Politecnico di Milano

Dipartimento di Architettura e Studi Urbani

MASTER UNIVERSITARIO DI II LIVELLO

"DATA PROTECTION OFFICER"

A.A. 2021-2022

La privacy nelle cure domiciliari

Relatore

Avv. Francesca Lonardo

Correlatore

Avv. Gabriele Tori

Tesi Master

Avv. Rossana Trombello

INDICE

I. INTRODUZIONE

1a. Definizione di cure domiciliari ed ambito di applicazione

Il Servizio sanitario nazionale, istituito con Legge n. 833 del 23 dicembre 1978[1], consiste in un sistema di strutture e servizi che hanno lo scopo di garantire a tutti i cittadini, in condizioni di uguaglianza, l'accesso universale all'erogazione equa delle prestazioni sanitarie, in attuazione dell'art. 32 della Costituzione.

Tale sistema garantisce percorsi assistenziali a domicilio alle persone non autosufficienti, in condizioni di fragilità e con patologie in atto. Tali percorsi sono costituiti dall'insieme organizzato di trattamenti medici, riabilitativi ed infermieristici, necessari a stabilizzare il quadro clinico, limitare il declino funzionale e migliorare la qualità della vita del paziente nel proprio ambiente familiare, evitando, quando possibile, il ricorso al ricovero in ospedale o in una struttura residenziale. Le aziende sanitarie, stando a quanto previsto e stabilito dal D.P.C.M. 12 gennaio 2017[2], sono tenute ad assicurare la continuità tra le fasi di assistenza ospedaliera e quelle di assistenza territoriale a domicilio, ove necessario.

Nell'ambito delle cure domiciliari l'intensità del bisogno clinico, funzionale e sociale del paziente viene accertato attraverso idonei strumenti di valutazione multidimensionale, che consentano la presa in carico del paziente e la definizione del c.d. «*Progetto di assistenza individuale*» (PAI) ovvero del c.d. «*Progetto riabilitativo individuale*» (PRI), che ne definiscono, rispettivamente, i bisogni assistenziali e riabilitativi. In relazione allo stato di salute dell'assistito ed al livello di intensità, complessità e durata dell'intervento assistenziale necessario, poi, l'attività di assistenza domiciliare si articola nei seguenti livelli:

a) cure di livello base, costituite da prestazioni professionali in risposta a bisogni sanitari di bassa complessità, anche ripetuti nel tempo, e di tipo medico, infermieristico e/o riabilitativo;

[1] La Legge n. 833 del 23 dicembre 1978 costituisce un'inversione di tendenza rispetto al passato, in quanto prevede il principio di *universalità* (la tutela della salute come fondamentale diritto dell'individuo ed interesse della collettività), di *globalità* (la promozione, il mantenimento ed il recupero della salute fisica e psichica), di *uguaglianza* (l'erogazione di prestazioni sanitarie a tutta la popolazione senza distinzione di condizioni individuali o sociali).

[2] Il D.P.C.M. 29.11.2001 contiene la prima disciplina dei LEA. I mutamenti intervenuti nel corso del tempo nell'ambito sociale e sanitario hanno, poi, reso necessario un adeguamento alle esigenze della comunità degli assistiti delle prestazioni minime assistenziali erogabili dal SSN, che sono state appunto oggetto di revisione con il D.P.C.M. 12.01.2017, che, in particolare, all'art. 22 disciplina l'attività di cure domiciliari.

b) cure integrate (ADI) di I^ o di II^ livello, costituite da prestazioni professionali prevalentemente di tipo medico, infermieristico e/o riabilitativo a favore di persone che, pur non presentando criticità specifiche o sintomi particolarmente complessi, necessitano di continuità assistenziale e di interventi programmati, che si articolano su cinque (I^ livello) o sei giorni (II^ livello). Quando necessari, sono assicurati anche gli accertamenti diagnostici, nonché la fornitura dei farmaci e dei dispositivi medici;
c) cure integrate (ADI) di III^ livello o ad elevata intensità: costituite da prestazioni professionali di tipo medico, infermieristico e riabilitativo, accertamenti diagnostici, fornitura dei farmaci e dei dispositivi medici, nonché dei preparati per nutrizione artificiale, a favore di persone con patologie che, presentando un elevato livello di complessità, instabilità clinica e sintomi di difficile controllo, richiedono continuità assistenziale ed interventi programmati.

La prestazione di cure domiciliari ha da sempre rivestito un ruolo centrale in ambito sanitario. L'attività di assistenza distrettuale, svolta a livello domiciliare, territoriale, semiresidenziale o residenziale, infatti, già con il D.P.C.M. del 29 novembre 2001, era stata annoverata tra i livelli essenziali di assistenza (LEA) garantiti a tutti i cittadini dal servizio sanitario nazionale. Nel prossimo futuro, inoltre, tale attività acquisirà ancora maggiore importanza. L'emergenza sanitaria legata al diffondersi del Covid-19, infatti, ha messo in evidenza la necessità di dare una nuova organizzazione alla rete sanitaria. In particolare, Regione Lombardia ha approvato la legge regionale n. 22 del 14 dicembre 2021, che, riformando il Titolo I ed il Titolo VII della previgente legge regionale n. 33 del 30 dicembre 2009, prevede, tra l'altro, il rafforzamento dell'assistenza domiciliare.

Da quanto esposto, risulta evidente come in tale ambito gli operatori sanitari vengano inevitabilmente a conoscenza dei dati personali e dei dati relativi alla salute dei pazienti presi in carico. Nella maggior parte dei casi, tali tipologie di dati sono contenuti all'interno della c.d. documentazione sanitaria, che consiste in ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di ogni evento o episodio clinico (documentazione relativa ad un ricovero o intervento chirurgico, esami diagnostici, referti di laboratorio, documentazione di diagnostica per immagini, consenso prestato o negato, informativa privacy datata e firmata)[3]. Tale documentazione, in

[3] A titolo meramente esemplificativo e non esaustivo, può essere considerata documentazione sanitaria, così come descritta, quella relativa ad un ricovero o intervento chirurgico, esami diagnostici, referti di laboratorio, documentazione di diagnostica per immagini, consenso prestato o negato, informativa privacy datata e firmata

alcuni casi risulta essere esistente, in altri, invece, viene prodotta sul campo dallo stesso operatore sanitario. In entrambi i casi, comunque, si tratta di documenti che rimangono in possesso dell'azienda sanitaria di riferimento. Pertanto, la sempre maggiore importanza rivestita dall'attività di cure domiciliari evidenzia l'esigenza di analizzare il rilevante aspetto legato sia al rispetto della normativa in materia di protezione dei dati personali in riferimento alla gestione dei dati personali e sanitari dei pazienti presi in carico, sia ad una corretta gestione della documentazione che li contiene.

II. IL TRATTAMENTO DEI DATI PERSONALI IN AMBITO SANITARIO

2a. La disciplina dal Codice Privacy al Regolamento UE n. 2016/679 ("GDPR")

Il D.lgs. 196/2003 - "*Codice in materia di protezione dei dati personali*", al Titolo V, denominato "*Trattamento di dati personali in ambito sanitario*", prevede una disciplina specifica di settore. Il citato decreto e, in particolare, il suddetto Titolo V sono stati modificati con il D.lgs. 101/2018, emanato al fine di adeguare il Codice Privacy previgente alle nuove disposizioni del GDPR, entrato in vigore il 24 maggio 2016 ed applicabile a decorrere dal 25 maggio 2018.

In particolare, il Codice Privacy previgente annoverava i dati personali relativi alla salute nella categoria dei c.d. dati sensibili, richiamando, così, già allora la necessità di riservare una disciplina specifica a tale tipologia di dati, specie quando trattati nel contesto sanitario. A tal proposito, infatti, il combinato disposto dell'art. 26 comma 1 e dell'art.76, oggi abrogati dal D.lgs. 101/2018, prevedeva, che i dati sanitari potessero essere oggetto di trattamento qualora vi fosse il consenso scritto del soggetto interessato e/o previa autorizzazione da parte dell'Autorità Garante per la Protezione dei dati personali (il "Garante Privacy"). La Corte di Cassazione, inoltre, già durante la vigenza del Codice Privacy ante modifica, con una serie di sentenze aveva affermato il concetto secondo il quale i dati riguardanti la salute ed il sesso degli interessati beneficino di una protezione rafforzata, in quanto "*involgenti la parte più intima della persona nella sua corporeità e nelle sue convinzioni psicologiche più riservate"* e, quindi, in definitiva, "*supersensibili"*[4]. A seguito dell'intervento riformatorio operato dal D.lgs. 101/2018, l'art. 75 del Codice Privacy attualmente prevede che il trattamento dei dati personali svolto per finalità di tutela della salute e dell'incolumità fisica dell'interessato o di terzi o della collettività debba essere effettuato ai sensi dell'articolo 9, paragrafi 2, lettere h) ed i), e 3 del Regolamento UE n. 2016/679, dell'articolo 2-septies del suddetto codice, nonché nel rispetto delle specifiche disposizioni di settore.

Il GDPR, a differenza del Codice Privacy previgente, non prevede una disciplina *ad hoc*, per il trattamento dei dati personali in ambito sanitario, ma contiene solo riferimenti specifici relativi all'applicazione di alcune norme o istituti. Il combinato disposto dell'art. 4 n. 15) e del considerando n. 35 del citato Regolamento UE n. 2016/679 definisce i dati relativi alla

[4] Cass. Civ., sez. VI, sent. 11 gennaio 2016, n. 222; sez. I, sent. 7 ottobre 2014, n. 21107; sez. I, sent. 1 agosto 2013, n. 18443; sent. 8 luglio 2005, n. 14390.

salute come quei dati personali attinenti alla salute fisica o mentale, passata, presente o futura di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute[5]. I dati sanitari vengono considerati una categoria particolare di dati personali e vengono disciplinati dall'art. 9 del GDPR, che riserva loro una tutela maggiore, in virtù del fatto che il loro trattamento potrebbe comportare rischi significativi per i diritti e le libertà fondamentali dell'interessato. In particolare, infatti, il paragrafo 1 del citato art. 9 del GDPR prevede un divieto generale di trattamento, tra gli altri, dei dati relativi alla salute di una persona fisica, a meno che non ricorrano le condizioni di liceità elencate al paragrafo 2.

In ambito sanitario tali circostanze sono riconducibili, in via generale, ai trattamenti necessari "*per motivi di interesse pubblico rilevante, sulla base del diritto dell'Unione o degli Stati membri*" (art. 9, par. 2, lett. g) del Regolamento UE n. 2016/679). A tal proposito, la normativa italiana, con l'art. 2-*sexies* del Codice Privacy novellato, considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono, tra l'altro, i compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario.

Il trattamento dei dati sanitari dell'interessato deve considerarsi lecito anche qualora sia "*necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che preveda misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale*" (art. 9, par. 2, lett. i) e considerando n. 54 del GDPR)[6]. Un'ulteriore condizione di liceità del trattamento di dati sanitari, infine, ricorre qualora sia necessario per il perseguimento delle c.d. finalità di cura, quale è la finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero di gestione dei sistemi e servizi sanitari o sociali (art. 9 par. 2 l. h) del GDPR). Si tratta, cioè, di tutti quei trattamenti essenziali al raggiungimento di una o più finalità determinate ed esplicitamente connesse

[5] Il considerando 35 del GDPR 679/2016 riporta un'elencazione non esaustiva dei dati sanitari ricompresi all'interno della definizione di dato sanitario fornita: "…*informazioni risultanti da esami e controlli effettuati su una parte del corpo o su una sostanza organica, compresi i dati genetici e i campioni biologici; qualsiasi informazione riguardante una malattia, una disabilità, un'anamnesi medica, i trattamenti clinici, lo stato fisiologico o biomedico dell'interessato…".*

[6] A titolo esemplificativo, si può fare riferimento ad emergenze sanitarie conseguenti a sismi e sicurezza alimentare.

alla cura della salute[7]. Al contrario, gli eventuali trattamenti attinenti, *lato sensu*, alla cura, in quanto non strettamente necessari[8], anche se effettuati da professionisti della sanità, richiedono una distinta base giuridica da individuarsi, eventualmente, nel consenso dell'interessato o in un altro presupposto di liceità[9]. Tuttavia, il paragrafo 3 dell'art. 9 del GDPR precisa che il trattamento di categorie particolari di dati personali per finalità di cura è possibile solo qualora venga effettuato da parte o sotto la responsabilità di un professionista soggetto al segreto professionale o da altra persona anch'essa tenuta all'obbligo di segretezza.

Quanto appena esposto, pone in rilievo una delle novità introdotte dal GDPR, rispetto a quanto previsto dal Codice Privacy previgente. Infatti, un professionista sanitario, indipendentemente dalla circostanza che operi in qualità di libero professionista ovvero all'interno di una struttura sanitaria pubblica o privata in qualità di dipendente subordinato[10], può trattare i dati sanitari dei pazienti anche senza il loro consenso esplicito, purché tale trattamento sia necessario alla prestazione sanitaria richiesta dall'interessato stesso[11].

Il GDPR, infine, con il combinato disposto del considerando n. 10 e dell'art. 9 par. 4, lascia un ampio margine di manovra ai singoli Stati membri, che, tramite l'emanazione di normative interne, possono precisare le disposizioni del regolamento stesso, anche con riguardo al trattamento di categorie particolari di dati personali. Tali Paesi possono, ad esempio, determinare con maggiore precisione le condizioni al verificarsi delle quali il trattamento debba considerarsi lecito oppure possono introdurre ulteriori limitazioni allo stesso. Pertanto, in attuazione di tale autonomia conferita agli Stati membri, la normativa italiana, in particolare con l'art. 2-*septies* del Codice Privacy novellato, ha previsto che i dati genetici, biometrici e relativi alla salute possano essere oggetto di trattamento, oltre che in presenza di una delle condizioni di cui all'art. 9 par. 2 del GDPR, anche in conformità alle

[7] *Cfr.* considerando n. 53 del GDPR.
[8] A titolo esemplificativo, il Garante della Privacy nei "*Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario"* (7 marzo 2019) vi fa rientrare i trattamenti connessi all'utilizzo di app mediche (*cfr*. Faq CNIL del 17 agosto 2018 sulle applicazioni mobili in sanità), trattamenti preordinati alla fidelizzazione della clientela effettuati dalle farmacie attraverso programmi di accumulo puti al fine di fruire di servizi o prestazioni accessorie, trattamenti effettuati in campo sanitario da persone giuridiche private per finalità commerciali o elettorali (*cfr*. provv. Garante Privacy del 6 marzo 2014, doc. web n. 3013267).
[9] *Cfr.* artt. 6 e 9, par. 2, GDPR 679/2016.
[10] Ci si rifà alla nozione comunitaria di professionista o esercente la professione sanitaria, ripresa anche ne "*Codice privacy: tutte le novità del D.lgs. 101/2018*" di L. Bolognini, E. Pellino – Il Civilista – Giuffrè Francis Lefebvre S.P.A, 2019.
[11] Tale novità viene sottolineata anche dal Garante nei "*Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*" (7 marzo 2019);

misure di garanzia, disposte dall'Autorità Garante per la protezione dei dati personali con provvedimento biennale. Tali misure possono individuare ulteriori condizioni al verificarsi delle quali il trattamento delle succitate categorie di dati sia consentito, quali, ad esempio, il ricorso a tecniche di cifratura, di pseudonimizzazione, di minimizzazione oppure a modalità di accesso selettivo alle informazioni. Ai sensi dell'art. 2-*septies* c. 6 del Codice Privacy novellato, le citate misure di garanzia sono adottate sentito il Ministro della salute che, a tal fine, acquisisce anche il parere del Consiglio superiore di sanità.

In ambito sanitario, in particolare, le misure di garanzia possono riguardare anche cautele da adottare relativamente a profili organizzativi e gestionali, come esplicitamente previsto dall'art. 2-*septies* c. 4 del Codice Privacy novellato. Il comma 8 del medesimo articolo, poi, prevede una misura di garanzia di estrema importanza, vietando che i dati personali genetici, biometrici e quelli relativi alla salute possano essere diffusi, ovvero resi disponibili a soggetti indeterminati. Al contrario, tali tipologie di dati possono essere comunicati a destinatari determinati. Questi ultimi, ai sensi dell'art. 9 del Regolamento UE 2016/679 e dell'art. 83 del Codice Privacy in combinato disposto con l'art. 22 c. 11 del D.lgs. 101/2018, possono essere sicuramente il paziente, ma anche terzi[12], purché a ciò legittimati sulla base di un idoneo presupposto giuridico[13] o previa delega scritta dell'interessato[14]. I termini "diffondere" e "comunicare", spesso, nel linguaggio quotidiano vengono utilizzati in modo intercambiabile, ma, in realtà, si differenziano rispetto, appunto, alle caratteristiche dei destinatari finali. La violazione del divieto di diffusione dei dati personali relativi alla salute, comunque, è soggetta ad una sanzione amministrativa fino a € 20.000.000,00, ai sensi del combinato disposto degli artt. 166 e 83, par. 5, del Regolamento UE 2016/679.

I dati relativi alla salute, oltre che comunicati, possono essere anche trasmessi a soggetti determinati, purché il trasferimento avvenga in forma cifrata[15]. In particolare, ad esempio, in caso di trasmissione dei dati tra *server* del titolare del trattamento e *client* dell'interessato, è stato specificato che questa debba avvenire "*attraverso protocolli di comunicazione sicuri,*

[12] *cfr*. Provv. dell'Autorità Garante per la Protezione dei dati personali del 15 aprile 2021e Provv. generale del 9 novembre 2005.
[13] A titolo esemplificativo, sono legittimati a conoscere i dati sanitari i dipendenti della cassa di assistenza sanitaria integrativa cui eventualmente il paziente si sia iscritto al fine di ottenere il rimborso di alcune prestazioni. In questo caso, la base giuridica che legittima una siffatta comunicazione è costituita dal contratto che il paziente ha firmato per aderire a tale servizio.
[14] Come avviene, ad esempio, per il ritiro di referti diagnostici o di certificazioni rilasciate da laboratori di analisi o da altri organismi sanitari, che può essere effettuato anche da persone diverse dai diretti interessati, purché, appunto, sulla base di una delega scritta e mediante la consegna delle stesse in busta chiusa.
[15] *Cfr*. Allegato B "*Disciplinare tecnico in materia di misure minime di sicurezza*" del Codice Privacy novellato.

basati sull'utilizzo di standard crittografici per la comunicazione elettronica dei dati, con la certificazione digitale dell'identità dei sistemi che erogano il servizio in rete (protocolli https ssl – Secure Socket Layer)". Ugualmente, l'Autorità Garante per la Protezione dei dati personali nelle "*Linee guida su referto online*" del 25 giugno 2009, ai fini della trasmissione come allegati di documenti contenenti dati sanitari, ha richiesto l'utilizzo di password o di chiavi crittografiche per l'apertura del file. In tal caso è, inoltre, necessario individuare con sicurezza il destinatario della comunicazione, procedendo, ad esempio, alla convalida degli indirizzi e-mail tramite apposita procedura di verifica on-line.

2b. L'informativa privacy in ambito sanitario

Il principio di trasparenza, previsto dall'art. 5, par. 1, lett. a) del Regolamento UE n. 2016/679, impone al titolare del trattamento di informare l'interessato sui principali elementi del trattamento, al fine di renderlo consapevole in merito alle principali caratteristiche dello stesso. In particolare, il suddetto regolamento esplicita il contenuto dell'informativa da somministrare all'interessato, elencandone gli elementi essenziali sia nei casi in cui i dati oggetto di trattamento siano stati raccolti presso l'interessato (art.13) sia nei casi in cui i dati siano stati raccolti presso terzi (art.14). Al riguardo, si sottolinea come il Regolamento UE n. 2016/679 non abbia completamente stravolto l'impianto dell'art. 13 del Codice Privacy previgente, ma abbia solamente introdotto alcuni elementi di novità[16].

In ambito sanitario, del quale qui si discorre, generalmente viene predisposta un'informativa ai sensi del citato art. 13, in quanto i dati vengono per lo più raccolti presso l'interessato. Pertanto, un'azienda sanitaria, in qualità di titolare del trattamento, per il tramite dei propri dipendenti, deve fornire al paziente le seguenti informazioni:

a) l'identità ed i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
c) le finalità del trattamento cui sono destinati i dati personali, nonché la base giuridica del trattamento;

[16] Le novità a cui si fa riferimento sono l'indicazione dei dati del DPO, in quanto figura introdotta proprio con il GDPR, le finalità del trattamento nonché la base giuridica, l'indicazione del periodo di conservazione dei dati o dei criteri utilizzati per determinarlo, il diritto di proporre reclamo e l'eventuale esistenza un processo decisionale automatizzato.

d) il legittimo interesse del titolare o di terzi, qualora il trattamento sia necessario per il perseguimento dello stesso, ai sensi dell'art. 6, par. 1, lett. f);
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'art. 46 o 47, o all'art. 49, par. 1, c. 2, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili;
g) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
h) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi allo stesso, oltre al diritto alla portabilità dei dati;
i) qualora il trattamento sia basato sull'articolo 6, par. 1, lett. a), oppure sull'art. 9, par. 2, lett. a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
j) il diritto di proporre reclamo ad un'autorità di controllo;
k) se la comunicazione di dati personali sia un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato abbia l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
l) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22, par.1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Ai sensi dell'art. 12 GDPR ed alla luce del principio di responsabilizzazione di cui al citato art. 5, spetta al titolare del trattamento scegliere le modalità di somministrazione dell'informativa ritenute più appropriate al caso di specie, tenendo conto di tutte le circostanze del trattamento e del contesto in cui viene effettuato. Deve, comunque, essere utilizzata una forma concisa, trasparente, intelligibile, facilmente accessibile e si deve fare

riscorso ad un linguaggio semplice e chiaro[17]. Le informazioni rese, inoltre, devono essere concrete, precise e non devono essere utilizzate espressioni astratte, termini ambigui o in grado di lasciare spazio a differenti interpretazioni. L'informativa, infine, può essere fornita in forma scritta o con altri mezzi[18], anche di tipo elettronico[19] se del caso.

