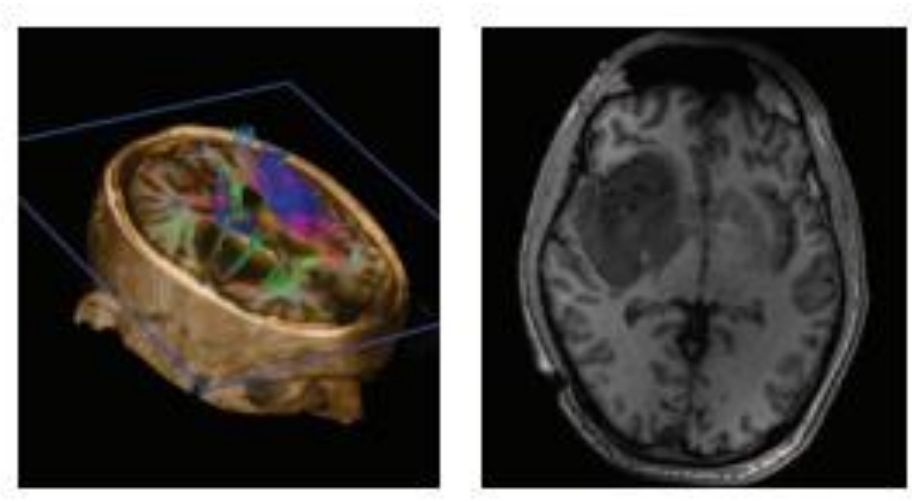

Figura 2.1.1: neurochirurgia guidata dalle immagini

I dati raccolti dai suddetti ospedali evidenziano che nel 40% degli interventi il chirurgo ha modificato l'approccio operatorio in base alle informazioni aggiuntive acquisite mediante imaging intraoperatorio. Prima dello sviluppo di tali tecnologie, queste informazioni erano invece disponibili solo dopo il completamento della procedura chirurgica.
In molti casi, per esempio, la RM intraoperatoria ha permesso di visualizzare e identificare residui di tessuto tumorale e ha permesso quindi una resezione completa, che altrimenti non sarebbe stata possibile se non sottoponendo il paziente ad un ulteriore intervento.

2.1.2. Software di pianificazione chirurgica 3D in odontoiatria

La tecnologia e l'innovazione permettono oggi di avere sul mercato anche software per la pianificazione chirurgica 3D, già da tempo impiegati nell'implantologia dentale. Con dei software molto evoluti che riescono a manipolare i dati delle TAC, trasformandoli in strutture anatomiche digitali, è possibile eseguire preventivamente l'intervento in modo virtuale. In implantologia dentale (Figura 2.1.2), per esempio, è possibile decidere diametro e lunghezza degli impianti che supporteranno la protesi fissa, la loro esatta posizione, la qualità e lo stato dell'osso in cui essi dovranno essere inseriti. Si tratta quindi di un vero e proprio intervento virtuale che permette una pianificazione nei minimi dettagli di quello che poi sarà l'intervento reale.
L'esecuzione di interventi pianificati attraverso software di ricostruzione 3D permette inoltre di ottenere risultati post-operatori migliori. I dati infatti dimostrano che anche la riabilitazione dei casi più complessi si ottiene con sole 24-48 ore di terapia contro gli 8-12 mesi necessari con le procedure tradizionali.

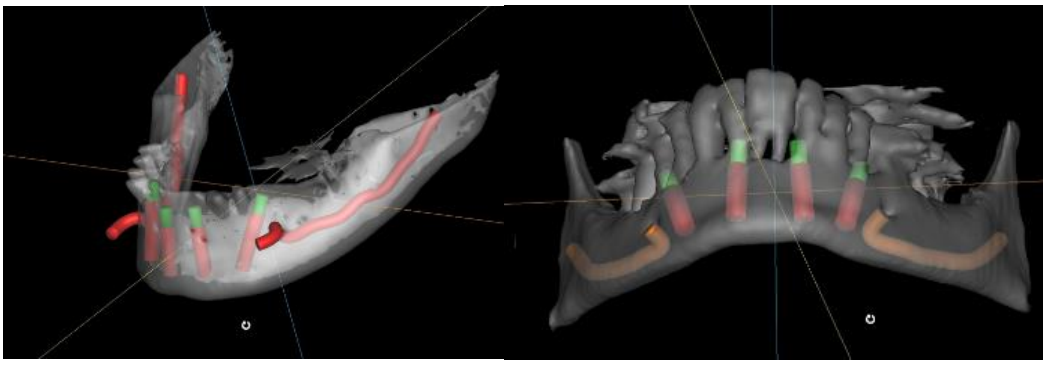

Figura 2.1.2: software 3D per la pianificazione di interventi di implantologia dentale

La pianificazione chirurgica mediante software di ricostruzione 3D viene impiegata anche per l'esecuzione di estrazioni molto complicate di denti che sono contigui a strutture anatomiche delicate, quali nervi o vasi sanguigni importanti.

2.1.3. Software di pianificazione chirurgica in ortopedia

Software di pianificazione chirurgica oggi trovano sempre più ampia applicazione anche in ambito ortopedico, per esempio per interventi di endoprotesi d'anca (Figura 2.1.3).

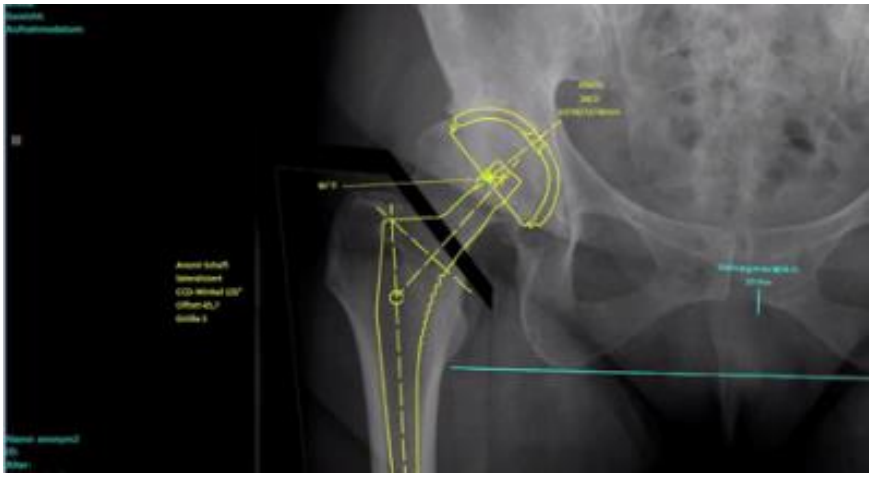

Figura 2.1.3: pianificazione di endoprotesi d'anca da immagini radiografiche

Il software si basa su metodi di pianificazione convenzionali per endoprotesi d'anca, un tempo eseguiti manualmente, tramite immagini radiografiche e matrici di protesi.
In modo rapido e mirato è possibile selezionare ed inserire una combinazione idonea di glena e guaina, correggere un'adduzione o abduzione, determinare la compensazione delle lunghezze delle gambe in sede pre-operatoria e post-operatoria e rappresentarla nell'immagine.
Un altro esempio è il software in grado di pianificare un'osteotomia correttiva femorale o tibiale con osteotomie semplici o multiple. Posizioni sbagliate degli assi vengono rilevate automaticamente e corrette automaticamente o manualmente.
Componenti idonei per osteosintesi come chiodi, piastre, viti ecc. possono essere selezionati da una banca dati.

2.2 Software diagnostici e software terapeutici

2.2.1 Software diagnostici

I software diagnostici sono impiegati per la creazione di dati o immagini, analogiche o digitali, sui quali il medico stabilisce la diagnosi del paziente.
Il trattamento delle immagini, coniugato a tecniche di riconoscimento automatico, è una disciplina che ha assunto via via maggiore importanza nei campi più svariati. In particolare, in ambito clinico, queste metodologie consentono di realizzare sistemi software in grado di riconoscere in maniera

automatica o semiautomatica la presenza di patologie in immagini diagnostiche, e possono quindi essere di ausilio per il medico nella usuale pratica clinica o in caso di screening.
Una delle metodiche digitali di diagnostica per immagini più diffuse è la tomografia assiale computerizzata (TAC), fondamentale per la diagnosi e la stadiazione di moltissimi tumori solidi. La TAC rappresenta una metodica di diagnostica ormai largamente diffusa data la sua possibile applicazione in tutti i distretti corporei. Inoltre, grazie a software dedicati, essa permette l'elaborazione tridimensionale delle immagini acquisite, ponendosi come metodica ottimale per lo studio anche di complesse strutture anatomiche. La tomografia computerizzata risulta un esame vantaggioso in quanto è poco invasivo, è in grado di evidenziare bene i dettagli anatomici e i rapporti tra le strutture ed è in grado di definire la densità degli organi interni e di stabilire la natura delle lesioni.

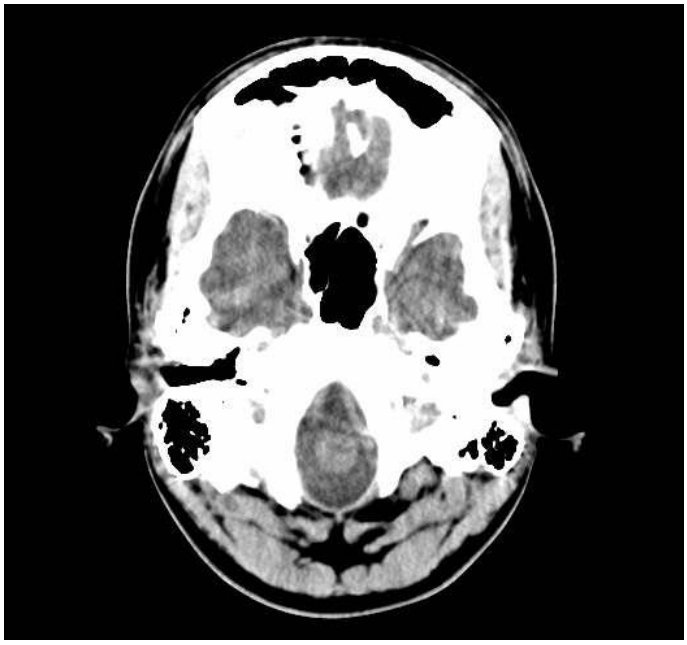

Figura 2.2.1: Immagine di una scansione TC del cervello.

Ad esempio la dotazione di software dedicati alla diagnostica delle ischemie cerebrali, esame molto frequente per una TAC di pronto soccorso, consente al medico radiologo di accertare in brevissimo tempo se il paziente soffre di deficit vascolari neurologici, responsabili delle ischemie.

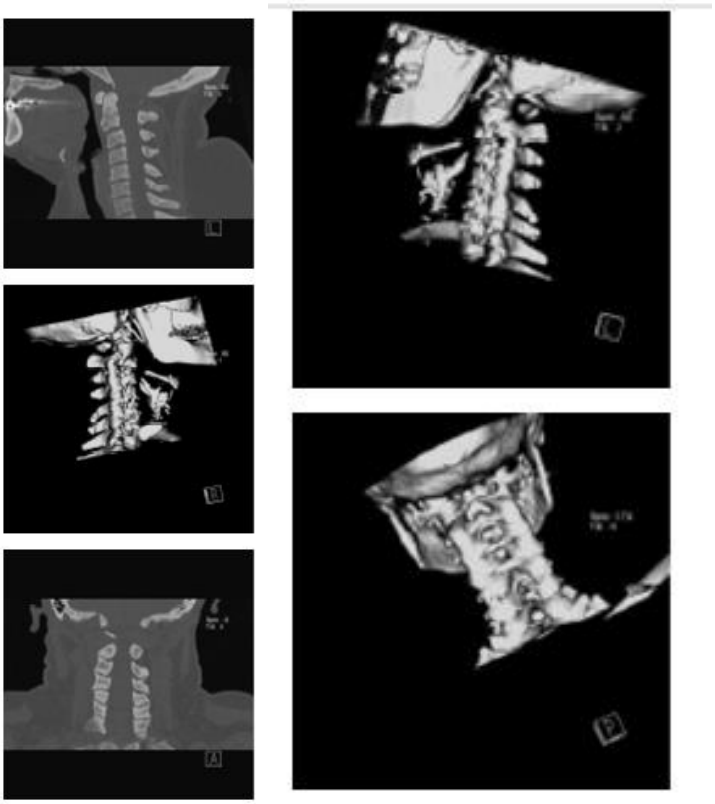

Figura 2.2.2: Immagini di una scansione TC per la diagnostica di ischemie cerebrali

2.2.2 Software terapeutici

I software terapeutici sono invece software collegati, attraverso la rete, ad un dispositivo terapeutico (rif. paragrafo 1.2) come ad esempio le apparecchiature fisioterapiche per il monitoraggio a distanza, i sistemi di pianificazione di radioterapia usati per calcolare la dose di radiazione ionizzata da somministrare al paziente, la pianificazione e dosaggio dell'insulina tramite software stand - alone.

Con l'obiettivo di supportare i centri di diabetologia nella gestione e consultazione dei dati dei pazienti diabetici, alcune aziende hanno sviluppato negli anni la Cartella Clinica informatizzata diabetologica, al fine di seguire il paziente sin dal suo primo accesso al Reparto memorizzando nel tempo gli esami di laboratorio, la valutazione delle complicanze in atto e pregresse, e guidandolo in un percorso educativo/nutrizionale. Ad ogni valutazione del paziente, il medico può effettuare la prescrizione terapeutica e farmacologica, rilasciando anche documenti personalizzati riepilogativi della visita effettuata. La valutazione periodica del Centro Diabetologico è necessaria per valutare gli esiti della terapia e controllare lo stato di salute del paziente. Il controllo in remoto si presenta come una soluzione innovativa e ottimale per mantenere un buon controllo metabolico.

