diritto&diritti dal 1996
diritto.it
fondatore Francesco Brugaletta

I tanti volti della e-health

Autore: Giulia De Paolis
In: Diritto civile e commerciale

Regolamento UE 679/2019

Tutela e gestione dei dati relativi alla salute

Il crescente processo di digitalizzazione che caratterizza il settore sanitario impone alle strutture sanitarie di tenere in debita considerazione gli aspetti legati al trattamento di dati idonei a rivelare lo stato di salute e la vita dei pazienti trattati con strumenti informatici e digitali[1].

La nascita della cd. **e-health**, come viene definita la possibilità di erogare servizi telematici in sanità, se da un lato rappresenta un'interessante potenzialità per lo scambio, l'integrazione e la condivisione di informazioni tra gli operatori sanitari, tra medici e strutture sanitarie e tra questi ultimi e il paziente, dall'altro lato rappresenta un rischio per le distorsioni che un sistema "informativo" non ben regolamentato può generare[2].

All'interno di queste infrastrutture informatiche occorre prendere in esame il cd. "**Fascicolo Sanitario Elettronico**'' (FSE), nuovo importante strumento a disposizione di coloro che operano in tale settore.
Esso si articola in due momenti: da un lato, quello dell'archiviazione di una massa di dati ed informazioni; dall'altro, quello della condivisione dei dati tra tutti gli operatori del sistema legittimati al trattamento. Lo sviluppo tecnologico ha dotato il professionista medico di strumenti nuovi per far sì che il flusso di informazioni provenienti dal paziente fosse più oggettivo ed affidabile. Grazie alle moderne tecniche di diagnostica, che si avvalgono di strumenti sempre più sofisticati, si è colmato il deficit informazionale tra medico e paziente. [3]

Il flusso informativo non è bidirezionale, bensì circolare. Infatti, le informazioni che provengono dal paziente, giungono al professionista sanitario, per poi essere da questi catalogate, rielaborate ed aggregate per ritornare, infine, al paziente sotto forma di cura, ossia di un percorso terapeutico. Si rende necessario affrontare il tema delle informazioni sanitarie dal punto di vista della tutela dei dati personali.[4]

La nozione italiana di FSE può essere resa, con approssimazione, con l'espressione anglosassone Electronic Health Record (EHR). Lo sviluppo delle tecnologie digitali ha reso sempre più evidente la necessità di implementare strumenti via via più evoluti, volti a proteggere i file e le informazioni raccolte nelle banche dati. La cd. "Computer security", ha ormai quasi del tutto preso il posto del vecchio sistema di controllo dati e della loro catalogazione in archivio cartaceo. Il primo aspetto da analizzare è quello

della c.d. "**confidentiality**" (riservatezza), con il tentativo di prevenire la divulgazione non autorizzata delle informazioni.

L'obiettivo principale è anzitutto quello di impedire agli utenti non autorizzati l'accesso alle informazioni sanitarie riservate (quali per esempio: particolari malattie, virus diffusi, patologie rare, interventi richiedenti cure particolari).

La confidentiality, intesa nei due aspetti che la caratterizzano, quelli della **privacy** e della **secrecy**, coglie questo aspetto della computer security. Il termine privacy va distinto da quello di secrecy: mentre il primo si riferisce principalmente alla protezione dei dati personali, il secondo, invece, riguarda invece la protezione dei dati posseduti da un'organizzazione, e nello specifico da un ente, struttura sanitaria o Ministero della Salute.[5] La riservatezza rappresenta certamente un punto di riferimento nell'ambito della sicurezza dei dati personali: si cerca di impedire che soggetti non autorizzati accedano alle informazioni. Sicurezza e protezione dei dati, pertanto, si intersecano: soltanto un sistema in grado di garantire il rispetto della seconda riuscirà a fornire uno strumento sicuro ai fruitori del nuovo servizio informatico.

Dal FSE, nel quale confluisce la storia clinica di una persona, generata da più strutture sanitarie, va tenuto distinto il **dossier sanitario elettronico**. Quest'ultimo è composto da un insieme di informazioni predisposto presso un'unica struttura sanitaria (ospedale, azienda sanitaria, casa di cura) che raccoglie informazioni sulla salute di un paziente per documentarne la storia clinica presso quella singola struttura e offrirgli un migliore processo di cura. Del dossier sanitario elettronico, con provvedimento 4 giugno 2015, il Garante per la protezione dei dati personali ha varato Linee guida, con lo scopo di definire un quadro di riferimento unitario per il corretto trattamento dei dati ivi raccolti.