L'art. 13 GDPR prevede, come regola generale, che le informazioni debbano essere rese note nel momento in cui i dati personali sono ottenuti e, quindi, prima del trattamento. L'art. 82 del Codice Privacy novellato, invece, prevede alcune eccezioni. L'informativa, infatti, può essere rese senza ritardo, successivamente alla prestazione, nel caso di emergenza sanitaria o di igiene pubblica, per la quale la competente autorità ha adottato un'ordinanza contingibile ed urgente, ai sensi dell'art. 117 del decreto legislativo 31 marzo 1998, n. 112. Un tale indugio viene tollerato anche in presenza delle seguenti circostanze:

a) impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, quando non è possibile rendere le informazioni, nei casi previsti, a chi esercita legalmente la rappresentanza, ovvero a un prossimo congiunto, a un familiare, a un convivente o unito civilmente ovvero a un fiduciario ai sensi dell'art. 4 della legge 22 dicembre 2017, n. 219 o, in loro assenza, al responsabile della struttura presso cui dimora l'interessato;
b) rischio grave, imminente ed irreparabile per la salute o dell'interessato;
c) rischio che la prestazione medica possa venire pregiudicata, in termini di tempestività o efficacia, dal preventivo rilascio dell'informativa.

Con specifico riferimento all'attività posta in essere da titolari del trattamento operanti in ambito sanitario e che effettuano una pluralità di operazioni connotate da particolare complessità (es. aziende sanitarie), l'Autorità Garante per la Protezione dei dati personali ha ritenuto opportuno "*suggerire di fornire all'interessato le informazioni previste dal Regolamento in modo progressivo"*[20]. Ciò significa che, nei confronti della generalità dei pazienti che si interfacciano ad una struttura sanitaria, potrebbero essere fornite solo le informazioni relative ai trattamenti che rientrano nell'ordinaria attività di erogazione delle

[17] Il WP29, nelle "*Linee guida sulla trasparenza ai sensi del Regolamento*", WP260 rev 01, fatte proprie dal Comitato europeo per la protezione dei dati, aveva già precisato che le informazioni dovrebbero essere fornite agli interessati nella maniera più semplice possibile, evitando complesse strutture sintattiche e linguistiche.
[18] L'art. 12 GDPR precisa che l'informativa, su richiesta dell'interessato, può essere fornita anche oralmente, purché venga comprovata con altri mezzi l'identità dell'interessato.
[19] Principio espresso anche dal considerando n. 58 del GDPR.
[20] *Cfr.* "*Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario"* – Autorità Garante per la Protezione dei dati personali - 7 marzo 2019.

prestazioni sanitarie. Gli elementi informativi relativi a particolari attività di trattamento (es. fornitura di presidi sanitari, modalità di consegna dei referti medici *on-line*, finalità di ricerca), invece, potrebbero essere resi in un secondo momento, solo ai pazienti effettivamente interessati da tali servizi ed ulteriori trattamenti. Il vantaggio di un'informativa progressiva, così come descritta, consiste sicuramente in una maggiore attenzione prestata dall'interessato alle informazioni veramente rilevanti, fornendo la piena consapevolezza circa gli aspetti più significativi del trattamento e senza costringere a visualizzare le molteplici categorie di informazioni in una sola volta[21].

Non sussiste, infine, un obbligo normativo di firmare in calce l'informativa. Tuttavia, in termini di *accountability*[22], è opportuno che il titolare del trattamento sia in grado di dimostrare che, al momento della raccolta dei dati o al loro primo utilizzo, se raccolti presso terzi, l'informativa sia stata presentata all'interessato. È, pertanto, consigliabile far firmare l'informativa privacy all'interessato, così da collezionarne la presa visione della stessa.[23]

[21] Anche il WP29, nelle "*Linee guida sulla trasparenza ai sensi del Regolamento*" WP260 rev 01, aveva raccomandato l'utilizzo di un'informativa a strati, in particolare nel contesto digitale, precisando che consente di soddisfare sia il requisito della completezza sia quello della comprensibilità, permettendo agli utenti di accedere direttamente alle sezioni dell'informativa che vogliono approfondire.

[22] Il regolamento pone con forza l'accento sulla "*responsabilizzazione"* (*accountability* nell'accezione inglese) di titolari *(si vedano artt. 23-25, in particolare, e l'intero Capo IV del regolamento)*. Si tratta di un elemento di novità per la protezione dei dati, in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento. Il titolare deve, però, essere in grado di dimostrare di aver concretamente posto in essere misure finalizzate ad assicurare l'applicazione del regolamento.

[23] "*GDPR, l'informativa privacy: a cosa serve e come farla*" – P. Calvi – *Network Digital 360* – 24 marzo 2020.

III. LA GESTIONE DELLA DOCUMENTAZIONE SANITARIA RELATIVA ALLE CURE DOMICILIARI

Costituisce documentazione sanitaria qualsiasi rappresentazione che testimonia gli eventi clinici e le attività che si verificano durante i processi di assistenza[24]. Tale documentazione viene prodotta e, successivamente, detenuta da una struttura sanitaria, per il tramite dei suoi operatori nello svolgimento di un'attività di pubblico interesse che è, appunto, la tutela della salute, ai sensi dell'art. 32 della Costituzione. A titolo esemplificativo, rientra all'interno della definizione appena delineata la documentazione relativa ad un ricovero o ad un intervento chirurgico, esami diagnostici, referti di laboratorio, documentazione di diagnostica per immagini.

La documentazione sanitaria costituisce un bene di straordinaria importanza, innanzitutto, sul piano clinico, scientifico e didattico. Se, infatti, vi sono riportati dati aggiornati e puntuali, questa contribuisce ad integrare ed a dare conoscenza alle decisioni dei molteplici attori coinvolti nei processi di assistenza, accrescendo conseguentemente la sicurezza del paziente. In secondo luogo, però, tale documentazione ha un valore anche giuridico, sia per il cittadino che se ne può servire per far valere i propri diritti, sia per la tutela degli operatori professionali in caso di vertenza.

La possibilità di giustificare, dimostrare, controllare, conservare e ritrovare ha fatto crescere in ogni ambito sociale l'esigenza di "lasciare traccia" di ciò che viene fatto. Ne deriva che una corretta gestione della documentazione sanitaria, dalla fase della sua produzione sino alla sua conservazione, riveste un ruolo di estrema importanza.

3a. Modalità e strumenti di acquisizione: le criticità legate all'utilizzo delle nuove tecnologie

L'emergenza legata alla diffusione del Covid-19 ha sicuramente portato ad un'accelerazione della digitalizzazione del Sistema sanitario nazionale. L'impiego delle nuove tecnologie anche in tale ambito, infatti, ha permesso di non interrompere l'erogazione delle prestazioni sanitarie nemmeno in quest'occasione. Il facile impiego e l'immediata disponibilità di strumenti multimediali, inoltre, ha reso possibile l'acquisizione, nel corso

[24] Definizione riportata anche dal "*Manuale della documentazione sanitaria e sociosanitaria*", approvato dalla Giunta di Regione Lombardia con DGR n. IX/ 4659 del 9 settembre 2013.

della pratica clinica, di una copiosa messe di immagini, registrazioni audio e biosegnali, di agevole condivisione anche con diversi professionisti sanitari.

Tuttavia, al giorno d'oggi, seppur le nuove tecnologie abbiano sicuramente aperto straordinarie possibilità operative, nello stesso tempo hanno sollevato problematiche nuove e non ancora del tutto esplorate, in particolare per quanto riguarda l'accesso alle informazioni, la protezione dei dati personali, nonché la classificazione, la conservazione ed i tempi di scarto delle differenti tipologie di documenti. In virtù di tali problematiche, spesso gli operatori sanitari, in particolare nell'ambito dello svolgimento delle cure domiciliari, si trovano davanti a fatti clinici degni di documentazione, senza, però, avere a disposizione strumenti che permettano loro di farlo tutelando, allo stesso tempo, in modo corretto i dati così registrati.

La normativa europea non esplicita quali siano gli strumenti ritenuti idonei ad effettuare un trattamento dei dati, ma demanda al titolare la loro individuazione. Il Regolamento UE n. 2016/679, all'art. 4, par. 1, n. 7), infatti, definisce il titolare del trattamento dei dati come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità ed i *mezzi* di tale trattamento. La scelta di tali strumenti deve, comunque, avvenire nel rispetto dei principi espressi dall'art. 5, par. 1, del GDPR. Il trattamento attuato con i mezzi scelti dal titolare, infatti, deve essere improntato al principio di:

a) liceità, correttezza e trasparenza nei confronti dell'interessato;
b) "*limitazione della finalità*", in quanto i dati devono essere raccolti per finalità determinate, esplicite e legittime e, successivamente, trattati in modo che non sia incompatibile con tali finalità;
c) "*minimizzazione dei dati*", in quanto devono essere trattati solamente i dati adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità;
d) esattezza, in quanto i dati devono essere esatti rispetto alle finalità e, se necessario, aggiornati[25];

[25] L'aggiornamento, in particolare, è di estrema importanza in ambito sanitario. I dati relativi alla salute, infatti, devono essere attuali e costantemente monitorati al fine, ad esempio, di identificare la corretta terapia da somministrare. Laddove, infatti, in sede diagnostica vengano utilizzati dati inesatti, le probabilità di errore aumentano notevolmente, esponendo il paziente a pericoli considerevoli.

e) "*limitazione della conservazione*", in quanto i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
f) integrità e riservatezza, in quanto il trattamento deve garantire un'adeguata sicurezza dei dati personali, compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale, mediante idonee misure tecniche ed organizzative.

In ambito ospedaliero, il titolare del trattamento dei dati è l'azienda sanitaria che, in quanto persona giuridica, lo pone in essere per il tramite dei suoi dipendenti. È, pertanto, al suddetto ente che spetta identificare gli strumenti idonei al trattamento dei dati personali. A tal proposito, la Regione Lombardia, ad esempio, riconoscendo il grande valore aggiunto delle nuove tecnologie anche in ambito sanitario ed in particolare nello svolgimento dell'attività di cure domiciliari, ha approvato alcune linee guida volte ad indirizzare correttamente l'operato sanitario alle prese con strumenti multimediali[26]. Così, al fine di effettuare la registrazione di un fatto clinico, Regione Lombardia suggerisce di utilizzare esclusivamente strumenti messi a disposizione dall'organizzazione sanitaria di riferimento. Ogni registrazione, poi, deve riportare, nel limite del possibile, le seguenti informazioni:

a) gli elementi identificativi dell'organizzazione sanitaria;
b) i dati che permettano l'identificazione certa dell'interessato. In luogo delle generalità complete, può essere sufficiente indicare il numero di ricovero oppure di contatto, se si tratta di altro regime assistenziale, purché univoco, facendo ricorso, quindi, ad una tecnica di pseudonimizzazione[27];
c) l'articolazione organizzativa e/o il professionista sanitario che l'ha disposta;
d) la data e l'ora di formazione.

L'azienda, inoltre, nel mettere a disposizione tali strumenti dovrà attenersi al principio di protezione per impostazione predefinita (c.d. "*privacy by default*"), ai sensi dell'art. 25, par. 2, del Regolamento UE n. 2016/679. Il titolare del trattamento dei dati, tenendo conto

[26] "*Immagini, suoni e biosegnali – Manuale per i percorsi di cura*", approvato con DGR n. X/3001 del 9 gennaio 2015; "*Le registrazioni dei pazienti. Audio e video effettuati in occasione di contatti con personale o strutture della sanità e apporti informativi direttamente",* approvato con DGR n. X/5765 del 8 novembre 2016.
[27] L'art. 4 del Regolamento UE n. 2016/679 definisce la pseudonimizzazione come "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche ed organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile".

dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto, delle finalità e dei rischi per i diritti e le libertà delle persone fisiche, dovrà dotare gli strumenti aziendali di misure tecniche adeguate a garantire che, per impostazione predefinita, siano oggetto di trattamento solo i dati personali necessari per ogni specifica finalità dello stesso.

In mancanza della disponibilità di *devices* aziendali, Regione Lombardia ha previsto la possibilità di ricorrere a strumenti specificamente autorizzati. Nell'ambito delle cure domiciliari, ad esempio, agli operatori sanitari potrebbe essere concesso di utilizzare i cellulari personali, di cui generalmente si ha la disponibilità in qualsiasi momento e luogo. In tale ipotesi l'azienda, al fine di tutelarsi da qualsivoglia responsabilità, potrebbe far sottoscrivere ai singoli dipendenti un'appendice al codice di comportamento che riguardi proprio il corretto utilizzo del cellulare personale per finalità lavorative. L'Azienda potrebbe, inoltre, imporre ai propri dipendenti l'osservanza di una serie di cautele, quale l'utilizzo di programmi o app specificamente indicate, in quanto dotate di misure adeguate al rispetto del succitato principio di *privacy by default*. Può essere anche imposto l'obbligo di scaricare, non appena possibile, la registrazione dal proprio device su un computer aziendale, rinominando il file, ad esempio, con il codice assegnato a ciascun paziente al momento della sua presa in carico. In questo modo, infatti, il documento verrebbe nel più breve tempo possibile trasferito all'interno di uno strumento aziendale, che come tale, deve essere dotato, già di per sé, delle suddette impostazioni predefinite per il trattamento dei dati personali nonché di programmi per la *cybersecurity*[28].

L'operatore sanitario, in particolare nell'ambito delle cure domiciliari, può dover fare ricorso all'utilizzo di strumenti tecnologici quando, recandosi presso il paziente al fine di attuare una terapia per un determinato problema di salute, si ritrovi davanti ad un fatto clinico che potrebbe rivelare l'insorgenza di un'altra patologia, rispetto alla quale, però, vi sia la necessità di interpellare un altro specialista che non sia lì presente in quel momento. Qualora l'urgenza della situazione dovesse sembrare tale da non poter attendere che il professionista competente si rechi personalmente presso il domicilio del paziente in questione, al fine di ottenere una diagnosi ed intraprendere un percorso di cure, l'operatore sanitario presente

[28] È nota oggigiorno l'importanza della c.d. sicurezza informatica aziendale, che consiste nell'insieme di analisi, software, tecniche e prevenzioni messe in campo da un'azienda di qualsiasi tipo ed ambito per evitare che un attore malevolo sia in grado di bucare gli *asset* digitali della propria impresa, comportando una violazione dei dati personali (c.d. "*data breach*") contenuti all'interno del dispositivo preso di mira. Gli attacchi cibernetici sono diretti sempre più spesso a sistemi informativi sanitari.

potrebbe accelerare le tempistiche, ad esempio, scattando una fotografia con il cellulare aziendale o, in mancanza, con il cellulare personale, qualora autorizzato. Tale riproduzione, che non deve in alcun modo rendere identificabile il paziente, potrebbe essere mostrata allo specialista competente, nel più breve tempo possibile, di persona oppure trasmettendola sul *device* di questi. È evidente come in tale caso specifico, ed in altri simili, l'utilizzo della tecnologia e la sua immediata disponibilità sul campo possa giocare un importante ruolo anche nella formulazione di una diagnosi precoce e, conseguentemente, nell'individuazione del corretto percorso terapeutico.

Più in generale, poi, l'utilizzo delle nuove tecnologie può essere utile nell'ambito di un qualsiasi colloquio tra un professionista sanitario ed un paziente che si rivolga al primo per problemi di salute. Tale incontro si caratterizza per uno scambio di informazioni, per lo più verbale, con notizie che il paziente fornisce al medico, anche in merito ai suoi trascorsi sanitari, allo scopo di aiutarlo a conoscere a fondo la propria condizione. Le notizie apportate dal paziente, infatti, rappresentano una preziosa fonte da cui il professionista sanitario attinge per un compiuto inquadramento del caso. In presenza di situazioni cliniche particolarmente complicate o ricche di dettagli, il sanitario potrebbe avere la necessità di registrare le informazioni fornite dal paziente. In questo modo, infatti, avrebbe eventualmente la possibilità di ascoltare nuovamente la testimonianza ed essere sicuro di non tralasciare alcun particolare[29].

Entrambi i casi pratici esposti mettono in rilievo come le nuove tecnologie diano la possibilità all'azienda sanitaria, per il tramite dei suoi dipendenti, di perseguire, in modo migliore rispetto al passato, la finalità di tutela della salute garantita ai sensi dell'art. 32 della Costituzione. Ciò ha creato, negli ultimi anni, una forte sinergia tra sanità, innovazione e privacy[30]. Tuttavia, l'acquisizione di qualsiasi rappresentazione di un fatto clinico deve sempre avvenire nel pieno rispetto della dignità dell'interessato, come previsto dall'art. 1 del Codice Privacy novellato. Tale principio è di assoluta importanza con particolare riguardo alle fasce deboli, quali i disabili, fisici e psichici, i minori, gli anziani, i soggetti che versano in condizioni di disagio o bisogno e, quindi, in definitiva, in ambito sanitario[31].

[29] Caso riportato a titolo esemplificativo ne "*Le registrazioni dei pazienti. Audio e video effettuati in occasione di contatti con personale o strutture della sanità e apporti informativi direttamente",* approvato con DGR n. X/5765 del 8 novembre 2016.
[30] "*Sicurezza del dato sanitario e condivisione*" – Intervento di Pasquale Stanzone, Presidente dell'Autorità Garante per la protezione dei dati personali – Panorama 18 febbraio 2022.
[31] *Cfr.* Autorità Garante per la protezione dei dati personali, Prescrizione del 9 novembre 2005, "*Strutture sanitarie: rispetto della dignità*", doc. web n. 1191411.

Infine, è doveroso in tale ambito fare un piccolo cenno alla telemedicina, che ha preso piede durante l'emergenza legata al diffondersi del Covid-19, quando le nuove tecnologie si sono rivelate utili a non interrompere l'erogazione di servizi sanitari importanti. La telemedicina costituisce, infatti, una modalità di "curare" il paziente erogando 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 ed il paziente non si trovino nella stessa località[32]. La telemedicina comporta la trasmissione sicura di informazioni e di dati di carattere medico nella forma di testi, suoni, immagini o altre forme necessarie per la prevenzione, la diagnosi, il trattamento ed il successivo controllo dei pazienti. I servizi di telemedicina vanno assimilati a qualunque servizio sanitario diagnostico/ terapeutico, senza, però, sostituire la prestazione sanitaria tradizionale nel rapporto personale medico-paziente, ma integrandola per migliorarne l'efficacia, l'efficienza e l'appropriatezza. Questa deve, pertanto, ottemperare a tutti i diritti ed obblighi propri di qualsiasi atto sanitario. Il rispetto rigoroso delle normative sul trattamento dei dati personali, sia comunitarie sia nazionali, è, quindi, considerato l'elemento essenziale di una corretta gestione anche della telemedicina[33].

In materia, un recente esempio è quello dello Sheba Medical Center di Tel Aviv[34], la struttura sanitaria più grande in Israele, che, in risposta all'epidemia da Covid-19, ha avviato il primo programma di telemedicina. Questo comprende una soluzione "robotica" per intervenire in modo sicuro in zone ad alta carica virale ed un'applicazione di telemedicina progettata da Datos Health[35] per l'assistenza domiciliare, in quanto il citato ospedale non disponeva di un gran numero di camere da isolamento. In questo modo, i pazienti con patologie più gravi e, per questo, ospedalizzati, vengono monitorati tramite un robot che entra nelle loro stanze, mentre lo staff sanitario rimane al di fuori senza correre il rischio di un eventuale contagio in caso di malattie infettive. I pazienti con sintomi minori, invece, rimangono nel *comfort* delle loro case e ad essi viene fornita la citata applicazione di

[32] *Cfr. "Telemedicina – Linee di indirizzo nazionali*" Conferenza Stato Regioni del 20 febbraio 2014.
[33] "*Sanità digitale, il ruolo dei dati per l'innovazione del settore: lo scenario ed i risvolti privacy*" – V. Giardino, Avv. R. Zani – Network Digital 360 - 22 aprile 2021.
[34]La rivista statunitense "*Newsweek*", che annualmente nel rapporto "*World Best Hospitals 2022*" stila la classifica dei migliori ospedali al mondo, posiziona lo Sheba Medical Center di Tel Aviv al decimo posto.
[35] Datos Health è una società di Tel Aviv che si occupa di gestione dei dati sanitari generati dal paziente. Monitora automaticamente tutte le informazioni rilevanti provenienti dai dispositivi medici personali e dai dispositivi indossabili.

telemedicina, attraverso la quale comunicano con i medici via video almeno due volte al giorno.