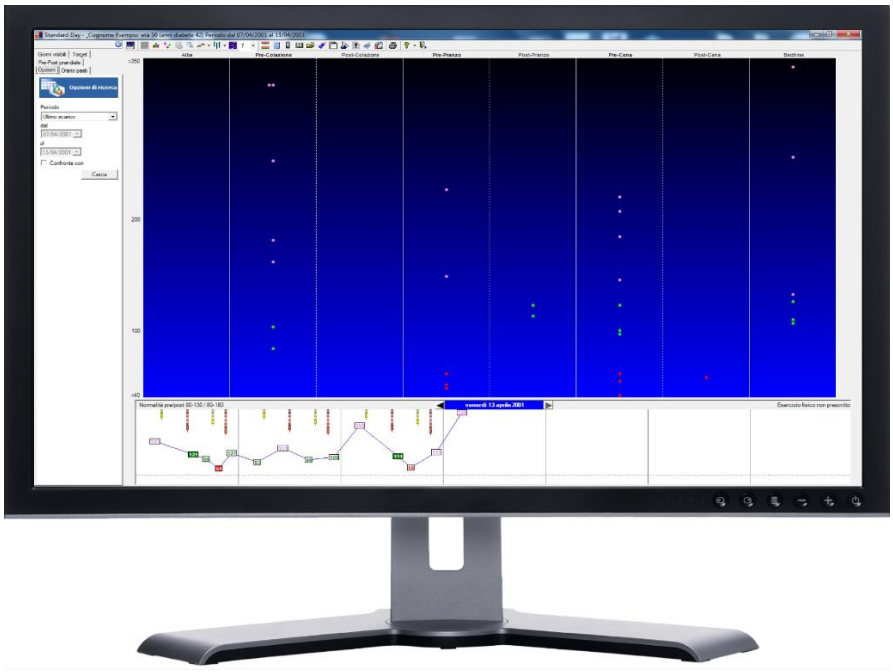

Figura 2.2.3: Cartella informatizzata diabetologica

In particolare, esistono numerosi software rivolti a tutte le persone diabetiche di tipo 1 e 2 e dedicati alla memorizzazione ed elaborazione dei dati clinici e dell'autocontrollo glicemico. Il servizio rappresenta un ponte digitale tra paziente e medico per la gestione e la condivisione dei dati sulle glicemie, sulle visite eseguite e sulla terapia insulinica, promuovendo una gestione del diabete più oculata e un trattamento meno asincrono rispetto all'attuale pratica ambulatoriale. Il software infatti raccoglie e mostra, in un unico ambiente, l'evoluzione dell'andamento glicemico nel tempo, permettendo al medico di correggere più rapidamente il trattamento insulinico prescritto e ottimizzando in tal senso anche la programmazione delle visite di controllo periodiche.

2.3 La Telemedicina

Per Telemedicina si intende una modalità di erogazione di servizi di assistenza sanitaria, tramite il ricorso a tecnologie innovative, in particolare alle Information and Communication Technologies (ICT), in situazioni in cui il professionista della salute e il paziente (o due professionisti) non si trovano nella stessa località. La telemedicina comporta quindi la trasmissione di informazioni e dati di carattere medico nella forma di testi, suoni, immagini o altre forme necessarie per la prevenzione, la diagnosi, il trattamento e il successivo controllo dei pazienti.

La telemedicina può essere impiegata per fare diagnosi, cura, riabilitazione, monitoraggio, ma anche prevenzione secondaria per i pazienti classificati a rischio o affetti da patologie come diabete o patologie cardiovascolari, i quali, pur conducendo una vita normale, devono sottoporsi a

costante monitoraggio di alcuni parametri vitali al fine di ridurre il rischio di insorgenza di complicazioni.

La telemedicina trova applicazione in diversi ambiti sanitari, tra cui:

- Continuità delle cure e integrazione ospedale-territorio: la gestione delle cronicità e la continuità dell'assistenza si avvalgono fortemente del contributo delle tecnologie innovative e dell'ICT. La telemedicina e la teleassistenza rappresentano esempi di come la tecnologia possa supportare l'inter-operatività dei medici nella gestione delle cronicità. Nello stesso modo, la telemedicina specialistica consente di monitorare e gestire patologie croniche in stati gravi e avanzati mantenendo il paziente a casa.
- Patologie rilevanti: pazienti affetti da patologie rilevanti, quali patologie cardiovascolari, cerebrovascolari, respiratorie, diabete, patologie psichiatriche, sia in età pediatrica che in età adulta e anche nel caso di anziani fragili, necessitano sempre di più di essere curati e assistiti senza doversi spostare da casa. In questo senso quindi i servizi di telemedicina diventano sempre più importanti nell'interazione fra territorio e strutture di riferimento.
- Sistema dell'Emergenza Urgenza: Gli interventi di assistenza in emergenza-urgenza possono avvalersi delle tecnologie al fine di gestire le attività di pronto intervento sanitario mirate all'eliminazione del rischio anche attraverso il collegamento ad altri nodi della rete sanitaria. L'utilizzo della telemedicina in questo contesto può rendere disponibili in modo tempestivo informazioni cliniche utili al miglioramento della gestione di pazienti critici.
- Un ramo della telemedicina è costituito dalla cosiddetta Telesalute, oggi sempre più diffusa e sempre più avanzata. La telesalute attiene principalmente all'ambito dell'assistenza primaria del paziente, il quale è messo in diretto collegamento con il medico che lo assiste nella diagnosi, nel monitoraggio, nella gestione e nella responsabilizzazione del paziente stesso. Attraverso la rete, un medico di medicina generale, spesso in collaborazione con un medico specialista, è messo nelle condizioni di poter interpretare a distanza i dati necessari per un corretto telemonitoraggio di un paziente e, nel caso, di poter prendere in carico il paziente stesso. La registrazione e trasmissione dei dati può essere automatizzata o realizzata da parte del paziente stesso o di un operatore sanitario.
- La Telesalute prevede un ruolo attivo del medico (presa in carico del paziente) e un ruolo attivo del paziente (autocura) in genere affetto da patologie croniche. Proprio per questo ruolo attivo delle parti la telesalute si differenzia dal Telemonitoraggio. La Telesalute comprende il Telemonitoraggio, ma lo scambio di dati (parametri vitali) tra il paziente (a casa, in farmacia, in strutture assistenziali dedicate, ecc) e una postazione di monitoraggio non avviene solo per l'interpretazione dei dati, ma anche per supportare i programmi di gestione della terapia e per migliorare l'informazione e formazione (knowledge and behaviour) del paziente.

Queste sono solo alcune delle potenziali applicazioni della telemedicina e, più in generale, dell'ICT in ambito medico sanitario.

Si può parlare addirittura di "*ricovero virtuale"* che è oggi una realtà tecnologicamente attuale, realizzabile con l'evoluzione e la diffusione della telematica. Infatti, tecnologie e strumenti telematici applicati alla sanità possono realizzare un'integrazione avanzata tra assistenza ospedaliera ed assistenza domiciliare: è l'ospedale che va a domicilio del malato.

Tra i vantaggi del ricovero virtuale vi è prima di tutto il fatto che il paziente risulta "ricoverato" prevalentemente nella sua abitazione, pertanto può continuare a svolgere le sue quotidiane attività anche durante il ricovero. Il medico inoltre può intervenire sul paziente utilizzando tutte le strutture sanitarie presenti sul territorio (ambulatori, laboratori, car hospital, ecc.) minimizzando lo spostamento del paziente e il tempo di attesa e massimizzando il trasferimento delle informazioni.

Non va dimenticato che con il ricovero virtuale è possibile fornire una migliore assistenza sanitaria anche alle comunità sparse territorialmente, per esempio nelle isole o in zone di montagna difficilmente raggiungibili.

Sulla base di quanto discusso finora, è piuttosto facile intuire che la tecnologia che permette di gestire il paziente in via telematica comporta necessariamente l'archiviazione e il trasferimento di una mole enorme di dati, la maggior parte dei quali sono dati personali e sensibili da cui dipendono la cura e il monitoraggio dello stato di salute del paziente.

2.4 Tecnologia wireless

La tecnologia ha invaso ogni aspetto della nostra vita, raggiungendo oggi un tasso di penetrazione quasi totale. In particolare, la tecnologia wireless permette di connettere tra loro dispositivi diversi senza fili. Infatti, grazie ad essa, con tablet e smartphone è possibile rilevare e monitorare una serie di indicatori dello stato di salute che prima potevano essere misurati soltanto con strumenti specifici che si trovavano negli studi medici. Attraverso questi strumenti ipertecnologici è possibile registrare e monitorare parametri biologici come pressione arteriosa, frequenza cardiaca, glicemia, saturazione di ossigeno e peso in modo semplice e veloce, avendo sempre a disposizione un quadro completo e aggiornato nel tempo. La possibilità di tenere sotto controllo questi indicatori biologici è fondamentale soprattutto nella cura di molte patologie croniche, in quanto il paziente viene responsabilizzato e stimolato a partecipare attivamente alla gestione della malattia con il medico stesso.

Nel 2013 a Milano, è stato impiantato per la prima volta in Italia un mini pacemaker "wireless", inserito nella cavità cardiaca senza bisogno di bisturi, ossia passando attraverso la vena femorale.

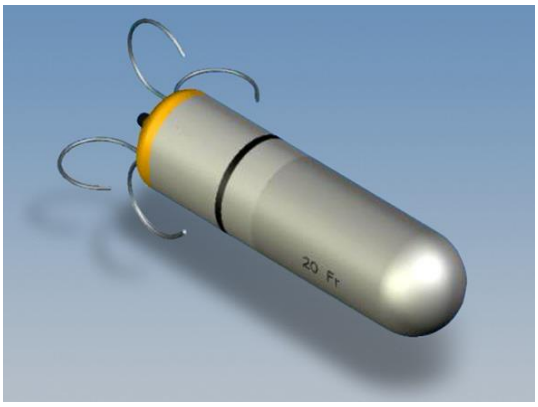

Figura 2.4.1: Mini Pacemaker wireless

La modalità di impianto non chirurgica ha permesso di ridurre il rischio di infezioni, l'assenza di fili ha ridotto la possibilità che il sistema potesse andare incontro a malfunzionamenti legati al danneggiamento dei cavi e la batteria a lunga durata ha assicurato al dispositivo una durata di circa 5-6 anni in più rispetto a quella standard. L'uso degli elettrodi è stato sostituito con delle apposite antenne che, toccando le pareti del cuore, ne trasmettono gli stimoli elettrici. I micro-pacemaker, tuttavia, poiché vengono collocati dentro una singola camera cardiaca, sono in grado di stimolare solo quell'area e non tutto il cuore contemporaneamente, come accade invece con i tradizionali pacemaker.

La mini tecnologia non si ferma solo a questo. Sono in sperimentazione i micro-monitor iniettabili in grado di registrare la funzionalità cardiaca e di inviare via wireless i dati ad uno smartphone o un dispositivo analogo.

Recentemente a Pisa è stato sperimentato un nuovissimo tavolo operatorio integrato, in grado di comunicare via wireless con il robot Da Vinci Xi.

Figura 2.4.2: Tavolo operatorio integrato, in grado di comunicare via wireless con il robot chirurgico

L’innovazione offerta da questo dispositivo è legata al fatto che esso è in grado di interagire con il robot, permettendo al chirurgo di cambiare la posizione del tavolo operatorio durante l’intervento in corso, senza la necessità di rimuovere gli strumenti robotici e scollegare il robot ad ogni movimento. Questo aspetto risulta particolarmente importante per potenziare la capacità del chirurgo-robot di eseguire interventi sincroni su più quadranti dell’addome.
In Italia, diversi sono i progetti per l’applicazione e diffusione della tecnologia wireless alle apparecchiature mediche compatibili con dispositivi Apple ed Android, che trasformano Smartphone e Tablet in vere e proprie stazioni diagnostiche avanzate, economiche e facili da usare. Tra questi dispositivi troviamo quelli che monitorano l’attività fisica, la qualità del sonno, le calorie giornaliere, i misuratori di pressione da polso e da braccio, bilance evolute che rilevano fino a nove parametri, ecc.

2.5 I software nei sistemi di monitoraggio dei parametri fisiologici e vitali

Sono ormai di uso comune e consolidato nella pratica clinica i sistemi di monitoraggio di parametri fisiologici e vitali dei pazienti.
Si tratta in particolare di piattaforme hardware e software per il monitoraggio al posto letto del paziente, ma anche di sistemi wireless che consentono di monitorare, in pazienti non ospedalizzati, parametri fisiologici quali pressione, temperatura, frequenza cardiaca e altri.
Alcuni software al posto letto, oltre al monitoraggio vero e proprio, offrono anche la possibilità al medico di interagire con tutte le valutazioni funzionali, di laboratorio e diagnostiche fino alla gestione della cartella clinica. Talvolta, quindi, per permettere questa duplice funzionalità, i sistemi di monitoraggio sono costituiti da due monitor separati, uno per le funzioni di monitoraggio e una per la gestione delle informazioni e dei dati del paziente (Figura 2.5.1).

Figura 2.5.1: sistema di monitoraggio dei parametri a doppio monitor

In alternativa, esistono anche sistemi che permettono entrambe le funzionalità sullo stesso monitor.

In caso di rilevazione di condizioni cliniche critiche per il paziente, il sistema di monitoraggio al letto del paziente, permette l'invio di segnali di allarme alla centrale di monitoraggio, consentendo così un più pronto intervento e una migliore assistenza da parte del personale sanitario.

E' chiaro però che attacchi informatici, virus o altro che dovessero colpire il software del sistema, e quindi la cartella clinica elettronica, potrebbero rivelarsi fatali per il paziente.

Inoltre, i sistemi di monitoraggio al posto letto sono collegati alla rete sanitaria aziendale, pertanto si interfacciano con altri applicativi ed altri software impiegati all'interno della struttura sanitaria.

In caso di sistemi di monitoraggio connessi wireless, il rischio di minacce informatiche è ancora più alto.

E' necessario quindi che anche questi sistemi siano dotati di sistemi di sicurezza efficaci e adeguati alla tipologia di dato che i software stessi gestiscono.