Nell'ambito più generale, con riferimento alla nozione di salute, occorre precisare che essa comprende sia quella fisica sia quella mentale.[6] Lo sviluppo tecnologico ha fornito al professionista medico strumenti nuovi per rendere sempre più oggettivo ed affidabile il flusso di informazioni che proveniva dal paziente. Con riguardo allo stato passato, presente e futuro del paziente, verranno inserite altresì valutazioni prognostiche, come ulteriore oggetto di informazione e valutazione.[7]

Il considerando 35 elenca una serie di tipologie di informazioni che a vario titolo forniscono elementi conoscitivi collegati con la salute dell'interessato.

Volume consigliato

Dallo stesso si evince che anche identificativi personali utilizzati a fini sanitari, quali un codice o un simbolo, sono considerati dati sanitari. [8]

Diritto & Diritti ISSN 1127-8579

Inoltre, sono anche **dati sanitari** tutte "le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro".

Per "**dati sensibili''** si intende qualunque informazione, relativa alla persona, in grado di rivelare l'origine etnica, le opinioni politiche, dati relativi a condanne penali, come anche dati genetici e lo stato di salute: i dati in esame non potranno essere deliberatamente diffusi ma, con il consenso dell'interessato, si potrà procedere al trattamento dei dati.

In tale cornice, il "**consenso**" si pone come qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Ne deriva che il consenso debba essere:

-**informato**, preceduto da informativa;

-**libero**, senza condizionamenti o vincoli;

-**specifico**, un consenso per ogni finalità;

-**inequivocabile**, deve esservi certezza che l'interessato l'abbia prestato.

Come enunciato dal considerando 32, il consenso prestato dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano. Ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara e concisa.

Diritto & Diritti ISSN 1127-8579

Trattamento dei dati in ambito sanitario

Con il sopracitato concetto di “trattamento” (processing) ci si riferisce a qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, la strutturazione, etc.[9]

Pertanto, qualsiasi attività svolta in funzione e gestione dei dati personali, anche di tipo non trasformativo, quale ad esempio un mero accesso, può essere oggetto di trattamento. Affinché un trattamento possa essere definito “lecito”i dati personali devono essere trattati nel rispetto dei principi di cui all'art. 5 del Registro Generale sulla Protezione dei Dati (RGPD) e di “**data protection-by-design**” (con gli obiettivi principali di protezione dei dati e protezione degli utenti). Tuttavia, occorre precisare che l'art. 23 del nuovo Regolamento introduce delle limitazioni all'applicazione dei suddetti principi, demandando proprio agli Stati membri e all'Unione la possibilità di gestire le relative limitazioni laddove vengano emanate norme funzionali all'adozione di misure necessarie per salvaguardare diversi interessi, tra cui: la tutela dell'interessato, i diritti e le libertà altrui; la sicurezza pubblica e nazionale; la prevenzione ed altri obiettivi di interesse pubblico generale come la sanità pubblica o la sicurezza sociale.

Infatti al considerando 39 viene evidenziato come qualsiasi trattamento di dati personali dovrebbe essere lecito e corretto. Dovrebbero essere trasparenti, in favore dei soggetti, le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. In questo modo i soggetti avranno il diritto di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano. È opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento. In particolare, le finalità del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta. I dati personali dovrebbero essere pertinenti e limitati a quanto necessario per le finalità del loro trattamento.

Per quanto riguarda il diritto di limitazione del trattamento, occorre ricordare 4 casi di deroga, previsti dall'art. 18 del nuovo Regolamento: 1) consenso dell'interessato; 2) esercizio giudiziale di un diritto; 3) tutela dei diritti di un terzo, persona fisica o giuridica; 4) motivi di interesse pubblico rilevante. Nelle suddette ipotesi è perciò possibile trattare i dati nonostante questi siano stati sottoposti a limitazione[10] L'istituto della limitazione può subire ulteriori deroghe in virtù dell'art. 23 e del considerando 73. L'elenco comprende: sicurezza nazionale, difesa, pubblica sicurezza, protezione sociale, tutela della vita umana. Pertanto, per quel che concerne più specificamente la disciplina relativa ai trattamenti in ambito sanitario, volta a realizzare un bilanciamento tra protezione dei dati personali e sicurezza collettiva, essa è particolarmente favorevole alla tutela del singolo ma subisce delle restrizioni allorquando vengano in

Diritto & Diritti ISSN 1127-8579

rilievo esigenze di protezione o tutela della collettività.

Al considerando 46 viene previsto come il trattamento di dati personali debba essere altresì considerato lecito quando è necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica. Il trattamento di dati personali fondato sull'interesse vitale di un'altra persona fisica dovrebbe avere luogo in principio unicamente quando il trattamento non può essere manifestamente fondato su un'altra base giuridica. Alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana.