L'Italia, al contrario, è in ritardo rispetto alla digitalizzazione ed all'utilizzo dei sistemi informativi in ambito sanitario. un'impennata dello sviluppo delle digitalizzazione sanitaria si è verificata sicuramente durante lo stato di emergenza. In tale situazione, infatti, vi era una forte restrizione anche degli accessi alle prestazioni sanitarie "tradizionali" e, pertanto, sia le istituzioni sanitarie che gli utenti hanno toccato con mano le potenzialità della dematerializzazione delle prestazioni resa possibile dalla digitalizzazione. È successo con riferimento alle piattaforme elettroniche e alle app per la prenotazione per le vaccinazioni, ma anche per prestazioni "estemporanee" di teleconsulto, teleconsulenza, teleasssitenza, spesso rese in modalità destrutturata e con i "device" personali a disposizione dei pazienti e degli operatori sanitari. Tuttavia, una ricerca demoscopica realizzata da *Deloitte*[36] nell'anno 2020 non ha, infatti, rilevato dati incoraggianti. Tale indagine, basata su oltre 3.500 interviste effettuate sul territorio nazionale, ha esaminato l'innovazione digitale in duplice prospettiva, sia in merito alla percezione dell'allora attuale offerta, sia relativamente alle abitudini dei pazienti, con lo scopo di verificare se e come le numerose dinamiche che stanno interessando il settore stiano effettivamente modificando le modalità di fruizione dei servizi sanitari da parte dei cittadini. In generale, secondo gli intervistati, la *digital transformation* in ambito sanitario appare ancora limitata. Il 29% dei partecipanti al sondaggio ha valutato come "buone" o "ottime" le competenze digitali degli operatori sanitari in Italia, ma il 38% ha ritenuto che il livello di digitalizzazione del comparto sanitario sia, comunque, inferiore rispetto a quello rinvenibile in altri settori. Poco più della metà della popolazione (precisamente il 59%), poi, conosce il fascicolo elettronico e l'utilizzo digitale dei servizi sanitari appare ancora circoscritto: poco più di un terzo del campione ha ricevuto un referto medico via e-mail (37%) o ha prenotato online una prestazione sanitaria (35%). Infine, solo l'8% ha fruito di servizi di telemedicina, quota inferiore rispetto a quanto registrato a livello globale (media che si attesta tra il13% ed il 29%).

[36] L'esito della ricerca è stato esposto il 22 gennaio 2020 a Roma nell'ambito della prima edizione dell'evento *Deloitte* "*Outlook Salute Italia 2021 — Prospettive e sostenibilità del Sistema Sanitario*". Obiettivo dell'incontro è stato stimolare una riflessione sulle opportunità e sulle sfide del nostro Sistema Sanitario Nazionale, uno dei più efficienti al mondo. L'evento si inseriva nel contesto del progetto "*Impact for Italy"* di *Deloitte*, con cui il *network* di servizi professionali vuole posizionarsi sempre di più come attore di cambiamento per l'Italia, con la *mission* di favorire e sostenere processi di crescita sostenibili e duraturi per la collettività, per le imprese e le Istituzioni.

Tuttavia, in Italia una riforma più strutturale della sanità, sia pubblica sia privata, con un forte impulso alla telemedicina, è stata prevista nel *Recovery Plan* o Piano Nazionale di Ripresa e Resilienza (PNRR). Tale piano è stato predisposto dal Governo Italiano e definitivamente approvato il 13 luglio 2021 con decisione di esecuzione del Consiglio dell'Unione Europea ed ha lo scopo di rilanciarne l'economia del Paese dopo la pandemia da Covid-19[37]. A tal fine, il PNRR prevede lo stanziamento di risorse volte, tra l'altro, al potenziamento della digitalizzazione del sistema sanitario nazionale e della telemedicina anche per le cure domiciliari.

Tutto ciò premesso, è opportuno ricordare quanto già precisato precedentemente[38]. Ai sensi dell'art. 13, par. 2, lett. f), infatti, nell'informativa privacy deve essere esplicitamente indicata l'eventuale esistenza di un processo decisionale automatizzato. Il titolare del trattamento, pertanto, in tutti quei casi in cui intenda utilizzare strumenti che consentano di prendere decisioni impiegando mezzi tecnologici e, conseguentemente, di influenzare o modificare l'esito del processo, deve renderne edotto l'interessato fornendo tutte le informazioni necessarie, nella maniera più chiara e trasparente possibile. L'interessato deve, inoltre, essere informato in merito alla possibilità che gli artt. 21 e 22 del Regolamento UE n. 2016/679 gli conferiscono di opporsi ad un trattamento siffatto.

3b. Tempi e modalità di conservazione

La conservazione consiste nell'attività finalizzata a garantire la tenuta in condizioni idonee, anche nel lungo periodo, di dati e documenti, in forma analogica o digitale. Le metodologie di conservazione hanno, ovviamente, subito ed assecondato il progresso tecnologico e nonostante in ambito sanitario non tutti i documenti siano stati digitalizzati, oggigiorno la conservazione può avvenire in forma analogica o digitale. Una corretta metodologia di conservazione è presupposto imprescindibile, innanzitutto, dal punto di vista giuridico-legale, per garantire all'interessato l'esercizio del diritto di accesso agli atti che lo riguardano[39], ai sensi della legge n. 241/1990, nonché dello stesso Regolamento UE n. 2016/679. Infatti, una richiesta di accesso agli atti, funzionale pertanto all'esercizio di un

[37] Il PNRR fa parte del programma dell'Unione europea noto come "*Next Generation EU*", un fondo da 750 miliardi di euro per la ripresa europea (per questo è noto in inglese come "*Recovery Fund*", cioè Fondo per la ripresa). All'Italia sono stati assegnati 191,5 miliardi.
[38] V. *supra §* 2b.
[39] V. *infra* § 4.

diritto legalmente riconosciuto, potrà essere evasa con facilità ed in tempi brevi solamente in presenza di un archivio correttamente organizzato. Quest'ultimo è utile, inoltre, da un punto di vista probatorio. Ad esempio, nell'ambito di una vertenza relativa alla responsabilità professionale degli operatori sanitari, infatti, può essere vantaggioso ricostruire i fatti clinici attraverso l'analisi della documentazione, che, però, deve essere facilmente reperibile. Infine, una corretta modalità di archiviazione della documentazione può essere funzionale anche per effettuare consultazioni ai fini di studio e di ricerca.

A tal proposito, l'art. 5, par. 1, lett. e) del Regolamento UE n. 2016/679 prevede che i dati personali "*debbano essere conservati […] per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati*". Tale disposizione, quindi, suggerisce i criteri generici da utilizzare per identificare, tra l'altro, i tempi di conservazione nell'ottica del c.d. principio di "*limitazione della conservazione*"[40]. La scelta delle tempistiche specifiche sulla base dei suddetti criteri viene, però, demandata al titolare del trattamento, rifacendosi al principio di responsabilizzazione di cui già si è discusso[41]. Ai sensi dell'art. 13 del Regolamento UE n. 2016/679[42], inoltre, il periodo di conservazione o, in alternativa, i criteri utilizzati dal titolare del trattamento per determinarlo, devono essere indicati all'interno dell'informativa privacy.

Nonostante la normativa europea non indichi tempistiche specifiche relativamente alla conservazione della documentazione in ambito medico, l'Autorità Garante per la Protezione dei dati personali ricorda che "*l'ordinamento giuridico"*, in alcuni casi specifici*, "prevede numerosi e differenziati riferimenti ai tempi di conservazione della stessa, che non sono stati modificati dalla disciplina sulla protezione dei dati personali, e che, quindi, restano pienamente in vigore*"[43]. Così, ad esempio, l'art. 5 del D.M. 18.02.1982 prevede che la documentazione inerente gli accertamenti effettuati nel corso delle visite per il rilascio del certificato di idoneità all'attività sportiva agonistica debba essere conservata, a cura del medico visitatore, per un periodo di almeno cinque anni. La Circolare del Ministero della Sanità n. 900 del 19 dicembre 1986, poi, prevede che le cartelle cliniche ed i relativi referti siano oggetto di conservazione per un periodo di tempo illimitato. L'art. 4 del D.M. 14 febbraio 1997, inoltre, prevede che la documentazione iconografica radiologica debba essere

[40] Il principio di "*limitazione della conservazione*" era già presente nel Codice Privacy previgente, all'art. 11 c. 1 lett. e), abrogato dal D.Lgs. 101/2018.
[41] V. *supra* § 2b.
[42] È uno degli elementi di novità relativamente al contenuto dell'informativa privacy.
[43] *Cfr*. "*Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario"* – Autorità Garante per la Protezione dei dati personali – 7 marzo 2019.

conservata per un periodo non inferiore a dieci anni. Infine, il tempo minimo di conservazione delle registrazioni costituenti parte integrante di una prestazione sanitaria, se non diversamente definito da normative vigenti e/o dal massimario di scarto dell'ente sanitario di riferimento, deve intendersi uguale a quello del documento principale a cui le registrazioni si riferiscano[44].

In riferimento alla modalità di conservazione, invece, il citato art. 5 del Regolamento UE n. 2016/679 prevede che "*i dati personali debbano essere conservati in una forma che consenta l'identificazione degli interessati".* La documentazione, poi, deve essere conservata in modo idoneo, cioè preservandola da distruzione, deterioramento, danneggiamento, asportazione, manomissione e falsificazione, rischi che ricorrono maggiormente se si adotta un sistema di archiviazione di tipo cartaceo. Il "*Codice dell'amministrazione digitale*" (CAD), emanato con il decreto legislativo 7 marzo 2005 n. 82, incentiva l'adozione di un sistema di archiviazione digitale. Tale normativa, infatti, prevede che debba essere assicurata la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale, utilizzando le tecnologie dell'informazione e della comunicazione nel rispetto della disciplina rilevante in materia di trattamento dei dati personali e del Codice stesso. Un archivio digitale, organizzato nel rispetto delle citate disposizioni normative vigenti in materia, inoltre, è in grado di preservare nel tempo le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti informatici, tutelando maggiormente dai rischi su citati. Infatti, si potrebbe fare ricorso a supporti di memorizzazione o a sistemi di elaborazione portatili o fissi, ad esempio, attraverso l'applicazione anche parziale di tecnologie crittografiche a *file system* o *database*, oppure tramite l'adozione di altre misure di protezione che rendano i dati inintelligibili ai soggetti non legittimati ad apprenderli.

Negli ultimi anni, l'utilizzo di sistemi informativi per la gestione e la consultazione delle informazioni relative alla storia clinica di un individuo ha trovato un'ampia diffusione nel settore sanitario sia nazionale sia internazionale. Il legislatore italiano, infatti, ha colto tale fenomeno attraverso la previsione di una disciplina giuridica, ad esempio, relativa al fascicolo sanitario elettronico[45], alla carella clinica elettronica ed alla refertazione online[46]. L'art. 47-*bis* c. 1 del D.L. 9 febbraio 2012, n. 5, recante "*Disposizioni urgenti in materia di*

[44] *Cfr.* "*Immagini, suoni e biosegnali – Manuale per i percorsi di cura*", approvato con DGR n. X/3001 del 9 gennaio 2015.
[45] V. *infra* § 3c.
[46] V. *infra* § 3d.

semplificazione e di sviluppo", convertito con modificazioni dalla L. 4 aprile 2012, n. 35 recante, a sua volta, *"Semplificazione in materia di sanità digitale"*, ha, poi, sancito la preminenza della gestione elettronica rispetto a quella tradizionale per quanto concerne le pratiche cliniche, attraverso, ad esempio, l'utilizzo della cartella clinica elettronica, così come i sistemi di prenotazione elettronica per l'accesso alle strutture da parte dei cittadini, nei limiti di sostenibilità anche finanziaria per gli enti sanitari pubblici e privati interessati. Tale ultima disposizione ha, inoltre, consentito, a partire dal 1° gennaio 2013, la conservazione anche soltanto digitale delle cartelle cliniche. È evidente come tale normativa sia stata emanata al fine di accelerare il processo di migrazione dei servizi sanitari ad una gestione prevalentemente o interamente informatica. D'altronde, l'attuazione di quest'ultima comporta opportunità di maggiore efficienza e di risparmio di risorse, che possono, così, essere allocate utilmente in altre direzioni:

- disponibilità di tutte le informazioni sanitarie con un click ed in ogni momento, tendenzialmente 24 ore su 24 e 7 giorni su 7;
- accessibilità alle informazioni sanitarie da qualsiasi terminale abilitato;
- completezza informativa;
- standardizzazione dei formati;
- abbattimento dei costi di archiviazione, grazie all'utilizzo di strumenti di *storage*;
- possibilità di verifica degli accessi alle informazioni sanitarie;
- automatizzazione dei sistemi di prenotazione delle visite e ritiro dei referti, con abbattimento dei costi per l'ente sanitario e risparmio di tempo per il cittadino;
- semplificazione del *workflow* documentale in ambito clinico ed amministrativo[47].

In riferimento all'adozione di un archivio digitale bisogna, però, tenere presente non solo i vantaggi connessi all'ampia fruibilità del dato sanitario elettronico, ma anche le correlate e peculiari vulnerabilità, dal punto di vista soprattutto della tutela dei dati personali, in virtù delle quali il titolare del trattamento deve eventualmente optare per l'adozione di misure di sicurezza che le prevengano. Si possono riscontrare, ad esempio, criticità legate all'eventuale trasferimento dei dati personali extra UE, ad un accesso abusivo ai dati, alla modificabilità, allo smarrimento parziale o integrale dei supporti di memorizzazione o dei sistemi di elaborazione portatili o fissi a seguito di eventi disastrosi, alla comunicazione a soggetti non

[47] *Cfr.* "*Cloud in Sanità: Vademecum essenziale sulla tutela della privacy. Manuale sui principi, sulle caratteristiche, sulle specifiche normative in materia di protezione dei dati da applicare in Italia all'erogazione di servizi sanitari con tecnologia cloud computing"* - Avv. Luca Bolognini1 – Avv. Enrico Pelino – 2016.

legittimati ed alla continuità operativa. In riferimento a quest'ultimo aspetto, occorre prendere in considerazione anche la scelta di mantenere comunque *in-house* una copia di quei dati, dalla cui perdita o indisponibilità potrebbero conseguire danni economici per l'immagine o in generale relativi alla missione ed alle finalità perseguite, a meno che vi siano soluzioni *cloud* che offrano ampie assicurazioni su questo aspetto[48]. Non a caso, infatti, il ricorso a tecnologie *cloud* è indicato espressamente dall'art. 68, co. 1, lett. d), del "*Codice dell'amministrazione digitale"*, quale opzione da tenere presente per la Pubblica Amministrazione nella scelta dei relativi servizi informatici. In linea generale, infatti, deve rilevarsi, che pur con determinate cautele, le soluzioni *cloud* appaiono pienamente compatibili con l'affidamento di servizi della sanità elettronica. In tal caso, si raccomanda, però, di porre particolare attenzione alla localizzazione *intra* o *extra* UE o, comunque, all'interno di un paese che offra un adeguato livello di protezione dei dati sanitari, specialmente nel servizio di *storage*.

Infine, in una fase di dematerializzazione della documentazione, soprattutto in ambito sanitario sarebbe utile orientare la scelta verso l'utilizzo di programmi di archivio improntati ad un principio di interoperabilità. La Commissione Europea, infatti, aveva identificato, già nel 1999, l'esigenza dell'interoperabilità tra le Pubbliche Amministrazioni, sostenendo sin da allora l'adozione di programmi per sviluppare, promuovere ed utilizzare soluzioni di questo tipo all'interno dell'Unione Europea. L'art. 68 c. 1-*bis* lett. b) del "*Codice dell'amministrazione digitale"* prevede, altresì, che le Pubbliche Amministrazioni, prima di procedere all'acquisto di programmi informatici o di parti di essi, debbano effettuare una valutazione comparativa delle diverse soluzioni disponibili, privilegiando *standard* in grado di assicurare l'interoperabilità e la cooperazione applicativa tra i diversi sistemi informatici di differenti enti pubblici. L'interoperabilità, infatti, è un fattore chiave per la realizzazione di una trasformazione digitale[49] e viene descritta dalla stessa Commissione Europea come la capacità di organizzazioni diverse e disparate di interagire, in vista di obiettivi comuni, concordati e reciprocamente vantaggiosi, ricorrendo alla condivisione di conoscenze ed

[48] *Cfr*. art. 50-*bis* c. 3 lett. b) del "*Codice dell'amministrazione digitale"*; "*Cloud Computing - La guida del Garante della Privacy per imprese e pubblica amministrazione"* – Autorità Garante per la protezione dei dati personali – 2012.

[49] Principio declinato nel nuovo "*European Interoperability Framework"* (EIF), oggetto della Comunicazione del 23.3.2017 dal titolo "*Quadro europeo di interoperabilità - Strategia di attuazione*" della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni.

informazioni per mezzo dei processi aziendali che permettano lo scambio di dati fra i rispettivi sistemi di Information and Communications Technology (TIC)[50].

Il carattere di interoperabilità di un sistema, inoltre, risulta anche propedeutico all'esercizio da parte dell'interessato del diritto alla portabilità dei dati. Ai sensi dell'art. 20 del Regolamento UE n. 2016/679, infatti, "*l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:*

a) *il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b);*
b) *il trattamento sia effettuato con mezzi automatizzati.*

Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile".

È evidente come, in ambito sanitario, l'adozione di un sistema di archiviazione della documentazione caratterizzato dall'interoperabilità consentirebbe ad ogni professionista che si approcci al medesimo paziente di avere una visione univoca, dettagliata e certa di tutta la vita clinica dello stesso. Una tale condivisione tra gli operatori sanitari delle informazioni sulla salute del paziente costituirebbe uno strumento volto a rendere più efficienti i processi di diagnosi e di cura di questi, nonché a ridurre i costi della spesa sanitaria derivanti, ad esempio, dalla ripetizione di esami clinici già effettuati ed ancora validi.

50 Definizione riportata nella Comunicazione del 16.12.2010 dal titolo "*Verso l'interoperabilità dei servizi pubblici europei*" della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, contenente in allegato la strategia europea per l'interoperabilità (SEI) ed il quadro europeo di interoperabilità (QEI). Da allora, il quadro europeo di interoperabilità ha rappresentato un punto di riferimento fuori e dentro l'Unione ed ha costituito la base per la maggior parte delle strategie e dei quadri nazionali di interoperabilità (QNI). Il programma sulle soluzioni di interoperabilità per le pubbliche amministrazioni europee (ISA) (2010-2015) ed il nuovo programma ISA (2016-2020) sono i principali strumenti attraverso cui sono stati attuati la strategia europea per l'interoperabilità ed il quadro europeo di interoperabilità vigenti. Ciò ha richiesto numerose azioni volte a migliorare la collaborazione digitale tra le pubbliche amministrazioni in Europa.

In Italia, un primo *input* all'avvio di un processo di dematerializzazione improntato al principio di interoperabilità è stato dato con l'adozione, ormai da parte di tutte le regioni, del fascicolo sanitario elettronico o FSE.

3c. Il Fascicolo Sanitario Elettronico (FSE): un esempio di sanità digitale e di interoperabilità

Il Fascicolo Sanitario Elettronico o FSE rappresenta uno dei pilastri della sanità digitale[51], oltre a costituire uno dei pochi esempi di interoperabilità attuati in ambito sanitario. Tale strumento, infatti, è stato definito come "*l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito"*[52]. Il FSE, inizialmente regolato solo sul piano della *soft law,* attraverso le "*Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario*" adottate dal Garante il 16 luglio 2009, ha successivamente trovato uno specifico fondamento normativo nell'art. 12 del D.L. 18 ottobre 2012 n. 179 recante "*Ulteriori misure urgenti per la crescita del Paese"*, convertito con modificazioni dalla legge 17 dicembre 2012 n. 221, e nel DCPM 29 settembre 2015, n. 178 recante il "*Regolamento in materia di fascicolo sanitario elettronico*".

Dalla citata definizione si evince che il fascicolo sanitario elettronico sia stato pensato come uno strumento commisurato all'intera vita del paziente e ad alimentazione continua nel tempo, ad opera dei soggetti del Servizio sanitario nazionale e dei servizi sociosanitari regionali che prendono in cura il medesimo paziente. Tale strumento, quindi, rende disponibile in formato digitale la storia clinica di una persona a tutti gli attori coinvolti, permettendo di inquadrare un paziente ancora sconosciuto. È innegabile come, in alcune circostanze, la conoscenza di tali informazioni possa risultare rilevante, o addirittura determinante, per un tempestivo intervento e, in alcuni casi, per la vita stessa del paziente o, comunque, per la qualità della sua vita. Grazie all'interoperabilità garantita dal Sistema Tessera Sanitaria, i dati presenti all'interno del FSE sono tra loro collegati per mezzo di

---

[51] Cfr. "*Fascicolo Sanitario Elettronico, cos'è, a che serve e come attivarlo*" - Anna Francesca Pattaro – *Network Digital 360* – 16 settembre 2021.

