

# LA RESPONSABILITÀ MEDICA A DUE ANNI DALLA RIFORMA GELLI

## Riflessioni e problemi aperti

*L'incidenza dell'uso delle nuove tecnologie sulle responsabilità professionali dal punto di vista del giurista*

di

Francesco Giulio Cuttaia

### **1. L'importanza della tecnologia informatica e telematica in ambito sanitario.**

Nel nostro Paese gli aspetti concernenti la sanità digitale sono sostanzialmente riassumibili nei seguenti: il Centro Unico di Prenotazione (CUP); Il Fascicolo Sanitario Elettronico (FSE); la progressiva dematerializzazione dei documenti sanitari (di cui costituiscono espressione l'inoltro in via telematica dei certificati medici di malattia, la ricetta medica elettronica, la cartella clinica elettronica); la telemedicina.

Mentre i primi tre aspetti rappresentano una mera azione di supporto della digitalizzazione rispetto alle attività sanitarie, la telemedicina segna un passaggio fondamentale nell'affermazione dell'importanza della tecnologia informatica e telematica in ambito sanitario.

È infatti ormai pacificamente condivisa l'opinione secondo cui l'innovazione tecnologica può contribuire ad una efficiente riorganizzazione dell'assistenza sanitaria, attraverso la predisposizione di modelli innovativi che facilitino

l'accesso alle prestazioni sul territorio evitandone la concentrazione esclusivamente sulle strutture ospedaliere.

Tale esigenza è particolarmente avvertita nei territori considerati remoti (montani, rurali, piccole isole) ma in generale la possibilità di erogazione delle prestazioni sanitarie e sociosanitarie attraverso la telemedicina è ritenuta in grado di assicurare una adeguata gestione delle cronicità, un agevole canale di accesso all'alta specializzazione, nonché una maggiore continuità delle cure dopo la dimissione del paziente dalle strutture ospedaliere e un fondamentale ausilio per i servizi di emergenze/urgenza.

Lo sviluppo della telemedicina sul finire degli anni novanta del secolo scorso e nei primi anni duemila, si è avuto con modalità estemporanee, improntate soprattutto a sperimentazioni non sempre riuscite. Il che ha indotto il Ministero della Salute a individuare un modello di *governance* condivisa che, sulla base delle esperienze maturate e degli obiettivi da perseguire, si è esplicitato nella adozione di linee di indirizzo nazionali, le quali sono periodicamente aggiornate.

Si tratta delle linee di indirizzo in materia di telemedicina elaborate dal Ministero della Salute e pubblicate nel 2014.

Già in precedenza, in sede europea erano stati evidenziati la rilevanza della telemedicina e il suo impatto sui profili sociali ed economici degli Stati europei.

La Commissione europea, con la comunicazione COM 2008/689 emanata il 4 novembre 2008, recante "Telemedicina a beneficio dei pazienti, dei sistemi sanitari e della società", ha inteso sostenere gli Stati membri nella realizzazione, su larga scala, di servizi di telemedicina attraverso specifiche iniziative volte a creare un clima di fiducia sulla sua affermazione da parte dell'opinione pubblica e degli addetti alle strutture sanitarie.

In tale contesto è stato previsto che ciascuno Stato membro adegui la propria normativa nazionale al fine di consentire un accesso più ampio ai servizi di telemedicina, affrontando questioni quali l'accreditamento, la responsabilità, i rimborsi, la tutela della sfera privata e dei dati personali.

L'evoluzione della telemedicina pone una serie di problematiche giuridiche che vanno dai profili in tema di autorizzazione e accreditamento a quelli riguardanti la tutela della riservatezza dei pazienti, la cui definizione e soluzione, in mancanza di specifiche disposizioni normative, è rimessa soprattutto alla valutazione della compatibilità delle prassi finora insorte con il quadro normativo generale.

Un primo spunto di riflessione in tema di compatibilità della telemedicina con il quadro normativo generale lo si può rinvenire nel riferimento alla forza espansiva del Codice dell'Amministrazione digitale, laddove, all' art. 9, è stabilito che "le amministrazioni pubbliche favoriscono ogni forma di uso delle nuove tecnologie per promuovere una maggiore partecipazione dei cittadini, anche residenti all' estero, al processo democratico e per facilitare l'esercizio dei diritti politici e civili e migliorare la qualità dei propri atti".