Ancora, nel considerando 52 la deroga al divieto di trattare categorie particolari di dati personali dovrebbe essere consentita anche quando è prevista dal diritto dell'Unione o degli Stati membri, fatte salve adeguate garanzie, per proteggere i dati personali e altri diritti fondamentali, laddove ciò avvenga nell'interesse pubblico; in particolare il trattamento dei dati personali nel settore del diritto del lavoro e della protezione sociale, comprese le pensioni, e per finalità di sicurezza sanitaria, controllo e allerta, la prevenzione o il controllo di malattie trasmissibili e altre minacce gravi alla salute. Tale deroga può avere luogoper finalità inerenti la salute, compresa la sanità pubblica e la gestione dei servizi di assistenza sanitaria.

Il trattamento di categorie particolari di dati personali può essere necessario per motivi di interesse pubblico nei settori della sanità pubblica, senza il consenso dell'interessato, quanto previsto dal considerando 54.

Dalla lettura del considerando 111, emerge come ci sia la possibilità di trasferire dati a carattere sanitario in determinate circostanze. L'interessato deve aver esplicitamente prestato il suo consenso invece, se il trasferimento è occasionale, si rende necessario un contratto o un'azione legale. I dati possono essere trasferiti soltanto se i soggetti interessati lo richiedano o ne siano destinatari, naturalmente salvaguardando la tutela degli interessi fondamentali e inviolabili della persona. Tali deroghe devono in particolare valere per il trasferimento di dati richiesti e necessari per importanti motivi di interesse pubblico, ad esempio nel caso di scambio internazionale di dati tra autorità sanitarie locali (e non) e servizi competenti in materia di sicurezza sociale e sanità pubblica: ad esempio in caso di ricerca di contatti per malattie contagiose o al fine di ridurre e/o eliminare il doping nello sport. Il trasferimento di dati personali dovrebbe altresì essere considerato lecito quando è necessario per salvaguardare interessi vitali dell'interessato o di altra persona, comprese la vita o l'integrità fisica, qualora l'interessato si trovi nell'incapacità di prestare il proprio consenso.

Infine, i cittadini hanno il diritto di essere avvertiti dalle pubbliche amministrazioni e dalle imprese delle violazioni dei loro dati personali (**data breach notification**) entro le 72 ore, obbligo previsto allo stato attuale soltanto in alcuni settori (fascicolo e dossier sanitario, settore bancario).

Diritto & Diritti ISSN 1127-8579

Conclusione

Sono immediatamente percepibili gli aspetti di sicuro vantaggio connessi alla possibilità di predisporre un sistema che garantisca ai soggetti che ne beneficiano la facoltà di delegare ad altri l'accesso al proprio FSE. Per altro verso, assumere che la salute dell'interessato, in possesso di capacità d'agire, possa essere oggetto di delega apparirebbe un concreto vulnus al suo diritto di autodeterminazione, realizzato tramite un'irragionevole ingerenza nella sfera dell'interessato stesso.

Nel contesto cartaceo la delega attiene al ritiro di un documento determinato contenente dati sanitari; diversamente, l'atto che abilita un soggetto a fare le veci dell'interessato delegante all'interno di un sistema di archiviazione e gestione in remoto dei dati inerenti la propria salute assumerebbe carattere generale, aumentando esponenzialmente i rischi connessi a possibili trattamenti illeciti dei dati sanitari. Occorre inoltre riflettere attentamente sull'esistenza di una serie di accorgimenti e di regole tecnologiche, nell'ottica di una gestione dei rischi, che permettano di evitare di optare per soluzioni regolative che finirebbero soltanto per rendere alquanto complesso e poco fruibile il meccanismo di delega.

E'opportuno qui sottolineare una pratica emersa negli utimi mesi (con riferimento a situazioni concrete: in Italia, in Belgio, in Spagna, ecc), che ha visto cittadini europei riconoscere un caro o se stessi raffigurati sui pacchetti di sigarette, senza previa autorizzazione e, per di più, per patologie non relative al consumo di tabacco. Allora occorre domandarsi: come si pone la Commissione europea di fronte a queste ingerenze nella privacy dei soggetti?

La soluzione del contrasto tra tutela del diritto alla privacy dell'utente e interesse superindividuale alla salute si pone come l'obiettivo teorico-pratico da raggiungere per coloro che si trovano chiamati, nei vari ambiti di competenza, a garantire che l'evoluzione di questo processo di digitalizzazione avvenga nel rispetto di regole e principi. Una loro corretta convergenza è in grado di assicurare i vantaggi che il fenomeno della digitalizzazione permette nel concreto di realizzare.