[52] La medesima definizione era già stata fornita dal Ministero della salute ne "*Il Fascicolo Sanitario Elettronico. Linee guida nazionali*" del 11 novembre 2010.

modalità informatiche che ne rendono possibile la consultazione unitaria, anche se generati da strutture ubicate al di fuori della regione di appartenenza.

Il nucleo minimo del FSE è costituito da referti, verbali di pronto soccorso e lettere di dimissione. A tale documentazione di base possono, poi, essere aggiunte prescrizioni specialistiche[53] o farmaceutiche, cartelle cliniche di ricovero ordinario e di *day hospital* e piani terapeutici. All'interno di tale fascicolo, infine, può essere ricompresa anche la documentazione relativa all'assistenza domiciliare, quale la relativa scheda, il programma, la cartella clinica e la scheda multidimensionale di valutazione. È evidente, quindi, come attraverso l'istituzione del Fascicolo Sanitario Elettronico sia stato inserito un *medium* tecnologico tra il medico ed il paziente. La tecnologia, infatti, si è frapposta nel rapporto interpersonale tra i due soggetti, in quanto questa mette a disposizione del medico tutte le informazioni sanitarie che, in mancanza, sarebbe stato il paziente a comunicargli[54].

Il FSE è istituito dalle regioni italiane e dalle province autonome, con finalità di prevenzione, diagnosi, cura, riabilitazione, studio e ricerca scientifica in campo medico, biomedico ed epidemiologico, programmazione sanitaria, verifica della qualità delle cure e valutazione dell'assistenza sanitaria, purché nel rispetto della normativa sulla protezione dei dati sanitari. La costituzione del FSE per ciascun cittadino, inoltre, non è obbligatoria, ma è demandata alla sua libera scelta e, qualora questa dovesse essere negativa, non determina nessuna conseguenza in ordine all'erogazione delle prestazioni sanitarie, che verrebbero, comunque, garantite. L'utilizzo di tale strumento, infatti, viene considerato come un servizio accessorio offerto ai pazienti e non strettamente necessario per il perseguimento delle finalità di diagnosi e di cura.

Naturalmente, l'attuazione del FSE, in merito alla raccolta dei dati e, in particolare, di dati relativi alla salute, rinvia a numerosi aspetti legati al loro trattamento. Occorre, infatti, garantire, ad esempio, che la raccolta, la consultazione e la conservazione dei dati personali avvenga nel pieno rispetto della normativa nazionale ed europea in materia. A tal proposito, si sottolinea che il trattamento effettuato attraverso il fascicolo sanitario elettronico rientrava

[53] L'ordinanza n. 651 del 19 Marzo 2020 "*Ulteriori interventi urgenti di protezione civile in relazione all'emergenza relativa al rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili"* ha consentito ai cittadini di ottenere dal proprio medico il numero di ricetta elettronica senza che vi sia più la necessità di ritirare fisicamente, e portare in farmacia, il promemoria cartaceo, rendendola disponibile automaticamente all'interno del FSE.

[54] *"I dati sanitari, in i dati personali nel diritto europeo",* P. *Guarda, a cura di V. Cuffaro, R. D'Orazio, V. Ricciuto, Giappichelli, 2019, p. 592.*

fra quelli in cui l'acquisizione del consenso, quale condizione di liceità dello stesso, era richiesta dalle specifiche disposizioni di settore, precedenti all'applicazione del Regolamento UE n. 2016/679, ed in particolare, dall'art. 12 c. 3-*bis* del D.L. 18 ottobre 2012 n. 179. Originariamente, infatti, l'inserimento di dati all'interno del FSE era subordinato al consenso prestato dal paziente, il quale doveva essere informato in merito a chi potesse avere accesso ai suoi dati e come questi potessero venire utilizzati. Successivamente, già nell'anno 2019, l'Autorità Garante per la Protezione dei dati personali aveva precisato che "*un'eventuale opera di rimeditazione normativa in ordine all'eliminazione della necessità di acquisire il consenso dell'interessato all'alimentazione del Fascicolo",* potesse essere ammissibile *"alla luce del nuovo quadro giuridico in materia di protezione dei dati"*[55]. In seguito, la normativa recentemente introdotta[56] ha previsto che, a decorrere dal maggio 2020, il cittadino sia chiamato a prestare, *una tantum*, un consenso di carattere generale per la costituzione del FSE e non più per la sua alimentazione da parte di strutture sia pubbliche sia private. Egli viene chiamato a rendere anche un consenso a carattere specifico, relativamente all'accessibilità al FSE medesimo, alla visibilità del suo contenuto ed al recupero dei dati pregressi a partire dal 1 gennaio 2008. La recente normativa, infatti, prevede che a decorrere da maggio 2020, qualora il cittadino abbia prestato il consenso alla creazione del FSE, i dati di tutte le prestazioni sanitarie già fruite vadano a confluire autonomamente in esso, senza che egli vi abbia esplicitamente consentito. Il consenso richiesto deve essere specifico, libero ed informato. Tale condizione può essere soddisfatta solamente tramite la somministrazione all'interessato di un'informativa privacy[57] c.d. diretta, ai sensi dell'art. 13 del Regolamento UE n. 2016/679, contenente, a titolo esemplificativo e non esaustivo, la definizione di FSE, le sue finalità, i dati identificativi del titolare del trattamento e del responsabile del trattamento eventualmente designato, le modalità di trattamento, il periodo di conservazione, i diritti dell'interessato e le modalità del loro esercizio. L'interessato ha il diritto di revocare in qualsiasi momento, anche in via telematica, il consenso in precedenza prestato, determinando l'interruzione dell'alimentazione del proprio FSE e la disabilitazione alla sua consultazione dei soggetti prima a ciò autorizzati.

[55] Cfr. *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario"* - (7 marzo 2019).
[56] D.L. "*Rilancio"* n. 34/2020 che ha modificato l'art. 12 del D.L. 179/2012 e che è stato adottato in piena pandemia legata alla diffusione del Covid-19.
[57] V. *supra* § 2b.

Con riguardo, invece, all'alimentazione del fascicolo con tutti i dati delle prestazioni sanitarie effettuate in epoca antecedente al maggio 2020, l'Autorità Garante per la protezione dei dati personali, con nota del 15 dicembre 2020[58], ha precisato al Ministero della Salute che l'ingresso delle informazioni all'interno del fascicolo sanitario elettronico sarebbe stato possibile solo a tre condizioni, peraltro ad oggi non ancora verificatesi:

a) avere proceduto ad un'idonea campagna nazionale di informazione;
b) avere puntualmente informato i cittadini delle Regioni interessate sulle novità relative all'alimentazione del Fascicolo;
c) avere riconosciuto a questi ultimi, dal momento in cui sono stati informati, un termine non inferiore a 30 giorni per manifestare la propria eventuale opposizione.

Tuttavia, come accennato precedentemente e come precisato dallo stesso Garante Privacy[59], anche a seguito di tale alimentazione automatica del FSE, i dati sanitari del cittadino, in assenza di uno suo specifico consenso[60], non saranno liberamente accessibili al personale sanitario. All'interessato, infatti, deve essere riconosciuto un ampio controllo sui propri dati sanitari inclusi nel FSE[61]. L'interessato ha, pertanto, il diritto di stabilire, tramite una manifestazione di consenso, quali soggetti possano consultare i dati sanitari contenuti all'interno del proprio FSE, fatta salva la possibilità di accedervi conferita a chi abbia redatto la documentazione sanitaria. Il professionista o l'organismo sanitario che ha in cura l'interessato, infatti, deve poter accedere al FSE, consultando i documenti sanitari dallo stesso redatti e quelli eventualmente formati da reparti o strutture della medesima struttura,

[58] L'Autorità Garante per la Protezione dei dati personali con tale nota ha precisato come non esista un termine di scadenza entro il quale esprimere la propria opposizione all'alimentazione del FSE con i dati clinici antecedenti al maggio 2020. La notizia era circolata in Rete a seguito dell'iniziativa presa dalla Regione Liguria che aveva erroneamente indicato l'11 gennaio 2021 come il termine entro il quale i cittadini liguri avrebbero dovuto comunicare la loro eventuale opposizione all'inserimento nel FSE dei dati relativi alle prestazioni sanitarie fruite, in ambito pubblico o privato, prima del maggio 2020. Tuttavia, il Garante precisa come l'imposizione di un termine in tal caso sia priva di un qualsiasi fondamento normativo.

[59] *Cfr. "Fascicolo Sanitario Elettronico nessuna scadenza per l'inserimento dei dati"* – 11 gennaio 2021.

[60] In ambito comunitario il Comitato dei Ministri del Consiglio d'Europa era intervenuto già con la Raccomandazione n. 81 del 1981 con la quale sono stati individuati "*i criteri di gestione delle banche di dati sanitari automatizzate, fornendo una serie di importanti direttive per l'utilizzo di tali banche dati, nei limiti in cui la coeva Convenzione di Strasburgo ne consentiva la creazione*". Importante è il riferimento che la Raccomandazione su citata presenta al punto 5.4, che così recita: "*senza il consenso espresso e cosciente della persona interessata, l'esistenza e il contenuto di un dossier sanitario che la riguardi non può essere comunicato a persone o organismi fuori dal campo delle cure mediche, della sanità pubblica o della ricerca medica, a meno che una tale comunicazione non sia permessa dalle regole del segreto professionale dei medici*".

[61] A tal riguardo si parla di *patient empowerment. "Ciò si traduce nel fatto che le scelte in ordine ... a livelli di condivisione e alle varie applicazioni che una piattaforma di sanità elettronica permette di amministrare possono essere gestite direttamente dal paziente attraverso lo strumento tecnico-giuridico del consenso*", in "*I dati sanitari"*, in *"I dati personali nel diritto europeo",* P. *Guarda, a cura di V. Cuffaro, R. D'Orazio, V. Ricciuto, Giappichelli, 2019*, p. 615.

anche relativi ad altri eventi clinici, quale ad esempio un ricovero pregresso o analisi cliniche antecedenti. In ogni caso, l'accesso al FSE da parte di soggetti a ciò abilitati deve essere riferito esclusivamente ai dati riferiti ai soggetti che assistono e per il periodo di tempo in cui si articola il percorso di cura per il quale l'interessato si sia rivolto ad essi[62].

La normativa in materia di fascicolo sanitario elettronico[63], inoltre, prevede che l'interessato possa oscurare dati e documenti ivi presenti, che saranno così accessibili solo dallo stesso interessato e dal medico che li ha generati. Tale diritto di oscuramento, la cui esistenza è stata più volte confermata anche dall'Autorità Garante per la Protezione dei dati personali[64], è esercitabile sia nel momento in cui sono generati i referti sia successivamente. Dal punto di vista informatico, il sistema che gestisce il fascicolo deve essere impostato in modo tale che l'"oscuramento" dell'evento clinico avvenga con modalità tali da garantire che gli altri soggetti abilitati all'accesso per le finalità di cura non possano venire automaticamente a conoscenza della scelta effettuata dall'assistito e dell'esistenza di dati "oscurati"[65]. L'opzione per l'oscuramento può essere anch'essa revocata in ogni momento da parte del cittadino.

Tutti i soggetti autorizzati ad accedere al FSE di un paziente, comunque, devono attenersi al rispetto del segreto professionale[66]. Un'eventuale condotta contraria a tale obbligo costituirebbe un illecito deontologico, sanzionato da tutti i Codici deontologici delle diverse figure di operatori sanitari. Verrebbe, altresì, a configurarsi anche la fattispecie del reato di "*rivelazione di segreto professionale*", sanzionato dall'art. 622 del codice penale, che così recita: "*chiunque, avendo notizia, per ragione del proprio stato o ufficio, o della propria professione o arte, di un segreto, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto, è punito, se dal fatto può derivare nocumento, con la reclusione fino a un anno o con la multa da euro 30 a euro 516. […] Il delitto è punibile a querela della persona offesa".*

---

[62] *Cfr. "Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario"* - 16 luglio 2009 – Autorità Garante per la Protezione dei dati personali.

[63] Cfr. D.P.C.M. 29 settembre 2015, n. 178, recante "*Regolamento in materia di fascicolo sanitario elettronico*".

[64] "*FAQ – Fascicolo Sanitario Elettronico*"; "Ordinanza ingiunzione nei confronti di Azienda Usl della Romagna" - 27 maggio 2021; *"Ordinanza ingiunzione nei confronti di Azienda provinciale per i servizi sanitari di Trento"* - 27 maggio 2021 - Autorità Garante per la Protezione dei dati personali.

[65] Si parla in questo caso di "*oscuramento dell'oscuramento*".

[66] Principio ribadito dall'art. 12 c. 5 del D.L. 18 ottobre 2012 n. 179, recante "*Ulteriori misure urgenti per la crescita del Paese".*

Il trattamento di dati personali effettuato attraverso il FSE, perseguendo esclusivamente finalità di prevenzione, diagnosi e cura dell'interessato deve essere posto in essere esclusivamente da parte di soggetti operanti in ambito sanitario, con conseguente esclusione di periti, compagnie di assicurazione, datori di lavoro, associazioni o organizzazioni scientifiche ed organismi amministrativi, anche operanti in ambito sanitario. Analogamente, l'accesso è precluso anche al personale medico nell'esercizio di attività medico-legale, quale ad esempio l'espletamento delle visite per l'accertamento dell'idoneità lavorativa o alla guida. Tali figure di professionisti, infatti, sebbene abbiano carattere sanitario, svolgono la loro attività professionale nell'ambito dell'accertamento di idoneità o *status*, e non anche all'interno di un processo di cura dell'interessato[67], cui, invece, è preposto il trattamento dei dati presenti nel FSE. Allo stesso modo, il personale amministrativo operante all'interno della struttura sanitaria, in cui venga utilizzato il fascicolo, può, in qualità di incaricato del trattamento, consultare solo le informazioni necessarie per assolvere alle funzioni amministrative cui è preposto e strettamente correlate all'erogazione della prestazione sanitaria. Così, ad esempio, il personale addetto alla prenotazione di esami diagnostici o visite specialistiche può consultare unicamente i dati indispensabili a tale finalità. In mancanza di consenso dell'interessato, infine, possono accedere al FSE soltanto gli organi di governo sanitario, quale il Ministero della Salute e la Regione, per lo svolgimento delle proprie funzioni istituzionali, tra cui vi rientra, ad esempio, la gestione delle emergenze sanitarie. Tuttavia, è bene precisare che, in tale ipotesi, l'accesso è consentito solo in relazione a dati pseudonimizzati[68].

Il Presidente del Consiglio dei ministri, nella fase di predisposizione del regolamento in materia di FSE[69], aveva chiesto all'Autorità Garante per la Protezione dei dati personali un parere, che poi si rivelerà favorevole[70], in riferimento alla proposta di prevedere che tutti gli accessi al fascicolo del singolo cittadino venissero registrati in un'apposita sezione di tale strumento. In questo modo, infatti, l'interessato avrebbe potuto effettuare ogni verifica che ritenesse opportuna, così da poter denunciare l'eventuale rinvenimento di accessi ritenuti

[67] *Cfr. "Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario*"- Autorità Garante per la Protezione dei dati personali - 16 luglio 2009.
[68] V. *supra* nota n. 27.
[69] Adottato, poi, con D.P.C.M. 29 settembre 2015 n. 178, recante il "*Regolamento in materia di fascicolo sanitario elettronico*".

[70] *Cfr. "Parere del Garante su uno schema di decreto del Presidente del Consiglio dei ministri in materia di fascicolo sanitario elettronico*" - 22 maggio 2014.

illegittimi[71]. In tale ultimo caso, infatti, si verrebbe a configurare una fattispecie di trattamento illecito di dati personali, sanzionato dall'art. 167 c. 2 del Codice Privacy novellato, che così recita: "*salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2-septies ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-quinquiesdecies arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni"*.

Il sistema informativo del fascicolo sanitario elettronico, in quanto strumento di archiviazione digitale di una numerosa mole di dati personali e sensibili, deve prevedere ed attuare le misure di sicurezza individuate dall'art. 23 del D.P.C.M. 29 settembre 2015 n. 178. Tale disposizione prevede che le operazioni sui dati personali vengano effettuate mediante strumenti elettronici con modalità e soluzioni necessarie per assicurare confidenzialità, integrità e disponibilità dei dati. In particolare, in riferimento alla consultazione in sicurezza dei dati contenuti nel FSE, devono essere assicurati:

- idonei sistemi di autenticazione e di autorizzazione per i soggetti abilitati, in funzione dei ruoli e delle esigenze di accesso e trattamento. Devono essere, pertanto, preferite soluzioni che consentano un'organizzazione modulare di tali strumenti, in modo da limitare l'accesso dei diversi soggetti abilitati alle sole informazioni indispensabili. In questo modo, alcune categorie di soggetti, quali, ad esempio, i farmacisti, che svolgono la propria attività in uno specifico segmento del percorso di cura, possono accedere al fascicolo, ma limitatamente ai soli dati indispensabili all'erogazione di farmaci. Essi potranno conoscere, ad esempio, solamente l'elenco dei farmaci già prescritti, al fine di valutare eventuali incompatibilità tra un farmaco da somministrare ed altri precedentemente assunti;
- procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati ai soggetti abilitati;

[71] Con riguardo a quest'ultimo punto, si richiama un recente provvedimento con cui il Garante Privacy ha inflitto una sanzione di € 30.000,00 ad un'azienda ospedaliera, i cui dipendenti avevano "sbirciato" dati dei colleghi contenuti nei FSE dei pazienti, mediante le credenziali di un medico che aveva lasciato incustodita la propria postazione; detti accessi sono stati sanzionati dall'Autorità Garante, poiché effettuati non per erogare prestazioni sanitarie, bensì per "mera curiosità" – "*Garante, no agli accessi indebiti ai dossier sanitari"* - *Newsletter* n. 462 del 18 febbraio 2020.

- protocolli di comunicazione sicuri basati sull'utilizzo di standard crittografici per la comunicazione elettronica dei dati tra i diversi titolari coinvolti;
- adozione di criteri per la cifratura o per la separazione dei dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali;
- tracciabilità degli accessi e delle operazioni effettuate;
- sistemi di *audit log* per il controllo degli accessi e per il rilevamento di eventuali anomalie;
- procedure di anonimizzazione degli elementi identificativi diretti;
- garantiti protocolli di comunicazione sicuri basati sull'utilizzo di *standard* crittografici per la comunicazione elettronica dei dati tra i diversi titolari coinvolti.

Il titolare del trattamento deve, infine, prevedere modalità informatiche idonee a consentire all'interessato una facile consultazione del proprio FSE, anche in riferimento al diritto, legalmente riconosciuto a quest'ultimo, di estrarne copia[72].

È significativo segnalare come l'emergenza sanitaria legata alla diffusione del Covid-19 abbia contribuito significativamente ad accrescere l'adesione, e si spera anche l'utilizzo, del fascicolo sanitario elettronico da parte dei cittadini. Infatti, in una situazione in cui la mobilità dei cittadini è stata talvolta limitata da disposizioni orientate alla salvaguardia della salute pubblica, aver avuto a disposizione uno strumento simile ha permesso di visionare, comunque, la documentazione sanitaria senza la necessità di spostarsi. Una maggiore diffusione di tale strumento è dovuta anche grazie al D.L. del 28 ottobre 2020, n. 137 recante "*Ulteriori misure urgenti in materia di tutela della salute, sostegno ai lavoratori e alle imprese, giustizia e sicurezza, connesse all'emergenza epidemiologica da Covid-19*" ed al D.L. del 3 novembre 2020 recante "*Modalità attuative delle disposizioni di cui all'articolo 19, comma 1, del decreto-legge n. 137 del 28 ottobre 2020 (c.d. "Decreto Ristori"*)". Tali disposizioni, infatti, hanno previsto che il referto elettronico del tampone effettuato venga reso disponibile direttamente sul FSE del cittadino. I medici predispongono il referto elettronico utilizzando le funzionalità del Sistema Tessera Sanitaria, che lo rende immediatamente disponibile per la visualizzazione da parte dell'assistito accedendo al proprio FSE. Successivamente, all'interno del fascicolo sanitario elettronico è stato reso disponibile anche il c.d. *green pass*, un altro documento, oltre al referto del tampone, che ha

[72] V. *infra* Capitolo IV.

avuto estrema importanza durante l'emergenza sanitaria. Pertanto, tale situazione, in cui i cittadini chiedevano con urgenza di impossessarsi delle proprie informazioni, dei risultati dei tamponi, delle vaccinazioni e oggi di accedere al *green pass*, ha permesso loro di scoprire l'importanza del fascicolo sanitario elettronico.

Per quanto riguarda l'effettiva diffusione, lo strumento del FSE è stato attivato da tutte le regioni italiane, anche se con livelli di operatività, di adesione e di utilizzo differenti. I dati di monitoraggio a livello nazionale dello stato di attuazione e di utilizzo del sistema del fascicolo sanitario elettronico da parte dei cittadini, disponibili sul sito dell'AgID[73], in riferimento alla Regione Lombardia ne indicano un livello pari al 100%. Tuttavia, in una panoramica nazionale, se l'indicatore di attuazione nelle differenti regioni italiane testimonia un livello elevato ed omogeneo di attuazione del FSE, con l'eccezione della sola Regione Abruzzo, lo scenario appare sensibilmente difforme se si analizza l'indicatore di utilizzo dello stesso da parte dei cittadini.