Poiché tra le amministrazioni pubbliche rientrano anche le amministrazioni che costituiscono il Servizio sanitario nazionale, ne discende la piena applicabilità, nell'ambito sanitario, dei principi affermati nel CAD, ferme restando le attribuzioni previste in tema di tutela della salute dall'art. 117 Cost. e le disposizioni che disciplinano la riservatezza e la protezione dei dati sensibili.

## **2. La telemedicina: profili normativi ed evolutivi**

### **2.1. I riferimenti della l. 24/2017 alla telemedicina e alla sanità digitale**

Il tema dell'utilizzo delle tecnologie informatiche in ambito sanitario non è trattato in maniera diretta dalla l. 24/2017. Esso però può essere fatto rientrare nel profilo concernente la responsabilità generale in ambito sanitario e quella specifica connessa al *risk management* e alla tutela della trasparenza dei dati.

Sia dalla evoluzione normativa successiva alla legge Gelli-Bianco che dalla prassi quotidiana possono trarsi spunti di riflessione tali da richiedere al legislatore un ulteriore sforzo di adeguamento alle esigenze poste dallo sviluppo della tecnologia informatica in ambito sanitario.

#### **2.1.1. Il profilo della responsabilità sotto l'aspetto generale**

Con riguardo al primo aspetto da esaminare, quello concernente la responsabilità nelle sue diverse articolazioni, civile, penale, amministrativa e all'approntamento di un contesto tale da definirne con esattezza gli ambiti, è bene preliminarmente chiarire che essendo il servizio di telemedicina assimilabile a qualunque servizio sanitario diagnostico - terapeutico, la prestazione in telemedicina non sostituisce la prestazione sanitaria tradizionale che si ha nel rapporto personale medico - paziente, ma integra quest'ultima per migliorarne l'efficacia, l'efficienza e l'appropriatezza.

Questa annotazione, ai fini dell'accertamento delle responsabilità in ambito sanitario in un contesto caratterizzato dall'utilizzo della tecnologia

informatica e telematica per l'assistenza e la cura dei pazienti, va tenuta costantemente presente in quanto la prestazione sanitaria mediata da Information and communication technology (ICT) è da ritenere assimilata alla prestazione erogata secondo le forme cosiddette tradizionali, avendo essa il fine precipuo di migliorare la qualità e l'appropriatezza delle cure complessivamente erogate dal sistema sanitario.

Tuttavia, ci sono delle specificità da porre in evidenza.

Il modello organizzativo del servizio di telemedicina comporta l'esistenza di un Centro Erogatore, il quale può essere costituito da strutture del Servizio sanitario nazionale, autorizzate o accreditate pubbliche o private o da operatori del S.s.n. quali medici di medicina generale, pediatri di libera scelta, medici specialistici, i quali erogano prestazioni sanitarie attraverso una rete di telecomunicazioni, e di un Centro Servizi, il quale ha la funzione di gestire (assicurandone il funzionamento) il sistema informativo, sulla base del quale il Centro Erogatore svolge la prestazione in telemedicina.

Il Centro servizi organizza, per così dire, il sistema di telemedicina, approntando l'installazione e la manutenzione degli strumenti nei siti individuati (che nella forma più semplice possono essere le abitazioni dei pazienti) nonché la fornitura, la gestione e la manutenzione dei mezzi di comunicazione (compresa la gestione dei messaggi di allerta) tra pazienti, medici e altri operatori sanitari e l'addestramento all'uso di tali strumentazioni sia per il personale sanitario che per i pazienti.

Al riguardo, pur considerando come i servizi di telemedicina si debbano collocare nella cornice normativa del Servizio sanitario nazionale, appare chiara l'urgenza della definizione, in sede normativa, di una strategia unitaria in grado di favorire la gestione dell'appropriatezza clinica e prescrittiva

nonché l'aderenza terapeutica e l'accessibilità a più elevati standard di servizi, in modo anche da integrare la disciplina delle responsabilità.

A quest'ultimo proposito va notato che ai soggetti giuridici costituiti dalla struttura sanitaria e dall' esercente la professione sanitaria, può venire ad aggiungersene un terzo, e cioè colui che (persona fisica o giuridica) gestisce il Centro Servizi o comunque fornisce le relative attrezzature informatiche, destinato inevitabilmente ad assumere un ruolo sempre più rilevante nel processo evolutivo della telemedicina.