2.6 Mobile Applications

Con l'espressione "mobile-health" (mHealth) si indica generalmente l'insieme di tecnologie "mobili", ossia l'uso di comunicazioni wireless (cellulari e smartphone, tablet, dispositivi digitali, con o senza sensori indossabili), applicate in ambito medico-sanitario. Una recente ricerca rivela che sul mercato sono presenti circa 100.000 app con una crescita costante negli anni. Esse sono distribuite su differenti piattaforme e circa il 70% di queste sono relative alla salute e al benessere del consumatore, mentre il 30% è dedicato alla consultazione e monitoraggio del paziente, all'imaging diagnostico, alle informazioni farmaceutiche ecc. Si stima che entro il 2017 circa 3,4 miliardi di persone nel mondo potranno disporre di smartphone sui quali verranno utilizzate applicazioni per la salute.
Si tratta certamente di tecnologie con enormi potenzialità migliorative per la salute pubblica ed individuale, come ad esempio:

- promozione di uno stile di vita salutare;
- facilitazione e velocizzazione della comunicazione medico/paziente; personalizzazione di trattamenti;
- miglioramento dell'efficienza del sistema sanitario;
- contributo alla ricerca: facilitazione della raccolta di dati individuali e ambientali, utili per il singolo e per la collettività;
- ampliamento di accesso alle cure con la possibilità di raggiugere utenti che altrimenti non avrebbero assistenza medica;
- possibilità di condivisione di casi clinici e richiesta di secondi pareri in real-time per i medici.

A fronte di questi benefici di straordinario interesse per il progresso scientifico e tecnologico, il Comitato Nazionale di Bioetica ha evidenziato però alcune problematicità etiche relativamente alla sicurezza ed efficacia, alla privacy, al consenso informato, alla dipendenza e vulnerabilità tecnologica e all'autogestione della salute.
Un primo elemento indispensabile è la determinazione di criteri per la distinzione delle applicazioni m-health che sono dispositivi medici da quelle che non lo sono. Nel primo caso le app sulla salute prima di essere autorizzate sul mercato devono essere conformi alle normative vigenti europee e ai requisiti di certificazione. Nel secondo caso invece non esiste una regolamentazione specifica, ma solo la generale tutela del consumatore. È probabile che sia questa la ragione che ha portato il mercato verso una maggiore diffusione delle applicazioni che rientrano nella categoria del benessere e del fitness, ovvero non classificate come dispositivi medici.
La considerevole quantità di dati raccolti e analizzati dagli utenti pone altresì molte e rilevanti problematiche riguardanti la privacy, tra cui:

- mancanza di informazione trasparente agli utenti prima di scaricare l'applicazione di dati, su: quali e quanti sono utilizzati per eventuali ricerche; da chi sono usati e gestiti; dove sono conservati;
- assenza di informazione sulla possibilità di revoca del consenso, rettificazione e distruzione/cancellazione dei dati;
- assenza di informazione sul rischio di identificazione, quando la parziale anonimizzazione non è possibile o garantita;
- mancanza di informazione sui rischi dell'accesso dei dati da parte di terzi e sulla possibilità che chi conserva i dati li "venda" per costruire database per ricerche (commerciali/scientifiche).

Accanto alla regolamentazione e ai controlli si pone però anche il problema più generale di educazione all'utilizzazione dei mezzi di informazione e al rapporto con il proprio corpo e con la salute.
Di seguito alcuni esempi specifici di applicazioni medicali per dispositivi mobile certificati secondo la Direttiva 93/42/CEE e s.m.i. o comunque approvati da Autorità Regolatorie:

- App che permettono il collegamento con dispositivi medici (via cavo o wireless) al fine di pilotare il dispositivo stesso o visualizzare, salvare, analizzare o trasmettere i dati del paziente provenienti dal dispositivo medico. Ad esempio:

    - Applicazioni mediche che controllano la frequenza cardiaca e la percentuale di saturazione dell'emoglobina del sangue grazie al collegamento con un pulsossimetro.

Figura 2.6.1: App collegata al pulsossimetro

- Dispositivi composti da sonde per ecografie addominali, cardiache, tiroidee e per alcuni esami prenatali, interfacciabili tramite porta USB a dispositivo mobile.

Figura 2.6.2: App collegata ad una sonda ecografica

- Software specifico per la visualizzazione di immagini a fini diagnostici in modalità RM, TAC, SPECT, PET e X-RAY: i dati possono essere scaricati da remoto previo accesso e idonea autorizzazione tramite l'app specifica.

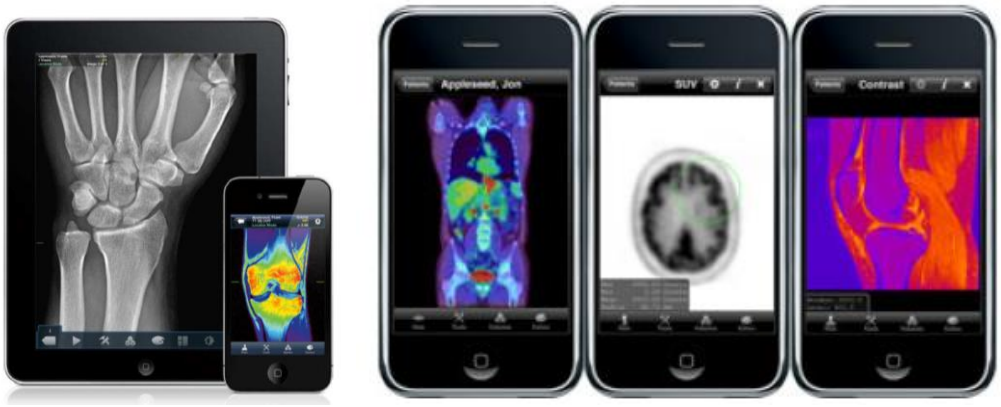

Figura 2.6.3: App per la visualizzazione di bioimmagini

- App medicali che trasformano smartphone o tablet in dispositivi medici regolati usando funzioni integrate quali la telecamera, il flash, gli accelerometri o attraverso l'uso di appositi sensori, accessori o schemi. Ad esempio:

  - Sensori ECG per smartphone, stetoscopi, sfigmomanometri, sistemi di monitoraggio.

Figura 2.6.4: App collegata a sistemi di monitoraggio di parametri fisiologici

- App medicali che effettuano analisi personalizzate sulla base delle quali forniscono diagnosi specifiche o indicazioni terapeutiche. Ad esempio:

    - Inserendo il valore di glicemia e le informazioni sui farmaci, il paziente riceve in tempo reale un feedback sui controlli glicemici e le successive azioni consigliate.

Figura 2.6.5: App di monitoraggio della glicemia

2.7 Conclusioni

Quelli riportati nei paragrafi precedenti sono solo alcuni esempi di software impiegati nella pratica clinica che fanno comprendere che tanto più è evoluta la tecnologia software, maggiori sono i benefici che si riescono ad ottenere, sia in termini di prestazioni cliniche sia in termini di risultati per il paziente, oltre che in termini di ausilio all'attività del medico e degli operatori sanitari. Al contempo però, maggiori sono i benefici apportati dalla tecnologia, più alto è il rischio per il paziente nel caso in cui il software venga attaccato da minacce esterne. Molte applicazioni software oggi sono paziente-specifiche, per cui le minacce e gli attacchi hacker al software si traducono inevitabilmente in danni, anche fatali, per il paziente.

3. La sicurezza informatica e la protezione dei dati

3.1 Avanzamento tecnologico e miglioramento delle prestazioni sanitarie vs cybersecurity

La telemedicina è uno strumento fondamentale per fornire cure mediche in situazioni fino a ieri impensabili. Essa è utile per trasmettere e condividere in rete vari tipi d'informazione (dati diagnostici, cartelle cliniche, esami di laboratorio, radiografie, immagini endoscopiche, ec), per monitorare con continuità i parametri vitali dei pazienti, per visualizzare immagini ad alta definizione, nonché per comunicare in sessioni video, riducendo così i difetti e gli inconvenienti che le applicazioni di cura in remoto e la lontananza dei pazienti hanno tradizionalmente manifestato.
È proprio l'avanzamento tecnologico dei semiconduttori, dell'elettronica embedded e dell'ICT che ha permesso e permette di migliorare continuamente le apparecchiature e le applicazioni, contribuendo così ad aumentare la qualità dell'assistenza sanitaria, espandendo la fruibilità delle cure e dei servizi di diagnosi e consulenza medica. Nello stesso tempo però la natura di questi dispositivi elettronici, connessi alla rete e in grado di comunicare in modalità remota tramite le tecnologie wireless, li espone sempre più anche ad attacchi e tentativi di violazione e manipolazione del loro normale funzionamento.
Un hacker, ad esempio, potrebbe inserirsi nei dati di dosaggio inviati per monitorare il diabete, modificando la quantità di insulina da somministrare sulla base dei livelli di glucosio, oppure uccidere un uomo usando il suo pacemaker wireless. Celebre in tal senso è il caso del vicepresidente USA Dick Cheney che nel 2013 rivelò come al suo defibrillatore, impiantato nel torace, venne disattivato il sistema wi-fi, capace di inviare informazioni in remoto, poiché si temeva una minaccia per la sua vita attraverso un attacco hacker al sistema che lo regolava. Possibili obiettivi sono inoltre i robot chirurgici, utilizzati nelle sale operatorie: è sufficiente introdursi nel router usato dal chirurgo per guidare a distanza il robot e mettere in pericolo la vita del paziente.
Anche i dati sanitari sono un nuovo "eldorado" per gli hacker, sempre più alla ricerca di database con informazioni sensibili. Negli Stati Uniti, come in Gran Bretagna, si registra un aumento di questa tipologia di violazione, anche a causa di una corsa alla digitalizzazione non accompagnata dalla realizzazione di strutture di difesa da cyber attacchi. I file preferiti dagli hacker sono i dati delle assicurazioni previdenziali o i numeri di identificazione medica, utilizzati soprattutto per commettere frodi. Modificando i dati sanitari, è possibile accedere anche a servizi o assistenze che eventualmente sarebbero a pagamento, poiché non coperte dall'assicurazione.
Anche il settore della mobile health è esposto a cyber attacchi; infatti sugli smartphone sono sempre più diffuse app che registrano l'attività fisica, il sonno, il battito cardiaco o in cui sono inserite informazioni relative alla salute dell'utente.

In Italia la sanità digitale ha iniziato a svilupparsi da poco tempo. Un esempio è costituito dall'FSE, ovvero il fascicolo sanitario elettronico che, previo consenso dell'assistito, viene costituito per finalità di prevenzione e diagnosi.
Pertanto l'adozione del cyberspace, ovvero il complesso ecosistema risultante dall'interazione di persone, software e servizi su Internet per mezzo di tecnologie, dispositivi e reti ad esso connesse, porta con sé problemi di vulnerabilità delle applicazioni e dei sistemi informatici.
Quindi la criticità nella gestione dei dispositivi in rete e dell'infrastruttura IT sta nel fatto che la sicurezza non è solo "safety" ma anche "security" e "privacy".
Tutte le minacce precedentemente elencate non possono però essere affrontate rinunciando alle potenzialità offerte dai sistemi informatici e dalla loro interconnessione in rete, perdendo quindi l'aumento della produttività ed efficienza che l'informatizzazione porta con sé.
Al contrario, la crescente frequenza di attacchi e minacce criminali nel campo informatico e le previsioni di sviluppo delle nuove tecnologie richiedono l'adozione di strategie difensive complesse e coordinate.
La cyber security è definita come quella pratica che consente a una entità (organizzazione, cittadino, nazione, ecc.) la protezione dei propri asset fisici e la confidenzialità, integrità e disponibilità delle proprie informazioni dalle minacce che arrivano dal cyber space.
La cyber security quindi non viene considerata semplicemente un aspetto tecnologico, ma impone piuttosto la considerazione dei doveri complessivi di natura giuridico-formale e i principi di utilità sociale verso cui pubblico e privato devono necessariamente convergere.

3.2 Big Data

La rapida evoluzione che negli ultimi anni ha caratterizzato l'ICT ha avuto, e continua ad avere, un profondo impatto sulla società in cui viviamo. La disponibilità pressoché ovunque di reti wireless aperte al pubblico ha favorito lo sviluppo e una continua rapida diffusione di dispositivi di vario tipo in grado di connettersi a Internet, dagli smartphone fino ai più recenti dispositivi indossabili (wearable device).
Questi dispositivi sono in grado di generare, raccogliere e condividere grandi quantità di dati spesso personali, indicati con l'espressione *Big Data.* Questa raccolta di dati, che può diventare facilmente dell'ordine dei Zettabyte (miliardi di Terabyte), è così estesa in termini di volume, velocità e varietà da richiedere tecnologie e metodi analitici specifici per poterli elaborare.
La mobile Health (mHealth) può facilitare la raccolta di una larga scala di dati medici (es. immagini mediche, misure, descrizione di sintomi) che possono essere archiviati in grandi database con il potenziale di migliorare la ricerca e l'innovazione in campo sanitario. Il grande potenziale del

cosiddetto “Big Data” giace proprio nell’abilità di analizzare questa moltitudine di dati non strutturati per trovare soluzioni comuni e aumentare sempre di più la sicurezza del paziente.
Infatti, comprendere una mole di dati biometrici permette in qualche misura di poter prevedere patologie e criticità e di seguire un paziente nell’arco del suo periodo di cura più da vicino. Ad esempio un piccolo ecosistema di dispositivi wearable, indossati dal paziente e che comprendono un cardiofrequenzimetro, un contapassi e un ECG, è in grado di tenere sotto controllo diversi parametri vitali nel tempo. Tali dati vengono periodicamente raccolti da un dispositivo cellulare e inviati a un sistema cloud che li immagazzina, classifica e, tramite un algoritmo predittivo, li correla e ne identifica le criticità. Queste informazioni saranno poi a disposizione anche del medico che potrà usare questi dati per valutare il proseguimento della terapia.
In questo senso il Nuovo Regolamento 2016/679 relativo alla Privacy fornisce la definizione di “*data concerning health*” come “i *dati personali relativi alla salute fisica o mentale di una persona, compresa l’erogazione di servizi di assistenza sanitaria, che rivelano informazioni circa il suo stato di salute”.*
La gestione di questa vastità di dati dipende dalla sicurezza dei dispositivi medici, integrità e cybersecurity, assicurando il livello più alto di qualità della produzione e sicurezza per pazienti e utilizzatori.

3.3 Privacy e trattamento dati

Il cuore della disciplina della privacy e del trattamento dei dati è rappresentato dalla Direttiva 95/46/CE, adottata il 24 ottobre 1995, dal Parlamento europeo e dal Consiglio con lo scopo preciso di armonizzare, all’interno del territorio dell’Unione Europea, la normativa concernente la tutela delle persone fisiche relativamente al trattamento e alla libera circolazione dei dati personali (paragrafo 3.3.1).
A partire dalle disposizioni contenute nella normativa europea in materia di privacy e trattamento dei dati, vengono individuati gli aspetti e i principi cardine della disciplina a cui si conformano le legislazioni nazionali degli Stati Membri (paragrafo 3.3.3).
La violazione del diritto alla protezione dei dati comporta l’applicazione di determinate sanzioni, nonché mezzi di ricorso – giudiziari ed extragiudiziari – in capo al soggetto titolare di tale diritto che sono trattati al paragrafo 3.3.4.