Pertanto, da parte delle diverse regioni italiane sono stati fatti numerosi passi avanti nella diffusione e nell'attuazione del Fascicolo Sanitario Elettronico, ma sembra che vi sia ancora un po' di strada da percorrere per quanto riguarda l'effettivo utilizzo di questo strumento da parte di cittadini, medici e altri operatori sanitari potenzialmente interessati. Emerge di fatto l'attuale limite del FSE, di essere cioè un contenitore pieno della documentazione minima prevista dalla normativa, ma priva di qualsivoglia utilità per il cittadino-paziente, come per gli stessi operatori sanitari.

Come accennato precedentemente[74], uno dei principali obiettivi del PNRR consiste proprio nel promuovere la digitalizzazione dell'assistenza sanitaria, al fine di consentire un'effettiva equità di accesso da parte della popolazione alle cure sanitarie e sociosanitarie, stabilendo *standard* qualitativi e quantitativi uniformi su tutto il territorio nazionale. Nelle intenzioni del legislatore, tale obiettivo verrà raggiunto anche attraverso il rafforzamento del FSE, al quale le recenti novità normative intendono dare un nuovo volto. Tale strumento, infatti, diventerà un *repository* digitale contenente l'intera storia clinica degli assistiti, su

[73] https://www.fascicolosanitario.gov.it/monitoraggio/a. L'Agenzia per l'Italia digitale (abbreviato AgID) è un'agenzia pubblica italiana istituita dal Governo Monti. Sottoposta ai poteri di indirizzo e vigilanza del Presidente del Consiglio dei Ministri o del ministro da lui delegato, svolge le funzioni ed i compiti ad essa attribuiti dalla legge, al fine di perseguire il massimo livello di innovazione tecnologica nell'organizzazione e nello sviluppo della Pubblica Amministrazione ed al servizio dei cittadini e delle imprese, nel rispetto dei principi di legalità, imparzialità e trasparenza e secondo criteri di efficienza, economicità ed efficacia.
[74] V. *supra* § 3 a.

tutto il territorio nazionale, alimentato costantemente grazie all'attività degli operatori sanitari[75]. La legge 28 marzo 2022 n. 25[76] prevede, infatti, un obbligo in capo agli operatori sanitari pubblici e privati, siano questi accreditati o autorizzati, coinvolti in tutte le fasi di diagnosi, cura e riabilitazione, di caricare sul FSE le informazioni sanitarie dei pazienti, entro cinque giorni dall'erogazione delle prestazioni. Il FSE, inoltre, avrà la funzione di alimentare il nuovo Ecosistema dei Dati Sanitari (EDS), istituito dalla citata legge 28 marzo 2022 n. 25. La suddetta alimentazione avverrà attraverso i dati resi disponibili tramite il "sistema tessera sanitaria", nonché attraverso quelli trasmessi dalle strutture sanitarie e sociosanitarie e dagli enti del Servizio sanitario nazionale.

In ogni caso, l'obiettivo del nuovo fascicolo sanitario elettronico è senz'altro ambizioso. Considerata la natura ed il volume delle informazioni che saranno disponibili al suo interno[77], inoltre, è molto probabile una crescita esponenziale dei rischi per la protezione dei dati personali degli assistiti. Ne è la prova il significativo aumento di cyberattacchi che ha interessato il settore della sanità, a seguito dell'emergenza pandemica[78]. Tuttavia, è ancora presto per esprimere giudizi accurati sui rischi che le innovazioni di cui si discute comporteranno per la tutela dei dati personali degli assistiti. Infatti, i contenuti del FSE, nonché le responsabilità ed i compiti degli operatori tenuti ad alimentare il citato *repository*, verranno stabiliti nel dettaglio con appositi decreti dal Ministero della Salute, di concerto con il Ministero per la Transizione Digitale. Tali decreti dovranno anche disciplinare le misure di sicurezza e le garanzie da adottare per assicurare la tutela dei dati personali degli interessati, la modalità di attribuzione agli assistiti di un codice identificativo univoco (tale da non consentirne l'identificazione diretta) ed i livelli diversificati di accesso sia al FSE sia all'EDS.

---

[75] *Cfr.* "*Il nuovo Fascicolo Sanitario Elettronico ed i rischi per la privacy degli assistiti"* - Cristina Criscuoli – 27 aprile 2022 - *Diritto al Digitale.*

[76] Si tratta della legge di conversione con modificazioni, del decreto-legge 27 gennaio 2022, n. 4, recante "*misure urgenti in materia di sostegno alle imprese e agli operatori economici, di lavoro, salute e servizi territoriali, connesse all'emergenza da COVID-19, nonché' per il contenimento degli effetti degli aumenti dei prezzi nel settore elettrico".*

[77] Proprio in considerazione di tali rischi, il Legislatore ha previsto il coinvolgimento del Garante per la protezione dei dati personali, che verrà chiamato ad esprimere il proprio parere sul testo dei menzionati decreti attuativi emanati dal Ministero della Salute, prima della loro approvazione.

[78] *Cfr.* "*Il nuovo Fascicolo Sanitario Elettronico ed i rischi per la privacy degli assistiti"* - Cristina Criscuoli – 27 aprile 2022 - *Diritto al Digitale: "Soltanto nel 2020, si è registrata una crescita del 47%, rispetto al 2019, di cyberattacchi rivolti ai sistemi sanitari all'interno dell'Unione europea".*

3d. Altri esempi di sanità digitale e di interoperabilità

Meritano un accenno anche altri interventi normativi nazionali, che hanno portato all'istituzione di ulteriori strumenti attuativi della c.d. sanità digitale. Anche l'attuazione di questi ultimi ha generato numerose ed importanti riflessioni rispetto al tema della protezione dei dati personali.

Il primo di tali strumenti è il Dossier Sanitario Elettronico o DSE, che contiene la storia clinica di un paziente all'interno di una stessa struttura sanitaria ed è finalizzato a fornire un miglior servizio di cura e ad ottimizzare i percorsi di diagnosi e di cura. Il *dossier* include solo le informazioni cliniche derivanti dagli accessi del paziente nella struttura sanitaria che utilizza lo stesso e non anche quelle relative agli accessi effettuati presso altre strutture pubbliche e private. La sua costituzione da parte della singola struttura sanitaria richiede lo specifico consenso dell'interessato. Un consenso aggiuntivo, autonomo e specifico è altresì richiesto, e specificato nell'informativa privacy, in riferimento a taluni dati, quali HIV, dipendenza da sostanze stupefacenti e/o alcool, atti di violenza sessuale o pedofilia[79]. Per il resto, la regolamentazione del dossier sanitario elettronico non è dissimile da quella del FSE. Il potenziale di tale strumento è stato, tra l'altro, sicuramente ridimensionato alla luce della facoltà, introdotta dal citato D.L. "Rilancio" n. 34/2020, in capo alle strutture sanitarie di alimentare direttamente il FSE del paziente.

Vi è, poi, la cartella clinica elettronica o fascicolo di ricovero, detta anche EMR (*electronic medical record*) o anche EPR (*electronic patient record*)[80] e disciplinata dall'art. 47-*bis* c. 1-*bis* del D.L. 9 febbraio 2012, n. 5 recante "*Disposizioni urgenti in materia di semplificazione e di sviluppo*", convertito con modificazioni dalla legge 4 aprile 2012 n. 35 recante, a sua volta, *"Semplificazione in materia di sanità digitale".* Tale strumento è stato definito dal Ministero della Sanità nel 1992[81] come un *"insieme di documenti che registrano un complesso eterogeneo di informazioni sanitarie, anagrafiche, sociali, aventi lo scopo di rilevare il percorso diagnostico-terapeutico di un paziente al fine di predisporre gli opportuni interventi sanitari e di poter effettuare indagini statistiche, scientifiche e medico-*

[79] *Cfr. "Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario*"- Autorità Garante per la Protezione dei dati personali - 16 luglio 2009.
[80] EMR è espressione di derivazione soprattutto statunitense. EPR, invece, proviene dall'esperienza del Regno Unito. Sono considerate espressioni grosso modo equivalenti.
[81] *Cfr. "Linee guida. La compilazione, la codifica e la gestione della scheda di dimissione ospedaliera istituita ex d.m. 28.12.1991"* – 17 giugno 1992 – Ministero della Sanità.

legali. È uno strumento informativo individuale finalizzato a rilevare tutte le informazioni anagrafiche e cliniche significative relative ad un paziente e ad un singolo episodio di ricovero". La cartella clinica, pertanto, differisce rispetto sia al FSE sia al DSE, in quanto contiene documentazione che si riferisce ad un unico e singolo episodio clinico, dal momento del ricovero a quello della dimissione. Dalla definizione esposta traspare una pluralità di finalità, che non sono soltanto di cura, ma anche di ricerca scientifica, statistica e di tutela dell'operato professionale. È evidente come, se correttamente gestita, la cartella clinica contribuisca ad integrare armoniosamente l'agire dei molteplici attori coinvolti nel processo assistenziale e ad accrescere la sicurezza del paziente, permettendo di assumere decisioni basate su aggiornati e puntuali riscontri documentali[82].

Il medico redige la cartella clinica, quale documento essenziale dell'evento ricovero, con completezza, chiarezza e diligenza, tutelandone anche la riservatezza, ed eventuali correzioni riportate devono essere da lui motivate e sottoscritte. L'operatore sanitario, inoltre, registra all'interno della cartella clinica i modi, i tempi dell'informazione ed i termini del consenso o dissenso della persona assistita o del suo rappresentante legale, anche relativamente al trattamento dei dati sensibili[83]. L'art. 92 del Codice Privacy novellato, poi, prevede la necessità di adottare opportuni accorgimenti al fine di assicurare la comprensibilità dei dati e di distinguere i dati relativi al paziente da quelli eventualmente riguardanti altri interessati, ivi comprese informazioni relative a nascituri. Il fascicolo di ricovero può articolarsi in sottofascicoli e questi ultimi in inserti, in caso di ricoveri protratti o con copiosa messe di documenti costitutivi. Un'articolazione in sottofascicoli potrebbe, inoltre, correlarsi a singoli *setting* assistenziali, in caso di trasferimenti interni. La generazione di un sottofascicolo può, infine, essere funzionale alla gestione riservata di taluni dati personali, in modo da facilitare il rispetto dei vincoli normativi per l'accesso a tali informazioni[84]. Si potrebbe, ad esempio, dare vita ad un sottofascicolo contenente solamente i dati della persona assistita che siano assoggettati ad una protezione rafforzata, quali i dati genetici. In questo modo, infatti, in caso di istanza di accesso agli atti, sarebbe possibile

[82] La Regione Lombardia ha riconosciuto che tale documento rappresenti un momento cruciale dell'attività di assistenza e, fin dal 2001, ha voluto fornire un contributo di riflessione ed indirizzo attraverso la redazione del "*Manuale della Cartella Clinica*". Il decorso del tempo, con i mutamenti normativi ed organizzativi intervenuti, ha consigliato una revisione del suddetto Manuale nel 2007. Il nuovo Manuale si pone come atto di indirizzo per una corretta gestione del documento "cartella clinica" per tutti gli ospedali, pubblici e privati accreditati della Regione Lombardia. Con DGR n. XI/2393 del 11.11.2019 "*Approvazione del Manuale del Fascicolo di ricovero 3A Edizione – 2019*", infine, la Giunta ha approvato un documento tecnico che rappresenta un'evoluzione coerente e coordinata dei manuali precedenti dedicati alla cartella clinica e fornisce raccomandazioni operative attinenti alla gestione della stessa.
[83] cfr. "*Codice di deontologia medica*", art. 26.
[84] V. *infra* § IV.

esibire solamente la parte di documentazione effettivamente necessaria e non l'intero fascicolo contenente indistintamente tutte le tipologie di dati.

Ogni file prodotto ed inserito all'interno della cartella clinica elettronica deve essere firmato digitalmente da personale che abbia veste di pubblico ufficiale, quale attestazione di conformità della copia all'originale da cui è tratto. La Suprema Corte si è ripetutamente espressa per una qualificazione del fascicolo di ricovero come atto pubblico, sostenendo quanto segue: "*la cartella clinica redatta da un medico di un ospedale pubblico è caratterizzata dalla produttività di effetti incidenti su situazioni giuridiche soggettive di rilevanza pubblicistica, nonché dalla documentazione di attività compiute dal pubblico ufficiale che ne assume la paternità*[85]*"*. Tuttavia, la cartella clinica, anzitutto, ha valore probatorio di atto pubblico solo per i fatti che il pubblico ufficiale attesti essersi verificati in sua presenza e da lui compiuti, ai sensi dell'art. 2700 del codice civile. Al contrario, tale documentazione non ha valore probatoria anche in riferimento alla valutazione fatta di detti eventi da parte del pubblico ufficiale e per gli effetti ulteriori degli stessi, in quanto tali elementi rimangono oggetto di accertamento, con ogni mezzo di prova, da parte del giudice[86]. In ogni caso la cartella clinica non fa piena prova a favore di chi l'abbia redatta, neanche per i fatti ivi indicati come compiuti alla presenza del pubblico ufficiale o direttamente da questi, allorché venga messa in discussione la sua responsabilità. Il presupposto del carattere vincolante dell'atto pubblico è, infatti, la terzietà del pubblico ufficiale nella sua funzione certificante con effetti probatori[87]. Tuttavia, tale requisito non può sussistere allorché si ponga in discussione la responsabilità della persona medesima che ha redatto l'atto, non essendo concepibile che quest'ultima sia la fonte di una prova a suo favore con carattere vincolante. In definitiva, quindi, seguendo questa corrente interpretativa, si configurerebbe atto pubblico, facente fede fino a querela di falso, la documentazione contenuta all'interno del fascicolo di ricovero recante dati oggettivi, dei quali il sanitario abbia avuto diretta conoscenza o che abbia posto in essere. Costituirebbe, invece, mera attestazione che crea certezze solo notiziali, superabili attraverso la semplice prova contraria, la restante parte della documentazione.

Infine, l'applicativo informatico che viene scelto dal titolare del trattamento dei dati per la gestione della cartella clinica elettronica deve aderire a standard internazionali in termini

[85] Cass. Pen. Sez. V, n. 1098/1997 e, in analogia: Cass. Pen. Sez. V, n. 23324/2004; Cass. Pen. Sez. V, n.13989/2004; Cass. Pen. Sez. V, n. 35167/2005.
[86] Cass. Civ. n. 12189/1992.
[87] *Cfr*. Cass. 18.9.1980, n. 5296.

funzionali, sintattici e semantici. A tal proposito, il CEN EN 12967 "*Health Informatics Service Architecture (HISA)"* è considerato lo standard di riferimento europeo. HISA è una specifica architettura unificata ed integrata, basata su un *middleware* di servizi informativi indipendenti da applicazioni o tecnologie proprietarie ed in grado di integrare, attraverso modelli di *mapping* e *standard* di comunicazione, i flussi di dati e le funzionalità comuni. Per quanto riguarda, invece, gli *standard* funzionali, l'"*Electronic Health Record System*" è il punto di riferimento per la definizione delle funzionalità che devono essere presenti nella cartella clinica elettronica[88]. In termini di *standard* semantici, poi, si fa riferimento agli *standard Eurorec* ed alle componenti di semantica clinica, come ad esempio SNOMED CT. Infine, per gli *standard* sintattici è utile considerare DICOM (*Digital Imaging and COmmunications in Medicine*), che definisce i criteri per la comunicazione, la visualizzazione, l'archiviazione e la stampa di informazioni ed immagini di tipo biomedico[89].

Il terzo ed ultimo strumento che integra la sanità digitale è costituito dalla refertazione *online*. Questa deve essere intesa come l'attività volta a rendere disponibile al paziente il referto tramite connessione *internet* ed è considerata meramente aggiuntiva, e non sostitutiva, di quella tradizionale resa in forma cartacea. Il referto *online* deve essere firmato digitalmente dal medico che lo ha formato, parallelamente a quanto avviene con la sottoscrizione della sua versione cartacea, e tale requisito deve essere preso in considerazione rispetto al sistema informatico che venga scelto al fine di gestire tale attività digitale. Anche in riferimento alla refertazione *online* è necessario che il paziente esprima il suo consenso, sempre revocabile, sulla base di un'informativa privacy specifica. Il consenso del cittadino, quindi, in questo caso viene richiesto in relazione alla modalità digitale di consegna del referto[90]. A tal proposito, risulta importante sottolineare come si tratti, in questo caso, di un consenso che può essere reso in ogni tempo selettivo. L'avere espresso consenso

[88]L'insieme di tali funzionalità viene raggruppato in:
- *Direct Care*: funzioni che influiscono direttamente sull'erogazione del servizio di cura;
- *Supportive*: caratteristiche che impattano indirettamente sul servizio clinico, come le funzioni gestionali, e servono come *input* agli altri sistemi informativi dell'ospedale (amministrazione, controllo di gestione, ...).
- *Information Infrastructure*: funzionalità che non riguardano l'attività di cura, ma sono infrastrutturali (es. sicurezza e *privacy* del paziente, efficienza del servizio ed interoperabilità fra diversi moduli o sistemi, ...).

[89] Cfr. "*Manuale del Fascicolo di Ricovero"* 3a edizione rev.01 2021, approvato dalla Giunta di Regione Lombardia con DGR n. XI/4298 del 15.02.2021; "*Linee guida Regionali per la Cartella Clinica Elettronica Aziendale*" del 19.02.2012 – Regione Lombardia.

[90] *cfr*. art. 5 D.P.C.M. 8 agosto 2013, "*Modalità di consegna, da parte delle Aziende sanitarie, dei referti medici tramite web, posta elettronica certificata e altre modalità digitali, nonché' di effettuazione del pagamento online delle prestazioni erogate, ai sensi dell'articolo 6, comma 2, lettera d), numeri 1) e 2) del decreto-legge 13 maggio 2011, n.70, convertito, con modificazioni, dalla legge 12 luglio 2011, n. 106, recante "Semestre europeo - prime disposizioni urgenti per l'economia".*

al servizio di refertazione *online*, cioè, non preclude all'interessato di escludere da una siffatta refertazione singoli esami clinici.

La normativa in materia prevede che i referti *online* siano resi disponibili all'interessato secondo due modalità: consultazione da parte del paziente tramite servizi *web* accessibili da *internet* oppure invio del referto allo stesso tramite posta elettronica. Nel primo caso, il paziente ha la possibilità di collegarsi al sito *internet* della struttura sanitaria che ha eseguito l'esame clinico, al fine di effettuare la copia locale (*download*) o la visualizzazione interattiva del referto. Ciò richiede l'adozione di specifiche cautele[91]: utilizzo di protocolli di comunicazione sicuri, basati su *standard* crittografici per la comunicazione elettronica dei dati, con la certificazione digitale dell'identità dei sistemi che erogano il servizio in rete (*protocolli https ssl – Secure Socket Layer*); tecniche idonee ad evitare la possibile acquisizione delle informazioni contenute nel file elettronico, nel caso di sua memorizzazione intermedia in sistemi di *caching*, locali o centralizzati, a seguito della sua consultazione *online*; utilizzo di idonei sistemi di autenticazione dell'interessato attraverso ordinarie credenziali o, preferibilmente, tramite procedure di *strong authentication*; disponibilità limitata nel tempo del referto *online* (massimo 30 gg.); possibilità da parte dell'utente di sottrarre i referti che lo riguardano alla visibilità in modalità *online* o di cancellare gli stessi dal sistema di consultazione, in modo complessivo o selettivo. La seconda modalità di consultazione, invece, prevede che il referto venga spedito in forma di allegato ad un messaggio *e-mail* e non come testo compreso nella *body part* del messaggio. Per l'apertura del file deve essere previsto l'utilizzo di una password o di una chiave crittografica, che vengono rese note all'interessato tramite canali di comunicazione differenti da quelli utilizzati per la spedizione dei referti. Può essere, infine, previsto anche un sistema di convalida degli indirizzi *e-mail*, tramite apposita procedura di verifica *online*, in modo da evitare la spedizione di documenti elettronici, pur protetti con tecniche di cifratura, verso soggetti diversi dall'utente richiedente il servizio.

Infine, l'archiviazione dei referti *online* è espressamente assoggettata dal Garante alla medesima disciplina del *dossier* sanitario elettronico o del FSE[92], cui, pertanto, si rimanda.

[91] Le misure di sicurezza, sia per la consultazione online dei referti sia per il loro invio tramite posta elettronica, sono individuate dall'Autorità Garante per la protezione dei dati personali ne "*Linee guida in tema di referti on-line*" - 25 giugno 2009.

[92] "*Linee guida in tema di referti on-line"* - 19 novembre 2009 – Autorità Garante per la protezione dei dati personali.

IV. DIRITTO DI ACCESSO AGLI ATTI

4 a. Le differenti tipologie di diritto di accesso

Come già accennato precedentemente[93], l'organizzazione della documentazione amministrativa all'interno di un corretto, semplice ed intuitivo sistema di archivio e di conservazione è presupposto logico per l'evasione entro i termini di legge o, comunque, in tempi brevi delle istanze di accesso agli atti.