Proprio al fine di definire, per così dire, a monte, anche gli aspetti collegabili alla individuazione di responsabilità, potrebbe rivelarsi utile integrare le modalità di accreditamento per i centri erogatori, quando questi ultimi operino con oneri a carico del Servizio sanitario nazionale e di autorizzazione per le strutture che operino in ambito esclusivamente privatistico.

Ma soprattutto andrebbero inseriti nei percorsi di accreditamento e/o autorizzazione anche i centri servizi o, qualora essi non siano costituiti, le aziende che forniscono e mantengono la relativa strumentazione informatica.

Sul piano dell'accertamento delle responsabilità possono essere in conclusione individuate tre categorie di soggetti responsabili: il centro servizi o, in mancanza di esso, l'azienda produttrice e distributrice del dispositivo e dei supporti informatici di funzionamento e di collegamento con la centrale remota; la struttura sanitaria che eroga il servizio di telemedicina; il medico che segue il paziente e gestisce le diverse problematiche cliniche afferenti alla prestazione sanitaria resa con la modalità di telemedicina.

A tal riguardo, indipendentemente dall'accertamento, caso per caso, delle singole responsabilità, si può dire che la l. 24/2017 ha comunque messo un punto fermo in tema di responsabilità civile, affermando nei confronti del

paziente, in ogni caso, la responsabilità contrattuale della struttura sanitaria, in virtù dell'espresso riferimento anche alla telemedicina fatto dal secondo comma dell'art. 7.

### **2.1.2. IL PROFILO DEL RISK MANAGEMENT**

Relativamente al profilo del *risk management* occorre rilevare come la sicurezza delle cure sia considerata dall'art. 1, co.1, l. 24/2017 "parte costitutiva del diritto alla salute" ed essa, ai sensi del comma 2, si realizzi "anche mediante l'insieme di tutte le attività finalizzate alla prevenzione e alla gestione del rischio connesso all'erogazione di prestazioni sanitarie e l'utilizzo appropriato delle risorse strutturali, tecnologiche e organizzative".

Proprio per il perseguimento di tale finalità, l'art. 3 ha previsto l'istituzione dell'Osservatorio nazionale delle buone pratiche sulla sicurezza nella sanità, che è stato costituito con decreto del Ministro della Salute del 29 settembre 2017 e si è insediato presso l'AGENAS nel marzo del 2018.

Il primo rapporto formulato dall'Osservatorio, riguardante l'anno 2018 e inviato al Parlamento il 25 febbraio scorso pone in evidenza come il compiuto conseguimento della sicurezza del paziente, delle cure e dell'intero sistema sanitario si fondi sui principi di decentramento ed estrema periferizzazione, fino a giungere al singolo operatore sanitario, della gestione del rischio; di accentrato della gestione dei sinistri a livello aziendale, interaziendale e/o anche solo regionale; di integrazione, in entrambi i sistemi di gestione, con piattaforme informatico - telematiche, volte alla reciproca alimentazione dei dati e delle attività di prevenzione e valutazione delle casistiche.

È presumibile che sulla base delle iniziative che verranno assunte nei territori, si definiscano buone pratiche per la sicurezza anche nell'ambito della

telemedicina, al fine di definire interventi che riducano il rischio di eventi avversi che possano essere determinati dall'uso non congruo o scarsamente professionale delle strumentazioni informatiche o dall'utilizzo di apparecchiature non adeguate.

Da questo punto di vista si può dire che il cammino è appena iniziato anche se alcuni territori annoverano già esperienze valide, ulteriormente avvalorate da forme di cooperazione interregionali o transnazionali.

È il caso questo, e mi piace qui ricordarlo, della Provincia autonoma di Trento con la sua partecipazione al progetto *NathCare*, elaborato nell'ambito del programma di cooperazione territoriale europea "Spazio alpino 2007-2013" mirante a creare una rete transnazionale di sistemi sanitari per buona parte incentrato proprio sulla sanità elettronica.