3.3.1 La Direttiva 95/46/CE sulla protezione dei dati

L'esigenza di tutelare e proteggere i dati personali viene avvertita dalle istituzioni europee già a partire dalla fine della seconda guerra mondiale, ovvero dal momento in cui creare uno Stato di diritto, promuovere la democrazia e lo sviluppo sociale, nonché garantire la massima tutela dei diritti dell'uomo, costituivano sfide e temi improrogabili per gli Stati d'Europa appena usciti dal secondo conflitto mondiale. E' in questo momento storico, più precisamente nel 1950, che viene adottata dal Consiglio d'Europa la "*Convenzione europea dei diritti dell'uomo*", la quale sancisce, tra i vari diritti, quello alla protezione dei dati personali, nonché le condizioni in virtù delle quali tale diritto può essere limitato.

Il progresso tecnologico, tuttavia, aveva condotto alla diffusione di nuove e avanzate tecnologie informatiche, determinando conseguentemente il bisogno di norme più specifiche per tutelare le persone e i relativi dati personali circolanti attraverso i nuovi mezzi di diffusione informatici. Tale esigenza si è tradotta nella ratifica della "*Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*" (Convenzione n.108 del 1981).

Con la Convenzione n. 108, vengono stabili i principi, le regole e le modalità attraverso i quali vengono effettuati la raccolta e il trattamento dei dati personali. In particolare, tale Convenzione stabilisce, da una parte, una serie di obblighi in capo al titolare del trattamento dei dati, e dall'altra, riconosce e garantisce nuovi diritti in capo agli interessati, al fine di proteggere le persone dagli abusi che potrebbero essere perpetrati a seguito della gestione di tali dati.

I principi statuiti all'interno della Convenzione n.108 hanno ispirato la maggior parte delle legislazioni nazionali europee e costituiscono la base sulla quale si sono sviluppate le regolamentazioni nazionali in materia di protezione dei dati personali.

Tuttavia, le singole legislazioni nazionali apparivano profondamente diverse le une dalle altre, tanto da creare un quadro normativo disomogeneo che mal si conciliava con i meccanismi del mercato unico europeo, caratterizzato dalla libera circolazione delle persone, delle merci, dei capitali e dei servizi.

Da quanto appena descritto è emersa conseguentemente l'esigenza di armonizzare, all'interno del territorio dell'Unione Europea, la normativa sulla tutela delle persone fisiche per ciò che concerne il trattamento e la libera circolazione dei dati personali, esigenza che si è concretizzata negli anni Novanta con l'adozione della Direttiva 95/46/CE, più comunemente conosciuta come la "direttiva sulla protezione dei dati" (GU L.281 del 23/11/1995).

La Direttiva 95/46/CE ha esplicitato e raccolto i principi del diritto alla vita privata che erano già stati contemplati nella Convenzione europea dei diritti dell'uomo e poi ampliati nella Convenzione n.108.

La Direttiva costituisce pertanto il principale strumento giuridico, a livello europeo, per la protezione dei dati personali: i punti di forza derivano dalla sua vasta applicazione territoriale (tutti gli Stati Membri e paesi extra-UE rientranti nello Spazio Economico Europeo, ossia Islanda, Liechtenstein,

Norvegia), nonché dal suo elevato grado di specificità, con lo scopo ultimo di garantire la protezione dei dati a seguito della loro circolazione sia all'interno dell'Unione europea che al di fuori di essa.

3.3.2 Terminologia della privacy e del trattamento dei dati

L'analisi dei contenuti principali della Direttiva 95/46/CE e, più in generale, della disciplina europea in materia di privacy e trattamento dei dati, non può prescindere dalla terminologia propria di questo ambito. La terminologia comunemente utilizzata, infatti, non sempre è coerente e corrispondete con quanto statuito dal diritto europeo.

Di seguito, un elenco dei termini maggiormente utilizzati in materia di privacy e trattamento dei dati, necessari per comprendere correttamente le disposizioni della normativa europea di settore.
Tale elenco è suddiviso, per maggior chiarezza e praticità, nelle macrocategorie "Concetti generali", "Dati" e "Soggetti".

Concetti generali

Diritto alla riservatezza: Diritto di ogni individuo a vedere protetta la propria vita privata dall'ingerenza delle autorità pubbliche, salvo casi specifici individuati e disciplinati dalla legge. Tale diritto è stato statuito all'interno della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, risalente al 1950.

Diritto alla protezione dei dati: Diritto dell'individuo a vedere protetti i propri dati personali, a seguito della diffusione, seppur legittima, di tali dati. Il diritto alla protezione dei dati emerge a seguito dello sviluppo delle nuove tecnologie e viene accolto, per la prima volta, all'interno della Convenzione n.108, risalente al 1981.

Trattamento dei dati personali: qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicati a dati personali. Tali operazioni consistono nella raccolta, registrazione, organizzazione, conservazione, elaborazione, modifica, estrazione, consultazione, impiego, comunicazione mediante trasmissione, diffusione, messa a disposizione, raffronto, interconnessione, congelamento, cancellazione e distruzione.
Il trattamento dei dati si riferisce perciò tanto al trattamento automatizzato quanto a quello effettuato manualmente negli archivi (es. fascicoli cartacei).

Il trattamento dei dati personali si realizza quando alla base vi è il consenso della persona i cui dati sono oggetto di trattamento, oppure quando esso è necessario nei casi seguenti:

- Dare esecuzione ad un contratto concluso con l'interessato;
- Tutelare l'interesse vitale dell'interessato;
- Adempiere un obbligo legale da parte del titolare del trattamento;
- Eseguire una funzione di pubblico interesse;
- Perseguire l'interesse legittimo del titolare del trattamento.

Dati

Dati personali: qualsiasi informazione concernente una persona fisica identificata o identificabile.

Dati sensibili: Informazioni che riguardano la sfera privata dell'individuo e idonee a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale o a partiti politici, lo stato di salute (cd. dati sanitari ex art. 8, paragrafo 1 della Direttiva 95/46/CE) e la vita sessuale dell'individuo. La Direttiva vieta il trattamento di tali dati, se non nei casi espressamente individuati e disciplinati all'interno della Direttiva stessa (es. nel caso in cui il trattamento è necessario alla prevenzione o alla diagnosi medica, alla somministrazione di cure o alla gestione dei centri di cura e viene effettuato da un professionista in campo sanitario soggetto al segreto professionale o da un'altra persona parimenti soggetta a un obbligo di segretezza equivalente) e con opportune garanzie da parte del legislatore nazionale (cfr. art. 8, paragrafo 3 della Direttiva 95/46/CE).

Dati anonimizzati: I dati sono anonimizzati quando gli elementi identificativi di una persona fisica (es. nome, data di nascita, sesso, ecc.) sono eliminati da un insieme di dati personali. I dati anonimizzati sono resi tali quando il titolare del trattamento intende conservarli dopo che questi sono divenuti obsoleti e non più utili per lo scopo a cui sono stati destinati originariamente. A seguito dell'attività di anonimizzazione, il dato non è più qualificabile come dato personale.

Dati pseudoanonimizzati: I dati sono pseudoanonimizzati quando gli elementi identificativi di una persona fisica (es. nome, data di nascita, sesso, ecc.) sono sostituiti da uno pseudonimo ottenuto, per esempio, attraverso crittografia di tali elementi presenti all'interno dei dati personali.

Soggetti

Interessato: La persona fisica identificata o identificabile, i cui dati sono soggetti a trattamento. Esso è il soggetto titolare del diritto alla protezione dei dati e, più in generale, del diritto al rispetto

della vita privata. La Direttiva 95/46/CE non disciplina la tutela delle persone giuridiche per ciò che concerne il trattamento dei dati che le riguardano; tuttavia, il legislatore nazionale di ciascuno Stato Membro può, a propria discrezione, disciplinare tale materia anche in riferimento alle persone giuridiche.

Titolare del trattamento dei dati: Colui che da solo, o insieme ad altri, determina le finalità, gli strumenti e le modalità del trattamento dei dati personali. In particolar modo, il titolare del trattamento è colui che ha gestito ed attuato il trattamento dei dati, anche nel caso di illegittima autorizzazione a trattarli.

Responsabile del trattamento dei dati: Colui che elabora i dati personali per conto del titolare del trattamento. Quest'ultimo può affidare al responsabile del trattamento anche solo determinati compiti o aspetti. Inoltre, il responsabile del trattamento è qualificabile come titolare del trattamento quando svolga un trattamento per proprio conto (es. gestione dei propri dipendenti, delle vendite, tenuta della contabilità).

Cotitolari del trattamento: Più entità giuridicamente distinte agiscono come titolari del trattamento per una finalità comune individuata previamente da un atto giuridico specifico (es. un contratto).

Terzo: La persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate all'elaborazione dei dati sotto la loro autorità diretta. Pertanto, i dati potranno essere trasmessi a terzi solo sulla base di uno strumento giuridico specifico.

Destinatario: La persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che riceve comunicazione di dati, che si tratti o meno di un terzo. Pertanto, il destinatario può essere un soggetto tanto interno quanto esterno al titolare o al responsabile del trattamento dei dati. Un'eccezione al concetto di destinatario è rinvenibile tuttavia nella Direttiva stessa allorché viene statuito che le autorità che possono ricevere comunicazione di dati nell'ambito di una missione d'inchiesta specifica non sono considerate destinatari.

3.3.3 Aspetti, principi e deroghe del diritto europeo in materia di privacy e trattamento dei dati

Per ciò che riguarda gli aspetti salienti alla base della Direttiva 95/46/CE e delle legislazioni nazionali di recepimento, sono individuati di seguito i concetti-chiave in materia di privacy e trattamento dei dati:

- **Consenso**: Il consenso, espresso dall'interessato, rappresenta la base giuridica del trattamento dei dati. Il consenso deve essere libero, ovvero espresso senza alcuna forma di pressione, coercizione o intimidazione; informato, ovvero relativamente all'oggetto del consenso e relative conseguenze (rif. punto "Informare l'interessato"); specifico per un determinato trattamento (rif. punto "Principio di finalità"). Il consenso, inoltre, può essere espresso dall'interessato in maniera esplicita o implicita; in entrambi i casi, però, il consenso deve palesarsi ed essere inequivocabile.
  Il consenso può essere revocato in qualsiasi momento dall'interessato, il quale può quindi esercitare tale diritto a propria discrezione.

- **Informare l'interessato:** Sussiste un preciso obbligo in capo al titolare del trattamento di informare l'interessato prima del trattamento stesso, nonché l'obbligo di mantenere informato l'interessato sulle modalità di utilizzo dei suoi dati. Devono essere comunicati all'interessato le finalità del trattamento (rif. punto "Principio di finalità"), l'identità e l'indirizzo del titolare del trattamento dei dati.

- **Accesso:** L'interessato può accedere ai propri dati con lo scopo di verificare se siano stati realizzati o meno trattamenti sui suoi dati personali, il tipo di dati trattati, le modalità, le finalità nonché i destinatari del trattamento stesso. Inoltre, sulla base del diritto di accesso dell'interessato, quest'ultimo può chiedere la rettifica, la cancellazione o il congelamento dei dati nel caso in cui tali dati non siano stati trattati secondo le disposizioni della Direttiva.

- **Opposizione:** L'interessato ha il diritto di opporsi, sulla base di motivazioni legittime, al trattamento dei propri dati, nonché al trattamento dei dati per finalità pubblicitarie.

Per ciò che concerne i principi in materia di privacy e trattamento dei dati alla base della Direttiva 95/46/CE e delle legislazioni nazionali di recepimento, sono individuati come segue:

- **Principio di liceità:** Sulla base di tale principio, il trattamento dei dati personali deve essere conforme alla legge, deve perseguire uno scopo legittimo e deve essere necessario, per una società democratica, al perseguimento di uno scopo legittimo.

- **Principio di finalità:** Sulla base di tale principio, la finalità trattamento dei dati personali deve essere ben definita ed espressa già prima dell'inizio del trattamento stesso, ciò in quanto l'interessato deve essere consapevole degli scopi a cui sono destinati i propri dati. Solo se lo scopo è determinato, infatti, il trattamento può considerarsi legittimo.

- **Principio di qualità dei dati:** Sulla base di tale principio, il trattamento deve riguardare solo ed esclusivamente i dati necessari e pertinenti alle finalità dichiarate dal titolare del trattamento prima dell'inizio del trattamento stesso. Tale principio si traduce nella necessità che i dati trattati siano esatti ed aggiornati, pertanto il titolare del trattamento deve adottare le misure più idonee a garantire la correttezza e l'aggiornamento dei dati stessi.

- **Principio di responsabilità:** Il titolare del trattamento dei dati è responsabile della conformità alla legge, tanto nazionale quanto europea, del trattamento e della protezione dei dati. Inoltre, tale principio implica che il titolare debba attuate tutte le misure necessarie per garantire la sicurezza e la riservatezza dei dati nonché, più in generale, che il trattamento avvenga secondo le disposizioni di legge.

3.3.4 Ricorsi e sanzioni

In caso di violazioni del diritto alla protezione dei dati, il diritto europeo ha demandato ai legislatori nazionali di prevedere e regolamentare i mezzi di ricorso e le sanzioni più adeguate contro tali violazioni.
Il soggetto legittimato a far valere il diritto violato deve identificarsi in colui che è titolare del diritto alla protezione dei dati, pertanto, si identificherà nell'interessato o in un suo rappresentante.
Prima di adire l'autorità giudiziaria nazionale, l'interessato, o il suo rappresentante, dovrà esercitare il proprio diritto nei confronti del titolare del trattamento. Quest'ultimo dovrà rispondere alla richiesta – disciplinata dal diritto nazionale – presentata dall'interessato e a cui dovrà seguire la risposta del titolare del trattamento secondo le modalità e i tempi stabiliti dalla normativa nazionale.
In caso di mancata risposta o di risposta non soddisfacente da parte del titolare del trattamento, l'interessato può rivolgersi all'autorità di controllo nazionale per la protezione dei dati, presentando una domanda di assistenza. Le decisioni dell'autorità di controllo nazionale possono essere giuridicamente esecutive sulla base di quanto statuito dal diritto nazionale. In particolar modo, il diritto nazionale stabilisce se la decisione può essere eseguita direttamente dall'autorità di controllo o, al contrario, se deve essere adita l'autorità giudiziaria.