La legge n. 241/1990, recante "*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi",* disciplina in maniera specifica il diritto di accesso ai documenti amministrativi. Tale istituto, attese le sue rilevanti finalità di pubblico interesse, costituisce principio generale dell'attività amministrativa al fine di favorire la partecipazione e di assicurarne l'imparzialità e la trasparenza. Quest'ultimo principio, infatti, impone alla Pubblica Amministrazione l'obbligo di assicurare la visibilità, la conoscibilità e la comprensibilità delle modalità operative e degli assetti strutturali con cui opera nell'assolvimento dei suoi compiti. Pertanto, pur nel rispetto delle disposizioni in materia di segreto di Stato, di segreto d'ufficio e di protezione dei dati personali, il principio di trasparenza amministrativa concorre ad attuare il principio democratico ed i principi costituzionali di eguaglianza, buon andamento, nonché di efficacia ed efficienza nell'utilizzo di risorse pubbliche da parte della Pubblica Amministrazione.

Il diritto di accesso viene definito dall'art. 22 della legge n. 241/1990 come "*il diritto degli interessati di prendere visione e di estrarre copia di documenti amministrativi"*. Gli interessati, a loro volta, sono definiti dalla medesima disposizione come tutti i soggetti privati, compresi quelli portatori di interessi pubblici o diffusi, che abbiano un interesse corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso. L'interesse vantato dal richiedente deve essere diretto, cioè appartenente alla sua sfera personale e non ad altri soggetti; concreto, in quanto deve esistere un collegamento fra il richiedente ed un bene concreto della vita coinvolto nel documento; attuale, in quanto deve ricorrere un interesse attualmente esistente e necessitante di un'eventuale tutela. Ne deriva che, ai sensi della legge n. 241/1990, non siano ammissibili istanze di accesso preordinate ad un controllo generalizzato dell'operato delle pubbliche

[93] *Cfr.* § 3b.

amministrazioni. L'interesse connesso all'oggetto della richiesta, infatti, deve anche essere specificato e, ove occorra, comprovato dallo stesso interessato, in quanto l'istanza di accesso ai documenti amministrativi deve essere necessariamente motivata. Il diritto di accesso può essere esercitato nei confronti delle pubbliche amministrazioni, delle aziende autonome e speciali, degli enti pubblici e dei gestori di pubblici servizi.

Oggetto del diritto di accesso sono tutti i documenti amministrativi di una Pubblica Amministrazione. Conseguentemente, la richiesta deve essere rivolta all'ente che abbia formato il documento o che lo detenga stabilmente, fino a quando sussista un obbligo in tal senso. Le modalità di presentazione dell'istanza di accesso agli atti sono state disciplinate, successivamente all'entrata in vigore della L. 241/1990, con il D.P.R. 12 aprile 2006 n. 184 "*Regolamento recante disciplina in materia di accesso ai documenti amministrativi*". Tale normativa, all'art. 5, prevede che il diritto di accesso possa essere esercitato in via informale mediante istanza, anche verbale, qualora in base alla natura del documento richiesto non risulti l'esistenza di controinteressati[94]. In caso contrario, la Pubblica Amministrazione è tenuta ad invitare l'interessato a presentare richiesta formale di accesso. In tal caso la Pubblica Amministrazione è tenuta ad informarne i controinteressati individuati, mediante invio di copia tramite raccomandata con avviso di ricevimento o per via telematica, per coloro che abbiano consentito tale forma di notifica. Entro dieci giorni dalla ricezione di tale comunicazione, i controinteressati possono presentare una motivata opposizione, anche per via telematica, alla richiesta di accesso. Decorso inutilmente tale termine, invece, la Pubblica Amministrazione potrà provvedere in merito all'istanza dell'interessato. Quest'ultima, inoltre, deve essere presentata in via formale anche nel caso in cui sorgano dubbi sulla legittimazione del richiedente, sulla sua identità, sui suoi poteri rappresentativi, sulla sussistenza dell'interesse alla stregua delle informazioni e delle documentazioni fornite o sull'accessibilità del documento. Le Pubbliche Amministrazioni, infine, sono tenute ad assicurare che il diritto d'accesso possa essere esercitato anche per via telematica.

In caso di richiesta sia formale sia informale, l'interessato deve indicare gli estremi del documento oggetto della stessa, ovvero gli elementi che ne consentano l'individuazione, e deve dimostrare la propria identità. Egli, inoltre, come precedentemente accennato, deve specificare e, ove occorra, comprovare l'interesse connesso all'oggetto della richiesta.

[94] L'art. 22 c.1 lett. c) della L. 241/1990 definisce i controinteressati come "*tutti i soggetti, individuati o facilmente individuabili in base alla natura del documento richiesto, che dall'esercizio dell'accesso vedrebbero compromesso il loro diritto alla riservatezza".*

L’istanza di acceso agli atti deve essere evasa in un termine massimo di trenta giorni, decorrenti dalla richiesta stessa. Ove quest’ultima risulti irregolare o incompleta, l'amministrazione, entro dieci giorni, ne dà comunicazione al richiedente tramite raccomandata con avviso di ricevimento ovvero con altro mezzo idoneo a comprovarne la ricezione. In tale caso, il termine del procedimento ricomincia a decorrere dalla presentazione della richiesta corretta. Trascorso inutilmente il termine dei trenta giorni, invece, l’istanza è da intendersi respinta ed in questo caso si parla del c.d. silenzio-diniego[95]. La richiesta viene evasa mediante indicazione della pubblicazione contenente le notizie richieste oppure mediante l’esibizione del documento, l’estrazione di copie dello stesso, ovvero mediante altra modalità idonea. L'accoglimento dell’istanza di accesso a un documento comporta anche la facoltà di prendere visione o estrarre copia degli altri atti nello stesso richiamati ed appartenenti al medesimo procedimento, fatte salve le eccezioni previste dalla legge.

L’esercizio del diritto di accesso da parte dell’interessato non può essere negato ove sia sufficiente fare ricorso al potere di differimento. Alla Pubblica Amministrazione è, infatti, possibile differire l’accesso agli atti nei casi in cui ciò sia sufficiente per assicurare una temporanea tutela ad interessi quale la sicurezza, la difesa, l’esercizio della sovranità nazionale e la correttezza delle relazioni internazionali. Il differimento è, inoltre, possibile nei casi in cui sia utile a salvaguardare specifiche esigenze dell'amministrazione, specie nella fase preparatoria dei provvedimenti, in relazione a documenti la cui conoscenza possa compromettere il buon andamento dell'azione amministrativa. L'atto che dispone il differimento dell'accesso deve indicarne anche la durata. L’art. 24 c.1 della legge 241/1990, comunque, prevede alcuni casi tassativi di divieto di accesso:

a) nei confronti di documenti coperti da segreto di Stato, ai sensi della legge 24 ottobre 1977 n. 80 e successive modificazioni, e nei casi di segreto o di divieto di divulgazione espressamente previsti dalla legge;

[95] Il silenzio della Pubblica Amministrazione costituisce un comportamento omissivo dell’amministrazione di fronte a un dovere di provvedere, di emanare un atto e di concludere il procedimento con l’adozione di un provvedimento entro un termine prestabilito, ai sensi degli artt. 2 co. 1, 5, e 20 della legge n. 241/1990. In tali casi di silenzio significativo, la norma qualifica il comportamento inerte dell’amministrazione come equivalente ad un provvedimento a contenuto positivo (c.d. silenzio accoglimento) o negativo (c.d. silenzio diniego). Pertanto, nel caso di silenzio diniego, decorso inutilmente un determinato periodo di tempo, la normativa prevede che il silenzio della P.A. equivale ad un provvedimento di diniego dell’istanza proposta.

b) nei confronti di procedimenti tributari, per i quali restano ferme le particolari norme che li regolano;
c) nei confronti dell'attività della Pubblica Amministrazione diretta all'emanazione di atti normativi, amministrativi generali, di pianificazione e di programmazione, per i quali restano ferme le particolari norme che ne regolano la formazione;
d) in riferimento ai procedimenti selettivi, nei confronti dei documenti amministrativi contenenti informazioni di carattere psico-attitudinale relativi a terzi.

Il differimento, la limitazione ed il rifiuto dell'accesso, nei soli casi espressamente previsti dal citato art. 24, devono essere sempre adeguatamente motivati.

In caso di diniego dell'accesso, espresso o tacito, o di differimento dello stesso nei casi su citati, il richiedente può presentare ricorso al Tribunale Amministrativo Regionale (TAR). Nei confronti degli atti delle amministrazioni comunali, provinciali e regionali, l'interessato può rivolgersi al Difensore Civico[96] competente per ambito territoriale, ove costituito, al fine di ottenere un riesame della determinazione di diniego o differimento. Qualora tale organo non sia stato istituito, la competenza è attribuita al Difensore Civico competente per l'ambito territoriale immediatamente superiore. Nei confronti degli atti delle amministrazioni centrali e periferiche dello Stato, invece, la richiesta di riesame può essere inoltrata alla Commissione per l'accesso ai documenti amministrativi[97] nonché all'amministrazione resistente. Il

[96] La figura del Difensore Civico, che era già prevista da numerose leggi regionali, è stata generalizzata dalla legge 8 giugno 1990 n. 142, recante *"Nuovo ordinamento delle autonomie locali"*, e da ultimo dalla legge 15 maggio 1997 n. 127, recante *"Misure urgenti per lo snellimento dell'attività amministrativa e dei procedimenti di decisione e controllo"*, che ne ha esteso le competenze anche alle amministrazioni periferiche dello Stato, ad eccezione di quelle competenti in materia di difesa, sicurezza pubblica e giustizia. L'art. 111 della legge 8 giugno 1990 n. 142 così recita: "*la legge può istituire l'ufficio del Difensore civico quale organo di garanzia nei rapporti tra il cittadino e la pubblica amministrazione. non è un giudice che emette sentenze, né irroga sanzioni o pene"*. In base alla legge. n. 142/1990, il Difensore civico svolge un ruolo di garante dell'imparzialità e del buon andamento della Pubblica Amministrazione, segnalando, anche di propria iniziativa, abusi, disfunzioni, carenze e ritardi delle amministrazioni nei confronti dei cittadini ed esercita le sue funzioni in piena autonomia ed indipendenza. Su tutto ciò che riguarda i principi di legalità, buon andamento ed imparzialità della pubblica amministrazione, infatti, il Difensore può acquisire informazioni, sentire i funzionari e compiere verifiche. Tenta cioè, con la mediazione ed in forma persuasiva, di sanare conflitti prevenendo il ricorso alla Giustizia Amministrativa. Il principio di azione di fondo del Difensore Civico è l'imparzialità, caratteristica indispensabile per poter garantire la mediazione fra cittadino e Pubblica Amministrazione. Il cittadino può accettare il giudizio formulato dal Difensore Civico oppure può rivolgersi alla Giustizia Amministrativa. Oggi la maggioranza delle Regioni si è dotata di un proprio Difensore Civico, come pure molte Province ed una parte significativa dei Comuni e nei loro statuti sono fissate le modalità di elezione della sua elezione, la durata della carica e le funzioni attribuite.

[97] Tale Commissione è disciplinata dall'art. 27 della legge n. 241/1990, è istituita presso la Presidenza del Consiglio dei Ministri ed è nominata con D.P.C.M., sentito il Consiglio dei Ministri. La Commissione è presieduta dal sottosegretario di Stato alla Presidenza del Consiglio dei Ministri ed è composta da dieci membri, dei quali due senatori e due deputati, designati dai Presidenti delle rispettive Camere, quattro scelti fra il

Difensore Civico o la suddetta Commissione si pronunciano entro trenta giorni dalla presentazione dell'istanza. Scaduto infruttuosamente tale termine, il ricorso si intende respinto. Se questi due organi ritengono illegittimo il diniego o il differimento, ne informano il richiedente e lo comunicano all'Autorità disponente. Se quest'ultima non emana il provvedimento confermativo motivato entro trenta giorni dal ricevimento della suddetta comunicazione, l'accesso è consentito. Se l'accesso è negato o differito per motivi relativi alla protezione dei dati personali di terzi, la Commissione, prima di provvedere, deve sentire l'Autorità Garante per la Protezione dei dati personali, che deve pronunciarsi entro dieci giorni dalla richiesta, durante i quali il termine per la pronuncia da parte della Commissione è sospeso. Decorsi inutilmente tali dieci giorni, il parere si intende reso. In ogni caso, le controversie relative all'accesso ai documenti amministrativi sono disciplinate dal Codice del processo amministrativo, approvato con il D.Lgs. 2 luglio 2010 n. 104 e successive modificazioni[98].

Successivamente, con l'emanazione del D.Lgs. 14 marzo 2013 n. 33, recante "*Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni",* al diritto di accesso ai documenti amministrativi, disciplinato dalla legge n. 241/1990 si affianca il c.d. accesso civico. Quest'ultimo istituto consente a chiunque di accedere a dati, documenti ed informazioni delle Pubbliche Amministrazioni, senza necessità di comprovare un interesse qualificato. Il D.Lgs. n. 33/2013, inoltre, a seguito delle modifiche apportate con il D.Lgs. n. 97/2016, recante "*Revisione e semplificazione delle disposizioni in materia di*

personale di cui alla legge 2 aprile 1979 n. 97, anche in quiescenza, su designazione dei rispettivi organi di autogoverno, ed uno scelto fra i professori di ruolo in materie giuridiche. È membro di diritto della Commissione il capo della struttura della Presidenza del Consiglio dei Ministri che costituisce il supporto organizzativo per il funzionamento di tale organo. Quest'ultima può avvalersi di un numero di esperti non superiore a cinque unità e delibera a maggioranza dei presenti. L'assenza dei componenti per tre sedute consecutive ne determina la decadenza. La Commissione è rinnovata ogni tre anni. Per i membri parlamentari si procede a nuova nomina in caso di scadenza o scioglimento anticipato delle Camere nel corso del triennio. La Commissione vigila affinché sia attuato il principio di piena conoscibilità dell'attività della Pubblica Amministrazione, con il rispetto dei limiti fissati dalla presente legge; redige una relazione annuale sulla trasparenza dell'attività della Pubblica amministrazione, che comunica alle Camere ed al Presidente del Consiglio dei Ministri; propone al Governo modifiche dei testi legislativi e regolamentari, che siano utili a realizzare la più ampia garanzia del diritto di accesso.

[98] Le modifiche sono stata apportate, da ultimo, con il D.L. 27 gennaio 2022 n. 4, "*Misure urgenti in materia di sostegno alle imprese e agli operatori economici, di lavoro, salute e servizi territoriali, connesse all'emergenza da COVID-19, nonché' per il contenimento degli effetti degli aumenti dei prezzi nel settore elettrico*" e convertito, con modificazioni, dalla L. 28 marzo 2022 n. 25.

prevenzione della corruzione, pubblicità e trasparenza, correttivo della legge 6 novembre 2012, n. 190 e del decreto legislativo 14 marzo 2013, n. 33, ai sensi dell'articolo 7 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche"[99], disciplina due tipologie di accesso civico, uno semplice ed uno generalizzato. Il primo consente a chiunque di richiedere documenti, dati o informazioni che le amministrazioni hanno l'obbligo di rendere visibili nella sezione "*amministrazione trasparente*" dei propri siti istituzionali, nei casi in cui gli stessi non siano stati pubblicati. Il secondo, invece, disciplina il diritto di chiunque di richiedere dati e documenti, ulteriori rispetto a quelli che le amministrazioni sono obbligate a pubblicare, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico, nel rispetto, comunque, dei limiti relativi alla tutela di interessi giuridicamente rilevanti. In caso di rifiuto totale o parziale dell'accesso civico o di mancata risposta entro trenta giorni dalla presentazione dell'istanza, il richiedente può presentare domanda di riesame al Responsabile della prevenzione della corruzione e della trasparenza, che decide con provvedimento motivato entro il termine di venti giorni. La decisione dell'amministrazione sulla richiesta ed il provvedimento del Responsabile della trasparenza possono essere impugnate davanti al Tribunale Amministrativo Regionale, ai sensi dell'art. 116 del Codice del processo amministrativo. Per tutti gli altri profili, la disciplina dell'accesso civico riprende quella, su esposta, del diritto di accesso agli atti amministrativi.

Da quanto esposto, risulta evidente come l'accesso civico, sia esso semplice o generalizzato, abbia caratteristiche differenti rispetto al diritto di accesso agli atti amministrativi, disciplinato dalla legge n. 241/1990. Per tale motivo, i due istituti si affiancano e coesistono, senza che l'uno sostituisca l'altro. Ai sensi del D.Lgs. n. 33/2013, infatti, legittimato non è solamente un soggetto che dimostri di avere un interesse qualificato rispetto alla documentazione di cui si richiede la presa visione, ma lo è qualunque cittadino. In secondo luogo, è espressamente previsto dal D.Lgs. n. 33/2013 che in particolare l'accesso

[99] Il D.Lgs. 97/2016, infatti, ha modificato l'art. 5 del D.Lgs. 33/2013 e vi ha introdotto l'art. 5-*bis*, che disciplina, appunto, l'accesso civico generalizzato. Quest'ultimo è conosciuto anche come "*accesso FOIA*", in quanto ispirato al "*Freedom Of Information Act*" di origine statunitense. Il Freedom of Information Act (FOIA), diffuso in oltre 100 paesi al mondo,è la normativa che garantisce a chiunque il diritto di accesso alle informazioni detenute dalle pubbliche amministrazioni, salvo i limiti a tutela degli interessi pubblici e privati stabiliti dalla legge. L'obiettivo del FOIA è dunque promuovere una maggiore trasparenza nel rapporto tra le istituzioni e la società civile e incoraggiare un dibattito pubblico informato su temi di interesse collettivo. Giornalisti, organizzazioni non governative, imprese, cittadini italiani e stranieri possono richiedere dati e documenti, così da svolgere un ruolo attivo di controllo sulle attività delle pubbliche amministrazioni.

generalizzato possa avere una finalità di controllo diffuso ed astratto sullo svolgimento dell'attività amministrativa, che, invece, è espressamente vietata dalla legge n. 241/1990. I due istituti hanno, comunque, in comune la finalità primaria della trasparenza amministrativa.

Infine, anche il Regolamento UE n. 2016/679 prevede all'art. 15 una disciplina del diritto di accesso, che può essere esercitato secondo due forme. L'interessato ha, infatti, prima di tutto, *"il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano";* in secondo luogo, qualora ne venga dato riscontro positivo, l'interessato avrà eventualmente il diritto *"di ottenere l'accesso ai dati personali e alle seguenti informazioni:*

a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un'autorità di controllo;
g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento".

L'interessato, legittimato all'esercizio di tale diritto è una persona fisica identificata o identificabile, direttamente o indirettamente, attraverso i dati trattati, quali possono essere il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online oppure uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica,

psichica, economica, culturale o sociale[100]. In ambito sanitario, pertanto, l'interessato è rappresentato sicuramente dal paziente o da persone da lui esplicitamente delegate. Qualora, però, questi non sia capace di intendere e di volere, il diritto in argomento può essere esercitato per il tramite degli esercenti la potestà o la tutela. Qualora, invece, il paziente sia minorenne oppure di maggiore età ma incapace di intendere o volere, legittimato all'accesso sarà l'amministratore di sostegno, se tale compito rientra tra quelli assegnatigli dal giudice tutelare. In caso di decesso del paziente, invece, il diritto di accesso può essere esercitato, ciascuno per proprio conto, dagli eredi legittimi[101] nonché dagli eredi testamentari che provino la loro posizione con dichiarazione sostitutiva di atto di notorietà, in quanto va rispettata in ogni caso la volontà del defunto quando risulti espressa in forma scritta. Gli eredi, comunque, devono essere portatori di un interesse proprio o devono agire a tutela dell'interessato-*de cuius* o per ragioni familiari meritevoli di protezione[102].

Anche ai fini dell'esercizio del diritto di accesso ai sensi dell'art. 15 del Regolamento UE n. 2016/679, l'istanza può essere avanzata sia in forma cartacea sia in via telematica. Nel primo caso, il titolare del trattamento fornirà al richiedente una copia dei dati personali oggetto di trattamento. Nel secondo caso, invece, salvo indicazione diversa dell'interessato, le informazioni verranno fornite in un formato elettronico di uso comune.

4 b. Diritto di accesso avente ad oggetto la documentazione sanitaria

Ai sensi della normativa analizzata in materia, oggetto del diritto di accesso sono atti e documenti detenuti dalle Pubbliche Amministrazioni. In particolare, ai sensi dell'art. 22 c. 1

[100] Definizione fornita dall'art. 4, par. 1 n. 1 del Regolamento UE n. 2016/679.

[101] Ai sensi dell'art. 565 del codice civile qualifica come successori legittimi nel seguente ordine: il coniuge, i discendenti, gli ascendenti, i collaterali e gli altri parenti.