### **2.1.3. La trasparenza dei dati relativi alla salute e il loro trattamento**

Per quanto riguarda la trasparenza dei dati relativi alla salute ed il loro trattamento, l'art. 4, co. 1, l. 24/2017 stabilisce che le prestazioni sanitarie erogate dalle strutture pubbliche e private sono soggette all'obbligo di trasparenza nel rispetto del codice di materia di protezione dei dati personali, il c.d. codice della privacy, che come noto è stato ampiamente modificato dal d.lgs. 101/2018 a sua volta emanato per adeguare il nostro sistema al Regolamento Ue 679/2016, divenuto pienamente operativo a partire dal 25 maggio 2018.

I successivi commi dell'art. 4 della l. 24/2017 configurano il diritto di accesso alla documentazione sanitaria come un diritto di accesso *sui generis*, azionabile anche nei confronti di soggetti privati, quali le strutture sanitarie



private, e distinguibile sia dal diritto di accesso ai documenti amministrativi sia dal diritto di accesso civico, ponendo in capo alla direzione sanitaria della struttura pubblica o privata di fornire entro 7 giorni al richiedente avente diritto la documentazione relativa al paziente “preferibilmente in formato elettronico” (art. 4, co. 2).

A prescindere dalle problematiche connesse al preciso configurarsi del diritto di accesso sul piano pratico (pensiamo alle modalità del suo esercizio, alla portata effettiva del concetto di documentazione disponibile, alla concreta sanzionabilità dell'inottemperanza all'obbligo di consegnare la documentazione entro il termine di 7 giorni, alla possibilità o meno di ricorrere in tale evenienza alla Garante per la protezione dei dati personali) quel che preme in questa sede porre in rilievo è come si stia evolvendo la disciplina del trattamento dei dati relativi alla salute quando siano utilizzati strumenti elettronici per la cura e l'assistenza a distanza dei pazienti.

In generale il trattamento dei dati personali che viene operato nell'espletamento dei servizi di telemedicina è assimilabile al trattamento dei dati personali di natura sensibile

I dati informativi relativi alla salute del paziente sono oggetto di particolare protezione.

Essi sono definiti dall' art. 4, n. 15, regolamento Ue 2016/679 quali “dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute”.

Questo fa sì che tali dati siano sottoposti ad un sistema particolarmente accurato che ne tutela il trattamento.

In generale, sulla base dell'art. 9, par. 1 del più volte citato regolamento Ue, che ricomprende i dati relativi alla salute nelle categorie particolari di dati personali, vige il principio del loro divieto di trattamento.

Il trattamento è tuttavia possibile quando si verifica uno dei casi indicati nel co. 2 del predetto articolo, il quale prevede al primo posto l'ipotesi in cui l'interessato abbia prestato il proprio consenso esplicito al trattamento di tali dati per una o più finalità specifiche.

Per i profili che qui interessano, ai sensi di quanto stabilito nella lett. h) del co. 2 del surrichiamato articolo, il trattamento è possibile quando "è necessario per finalità di medicina preventiva o di medicina del lavoro...diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità".

Ebbene, sostanzialmente quando ricorre l'esigenza di cura o diagnosi, il trattamento dei dati sanitari non solo non subisce divieti ma è praticabile prescindendosi dal consenso dell'interessato.

Il regolamento Ue 2016/679 appare, in generale, particolarmente attento ai processi della evoluzione tecnologica, tant'è che nel *considerando* (6) viene fatto rilevare che "la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali" e nel *considerando* (7) viene sottolineato che l'evoluzione tecnologica "richiede un quadro più solido e coerente in materia di protezione dei dati dell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno".

All'art. 35, par. 1, allorquando il trattamento dei dati preveda l'uso di nuove tecnologie (in considerazione altresì, del contesto e delle finalità del

trattamento) , possa presentare un rischio elevato per i diritti e le libertà della persona, è prescritta una preventiva valutazione dell'impatto del trattamento medesimo sulla protezione dei dati personali, con le modalità dettagliatamente descritte nel successivo paragrafo del succitato articolo. Il problema di maggior rilievo che si pone a proposito di trattamento di dati sanitari in telemedicina è quello di garantire la sicurezza delle informazioni.

In generale il titolare del trattamento ha il compito di predisporre le misure di ordine tecnico e organizzativo che siano idonee e adeguate al soddisfacimento di tale esigenza (art. 32 reg. UE. 2016/679).