Volume consigliato

Note

[1]Sul tema della telemedicina, v. L. SARTORI, La tutela della salute pubblica nell'Unione europea, Cittadella, 2009, 116-121; U. IZZO, Medicina e diritto nell'era digitale: i problemi giuridici della cibermedicina, in Danno e resp. 2000, 807; A. SINHA, An Overview of Telemedicine: The Virtual Gaze of Health Care in the Next Century, in Medical Anthropology Quarterly, New Series, vol. 14, n. 3 (Sep. 2000), 291-309.

Diritto & Diritti ISSN 1127-8579

[2] Conriferimentoalla disciplina della protezione dei dati personali nel contesto europeo, si v.I.J. LLOYD, Information technology law, V ed., Oxford, 2008, 1 ss.; N. LUGARESI, Protezione della privacy e protezione dei dati personali: i limiti dell'approccio comunitario, in Giust. amm., 2004, 289; R. PARDOLESI, Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità, in R. PARDOLESI (a cura di), Diritto alla riservatezza e circolazione dei dati personali, Milano, 2003, 1-57; L.A. BYGRAVE, Data Protection Law. Approaching Its Rationale, Logic and Limits, The Hague – London - New York, 2002; P. PALLARO, Libertà della persona e trattamento dei dati personali nell'Unione europea, Milano, 2002.

[3] Cfr. H.G. GADAMER, Dove si nasconde la salute, Milano, 1994, 135 ss.; J.G. MAZOUÈ, Diagnosis Without Doctors, 15 Med. & Phi. 559 (1990); R.A. MILLER, Why the Standard View is Standard: People, not Machines, Understand Patients' Problems, 15 J. Med., & Phi. 581 (1990).

[4] Cfr. SARTORI, La tutela della salute pubblica nell'Unione europea, cit., 33-49; L. BUCCOLIERO, C. CACCIA, G. NASI, e-he@lth Percorsi di implementazione dei sistemi informativi in sanità, Milano, 2005, 1-3.

[5] BUCCOLIERO, CACCIA, NASI, e-he@lth. Percorsi di implementazione dei sistemi informativi in sanità, cit., 3, dovein nota è riportata un'osservazione di G. EYSENBACH, What is e-health? [editorial], in Journal of Medical Internet Research, vol. 3, n. 2, 2001, e(20): «[…] the term characterizes not only a technical development, but also a state-of-mind, a way of thinking, an attitude, and a commitment for networked, global thinking, to improve health care […]».

[6] Considerando 35 del nuovo Regolamento privacy 679/16.

[7]Il flusso di informazioni, intese in senso soggettivo (derivanti dal paziente) e oggettivo (derivanti da indagini strumentali)diviene «esperienza» per la comunità scientifica.

[8]V. IZZO, Medicina e diritto nell'era digitale, cit., 809; v. con specifico riferimento agli Electronic Health Record, saggio di S. HOFFMAN, A. PODGURSKI, EHealth Hazards: Provider Liability and Electronic Health Record Systems, 24 Berkeley Tech. L.J. 1523 (2009), nelle cui conclusioni si legge: «EHR systems cannot remain unregulated and largely unscrutinized. Only with appropriate interventions will they become a blessing rather than a curse for health care professionals and patients».

[9]In riferimento al trattamento dei dati inerenti lo stato di salute nel sistema giuridico italiano, v. per approfondimenti G. FINOCCHIARO, Il trattamento dei dati sanitari: alcune riflessioni critiche a dieci anni dall'entrata in vigore del Codice in materia di protezione dei dati personali, in G.F. FERRARI (a cura di), La legge sulla privacy dieci anni dopo, Milano, 207-220; S. VICIANI, Brevi osservazioni sul trattamento dei dati inerenti la salute e la vita sessuale in ambito sanitario, in Riv. crit. dir. priv., 315; F. CAGGIA, Il trattamento dei dati sulla salute, con riferimento all'ambito sanitario, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), Il codice del trattamento dei dati personali, Torino, 2007, 405; S. CORONATO, La

Diritto & Diritti ISSN 1127-8579

tutela della privacy in ospedale, in Ragiusan, 2006, fasc. 265/266, 6; P. DE CAMELIS, Privacy e potere informatico – Cenni al trattamento dei dati inerenti la salute, in Rass. amm. sanità, 1998, 4; A. CIATTI, La protezione dei dati idonei a rivelare lo stato di salute nella legge n. 675/1996, in Contratto e impr./Europa, 1998, 368.

[10] L.BOLOGNINI, C. BISTOLFI, E. PELINO, Il Regolamento Privacy europeo, Giuffrè ed., 2016, pp. 65-101.

https://www.diritto.it/i-tanti-volti-della-e-health/

Diritto & Diritti ISSN 1127-8579