[102] A tal proposito il D.Lgs. 101/2018 introduce, all'art. 2-*terdecies*, una significativa novità. Viene riconosciuto, infatti, all'interessato un potere di "veto" o di divieto rispetto all'esercizio *post mortem* dei suoi diritti privacy da parte di terzi soggetti a ciò legittimati. Sostanzialmente tale diritto di veto ha un contenuto esattamente opposto rispetto alle pretese di questi ultimi e vale a neutralizzarle. La volontà di veto dell'interessato deve risultare in modo non equivoco, specifico e da dichiarazione scritta da presentare al titolare del trattamento o a quest'ultimo comunicata. L'esercizio di tale diritto, inoltre, non può avere portata generale, ma è previsto solo limitatamente all'offerta diretta di servizi della società dell'informazione. Tra tali servizi rientrano, ad esempio, i servizi *web* offerti dai motori di ricerca. Non è, quindi, arduo immaginare che un ambito di applicazione tipico riguarderà proprio servizi *web*, quali la casella di posta elettronica, i profili di *social network*, servizi di acquisto *online*. Il divieto non può, in ogni caso, produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato nonché del diritto di difendere in giudizio i propri interessi. Sembra che la *ratio* possa essere ravvisata nell'esigenza di apprestare tutela ad aspetti privatissimi che l'interessato potrebbe desiderare di non esporre *post mortem* all'altrui conoscenza. *Cfr.* "*Codice privacy: tutte le novità del D.lgs. 101/2018*" di L. Bolognini, E. Pellino – Il Civilista – Giuffrè Francis Lefebvre S.P.A, 2019.

lett. d) della legge n. 241/1990, costituisce documento amministrativo "*ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale".* In virtù di tale definizione, ci si potrebbe chiedere se anche la documentazione sanitaria, analizzata nei paragrafi precedenti, possa costituire oggetto di accesso. A tal proposito, risulta utile citare l'interpretazione condivisa dal Tar Sicilia – Catania – Sez. IV – con sentenza n. 879 del 7 maggio 2009. Il Giudice Amministrativo, infatti, ha esplicitato come la documentazione sanitaria relativa ad un ricovero ed eventuale intervento chirurgico, con i relativi esami diagnostici, rientri nell'amplissima nozione di "*documento amministrativo*", di cui all'art. 22 c. 1 lett. d) della legge n. 241/1990. Si tratterebbe, infatti, di atti interni detenuti da una struttura ospedaliera, in relazione ad un'attività di pubblico interesse dalla stessa svolta, quale quella di assicurare al cittadino un'adeguata assistenza sanitaria e, in definitiva, il diritto primario e fondamentale alla salute. Peraltro, proprio perché tale documentazione contiene dati relativi alla salute del cittadino, non può non essere portata a conoscenza del diretto interessato, come previsto dalla legge n. 241/1990.

Riferimenti espliciti alla possibilità che anche la documentazione sanitaria possa essere oggetto del diritto di accesso sono dati anche dalla normativa, oltre che dalla giurisprudenza. A tal proposito, infatti, ad esempio l'art. 92 c. 1 del Codice Privacy novellato disciplina l'accesso alla cartella clinica, prevedendo quanto segue: "*eventuali richieste di presa visione o di rilascio di copia della cartella e dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità:*

a) di esercitare o difendere un diritto in sede giudiziaria, ai sensi dell'articolo 9, paragrafo 2, lettera f), del Regolamento, di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale;

b) di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale".

L'Autorità Garante per la Protezione dei dati personali, poi, con suo provvedimento[103], ha prescritto l'obbligo, e non la facoltà, per un'azienda sanitaria di consentire l'accesso da parte del diretto interessato ad una registrazione effettuata nel corso di un intervento chirurgico svolto in "videolaparoscopia", cui lo stesso si era sottoposto.

Un'ultima conferma proviene anche dal manuale approvato dalla Giunta di Regione Lombardia che disciplina il fascicolo di ricovero[104], il quale prevede che la persona alla quale i dati vi si riferiscano abbia diritto di disporre del suo contenuto, sia nel corso della degenza, a cartella cosiddetta aperta, sia dopo la sua conclusione.

Il citato manuale, inoltre, prevede che il contenuto della documentazione sanitaria debba avere alcune caratteristiche ben precise. Queste ultime, insieme alla modalità di conservazione degli atti, possono essere considerate un altro requisito necessario affinché un'istanza di accesso, soprattutto in ambito sanitario, venga evasa correttamente da parte di una Pubblica Amministrazione. Tali caratteristiche sono: chiarezza, accuratezza, veridicità, attualità, completezza, essenzialità e pertinenza[105]. Il requisito della chiarezza viene richiesto, in primo luogo, in riferimento al contenuto dell'atto. Il testo, infatti, non deve essere passibile di interpretazioni dissonanti e, quindi, devono essere utilizzate espressioni semplici, coerenti e non ampollose. A tal proposito, i regolamenti interni, possono anche prevedere un divieto di ricorso ad abbreviazioni, acronimi o sigle. Viene, però, richiesta chiarezza anche in riferimento alla grafia di chi compila il documento analogico. È essenziale, infatti, che chi scrive tenga presente che la sua traccia è destinata ad essere letta e compresa da altri per assumere decisioni e risolvere problemi. A tal proposito, l'Autorità Garante per la Protezione dei dati personali ha accolto il ricorso nei confronti di un'azienda ospedaliera da parte di un paziente, che aveva chiesto chiarimenti sui dati personali contenuti nella sua cartella clinica ed in risposta aveva ricevuto una copia della stessa, che però, a suo parere, risultava "*illeggibile per la pessima grafia degli autori"*. Pertanto, nonostante la documentazione fosse stata materialmente rilasciata, la richiesta di accesso non poteva

[103] *Cfr*. Provvedimento del 20 settembre 2006.
[104] "*Approvazione del Manuale del Fascicolo di ricovero 3A Edizione – 2019"* - DGR n. XI/2393 del 11.11.2019.
[105] Cfr. "*Approvazione del Manuale del Fascicolo di ricovero 3A Edizione – 2019"*- DGR n. XI/2393 del 11.11.2019.

ritenersi correttamente evasa[106]. La leggibilità dei dati comunicati all'interessato, infatti, è la prima condizione necessaria, ancorché non sufficiente, ai fini della loro piena comprensione. Anche la Corte di Cassazione ha in più occasioni affermato che un'imperfetta compilazione della documentazione di ricovero costituisce inadempimento di un'obbligazione posta in capo all'operatore sanitario, che consiste nel controllo della completezza ed esattezza del contenuto della cartella clinica e dei referti allegati. Tale obbligazione è, inoltre, di tipo strumentale, in quanto il suo adempimento è funzionale all'eventualità di dover provare in giudizio il nesso causale che intercorso tra la condotta e l'evento danno. Ai sensi della recente normativa in materia di responsabilità professionale medica[107], infatti, l'onere di provare sia il l'evento dannoso sia il suddetto nesso causale grava sul paziente. È evidente, però, che, se dall'inadempimento dell'obbligo di corretta compilazione della documentazione sanitaria da parte del medico dovesse derivare l'impossibilità per il paziente e per il Giudice di trarre elementi di valutazione utili ad accertare le cause di un evento lesivo, le conseguenze non potrebbero essere fatte ricadere sul paziente, ad ulteriore danno dello stesso, bensì sul professionista che abbia agito in modo non diligente. La Corte di Cassazione, per di più, ha ritenuto che, qualora dalle indagini la condotta del sanitario risultasse astrattamente idonea a cagionare il danno, l'errore medico verrebbe addirittura presunto[108].

In riferimento al requisito dell'accuratezza, invece, si sottolinea come i contenuti di un documento debbano essere esposti con precisione. Per attualità, invece, si richiede che gli eventi vengano registrati in un tempo quanto più possibile ravvicinato al loro verificarsi. In questo caso, pertanto, l'indicazione temporale di data e ora della registrazione risulta funzionale ad una lettura coerente e consequenziale degli avvenimenti e, quindi, in definitiva ad una migliore comprensione della realtà.

---

[106] "*Le cartelle cliniche devono essere leggibili*" - Autorità Garante per la Protezione dei dati personali – 11 aprile 2003 - *Newsletter Garante;* per un caso analogo si veda anche "*Diritto di accesso - Accesso a dati incomprensibili per la grafia o per l'uso di codici"* - 26 marzo 2001.

[107] La responsabilità professionale medica è stata disciplinata, da ultimo, dalla legge 8 marzo 2017 n. 21 o legge Gelli-Bianco, entrata in vigore l'1 aprile 2017, e recante "*Disposizioni in materia di sicurezza delle cure e della persona assistita, nonché in materia di responsabilità professionale degli esercenti le professioni sanitarie*". Tale legge disciplina fondamentali aspetti del ruolo e delle funzioni del medico, principalmente con l'intento di prevenire il rischio clinico, ridurre il contenzioso sulla responsabilità medica, arginare la fuga delle assicurazioni dal settore sanitario e contenere gli ingenti costi della cosiddetta medicina difensiva.

[108] Cassazione civile, sez. III, ordinanza 23/03/2018 n. 7250; Cass. Civ. III, n. 9290 dell'8.6.2012. Cass. Civ, sez. II, n. 22639 del 8.11.2016.

Infine, l'ultimo requisito dell'essenzialità e pertinenza, richiama il principio di "*minimizzazione dei dati*", sancito dall'art. 5 del Regolamento UE n. 2016/679 ed a cui si è già fatto cenno[109]. In fase di anamnesi medica, ad esempio, con riguardo alla rilevazione degli stili di vita, del contesto familiare, lavorativo e sociale dell'assistito, ci si può chiedere fino a quale punto possa estendersi la raccolta dei dati senza violare il diritto della persona al riserbo sulla sua sfera più privata e, quindi, senza incorrere nel vizio di eccedenza nel trattamento dei dati personali rispetto alle finalità sanitarie da perseguire. Nulla obbliga, infatti, il medico a trascrivere notizie anamnestiche del tutto indifferenti dal punto di vista sanitario, soprattutto qualora queste siano di carattere intimo. In alcune circostanze, però è da ritenere prevalente l'interesse alla tutela della salute piuttosto che della sua riservatezza, come può avvenire, ad esempio, in caso di intossicazione voluttuaria cronica da alcool o da stupefacenti di soggetto ricoverato per altro motivo. In questo caso, infatti, la conoscenza di tali dipendenze può essere fondamentale al fine di individuare la corretta terapia per la cura di un altro problema sanitario.

In tale ultimo ambito, un altro caso di particolare interesse, che è stato analizzato anche dall'Autorità Garante per la Protezione dei dati personali[110], riguarda la raccolta da parte dei sanitari di dati inerenti al credo religioso professato dai parenti ricoverati. Il Garante Privacy ha stabilito che la finalità di assicurare durante la degenza un regime alimentare aderente alla volontà espressa dell'interessato, nonché quella di rispettare le scelte terapeutiche espresse in modo consapevole dallo stesso, quale ad esempio il rifiuto al trattamento trasfusionale, alla luce dei richiamati principi di indispensabilità possano essere utilmente perseguite dalle strutture sanitarie senza raccogliere le informazioni relative alla religione di appartenenza del paziente. A quest'ultimo, pertanto, deve essere consentito di esprimere tali volontà, senza che siano raccolte le eventuali motivazioni religiose che ne sono alla base.

4 c. Il necessario bilanciamento tra diritto di accesso e diritto alla protezione dei dati personali

Tutte le normative richiamate, nel disciplinare il diritto di accesso, rimandano anche alla disciplina della protezione dei dati personali. Così, l'art. 5-*bis* c. 2, lett. a), del D.Lgs. n.

[109] V. *supra* 3 a.
[110] "*Informazioni sulle convinzioni religiose dei pazienti: i casi in cui possono essere raccolte durante il ricovero"* - 12 novembre 2014 – Autorità Garante per la Protezione dei dati personali.

33/2013 prevede che l'accesso civico venga rifiutato qualora il diniego sia necessario per evitare un pregiudizio concreto alla protezione dei dati personali, "*in conformità con la disciplina legislativa in materia*". L'art. 24 c. 7 della L. 241/1990, invece, prevede che, nel caso in cui oggetto del diritto di accesso dovessero essere documenti contenenti dati sensibili, giudiziari o idonei a rivelare lo stato di salute e la vita sessuale, il suo esercizio è consentito nei limiti in cui sia strettamente indispensabile e nei termini previsti dalla normativa in materia di tutela di tali dati. Infine, lo stesso art. 15 del Regolamento UE n. 2016/679 sottolinea che il diritto di ottenere una copia dei dati viene esercitato lecitamente solamente se ciò non comporti una lesione dei diritti e delle libertà altrui.

I riferimenti alla normativa sulla tutela dei dati personali rimandano, in particolare, agli artt. 5 e 86 ed al considerando n. 154 del Regolamento UE n. 2016/679. La prima disposizione, infatti, disciplina i principi applicabili al trattamento dei dati personali, di cui si è già discorso[111] e tra i quali si ricorda quello di liceità, limitazione delle finalità, integrità e correttezza. Tale riferimento è legittimato dal fatto che evadere un'istanza di accesso agli atti costituisce di fatto un trattamento dei dati che vengono, così, comunicati. Pertanto, anche tale attività amministrativa deve rifarsi ai principi citati, che devono essere osservati per qualsiasi tipologia di trattamento.

L'art. 86 del Regolamento, invece, disciplina il trattamento e l'accesso del pubblico a documenti ufficiali, prevedendo, in particolare che "*i dati personali contenuti in documenti ufficiali in possesso di un'autorità pubblica o di un organismo pubblico o privato per l'esecuzione di un compito svolto nell'interesse pubblico possono essere comunicati da tale autorità o organismo conformemente al diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti, al fine di conciliare l'accesso del pubblico ai documenti ufficiali e il diritto alla protezione dei dati personali ai sensi del presente regolamento".*

Il considerando n. 154 del Regolamento UE n. 2016/679, poi, prevede che "*il presente regolamento ammette, nell'applicazione delle sue disposizioni, che si tenga conto del principio del pubblico accesso ai documenti ufficiali. L'accesso del pubblico ai documenti ufficiali può essere considerato di interesse pubblico. I dati personali contenuti in documenti conservati da un'autorità pubblica o da un organismo pubblico dovrebbero poter essere*

[111] V. *supra* § 3 a.

diffusi da detta autorità o organismo se la diffusione è prevista dal diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti. Tali disposizioni legislative dovrebbero conciliare l'accesso del pubblico ai documenti ufficiali e il riutilizzo delle informazioni del settore pubblico con il diritto alla protezione dei dati personali e possono quindi prevedere la necessaria conciliazione con il diritto alla protezione dei dati personali, in conformità del presente regolamento".

Il richiamo espresso alla disciplina legislativa sulla protezione dei dati personali sottolinea come la Pubblica Amministrazione investita di una richiesta di accesso agli atti, prima di evadere quest'ultima, debba verificare se ciò possa arrecare danno in termini di *privacy*. È chiaro come tale interrogativo sussista soprattutto in quei casi in cui il richiedente sia un soggetto diverso rispetto al titolare del diritto alla protezione dei dati. Nel caso in cui l'amministrazione dovesse ritenere sussistente il rischio di un tale pregiudizio, dovrà rigettare l'istanza di accesso, come espressamente previsto anche dalla normativa su richiamata. In alcuni casi, tuttavia, l'amministrazione potrà ritenere opportuno accogliere la richiesta, oscurando i dati personali eventualmente presenti e le altre informazioni che possono consentire l'identificazione, anche indiretta, del soggetto interessato. L'ente destinatario dell'istanza, infatti, in linea generale, dovrebbe scegliere le modalità meno pregiudizievoli per i diritti dell'interessato e quest'ultima opzione prospettata deve essere senz'altro privilegiata quando possibile. Un esempio pratico in cui l'operazione di bilanciamento su esposta ha portato a non penalizzare nessuno dei due diritti in gioco, pur soddisfacendoli entrambi, è presente nella pronuncia dell'Autorità Garante per la Protezione dei dati personali, in merito all'accesso alla registrazione di un intervento chirurgico svolto in "videolaparoscopia"[112]. In questo caso, infatti, il Garante Privacy ha disposto, che venisse messa a disposizione della ricorrente interessata soltanto la partizione di videoregistrazione contenente i dati personali di quest'ultima, previo oscuramento delle immagini relative a soggetti terzi. In questo modo, infatti, sarebbe stato soddisfatto sia il diritto di accesso del paziente sia il diritto alla protezione dei dati personali di tutti gli altri soggetti coinvolti nelle registrazioni.

In riferimento alla valutazione che l'amministrazione destinataria della richiesta di accesso da parte di un terzo è chiamata ad effettuare, si è pronunciata in diverse occasioni il Garante Privacy, precisando che in tali circostanze sia necessario operare un bilanciamento

[112] *Cfr*. Provvedimento del 20 settembre 2006.

tra due diritti, quello di accesso dell'interessato e quello alla protezione dei dati personali. Tale bilanciamento deve essere il frutto di una valutazione concreta e ponderata dei due interessi in gioco. Entrambi i diritti, infatti, sono meritevoli di tutela in egual misura e, proprio per tale motivo, il suddetto bilanciamento non risulta sempre agevole da effettuare. Da una parte, infatti, il diritto all'accesso tutela il diritto del singolo di conoscere il contenuto di documenti amministrativi, garantisce i principi di trasparenza, imparzialità e buon andamento dell'amministrazione e, spesso, costituisce, peraltro, presupposto per l'esercizio del diritto di difesa in giudizio[113]. Dall'altra parte, invece, il diritto alla riservatezza interviene nella tutela della sfera privata di ciascun soggetto, risultando un componente essenziale del doveroso rispetto della dimensione intima della personalità. In quanto entrambi meritevoli di tutela, il bilanciamento non può essere effettuato sulla base di un'astratta scala gerarchica dei diritti in contesa, bensì deve tenere conto delle specifiche circostanze di fatto destinate a connotare il singolo caso concreto[114], senza che nessuno dei due ne risulti compromesso.

L'Autorità Garante per la Protezione dei dati personali, al fine di guidare la Pubblica Amministrazione di volta in volta chiamata ad effettuare tale valutazione, ha delineato il principio del c.d. *"diritto di pari rango"*[115]. Ai sensi di tale principio, al fine di valutare se l'accesso a dati sensibili possa essere consentito, occorre considerare se il diritto invocato dal richiedente abbia pari rango rispetto a quello alla protezione dei dati personali dell'interessato. In tale ottica, ad esempio, deve sempre essere garantito ai richiedenti l'accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici, come previsto espressamente anche dall'art. 24 c. 7 della L. 241/1990. Se, però, un terzo invoca a motivo della propria richiesta la necessità di tutelarsi in sede giudiziaria, ai fini del bilanciamento, si deve il diritto di accesso deve essere messo a raffronto con il sottostante diritto che il terzo intenda far valere in giudizio, che può essere, ad esempio, il diritto di personalità oppure di proprietà. Non deve, invece, essere preso in considerazione il solo diritto di azione alla difesa, pure costituzionalmente protetto,

[113] Come espressamente previsto anche dall'art. 24 c. 7 della L. 241/1990 che così recita: "*deve comunque essere garantito ai richiedenti l'accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici".*

[114] *Cfr*. Cons. Stato, Sez. VI n. 1882/2001; Cons. Stato, Sez. VI n. 2542/2002.

[115] Tale principio è stato delineato per primo dall'Autorità Garante per la Protezione dei dati personali al punto 1 lett. a) dell'Autorizzazione n. 6/2002 al trattamento di dati sensibili da parte degli investigatori privati. Successivamente, tale principio è stato espressamente previsto dal Codice Privacy novellato, in particolare all'art. 60, 71 e 92 c. 2.

in quanto questo merita in generale protezione a prescindere dall'"importanza" del diritto sostanziale che si vuole difendere[116].

Quando, invece, il trattamento concerne dati genetici oppure dati relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, bisogna fare riferimento agli articoli 60, cui espressamente rimanda anche l'art. 24 c. 7 della L.241/1990, 71e 92 c. 2 lett. b) del Codice Privacy novellato, che riprendono il principio del "diritto di pari rango" delineato dall'Autorità Garante per la Protezione dei dati personali. Tali disposizioni prevedono che il trattamento delle citate tipologie di dati è consentito solamente qualora la situazione giuridicamente rilevante che si intenda tutelare con la richiesta di accesso ai documenti amministrativi sia di rango almeno pari ai diritti dell'interessato, ovvero consista in un diritto della personalità o in un altro diritto o libertà fondamentale. In ogni altra situazione, quindi, non sarà possibile aderire alla richiesta di accesso o di comunicazione da parte di terzi se i dati o il documento sono ritenuti utili dal richiedente finalizzata a tutelare in giudizio un interesse legittimo o un diritto soggettivo. Questi ultimi, infatti, possono essere anche di rilievo, ma restano comunque subvalenti rispetto alla concorrente necessità di tutelare la riservatezza, la dignità e gli altri diritti e libertà fondamentali dell'interessato. Quanto esposto comporta, ad esempio, che nella maggior parte dei casi riguardanti meri diritti di credito non sia possibile accogliere l'istanza di accesso.

Il riferimento normativo ai diritti della personalità e ad altri diritti e libertà fondamentali costituisce un rinvio ad un elenco aperto di posizioni soggettive, che può essere soggetto a variazioni a seconda del periodo storico preso in considerazione e della valutazione del caso concreto. In questo modo, si evita che le amministrazioni, gli altri destinatari delle richieste ed il giudice in caso di impugnazione di un eventuale rigetto, addivengano a soluzioni precostituite poggianti su un'astratta scala gerarchica dei diritti in contesa[117]. Pertanto, a titolo meramente esemplificativo, all'interno di questo elenco aperto possono annoverarsi la libertà personale di circolazione e soggiorno, di riunione, di associazione, di fede, di manifestazione del pensiero, il diritto alla vita, all'integrità fisica, alla salute, all'onore, alla riservatezza, alla libera esplicazione della propria attività, all'istruzione.