Contro la decisione dell'autorità di controllo, tanto l'interessato quanto il titolare del trattamento hanno la possibilità di adire l'autorità giudiziaria nazionale. La possibilità di rivolgersi direttamente all'autorità giudiziaria può essere prevista dal singolo legislatore nazionale anche nel caso in cui l'interessato ritenga non soddisfacente la risposta del titolare del trattamento al proprio quesito.
Infine, in caso di violazione dei diritti alla tutela dei dati, rimane ferma la possibilità di presentare ricorso, in ultima istanza e in presenza di determinate condizioni, davanti alla Corte europea dei diritti dell'uomo. Tale ricorso può essere presentato se la violazione è stata perpetrata a livello nazionale da una parte contraente della Convenzione dei diritti dell'uomo.
Per ciò che concerne l'apparato sanzionatorio, esso è regolamentato dal legislatore nazionale, il quale deve prevedere sanzioni efficaci, equivalenti, proporzionali nonché dissuasive.
Infine, chiunque subisca un danno a seguito di illecito o illegittimo trattamento dei dati, o in violazione della normativa nazionale di attuazione della Direttiva 95/46/CE, ha il diritto di ottenere il risarcimento del danno cagionato.

3.4 Come cambierà lo scenario della privacy nel prossimo futuro

A livello europeo, in materia di privacy e di trattamento dei dati personali, è stato recentemente intrapreso un percorso che ha condotto ad una riforma significativa di tale materia, a distanza di ben ventuno anni dalla prima disciplina europea.
In particolar modo, l'iter normativo ha portato alla promulgazione del nuovo Regolamento europeo sulla privacy (paragrafo 3.4.1), di cui si illustrano le novità più significative che sono destinate a mutare, nel futuro prossimo, lo scenario attuale (paragrafo 3.4.2).

3.4.1 Evoluzione della Direttiva 95/46/CE

La volontà di avviare un processo di riforma della disciplina sulla privacy e sul trattamento dei dati personali, emerge già a partire dal 2003 in occasione della trasmissione da parte della Commissione europea al Parlamento europeo della prima relazione sull'applicazione della Direttiva 95/46/CE (COM(2003) 265), a cui ha fatto seguito la risoluzione del Parlamento europeo (COM(2003) 265 – 2003/2153(INI)).
La relazione sopracitata ha portato alla luce non poche criticità relativamente all'applicazione della Direttiva europea sulla privacy, in particolare:

- insufficienza di risorse per l'applicazione della Direttiva;

- applicazione disomogenea della Direttiva da parte dei titolari e dei responsabili del trattamento dei dati nel territorio dell'Unione Europea;
- mancata consapevolezza dei propri diritti da parte dei soggetti interessati;
- esclusione dal campo di applicazione della Direttiva di settori quali la sicurezza, la difesa, la cooperazione giudiziaria;
- diffusione di nuove tecnologie e internazionalizzazione dei flussi di dati (es. internet, social network, app, ecc.) con conseguente rischio per gli individui di diminuire o perdere il controllo sui propri dati.

Per far fronte alle criticità come sopra delineate e, in particolar modo, per superare le disparità tra le legislazioni dei singoli Stati Membri in materia di privacy, è emersa la volontà di riformare l'intera disciplina, volontà che si è tradotta concretamente negli anni successivi nella proposta di riforma da parte della Commissione europea (25 gennaio 2012).
A tale proposta è stata attribuita la forma giuridica del Regolamento europeo, col fine ultimo di livellare ed uniformare la tutela in materia di privacy nel territorio dell'Unione europea, in virtù della sua applicazione diretta ed immediata agli Stati Membri, ovvero senza necessità di un atto di recepimento da parte degli organi legislativi nazionali.
La nuova disciplina è stata emanata il 14 aprile 2016 a seguito di approvazione da parte del Parlamento europeo del **Regolamento europeo 2016/679 del Parlamento europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati**.
Il nuovo Regolamento, che abroga la Direttiva 95/46/CE, è stato pubblicato il 4 maggio 2016 nella Gazzetta Ufficiale Europea (GUE L 119), ed è entrato in vigore il 25 maggio 2016; esso diventerà direttamente ed immediatamente esecutivo in tutti gli Stati Membri a partire dal 25 maggio 2018.
Tale Regolamento, tuttavia, non rappresenta l'unico provvedimento europeo atto a ridefinire la materia privacy e protezione dati, in quanto esso si inserisce all'interno di quello che, insieme alla Direttiva 2016/680 che regola i trattamenti di dati personali nei settori di prevenzione, contrasto e repressione dei crimini (entrata in vigore il 5 maggio 2016), è stato definito il "*Pacchetto europeo protezione dati*".

3.4.2 Le novità del Regolamento europeo 2016/679

Le novità maggiori contenute nel nuovo Regolamento sulla privacy trovano fondamento nel progresso tecnologico e nel più ampio fenomeno della globalizzazione. Questi elementi, infatti, hanno modificato in maniera profonda le modalità attraverso le quali avvengono la raccolta e il trattamento dei dati personali.

L'ulteriore ragione alla base della riforma sulla privacy, come visto al paragrafo 3.4.1, consisteva nel superare la frammentazione e la disomogeneità che caratterizzava le legislazioni nazionali nonché pervenire ad una regolamentazione uniforme, coerente e armonica.

Qui di seguito le più importanti novità introdotte dal Regolamento:

- **Tutela dei cittadini europei**

  Nel campo di applicazione della disciplina in materia di privacy e protezione dati, rientrano, per la prima volta, anche i trattamenti dei dati che si realizzano al di fuori del territorio dell'Unione europea, se relativi all'offerta di beni o sevizi a cittadini europei o relativi al monitoraggio del loro comportamento, nella misura in cui tale comportamento abbia luogo all'interno dell'Unione europea. La disciplina, quindi, si applica indipendentemente dalla sede del titolare del trattamento.

  Tale modifica ha grande impatto, in quanto innalza il livello di tutela per i cittadini europei all'interno dello spazio digitale, soprattutto nell'era del "*cloud computing*", in cui cioè sempre più imprese, non avendo però sede in Europa, offrono servizi via internet.

- **Diritto all'oblio**

  A partire dalla sentenza della Corte di giustizia europea del 13 maggio 2014 che ha sdoganato il diritto all'oblio, è stato accolto all'interno del nuovo Regolamento il diritto dell'interessato ad ottenere dal titolare del trattamento dei dati personali la cancellazione totale dei dati che lo riguardano e la rinuncia ad una loro ulteriore diffusione quando: a) non più necessari per le finalità per le quali sono stati raccolti; b) nel caso di revoca del consenso; c) quando l'interessato si sia opposto al trattamento dei dati personali che lo riguardano; d) quando il trattamento dei suoi dati personali non sia altrimenti conforme al Regolamento.

  La tutela del diritto all'oblio comporta delle inevitabili ripercussioni sul diritto di espressione e su quello di cronaca. La questione è spinosa e, venendo in contrasto con due ulteriori diritti di pari rango, il bilanciamento che di volta in volta si deve raggiungere non può essere discrezionale ma deve rispondere a precisi criteri (assenza di interesse pubblico all'acquisizione della notizia e non attualità della stessa).

  Il diritto all'oblio potrà essere limitato solo in alcuni casi specifici: per garantire l'esercizio della libertà di espressione o il diritto alla difesa in sede giudiziaria; per tutelare un interesse generale (ad esempio, la salute pubblica); oppure quando i dati, resi anonimi, sono necessari per la ricerca storica o per finalità statistiche o scientifiche.

- **Diritto alla portabilità dei dati personali**

  È stato introdotto il diritto dell'interessato a trasferire i propri dati da un sistema elettronico ad un altro e ad ottenere gli stessi in un formato elettronico strutturato, di uso comune e leggibile dal dispositivo automatico, e che consenta di farne un ulteriore uso.

  Il soggetto interessato, pertanto, ha il diritto di trasmettere i dati a un altro titolare del trattamento senza impedimenti da parte del precedente titolare, qualora l'interessato abbia fornito il proprio consenso al trattamento o se questo sia necessario per l'esecuzione di un contratto.

  Tuttavia, quando si tratta di dati contenuti in archivi di interesse pubblico, come ad esempio le anagrafi, il diritto di portabilità dei dati personali viene meno.

- **Diritti dei minori**

  In considerazione della sempre più elevata diffusione delle tecnologie tra i più giovani, è stata posta un'attenzione particolare ai mezzi attraverso i quali ottenere il consenso per il trattamento dei dati personali appartenenti a persone minorenni. In particolare, i fornitori di servizi Internet e i social media dovranno richiedere il consenso ai genitori o a chi esercita la potestà genitoriale per trattare i dati personali dei minori di 16 anni.

- **Obblighi del titolare del trattamento dei dati**

  Il titolare del trattamento dei dati ha l'obbligo di conservare adeguata documentazione sull'attività di trattamento. Egli deve infatti essere in grado di dimostrare che i trattamenti effettuati sono conformi alla normativa. In particolar modo, il titolare del trattamento ha l'obbligo di tenere un registro delle attività di trattamento svolte sotto la propria responsabilità. Inoltre, egli ha l'obbligo di effettuare una "valutazione di impatto sulla protezione dei dati" (cd. *Privacy Impact Assessment* – PIA) in relazione, ad esempio, ai trattamenti automatizzati, ivi compresa la profilazione, o con riguardo ai trattamenti su larga scala di categorie particolari di dati (sensibili), o relativamente ai dati ottenuti dalla sorveglianza sistematica, sempre su larga scala, di zone accessibili al pubblico. Sarà ad ogni modo l'Autorità, a redigere e a rendere pubblico l'elenco delle tipologie di trattamenti soggetti al requisito della "valutazione di impatto sulla protezione dei dati". In caso di trattamenti rischiosi, il titolare del trattamento dei dati ha l'obbligo di prevedere valutazioni e verifiche preventive da parte dell'Autorità al fine di limitare i rischi. Egli tuttavia non ha più l'obbligo di notificare i trattamenti all'Autorità, con evidente semplificazione amministrativa e, conseguentemente, risparmio economico per le imprese.

  Sulla base del comma 5 dell'art. 30 del Regolamento, gli obblighi sopracitati non si applicano alle piccole e medie imprese (aziende con meno di 250 dipendenti), a meno che, però, "*[…] il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà*

dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati (sensibili) […] o i dati personali relativi a condanne penali […]".

Infine, per ciò che concerne i limiti alla possibilità per il titolare del trattamento di adottare decisioni solo sulla base di un trattamento automatizzato dei dati, le decisioni che producono effetti giuridici (come, la concessione di un prestito) non potranno essere basate esclusivamente sul trattamento automatizzato dei dati. Fanno eccezione i casi in cui l'interessato abbia rilasciato un consenso esplicito al trattamento automatizzato dei suoi dati, questo tipo di trattamento risulti strettamente necessario per la definizione di un contratto o avvenga in base a specifici obblighi di legge. In ogni caso, sono previste garanzie per gli interessati, come il diritto di opporsi alla decisione adottata sulla base di un trattamento automatizzato o il diritto di ottenere anche l'intervento umano rispetto alla decisione stessa. Se il trattamento è finalizzato ad attività di marketing diretto, l'interessato ha sempre il diritto di opporsi alla profilazione.

- **Principio di accountability**

  Il titolare dovrà dimostrare l'adozione di approcci e politiche sulla privacy e di misure adeguate in conformità al Regolamento. Il Regolamento, pertanto, promuove la responsabilizzazione dei titolari del trattamento, i quali dovranno tenere conto, costantemente, del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.

- **Privacy by design**

  Il titolare del trattamento deve attuare adeguate misure tecniche e organizzative sia all'atto della *progettazione che all'atto di esecuzione del trattamento.*

- **Privacy by default**

  Il titolare deve trattare i dati solamente per le finalità previste e per il periodo strettamente necessario a tali fini. Tale principio era già insito nella disciplina della Direttiva 95/46/CE (principio di necessità), tuttavia, esso viene maggiormente esplicitato e dettagliato all'interno del nuovo Regolamento.

- **Obbligo di notifica delle violazioni (cd. Data breach)**

  Nei casi di violazione della sicurezza dei dati idonee a provocare, anche accidentalmente, la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso a dati personali, il titolare del trattamento ha l'obbligo provvedere alla relativa notifica alle Autorità entro 72 ore e, in determinati casi, ai diretti interessati senza ritardo ingiustificato. Il mancato rispetto di tale obbligo comporta sanzioni penali in capo al titolare del trattamento dei dati.

- **Data Protection Officer (o Privacy Officer)**

  La figura del Data Protection Officer (Responsabile della protezione dei dati) era già prevista da alcuni Paesi dell'Unione europea. Tuttavia, per uniformarne la disciplina e per far sì che tale figura fosse accolta anche all'interno delle legislazioni dei Paesi che ne erano privi, è stata resa obbligatoria la sua istituzione per tutti i soggetti pubblici e per tutte le aziende ove i trattamenti presentino specifici rischi, come ad esempio le aziende nelle quali sia richiesto un monitoraggio regolare e sistematico dei soggetti interessati, su larga scala, e quelle che trattano i c.d. "dati sensibili".

Il Data Protection Officer ha molteplici responsabilità, come:

a) informare e consigliare il titolare o il responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento;
b) verificare l'attuazione e l'applicazione della normativa, oltre alla sensibilizzazione e formazione del personale e dei relativi auditors;
c) fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati (cd. PIA) e sorvegliare i relativi adempimenti, con particolare riguardo ai requisiti concernenti la protezione e la sicurezza dei dati fin dalla progettazione del processo aziendale e degli applicativi informatici di supporto;
d) fungere da punto di contatto per i soggetti interessati, in merito a qualunque problematica connessa al trattamento dei loro dati nonché all'esercizio dei loro diritti;
e) fungere da punto di contatto per il Garante per la protezione dei dati personali oppure, eventualmente, consultare il Garante di propria iniziativa.