In tale contesto assume una particolare valenza il principio della *accountability*, in quanto il reg UE dianzi citato prescinde dalla imposizione di misure minime (o, comunque, qualificabili come sufficienti), indicandole nel dettaglio, ma prescrive l'adozione di misure che debbono essere effettivamente idonee ed adeguate.

Anche sotto questo aspetto la normativa statale si è adeguata al principio generale introdotto dal regolamento UE e, comunque, già prima dell'entrata in vigore del d.lgs. 101 2018, le sezioni unite della Cassazione avevano evidenziato il profilo della idoneità delle misure da adottare, precisando che "i dati sensibili idonei a rivelare lo stato di salute possono essere trattati soltanto mediante modalità organizzative quali tecniche di cifratura o criptatura che rendono non identificabile l'interessato. Ne consegue - rilevano le Sezioni Unite - che i soggetti pubblici o le persone giuridiche private, anche quando agiscano rispettivamente in funzione della realizzazione di una finalità di pubblico interesse o in adempimento di un obbligo contrattuale, sono tenuti all'osservanza delle predette cautele nel trattamento dei dati in questione".

La legislazione italiana riserva una qualche attenzione ai profili concernenti la tutela dei dati relativi alla salute la cui acquisizione abbia luogo attraverso l'uso di nuove tecnologie.

Un profilo particolare nel contesto dell'informatizzazione dei dati sanitari è quello riguardante il fascicolo sanitario elettronico, istituito dall'art. 12, d.l. 179/2012.

Tale strumento informatico riunisce i dati e i documenti digitali o digitalizzati di tipo sanitario e socio sanitario, relativi al paziente.

Esso è costantemente aggiornato ed è accessibile, oltre che all'interessato, al personale sanitario autorizzato, mentre è esclusa la possibilità di accesso a datori di lavoro, periti assicurativi e terzi in generale.

Nonostante tali garanzie, l'inserimento dei dati all'interno del fascicolo sanitario elettronico è subordinato al consenso del paziente, il quale deve essere informato su chi ha accesso ai dati contenuti nel fascicolo e su come i dati stessi possano essere utilizzati.

In mancanza di una abrogazione espressa dell'art. 12, è da ritenere che la disposizione concernente la preventiva, obbligatoria acquisizione del consenso sia tuttora vigente.

Infatti, pur sancendo l'art. 75 del codice della privacy, nella sua nuova formulazione, che per il trattamento dei dati effettuati per finalità di cura e diagnosi non occorra più, in generale, come abbiamo visto, il consenso dell'interessato, conformemente a quanto previsto dall'art. 9 reg. 2016/679, ciò non equivale all'abrogazione *tout court* di quelle disposizioni legislative che prevedono il consenso dell'interessato, giacché proprio ai sensi della normativa europea è rimessa agli Stati membri la valutazione circa l'opportunità "di mantenere ulteriori condizioni, comprese limitazioni, con

riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute” (art. 9, par. 4, reg. Ue 2016/679).

D'altra parte è da ritenere applicabile, sia pur in via analogica, il principio di conservazione delle misure di protezione dei dati relativi alla salute, esplicitato dal cit. art. 22, co. 11 d.lgs. 101/2018.

A tal riguardo è intervenuta una recente pronuncia del Garante della Privacy, il quale ha confermato tale impostazione.

Tutto ciò a conferma ulteriore della flessibilità con cui la normativa europea consente alle legislazioni nazionali di intervenire nella definizione di ulteriori strumenti a protezione di dati particolarmente sensibili come sono quelli attinenti alla salute, i quali, con la diffusione delle tecnologie informatiche (senz'altro utili ad assicurare la diffusione, l'efficacia e l'efficienza delle prestazioni sanitarie) potrebbero subire rischi di sovraesposizione.

## Conclusioni

In conclusione si può affermare come la diffusione delle procedure e delle piattaforme digitali possa svolgere un ruolo chiave nella elaborazione di nuovi modelli di cura e di assistenza sanitaria.

Permangono diverse problematiche applicative, cui abbiamo fatto cenno, soprattutto di compatibilità con i tradizionali contesti normativi e amministrativi.

Il superamento di tali problematiche non può essere rimesso a interventi limitati ed episodici ma esige l'approntamento di un sistema organico per la sanità digitale in grado di fornire garanzia agli operatori e ai pazienti, fissando con chiarezza gli ambiti di responsabilità.