   Può trattarsi di una figura interna o esterna all'azienda, (in quest'ultimo caso, eventualmente sulla base di un contratto di servizi), deve essere indipendente, con un'ampia conoscenza della normativa, e funzionalmente dipendente dai vertici aziendali (art. 38, comma 3). Ciascuna azienda deve rendere noti i dati del proprio Data Protection Officer, in quanto, come detto sopra, dovrà essere contattabile da tutti i soggetti interessati, e deve comunicarli al locale Garante per la protezione dei dati personali. Le società facenti parte di uno stesso gruppo, a livello nazionale o transfrontaliero, potranno nominare un unico Data Protection Officer, a condizione che lo stesso sia facilmente raggiungibile da ciascuna società del gruppo stesso.

   Tuttavia, sulla base del comma 5 dell'art. 30 del Regolamento, l'obbligo di nominare un Data Protection Officer non si applica alle piccole e medie imprese (aziende con meno di 250 dipendenti), a meno che, però, "*[…] il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati (sensibili) […] o i dati personali relativi a condanne penali […]*".

- **Icone**

  Il nuovo Regolamento introduce la possibilità di utilizzare, a livello europeo, icone per "targare" le caratteristiche dello specifico trattamento di dati personali, al fine di evitare informative lunghe e poco fruibili dai destinatari dell'informativa stessa.

- **Apparato sanzionatorio**

  In caso di violazioni relative al trattamento dei dati, è stato aumentato l'ammontare delle sanzioni amministrative pecuniarie, le quali potranno arrivare fino ad un massimo di 20 milioni di Euro (per i privati e le imprese non facenti parte di gruppi societari) o fino al 4% del fatturato mondiale totale annuo (per gruppi societari), lasciando peraltro ciascuno Stato membro libero di adottare norme relative ad altre sanzioni.

3.4.3 Conclusioni

Nel futuro prossimo, lo sforzo maggiore sarà quello di prepararsi alle diverse previsioni sopra illustrate e di dissipare i dubbi interpretativi dovuti alla coesistenza di norme diverse, a livello nazionale, che regolano gli stessi fenomeni. Un aiuto in tal senso può provenire dal Considerando 8 del Regolamento: *Ove il presente regolamento preveda specificazioni o limitazioni delle sue norme ad opera del diritto degli Stati membri, gli Stati membri possono, nella misura necessaria per la coerenza e per rendere le disposizioni nazionali comprensibili alle persone cui si applicano, integrare elementi del presente regolamento nel proprio diritto nazionale*. Tale disposto ha pertanto previsto la possibilità anche per i Legislatori nazionali di produrre normativa integrativa del Regolamento. Tuttavia, in tale Considerando, è insito il rischio di creare diversità tra normative nazionali, con conseguente possibilità di ricreare le stesse problematiche che hanno dato luogo alla proposta di nuovo Regolamento europeo in materia di privacy e di trattamento dei dati personali.

4. La Cybersecurity in Europa

All'interno dell'Unione Europea, i primi documenti ufficiali relativi alla sicurezza delle reti e delle informazioni risalgono agli inizi del 2000. La cybersecurity in Europa rappresenta ancora oggi un vero work in progress, caratterizzato dalla progressiva definizione delle nuove minacce via via emergenti dal cyber spazio. La definizione di una strategia di cybersecurity dell'Unione europea, il 7 febbraio 2013, è stata la base per la necessaria evoluzione verso l'elaborazione di strumenti più specifici dal punto di vista operativo. Il 6 luglio 2016 è stata approvata una Direttiva comunitaria per la sicurezza delle reti e dell'informazione, nota anche come Direttiva NIS (*Network and Information Security*). Essa stabilisce i requisiti minimi per la sicurezza informatica per gli operatori di infrastrutture in diversi settori tra cui la stessa sanità. La Direttiva fa parte del percorso sulla cybersecurity che l'Unione Europea ha iniziato nel 2013 ed è la risposta dell'Unione Europea al crescente numero di attacchi informatici contro i servizi erogati dalle infrastrutture critiche di ciascuno Stato membro. La condivisione delle informazioni tra gli Stati è un pilastro della direttiva NIS: le organizzazioni hanno infatti l'obbligo di segnalare gravi incidenti informatici ai CSIRT (*Computer Security Incident Response Team*) nazionali. Un ruolo fondamentale è coperto dall'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), che opera per facilitare la collaborazione tra gli Stati e la condivisione delle informazioni. Gli Stati membri hanno ventun mesi di tempo per adeguarsi alla direttiva NIS e sei mesi supplementari per identificare gli operatori addetti alle infrastrutture critiche nazionali.

4.1 Inquadramento normativo e assetto regolatorio

Oggi la massiccia diffusione di dispositivi medici dotati di interfaccia di rete (o comunque capaci di interagire con l'infrastruttura informatica) ha profondamente cambiato lo scenario all'interno delle aziende sanitarie.
L'infrastruttura IT di una azienda sanitaria ha almeno due peculiarità:

- presenza in rete di apparecchi elettromedicali o software medicali stand-alone;
- trattamento di dati personali, per lo più sensibili.

Con riguardo al primo punto, il fabbricante è tenuto a dimostrare la sicurezza dei dispositivi anche con riguardo agli aspetti di cybersecurity. Ciò può avvenire attraverso l'applicazione di norme tecniche armonizzate. Un primo fondamentale riferimento è la norma EN IEC 62304 per dispositivi che incorporano un software o che costituiscono in sé un software medicale. Questa norma è relativa alla validazione e gestione del ciclo di vita del software sia in fase di sviluppo che di manutenzione.

La norma EN IEC 62304 chiede espressamente che la gestione del rischio software sia condotta in conformità alla norma EN ISO 14971. Il software di un dispositivo medico può contribuire infatti al verificarsi di situazioni pericolose, che devono essere gestite. La serie di eventi che possono portare a situazioni pericolose possono rientrare in due categorie:

- errori nelle specifiche del software;
- errori nell'implementazione del software.

L'analisi del rischio viene effettuata attraverso l'identificazione di potenziali funzionalità del software che possono portare a situazioni pericolose. In tal senso il report tecnico IEC 80002-1 (IEC/TR 80002-1:2009 *"Medical device software- Guidance on the application of ISO 14971 to medical device software")* fornisce una guida utile sull'applicazione dei requisiti considerando le norme EN ISO 14971 e EN IEC 62304.

Mentre ci sono specifiche norme tecniche e riferimenti legislativi che si occupano della sicurezza e della validazione del software in ambito medicale manca ancora una precisa e completa struttura regolatoria per la gestione e regolamentazione dei dispositivi medici connessi ad una rete. A parte lo standard IEC 60601-1, si può fare riferimento alla norma IEC 80001-1. Questo standard riconosce una responsabilità condivisa tra il fabbricate e il professionista medico (o l'azienda ospedaliera), che devono collaborare per gestire in modo sicuro la connessione del dispositivo ad una rete.

Lo **standard IEC 80001-1** definisce le funzioni, le responsabilità e le attività necessarie alla gestione dei rischi delle reti IT incorporanti dispositivi medici ai fini di sicurezza, efficienza e sicurezza dei dati e del sistema.

Eccone i principi base:

- L'incorporazione o rimozione di un dispositivo medico o altri componenti in una rete IT è un compito che richiede un piano d'azione che potrebbe essere fuori dal controllo del fabbricante del dispositivo medico.
- La gestione del rischio deve essere effettuata prima che il dispositivo medico venga connesso ad una rete IT e durante l'intero ciclo di vita della rete IT che incorpora il dispositivo.
- Il fabbricante del dispositivo medico è responsabile per l'analisi del rischio del dispositivo, quale processo continuo per tutta la vita utile del dispositivo.
- Il fabbricante di un dispositivo medico destinato a essere incorporato in una rete IT deve fornire le informazioni necessarie per consentire una gestione del rischio in accordo con lo standard IEC 80001-1.
- Deve essere predisposto un *documento di accompagnamento* al dispositivo contenente le istruzioni per una corretta connessione alla rete IT, dettagli sul modo in cui vengono trasferite informazioni attraverso la rete e le caratteristiche minime che la rete IT deve avere affinché il

dispositivo funzioni correttamente, oltre alle avvertenze sui pericoli associati ad un uso scorretto o improprio della rete IT.

- Possono essere stabiliti uno o più accordi di responsabilità che coinvolgono le varie parti interessate. Un accordo di responsabilità può riguardare uno o più progetti o il mantenimento di una o più reti IT medicali. Esso deve altresì identificare le responsabilità per tutti gli aspetti del ciclo di vita della rete e tutte le attività che ne fanno parte.
- L'organizzazione responsabile è tenuta a individuare personale specifico come, per esempio, il manager per la gestione del rischio delle reti IT medicali.
- Il manager per la gestione del rischio delle reti IT medicali deve assicurarsi che la gestione del rischio si svolga sia durante il periodo di pianificazione e progettazione per nuove incorporazioni di dispositivi medici o relativi cambiamenti, sia durante l'uso, compresa la gestione dei change-release.

4.1.1 Ruoli e responsabilità legati alle reti IT e alla gestione dei rischi

Sono diverse le figure che, con riguardo alla cybersecurity, hanno obblighi e responsabilità.
Prima fra tutte c'è l'**Organizzazione Responsabile**, che è quell'ente responsabile dell'uso e della manutenzione di un apparecchio o di un sistema elettromedicale, della rete IT e del software dispositivo medico (es. azienda ospedaliera). Questa organizzazione è quindi responsabile di tutto il processo di gestione del rischio per le reti IT medicali e si deve quindi occupare di tutto ciò che le riguarda, dalla progettazione all'istallazione fino, eventualmente, alla messa fuori uso.
Parte dell'organizzazione responsabile, il **Top Management** si occupa di creare politiche per stabilire le attività di gestione del rischio e nomina il **Manager della gestione del rischio** delle rete IT che è la persona responsabile per la gestione e l'esecuzione dei processi di gestione del rischio della rete. Tra le responsabilità del manager c'è quella di raccogliere, analizzare, valutare e memorizzare i dati provenienti dall'organizzazione sanitaria, dal fabbricante del dispositivo medico e dal fornitore di tecnologie informatiche.
Ogni **fabbricante** di un dispositivo medico che deve essere integrato in una rete IT deve descrivere, nelle istruzioni per l'uso le istruzioni per l'implementazione delle relative connessioni ossia, per esempio, le caratteristiche della rete, le procedure di configurazione, le specifiche tecniche della connessione. E' dunque a carico del fabbricante il processo completo di gestione del rischio, incluse le interconnessioni e interazioni del dispositivo medico con altri dispositivi attraverso la rete IT di cui è parte. Un ruolo importante è anche quello dei **fornitori di tecnologie informatiche** (componenti dell'infrastruttura, server, software applicativi, dispositivi client che non sono dispositivi medici, middleware, ecc.) che possono fornire all'organizzazione responsabile ulteriori informazioni per sostenere le attività di gestione del rischio.

4.1.2 Gestione del rischio per le reti IT medicali

Il processo di gestione del rischio per le reti IT medicali, in conformità allo standard IEC 80001-1, si articola in fasi analoghe a quelle previste dalla norma EN ISO 14971 per i dispositivi medici: analisi, stima, valutazione, controllo del rischio e valutazione del rischio residuo. Tutte queste fasi devono essere documentate all'interno del piano di gestione del rischio associato alla rete IT.

4.2 Responsabilità dei fabbricanti

Come abbiamo già visto nel capitolo 1, nella definizione di dispositivo medico è incluso anche il software medicale stand alone e, per la dimostrazione di sicurezza di quest'ultimo, ne è richiesta la validazione.
Un passaggio essenziale del processo di dimostrazione della conformità è la gestione dei rischi. Dal momento che ormai molti dispositivi medici sono dotati di interfaccia di rete e si connettono alla rete IT dell'ospedale o di altre strutture, il fabbricante non può effettuare una gestione del rischio completa e corretta se non conosce preventivamente la tipologia e le caratteristiche dell'infrastruttura IT con cui il dispositivo viene integrato. È poi l'ospedale o la struttura sanitaria che deve occuparsi della gestione del rischio legata al funzionamento del dispositivo medico in rete (da qui il termine di organizzazione responsabile).

5. La Cybersecurity in USA

I dispositivi medici nel corso degli anni sono stati oggetto di un'evoluzione tecnologica di grande importanza e che è diventata via via sempre più veloce.
In passato, i dispositivi medici erano applicati al paziente attraverso un collegamento di tipo fisico. I dispositivi erano essi stessi degli oggetti fisici e i dati da questi ottenuti venivano trascritti e conservati su carta. Inoltre, la cura del paziente poteva essere effettuata solo all'interno di strutture sanitarie.
Oggi, invece, i dispositivi medici possono essere connessi al paziente o ad altri dispositivi via wireless. I dispositivi includono software o sono essi stessi dei software o ancora includono database di informazioni sanitarie e dati clinici. I dati ottenuti da tali dispositivi sono conservati su spazio virtuale, pertanto sono accessibili da remoto da qualsiasi parte del mondo. La cura del paziente può essere gestita anche semplicemente attraverso un'App installata su un dispositivo mobile.
Attraverso il progresso tecnologico aumentano i benefici per il paziente, ma al tempo stesso aumentano anche dei rischi. Tra questi, il rischio di attacchi informatici che potrebbero corrompere, modificare, eliminare dati su cui si basa la gestione clinica di un paziente.
Le minacce informatiche sono sempre più frequenti e comportano costi molto alti: recenti dati confermano che nel 2014 l'85% delle grandi strutture sanitarie americane ha subito almeno un attacco informatico e che il 18% degli attacchi è costato più di un milione di dollari per la loro risoluzione.
Recentemente, inoltre, si è scoperto come attentati terroristici possano essere effettuati anche attraverso attacchi informatici a software medicali, in particolare a software di monitoraggio di parametri vitali oppure a dispositivi impiantabili attivi come pacemaker.
Per questo motivo negli U.S.A., FDA già da tempo si preoccupa anche di aspetti di cybersecurity e negli anni ha emesso diverse linee guida e documenti regolatori che danno supporto ai fabbricanti di dispositivi medici a gestire correttamente la sicurezza informatica.

5.1 Regolamentazione e linee guida

Già nel gennaio 2005 l'FDA aveva emesso una linea guida sulla cybersecurity per i dispositivi contenenti software off-the-shelf connessi ad una rete.
A questo documento sono seguiti poi diversi anni di "silenzio".
Solo nel febbraio 2013 il Presidente Obama ha emesso un ordine esecutivo per migliorare il livello di cybersecurity delle infrastrutture critiche. Pochi mesi dopo, nel giugno del 2013, l'FDA ha poi

emesso una linea guida in versione draft sulla cybersecurity dei dispositivi medici. Negli stessi giorni l'FDA ha inoltre emesso delle precauzioni di carattere generale sulla cybersecurity dei dispositivi basate sulle vulnerabilità già note dei software.
Poco più di un anno dopo, nell'ottobre del 2014, il draft di linea guida sulla cybersecurity dei dispositivi medici diventa definitiva e stabilisce che le informazioni relative alla cybersecurity dei dispositivi medici debbano essere incluse nelle procedure di controllo pre-market ai fini della commercializzazione di dispositivi medici con software e software medicali nel territorio. Il 2 ottobre 2014 l'FDA emette perciò la linea guida denominata *"Content of Premarket Submissions for Management of Cybersecurity in Medical Devices".*
La più recente è infine il draft di linea guida emessa lo scorso gennaio 2016 denominata *"Postmarket Management of Cybersecurity in Medical Devices",* che descrive invece gli adempimenti post-market per il mantenimento della cybersecurity dei dispositivi.

5.2 Cybersecurity in fase pre-market

Come specificato al paragrafo precedente, il primo documento emesso da FDA relativamente alla cybersecurity risale al 2005 ed è la linea guida *"Cybersecurity for networked medical devices containing Off-the-Shelf (OTS) Software"*, che è ancora oggi un documento di riferimento per i fabbricanti di dispositivi medici che incorporano uno o più software OTS, per fabbricanti di software medicali che includono moduli software OTS e per fabbricanti di software connessi ad una rete intranet privata o ad una rete internet pubblica. La guida risulta utile anche agli amministratori delle reti nelle strutture sanitarie e in chi opera in ambito Information Technology (IT).
Essa specifica che è il fabbricante di dispositivi che incorporano software OTS ad essere responsabile della sicurezza e dell'efficacia del dispositivo medico, ed è responsabile anche della sicurezza del software OTS incluso nel dispositivo stesso.
In particolare, la guida specifica che le modifiche apportate al software per migliorare il livello di cybersecurity sono modifiche di progettazione, pertanto devono essere validate prima dell'approvazione e del rilascio, ai sensi del 21 CFR 820.30. Qualora il dispositivo che contiene il software sia già stato approvato da parte di FDA attraverso una procedura di *Pre-marketing Clearance* (510(k)), tali modifiche al software non richiedono una nuova revisione da parte di FDA, quindi il fabbricante può gestire le modifiche in GMP senza obbligo di presentare una nuova 510(k). Le modifiche al software devono essere riviste da FDA solo se comportano una variazione della destinazione d'uso del dispositivo o se possono significativamente inficiare la sicurezza e l'efficacia precedentemente dimostrati.
Allo stesso modo, per i dispositivi che sono stati oggetto di *Pre-Market Approval Application (PMA)*, una software patch richiede un supplemento alla PMA solo se cambiano le indicazioni per

l'uso del dispositivo o se può avere un impatto negativo sulla sicurezza e l'efficacia del dispositivo medico approvato. Altrimenti, il fabbricante può documentare e riportare all'FDA attraverso l'Annual Report (21 CFR 814.39(b) e 21 CFR 814.84) la decisione di implementare la patch al software del dispositivo medico.

Alla linea guida sulla cybersecurity relativa ai software OTS seguono diversi anni di silenzio da parte dell'FDA, anni durante i quali non si parla più di sicurezza informatica per i dispositivi medici. Eppure la tecnologia e lo stato dell'arte dei dispositivi medici evolve molto rapidamente, così come rapidamente nascono nuove minacce informatiche.

Solo nel 2013 FDA pubblica un nuovo draft di linea guida, finalizzata poi nel 2014, che specifica il contenuto di una pratica pre-market (Premarket Notification - 510(k), De Novo, Premarket Approval Application, Product Development Protocols, Humanitarian Device Exemption (HDE) submissions) in termini di cybersecurity.

In particolare, FDA sottolinea ai fabbricanti che già in fase di progettazione e di sviluppo è necessario analizzare le vulnerabilità del software. La cybersecurity in questo modo diventa parte dell'intero ciclo di sviluppo del software e sviluppata prima di tutto in analisi dei rischi.

I dispositivi medici che sono in grado di essere collegati ad un altro dispositivo, ad internet o ad un'altra rete, in modalità wireless o cablata, o che possono essere collegati ad un supporto portatile (per esempio, una chiavetta USB o un CD), sono generalmente più vulnerabili alle minacce di cybersecurity rispetto ai dispositivi non connessi. Nell'implementare misure di controllo del rischio da minacce informatiche, deve essere mantenuto un certo equilibrio tra la garanzia di sicurezza informatica e l'usabilità del dispositivo medico, affinché le misure di controllo scelte ed implementate siano appropriate. Per esempio, i controlli di sicurezza non dovrebbero irragionevolmente ostacolare l'accesso ad un dispositivo destinato ad essere utilizzato durante una situazione di emergenza.

La linea guida specifica anche chiaramente quali sono le informazioni che devono essere inoltrate a FDA in fase pre-market, tra cui:

- un elenco di tutti i rischi di sicurezza informatica che sono stati considerati nella progettazione del dispositivo;
- un elenco di tutti i controlli di sicurezza informatica;
- una tabella di rintracciabilità che evidenzia il collegamento tra le misure di controllo realmente implementate e i rischi di cybersecurity individuati per il dispositivo medico;
- una descrizione sommaria del piano per la fornitura di aggiornamenti software e patch convalidati e di come questi saranno gestiti per tutto il ciclo di vita del dispositivo medico affinché possa continuare a garantire la sua sicurezza ed efficacia;
- una descrizione dei controlli che sono messi in atto affinché il software mantenga la sua integrità;

- istruzioni per l'uso del dispositivo medico e specifiche di prodotto relative ai controlli di cybersecurity raccomandati per l'ambiente in cui il dispositivo è destinato ad essere utilizzato (per esempio software antivirus, uso di firewall, ecc.).

La linea guida FDA riporta anche alcuni esempi di possibili misure di controllo della cybersecurity che un fabbricante può implementare. Alcuni di questi esempi sono relativi a misure di sicurezza informatica ormai da tempo consolidate, come l'accesso alle funzionalità del software attraverso credenziali personali per ciascun utente, oppure una gestione dei privilegi di utilizzo del software in relazione al ruolo di ogni singolo utente. E' possibile inoltre prevedere metodi temporizzati automatici per terminare le sessioni all'interno del sistema. Oltre a ciò e poiché moltissime minacce informatiche e virus si nascondono all'interno degli aggiornamenti, è opportuno implementare una misura di controllo che richieda un'autorizzazione prima del loro download.
Tali misure di controllo costituiscono a tutti gli effetti dei requisiti del software e, come tali, devono seguire tutte le fasi del ciclo di sviluppo, dall'identificazione, alla definizione delle specifiche, alla verifica della corretta implementazione fino alla loro validazione.

5.3 Cybersecurity in fase post-market

Le minacce informatiche e i virus sono in continua evoluzione, pertanto non è possibile eliminare completamente o ridurre al minimo i rischi di cybersecurity solo attraverso controlli premarket.
E' necessario quindi che il fabbricante implementi processi adeguati di gestione dei rischi di cybersecurity, in conformità ai *Design Controls* di cui al 21 CFR 820.30.
Attraverso la linea guida *"Postmarket Management of Cybersecurity in Medical Devices"* (emessa al momento solo in draft), FDA conferma la propria raccomandazione ai fabbricanti di gestire gli aspetti di cybersecurity in maniera proattiva.
A partire dal febbraio 2015, ossia dall'ordine esecutivo "*Promoting Private Sector Cybersecurity Information Sharing"*, sono state istituite sul territorio americano numerose organizzazioni che si occupano di analisi e di condivisione delle informazioni di cybersecurity, le cosiddette ISAO (Information Sharing and Analysis Organizations). Anche il CDRH, Dipartimento dell'FDA, ha stipulato un protocollo d'intesa con una di queste organizzazioni, il National Health Information Sharing & Analysis Center, al fine di contribuire a promuovere la collaborazione e la comunicazione tra le parti interessate ed incoraggiare la condivisione delle informazioni legate alle minacce e vulnerabilità della sicurezza informatica che possono influenzare la sicurezza, l'efficacia e l'integrità dei dispositivi medici e delle reti IT di cui fanno parte.
Il draft *"Postmarket Management of Cybersecurity in Medical Devices"* suggerisce proprio ai fabbricanti di dispositivi medici di includere all'interno del programma di gestione dei rischi di

cybersecurity alcuni aspetti del *NIST Framework for Improving Critical Infrastructure Cybersecurity*, promosso dal Presidente degli Stati Uniti Obama il 12 febbraio 2013 con l'Ordine Esecutivo 13636, "Improving Critical Infrastructure Cybersecurity". Con questo ordine esecutivo, viene chiesta la costituzione di una struttura di cybersecurity volontaria che fornisca un approccio basato su priorità e prestazioni, che sia flessibile, ripetibile e "cost-effective" e al fine di gestire il rischio di sicurezza informatica per quei processi, informazioni e sistemi direttamente coinvolti nella fornitura di servizi di infrastrutture critiche.

Lo stesso ordine esecutivo definisce le infrastrutture critiche come quei "sistemi e beni, fisici o virtuali, di importanza così vitale per gli Stati Uniti che la loro mancata funzionalità o distruzione avrebbero un impatto devastante sulla sicurezza nazionale, sulla sicurezza economica e/o sulla salute pubblica".

Il NIST framework è un metodo piuttosto complesso di gestione del rischio di sicurezza informatica, ma che si può riassumere nelle seguenti fasi principali:

1. Identificare;
2. Proteggere;
3. Rilevare;
4. Rispondere e reagire;
5. Recuperare.

I dispositivi medici non rientrano propriamente nella definizione di infrastruttura critica data dall'Ordine Esecutivo 13636, ma è indubbio che gli effetti di potenziali vulnerabilità del software sulle prestazioni cliniche essenziali del dispositivo possono causare problemi sulla salute del paziente. Inoltre le vulnerabilità che sembrano in prima battuta non avere un impatto sulle prestazioni del dispositivo, devono comunque essere valutate dal fabbricante perché potrebbero avere un impatto futuro.

L'FDA riconosce già da tempo che i dispositivi medici e le reti a cui sono collegati non possono essere completamente protetti, pertanto chiede ai fabbricanti il massimo scrupolo e la massima attenzione possibile nel processo di gestione del rischio. In particolare, secondo quanto specificato nel draft "Postmarket Management of Cybersecurity in Medical Devices", i fabbricanti di dispositivi medici dovrebbero stabilire, documentare e mantenere per tutta la vita utile del dispositivo un processo per identificare i pericoli associati alla sicurezza informatica, stimare e valutare i rischi associati, controllare tali rischi e monitorare l'efficacia delle misure di controllo adottate ed implementate.

Gestione della cybersecurity post-market significa anche gestione delle modifiche al software per il miglioramento della cybersecurity. In fase pre-market si possono infatti analizzare i rischi derivanti da tutte le minacce prevedibili, ma poi possono verificarsi attacchi informatici che non erano stati presi in considerazione. Questo potrebbe portare alla necessità di implementare delle modifiche al

software, che di fatto sono delle modifiche in progettazione. Questo significa allora che la cybersecurity non entra a far parte del solo ciclo di sviluppo del software ma anche nel suo ciclo di manutenzione.
In particolare, le modifiche al software effettuate in fase post-market per un miglioramento della cybersecurity devono essere validate come richiesto dal 21 CFR 820.30, ma è sufficiente gestirle a sistema qualità e non è necessario invece sottometterle a nuova revisione da parte dell'FDA mediante, ad esempio, una nuova procedura 510(k).
Questo è stato risottolineato ad agosto 2016 dalla linea guida in corso di pubblicazione definitiva (*"Deciding when to submit a 510(k) for a software change to an existing device")*, che dettaglia quali sono le modifiche al software che richiedono l'inoltro di una nuova pratica 510(k). Tale principio è presente anche nelle linee guida *"Postmarket Management of cybersecurity in medical devices"* e *"Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software".*

5.4 Medical Mobile Apps

Il 9 febbraio 2015, l'FDA ha pubblicato la linea guida "*Mobile Medical Applications"* specificamente dedicata alle App medicali. Ad oggi sono numerosissime e sempre in aumento le app per smartphone, tablet o PC che possono avere finalità mediche o che sono esse stesse dei dispositivi medici. L'FDA pertanto si è preoccupata di emettere una linea guida specifica, rivolgendosi ai fabbricanti di App medicali, per chiarire come intende comportarsi per quanto riguarda gli aspetti di analisi, regolamentazione e controllo delle suddette App.
La linea guida per prima cosa chiarisce cosa si intende per app medicale e chi è considerato fabbricante di app.
Qualunque tipologia di Applicazione Mobile, per funzionare, ha bisogno di una *"mobile platform"*, piattaforme off-the-shelf di natura portatile, con o senza connettività wireless.
La linea guida specifica la differenza tra *"mobile app"*, applicazione mobile che può essere eseguita su piattaforma mobile o un'applicazione software web-based, e *"medical mobile app"*, ossia una applicazione mobile che soddisfa la definizione di dispositivo di cui alla sezione 201(h) della Federal Food, Drug, and Cosmetic Act, o di accessorio di un dispositivo medico.
Quindi è la destinazione d'uso di una App a determinare se essa sia o meno un "device".
Se infatti una App è destinata ad essere impiegata con funzione di diagnosi di una malattia, o per la cura, la mitigazione, il trattamento o la prevenzione di una malattia, allora essa è un dispositivo medico, indipendentemente dalla piattaforma mobile su cui viene eseguita.

Ai sensi della linea guida FDA, è considerato fabbricante di una mobile medical app qualsiasi persona o entità the produce e fabbrica app medicali, incluso chi definisce le specifiche, la progettazione e le etichette o chi crea per un dispositivo medico un sistema software o una applicazione nel suo insieme o a partire da diversi componenti software. Nel caso in cui, per esempio, uno sviluppatore crea una app sulla base delle specifiche dell'ideatore della app stessa, quindi del suo autore, l'autore dell'app che ha per primo sviluppato le specifiche è considerato fabbricante di quella app ai sensi del 21 CFR 803.3. Pertanto, si può affermare che gli sviluppatori software non sono necessariamente fabbricanti di app: se sono responsabili solamente delle attività di progettazione e sviluppo al fine di trasformare le specifiche dell'autore in una app medicale, non sono fabbricanti.

L'FDA specifica nella linea guida *"Mobile Medical Apps"* quali sono le app per le quali intende applicare per intero la regolamentazione prevista per i dispositivi medici e per quali invece intende applicare l'enforcement discretion, poiché di rischio molto basso per il paziente.

Una App che sia essa stessa un dispositivo medico è soggetta ai requisiti di classificazione propri dei dispositivi medici, pertanto il fabbricante deve identificare l'appropriato Product Code e sulla base di quest'ultimo classificare la propria app come dispositivo medico di classe I, II o III. Anche le procedure di approvazione alla commercializzazione delle app, in questo caso, sono le stesse previste per i dispositivi medici, per cui General Controls per le app di classe I, General Controls e Special Controls per App di classe II e procedure di Pre-Marketing Approval Application per App di classe III.

Anche i fabbricanti di App medicali, infine, hanno l'obbligo di implementare un Sistema di Gestione della Qualità conforme ai requisiti del 21 CFR 820 et alter.

6. Scenario futuro

Recentemente, in particolare a giugno 2015, l'IEC ha emendato la norma IEC 62304. Tale emendamento tuttavia non è ancora stato recepito dal CENELEC e quindi non ancora "armonizzato". In ogni caso entro il 2019 è prevista una nuova edizione dello standard nel quale ci si aspetta:

- l'inserimento dei requisiti del LEGACY SOFTWARE, ovvero un software vecchio ma che continua ad essere usato perché l'utente non intende o non può sostituirlo. A volte infatti è necessario ricorrere a software retrodatati per questioni di compatibilità;
- l'allineamento della classificazione basata sul rischio al sistema FDA (Major, Moderate, Minor).

Lo standard IEC 62304 può essere applicato nello sviluppo e nella manutenzione di *Medical Device Software* quando il software è esso stesso un dispositivo medico o quando è parte integrante del dispositivo medico finale. I *Medical Device Software* fanno parte degli *Health Software*, ossia i software destinati ad essere usati in particolare per mantenere e migliorare la salute delle singole persone o la prestazione delle cure. La definizione di Health Software viene data all'interno dello standard IEC 82304-1 "Health software --Part 1: General requirements for product safety", che però è ancora in fase di sviluppo. Si tratta infatti di un Draft International Standard (DIS), la cui ultima versione è stata pubblicata per commenti nel luglio del 2015. Il suo campo di applicazione include tutti i tipi di software che hanno un effetto sia diretto che indiretto sulla salute.

Mentre la IEC 62304:2015 dà la definizione di software come dispositivo medico e riguarda il sistema software che è stato sviluppato col fine ultimo di essere incorporato in un dispositivo medico in fase di sviluppo o che è inteso ad essere usato come dispositivo medico a sé, nella IEC 82304-1 si trova invece la definizione di Health Software e di *Health Software Product*. La norma IEC 82304-1 e la IEC 62304 sono quindi considerate complementari.

I seguenti tipi di software ricadono all'interno del campo di applicazione dello standard IEC 82304-1 e non della IEC 62304:

- Radiology Information System (RIS),
- Prescription Management Systems (PMS),
- Laboratory Information Management Systems (LIMS),
- Mobile Apps, che non sono applicazioni medicali secondo la relativa guida FDA,
- Software che non sono considerati dispositivi medici secondo la MEDDEV 2.1/6.

Quindi contrariamente alla norma IEC 62304, lo standard IEC 82304-1 riguarda solo i software stand-alone e non quelli inglobati nei dispositivi medici o in dispositivi con specifico hardware. Pertanto solo i software in esecuzione su PC, server, tablet o smartphone con un sistema

operativo a scopo generico sono regolati dalla norma 82304-1 come si può vedere nello schema riassuntivo illustrato in figura 6.1:

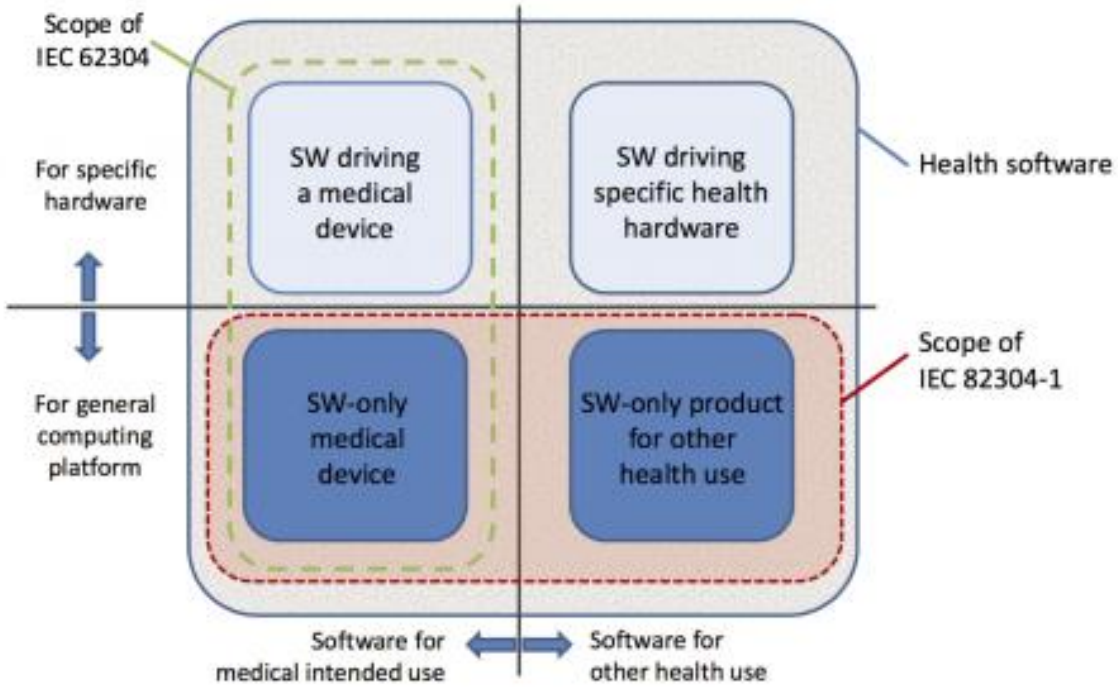

Figura 6.1: scopo e campo di applicazione delle norme IEC 62304 e IEC 82304-1

La norma IEC 82304-1 definisce i requisiti a livello di sistema per gli Health Software Systems e, per quanto riguarda il ciclo di vita del software, fa riferimento a un insieme di requisiti contenuti anche nello standard IEC 62304, come si può vedere dallo schema riassuntivo illustrato di seguito:

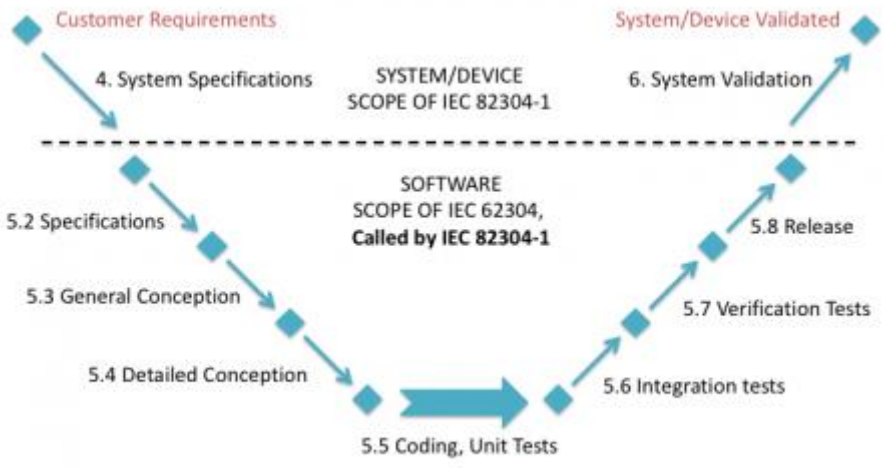

Figura 6.2: ciclo di sviluppo secondo le norme IEC 62304 e IEC 82304-1

Quindi, se si applica la norma IEC 82304-1 al software, occorre applicare anche la norma IEC 62304. Inoltre lo standard IEC 82304-1 è in relazione anche con la norma ISO 14971, relativa alla gestione del rischio, come mostrato in figura 6.3:

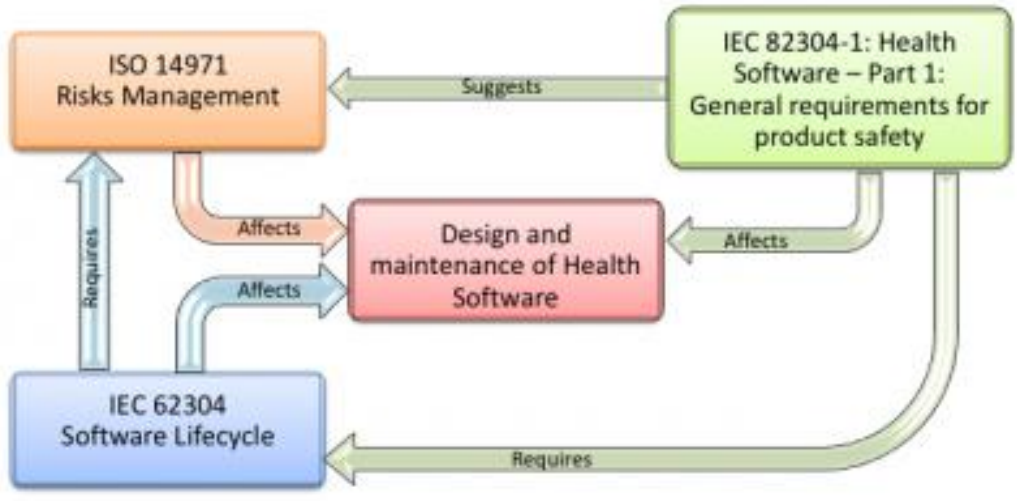

Figura 6.3: relazione con la norma ISO 14971

Possiamo aspettarci un'imminente pubblicazione della versione definitiva della norma IEC 82304-1, che potrebbe avvenire entro la fine del 2016. E' possibile inoltre che tale norma venga inserita tra gli standard armonizzati della Commissione Europea ed è molto probabile altresì che venga riconosciuta anche da FDA. Attualmente però il contesto normativo è ancora, incerto e in attesa, ad esempio anche della pubblicazione del testo definitivo dei Nuovi Regolamenti relativi a dispositivi medici e IVD.

7. Conclusioni

Il progresso tecnologico si sviluppa in contemporanea all'evoluzione di fattori sociali ed economici, ma non sempre la direzione è la stessa e non sempre la velocità di trasformazione è paragonabile.
In un contesto sociale, non solo europeo, in cui si assiste già da diversi anni ad una continua diminuzione delle nascite, contestuale ad un miglioramento delle cure, si va incontro inevitabilmente ad un conseguente aumento della vita media della popolazione e, quindi, ad un inarrestabile invecchiamento della popolazione.
In questo contesto però cambiano anche gli stili di vita: durata media e qualità della vita sono infatti due variabili che non possono non essere considerate.
La forte disoccupazione giovanile, e non solo, che ha colpito il mondo intero in questi anni di crisi economica globale, porta ad un ingresso nel mondo del lavoro in un'età già avanzata rispetto a quanto succedeva qualche decennio fa, cosicché anche l'uscita dal lavoro stesso risulterà sempre più lontana. Inoltre, ritmi di vita via via sempre più frenetici, stili di vita sedentari e cattiva alimentazione aumentano e sono sempre più spesso causa di patologie che evolvono rapidamente verso la cronicità.
Questo scenario richiede inevitabilmente un miglioramento delle cure, della qualità delle prestazioni sanitarie e una riduzione delle disuguaglianze nei trattamenti. Al tempo stesso, però, la tendenza di molte patologie a diventare croniche e la sempre maggiore richiesta di cure comportano un aumento dei costi della salute e della spesa sanitaria.
Le nuove tecnologie e dispositivi medici avanzati ci vengono in aiuto, ma al tempo stesso si rende necessario un cambiamento delle modalità di somministrazione delle cure.
Tecnologie "software-based" e wireless trovano sempre più spazio nel mercato medicale, perché lo stato di avanzamento tecnologico proprio delle ultime generazioni di questi dispositivi fa sì che il paziente possa essere curato e monitorato da remoto, garantendo comunque un'assistenza sanitaria di alto livello.
La gestione clinica del paziente da remoto, e quindi l'aumento dei pazienti domiciliarizzati, riduce poi inevitabilmente anche la spesa sanitaria e aumenta la disponibilità di posti letto, tecnologie e personale medico-sanitario da dedicare a pazienti con patologie acute.
Tutto questo è reso possibile soprattutto dalle nuove tecnologie, dall'evoluzione dei software medicali e delle reti IT, il cui sviluppo ha aperto però una nuova sfida per la sicurezza del paziente.
Che dire in conclusione? Forse anche questa volta l'evoluzione tecnologica è stata decisamente più rapida della definizione dell'impianto legislativo e di controllo, che è, ricordiamolo, il minimo indispensabile per prendersi cura in modo efficace e sicuro dei nostri pazienti.
Ci auguriamo per il futuro una maggiore reattività dei legislatori non solo nell'agire immediatamente, ma nel prevenire, disciplinando in anticipo le criticità apportate dallo sviluppo di tecnologie evolute.

Infine ricordiamo che il progresso tecnologico non è nulla se non è gestito adeguatamente, facendo i conti con le realtà di emergenza, criticità e immediatezza che ci troviamo ad affrontare oggi per curare i nostri cari.

Thema s.r.l.

via Saragat, 5 - 40026 Imola (BO) - Italia
www.thema-med.com info@thema-med.com