[116] Provvedimento del 9 luglio 2003, "*Dati sanitari. Provvedimento generale sui diritti di pari rango"* – Autorità Garante per la Protezione dei dati personali.
[117] *Cfr*. Cons. Stato, Sez. VI n. 1882/2001; Cons. Stato, Sez. VI n. 2542/2002.

L'attività di raffronto fra situazioni giuridiche volta a stabilirne il rango non esaurisce, comunque, i compiti dell'interprete che si trovi a dover dare riscontro ad un'istanza di accesso a dati personali o a documenti che li contengano. Occorre, infatti, svolgere una verifica volta, altresì, ad appurare se i dati o tutti i dati oggetto della richiesta, siano effettivamente necessari a far valere o difendere i diritti di "pari rango", ai sensi dei principi di necessità, pertinenza e non eccedenza dei dati[118]. Una tale valutazione potrebbe portare anche ad un accoglimento parziale della richiesta di accesso, qualora apparisse che con i dati concessi il richiedente sia comunque in grado di far valere o difendere le proprie prerogative. Pertanto, il rispetto dei principi su citati non deve solo conformare la decisione della Pubblica Amministrazione nel momento della valutazione dell'istanza di accesso, ma deve orientare la scelta dell'amministrazione anche in chiave prospettica, con riguardo al momento del successivo utilizzo dei documenti e dati forniti. La Pubblica Amministrazione, inoltre, dovrà anche valutare, caso per caso, l'effettiva necessità di anticipare o meno l'autonoma conoscibilità mediante accesso ad un documento o che sia già stato prodotto agli atti di un procedimento giudiziario di cui si è parte e, pertanto, già conoscibile per altra via in tale sede oppure che verrà inevitabilmente acquisito dal Giudice su sua iniziativa, in un secondo momento.

Relativamente all'intersezione tra la nuova disciplina della protezione dei dati personali e la normativa in materia di accesso, che espressamente richiama alla prima, occorre, tuttavia, fare due brevi osservazioni. In primo luogo, la legge n. 241/1990 continua a far riferimento ai "*dati sensibili*", secondo la precedente definizione del Codice Privacy, mentre ormai l'art. 9 del Regolamento UE n. 2016/679 li denomina "*categorie particolari di dati personali*". Si riscontra, dunque, una discrepanza terminologica tra le due discipline, che si riflette anche dal punto di vista sostanziale. Infatti, sia l'art. 9 del Regolamento sia l'art. 60 del Codice Privacy novellato fanno riferimento anche ai dati genetici, i quali non vengono menzionati dalla legge n. 241/1990. Occorrerebbe, dunque, procedere ad un aggiornamento di alcune disposizioni al fine di coordinare le due normative. Inoltre, come è stato notato, "*l'imprecisione del coordinamento si manifesta in modo clamoroso nel curioso equivoco dei linguaggi: per la legge n. 241/1990 l'interessato è colui che chiede l'accesso, mentre il*

[118] *Cfr*. Cons. Stato, Sez. VI n. 2542/2002; TAR Emilia-Romagna-Bologna sent. n. 1207/2001; Corte di Giustizia (Grande Sezione), 29 giugno 2010, procedimento C-28/08 P, Bavarian Lager c. Commissione europea; Consiglio di Stato, 12/8/2016, n. 3631.

controinteressato è il titolare del diritto alla riservatezza; ma nel Codice della privacy l'interessato è proprio il soggetto cui si riferiscono i dati personali"[119].

In conclusione, quindi, non è possibile affermare l'esistenza di una regola generale in virtù della quale il diritto di accesso, quando comporti la conoscenza di dati personali e relativi alla salute, debba essere sempre soddisfatto a priori. Non sussiste, infatti, una soluzione precostituita, ma occorre effettuare un bilanciamento del peso che hanno nel caso concreto i due diritti in gioco. Il principio della trasparenza, che deve caratterizzare l'intero agire amministrativo e di cui il diritto di accesso agli atti è piena espressione, può, pertanto, incontrare dei limiti. Non si può considerare la trasparenza come un valore assoluto, non soggetto al bilanciamento con altri diritti e valori costituzionali[120]. Lo stesso art.1 c. 2 del D.Lgs. n. 33/2013 prevede, infatti, l'esistenza di limiti alla trasparenza in funzione di altri interessi protetti dall'ordinamento, sia di natura pubblica, come quelli che si evincono dalle disposizioni in materia di segreto di Stato e di segreto d'ufficio, sia di natura privata, come quelli in materia di protezione dei dati personali. Pertanto, sull'altare della trasparenza non potrà essere sacrificato, in ogni caso, un diritto fondamentale della persona.

[119] *Cfr. "Il complesso bilanciamento tra il principio di trasparenza e il diritto alla privacy: la disciplina delle diverse forme di accesso e degli obblighi di pubblicazione"* – Carlo Colapietro - *Federalismi.it – Rivista di diritto pubblico italiano, comparato, europeo* – 13 maggio 2020; M. LIPARI, "*Il diritto di accesso e la sua frammentazione dalla legge n. 241/1990 all'accesso civico: il problema delle esclusioni e delle limitazioni oggettive"* - *Federalismi.it – Rivista di diritto pubblico italiano, comparato, europeo* – 18 settembre 2019.

[120] *Cfr. "Il complesso bilanciamento tra il principio di trasparenza e il diritto alla privacy: la disciplina delle diverse forme di accesso e degli obblighi di pubblicazione"* – Carlo Colapietro - *Federalismi.it – Rivista di diritto pubblico italiano, comparato, europeo* – 13 maggio 2020

V. CONCLUSIONI

Il presente lavoro nasce da un'esigenza concreta, espressa dal personale sanitario impegnato nelle cure domiciliari e dipendente di un'azienda ospedaliera milanese. Vi è, infatti, la necessità di individuare gli strumenti e le procedure idonee al rispetto del diritto alla protezione dei dati personali del paziente, senza, però, trascurare le cure da prestare allo stesso.

Il diritto alla salute viene garantito dall'art. 32 Costituzione, che costituisce una fonte primaria all'interno della gerarchia delle fonti dell'ordinamento giuridico italiano[121]. Il diritto alla protezione dei dati personali, invece, è tutelato, da ultimo, dal Regolamento UE n. 2016/679, che, tra l'altro, prevede una disciplina di maggior riguardo per i dati relativi alla salute. In questo caso, quindi, la suddetta tutela è apprestata da un atto normativo avente portata generale, obbligatorio in tutti i suoi elementi e direttamente applicabile negli ordinamenti degli Stati membri.

Ai sensi dell'art. 117 della Costituzione[122], le fonti del diritto comunitario si collocano, all'interno della gerarchia delle fonti dell'ordinamento giuridico italiano, in posizione paritaria rispetto alle fonti costituzionali e di rilievo costituzionale. Vi è, però, un unico limite gerarchico imposto all'attuazione delle fonti comunitarie, che è il c.d. "*nucleo rigido*" della Costituzione. Le fonti dell'Unione Europea, infatti, seppur primarie, si collocano immediatamente al di sotto dei principi fondamentali e dei diritti inviolabili disciplinati dalla Costituzione, tra cui l'art. 2 vi fa rientrare il diritto alla salute.

La difficoltà di bilanciare i due diritti in gioco, tra l'altro, è stata maggiormente accentuata a seguito del progresso tecnologico, che ha investito anche l'ambito sanitario. Le nuove tecnologie, infatti, se da un lato agevolano molto la prestazione delle cure, talvolta rendendole anche più efficaci ed immediate, dall'altro lato spesso si rivelano vulnerabili

[121] Il sistema delle fonti del diritto italiano viene comunemente rappresentato come una piramide, al cui vertice sono collocate le fonti di rango più alto e via via quelle di livello inferiore, man mano che si discende verso la base. Esiste dunque una vera e propria gerarchia delle fonti e delle norme giuridiche da esse prodotte, che consente anche di risolvere eventuali contrasti tra fonti giuridiche coeve ma dotate di forza giuridica diversa. Il criterio gerarchico sancisce infatti la prevalenza della fonte di rango superiore rispetto a quella di livello inferiore, precludendo a quest'ultima di derogarvi o di porsi in contrasto con il contenuto della fonte sovraordinata, pena la declaratoria di illegittimità e la sua definitiva rimozione dall'ordinamento. Così, ad esempio, le leggi ordinarie non possono contrastare con la Costituzione, o i regolamenti governativi non possono derogare alla legge ordinaria, mentre possono contravvenire a fonti di rango inferiore. Si parla a tal proposito di piramide di Kelsen, dal nome il massimo esponente del normativismo giuridico, cioè di quell'indirizzo metodologico che riduce tutto il diritto a norma.

[122] L'art. 117 della Costituzione espressamente recita: "*La potestà legislativa è esercitata dallo Stato e dalle Regioni nel rispetto della Costituzione, nonché dei vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali".*

perché facilmente attaccabili. Ciò, ovviamente, crea non pochi problemi dal punto di vista della *privacy*, in quanto gli strumenti digitali vengono utilizzati per raccogliere una grande quantità di dati personali e relativi alla salute.

È stato appurato come gli operatori sanitari siano legittimati al trattamento dei dati personali dei propri pazienti e relativi alla loro salute, qualora sia funzionale al perseguimento di finalità di cura. Premesso ciò, sicuramente durante l'intera fase della prestazione delle cure, il bilanciamento tra il diritto alla salute ed il diritto alla protezione dei dati personali risulta maggiormente difficile. In tale circostanza, infatti, fatta salva comunque la somministrazione di una corretta informativa *privacy* corredata di tutti gli elementi indicati dalla normativa europea, non si può sempre sacrificare il diritto alla salute in nome di una rigida tutela dei dati personali. Spesso, infatti, si tratta di situazioni caratterizzate da urgenza, in cui, pertanto, la velocità e la sostanza delle cure da prestare devono essere predilette rispetto alla loro forma. La velocità può senz'altro essere facilmente garantita dall'utilizzo delle nuove tecnologie, che, in una situazione ideale, dovrebbero essere fornite direttamente dall'azienda agli operatori coinvolti. Stante la pericolosità delle nuove tecnologie, inoltre, queste, secondo il principio di *privacy by default,* devono essere dotate di misure di garanzia idonee alla tutela dei dati oggetto di registrazione.

Tuttavia, tale situazione ideale spesso non si verifica oppure gli strumenti messi a disposizione dall'azienda non sono un numero sufficiente. Da qui nasce la necessità di individuare strumenti di registrazione che siano nella disponibilità concreta dei singoli operatori, ma che, allo stesso tempo, siano rispettosi della normativa in materia di protezione dei dati personali.

Nella fase di conservazione della documentazione sanitaria, invece, non sussiste la componente dell'urgenza ed il diritto alla salute è ormai stato soddisfatto. Pertanto, in tale occasione gli operatori sanitari devono concentrarsi esclusivamente sul rispetto del diritto alla protezione dei dati personali degli assistiti. A tal proposito, il progresso tecnologico ha diffuso un maggior utilizzo di numerosi strumenti di conservazione digitali, quali la refertazione online, la cartella clinica elettronica ed il fascicolo sanitario elettronico. L'importanza di quest'ultimo strumento, in particolare, è legata al suo carattere di interoperabilità, sottolineato, da ultimo, anche dal PNRR, che prevede lo stanziamento di risorse per lo sviluppo digitale anche in ambito sanitario. Tale piano, infatti, delinea il suddetto fascicolo come un *repository* digitale contenente l'intera storia clinica degli

assistiti, su tutto il territorio nazionale, grazie al costante aggiornamento da parte degli operatori sanitari. In virtù della tipologia di dati oggetto di conservazione, anche tali strumenti digitali di conservazione, comunque, devono essere dotati di misure di garanzie previste dalla normativa in materia.

La fase della conservazione e le relative modalità sono estremamente importanti al fine di evadere le eventuali istanze di accesso alla documentazione sanitaria che dovessero pervenire. Qualora tale richiesta dovesse essere avanzata da un soggetto differente rispetto a quello cui i dati conservati facciano riferimento, anche in questo caso l'azienda sanitaria interpellata sarà chiamata ad effettuare un bilanciamento, questa volta, tra il diritto di accesso ed il diritto alla protezione dei dati personali, entrambi tutelati dall'ordinamento giuridico. In tal caso, però, i due diritti hanno una tutela di rango differente. Il primo, infatti, è disciplinato da una legge ordinaria interna e, pertanto, da una fonte di rango secondario e non primario, all'interno della scala gerarchica delle fonti dell'ordinamento giuridico italiano.

In conclusione, quindi, l'intera attività svolta dagli operatori sanitari e finalizzata alla tutela della salute può essere suddivisa in tre fasi: la prestazione concreta delle cure in cui la documentazione sanitaria viene creata spesso tramite l'utilizzo di strumenti digitali, la conservazione di tali atti e l'evasione di istanze di accesso. Sia nella prima sia nella terza fase, gli operatori sono chiamati ad operare un bilanciamento tra due diritti, entrambi tutelati dalla legge, ma la cui tutela spesso non può coesistere nel caso concreto. Tale bilanciamento, inoltre, conduce ad un esito differente nelle due fasi. Nella prima, infatti, i due interessi in gioco sono il diritto alla salute ed il diritto alla protezione dei dati personali ed il bilanciamento spesso culmina con un risultato a sfavore del secondo ed a favore del primo, che, anche nella scala gerarchica delle fonti del diritto italiano, riceve una tutela maggiormente rafforzata. Nella terza fase, invece, vi sono il diritto alla protezione dei dati personali ed il diritto di accesso agli atti. In questo caso, sovente il bilanciamento culmina con un risultato a favore del primo ed a sfavore del secondo, la cui tutela, comunque, deriva da una fonte di rango inferiore all'interno della suddetta gerarchia.

La fase di conservazione, invece, è quella in cui la tutela dei dati personali e dei dati relativi alla salute del paziente può e deve essere l'unico obiettivo. Pertanto, pur facendo ricorso anche a strumenti digitali, occorre semplicemente attuare le giuste misure di garanzia suggerite dalla normativa in materia *privacy.*

FONTI

1. Normativa

- Costituzione Italiana;
- Regolamento UE n. 2016/679, "*Regolamento generale sulla protezione dei dati";*
- D.Lgs. n. 196/2003, "*Codice in materia di protezione dei dati personali*";
- D.Lgs. 101/2018, "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*";
- D.Lgs. 2 luglio 2010 n. 104, "*Attuazione dell'articolo 44 della legge 18 giugno 2009, n. 69, recante delega al governo per il riordino del processo amministrativo";*
- D.Lgs. n. 33/2013, "Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni";
- Legge n. 241 del 7 agosto 1990, "*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi"*;
- D.L. 27 gennaio 2022 n. 4, "*Misure urgenti in materia di sostegno alle imprese e agli operatori economici, di lavoro, salute e servizi territoriali, connesse all'emergenza da COVID-19, nonché' per il contenimento degli effetti degli aumenti dei prezzi nel settore elettrico*" e convertito, con modificazioni, dalla L. 28 marzo 2022 n. 25;
- Legge 8 marzo 2017 n. 21 o legge Gelli-Bianco, entrata in vigore l'1 aprile 2017, e recante "*Disposizioni in materia di sicurezza delle cure e della persona assistita, nonché in materia di responsabilità professionale degli esercenti le professioni sanitarie*";
- D.Lgs. n. 82 del 7 marzo 2005, "*Codice dell'Amministrazione Digitale";*
- D.L. 18 ottobre 2012 n. 179, "*Ulteriori misure urgenti per la crescita del Paese".*
- D.L. 9 febbraio 2012 n. 5, "*Disposizioni urgenti in materia di semplificazione e di sviluppo"*, convertito con modificazioni dalla L. 4 aprile 2012 n. 35 "*Semplificazione in materia di sanità digitale*";
- D.P.C.M. 29 settembre 2015 n. 178, "*Regolamento in materia di fascicolo sanitario elettronico*";

- D.P.C.M. 8 agosto 2013, "*Modalità di consegna, da parte delle Aziende sanitarie, dei referti medici tramite web, posta elettronica certificata e altre modalità digitali, nonché' di effettuazione del pagamento online delle prestazioni erogate, ai sensi dell'articolo 6, comma 2, lettera d), numeri 1) e 2) del decreto-legge 13 maggio 2011, n.70, convertito, con modificazioni, dalla legge 12 luglio 2011, n. 106, recante «Semestre europeo - prime disposizioni urgenti per l'economia"*;
- D.L. "Rilancio" 19 maggio 2020 n. 34;
- D.M. del 18 febbraio 1982, "*Norme per la tutela sanitaria dell'attività sportiva agonistica*";
- Circolare Ministero della Sanità del 19 dicembre 1986, n. 900;
- "*Il Fascicolo Sanitario Elettronico. Linee guida nazionali*" -11 novembre 2010 - Ministero della salute;
- D.M. 14/02/1997, "*Determinazione dei criteri minimi di accettabilità delle apparecchiature radiologiche ad uso medico ed odontoiatrico nonché di quelle di medicina nucleare, ai sensi dell'art. 112, comma 3, del D.Lgs. 17 marzo 1995, n. 230. Pubblicato nella Gazz. Uff. 11 marzo 1997, n. 58";*
- *"Linee guida. La compilazione, la codifica e la gestione della scheda di dimissione ospedaliera istituita ex d.m. 28.12.1991"* – 17 giugno 1992 – Ministero della Sanità;
- *"Telemedicina – Linee di indirizzo nazionali*" - Conferenza Stato Regioni del 20 febbraio 2014;
- D.P.R. 12 aprile 2006 n. 184 "*Regolamento recante disciplina in materia di accesso ai documenti amministrativi*";
- Il Piano nazionale di Ripresa e Resilienza (PNRR);
- Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni dal titolo "*Quadro europeo di interoperabilità - Strategia di attuazione*" del 23.3.2017;
- Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni dal titolo "*Verso l'interoperabilità dei servizi pubblici europei*" del 16.12.2010.

2. Provvedimenti e Documenti del Garante della Privacy

- Comunicato stampa del 5 ottobre 2004, "*Nessun conflitto tra diritto di accesso agli atti e diritto alla riservatezza";*

- Provvedimento del 9 luglio 2003, "*Dati sanitari. Provvedimento generale sui diritti di pari rango"*;
- "*Le cartelle cliniche devono essere leggibili*" - Autorità Garante per la Protezione dei dati personali – 11 aprile 2003 - *Newsletter Garante;*
- *"Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario"* - 16 luglio 2009 – Autorità Garante per la Protezione dei Dati Personali;
- Linee guida in materia di Dossier sanitario - 4 giugno 2015;
- *"Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario"* - 7 marzo 2019;
- Provvedimento dell'Autorità Garante per la Protezione dei dati personali del 15 aprile 2021;
- Provvedimento generale dell'Autorità Garante per la Protezione dei dati personali del 9 novembre 2005;
- "*Sicurezza del dato sanitario e condivisione*" – Intervento di Pasquale Stanzone, Presidente del Garante per la protezione dei dati personali – Panorama 18 febbraio 2022;
- Garante per la protezione dei dati personali, Prescrizione del 9 novembre 2005, "*Strutture sanitarie: rispetto della dignità*";
- *"Fascicolo sanitario elettronico: nessuna scadenza per l'inserimento dei dati"*, 11 gennaio 2021;
- "*Cloud Computing - La guida del Garante della Privacy per imprese e pubblica amministrazione"* – Autorità Garante per la protezione dei dati personali – 2012;
- *"Fascicolo Sanitario Elettronico nessuna scadenza per l'inserimento dei dati"* – 11 gennaio 2021*;*
- "*Linee guida in tema di referti on-line"* - 19 novembre 2009 – Autorità Garante per la protezione dei dati personali;
- "*FAQ – Fascicolo Sanitario Elettronico*" – pubblicate sul sito *web* dell'Autorità Garante per la protezione dei dati personali;
- "Ordinanza ingiunzione nei confronti di Azienda Usl della Romagna" - 27 maggio 2021- Autorità Garante per la protezione dei dati personali;
- *"Ordinanza ingiunzione nei confronti di Azienda provinciale per i servizi sanitari di Trento"* - 27 maggio 2021 - Autorità Garante per la protezione dei dati personali;

- *"Parere del Garante su uno schema di decreto del Presidente del Consiglio dei ministri in materia di fascicolo sanitario elettronico*" - 22 maggio 2014;
- "*Informazioni sulle convinzioni religiose dei pazienti: i casi in cui possono essere raccolte durante il ricovero"* - 12 novembre 2014 - Autorità Garante per la Protezione dei dati personali;
- WP29, "*Linee guida sulla trasparenza ai sensi del Regolamento"*, WP260 rev 01;
- Provvedimento del 20 settembre 2006 – Autorità Garante per la Protezione dei dati personali;
- "*Diritto di accesso - Accesso a dati incomprensibili per la grafia o per l'uso di codici"* - 26 marzo 2001 - Autorità Garante per la Protezione dei dati personali;

3. Giurisprudenza

- Raccomandazione n. 81 del 1981 - Comitato dei Ministri del Consiglio d'Europa;
- Raccomandazione n. (97)5 del 1997 - Consiglio d'Europa;
- Cass. civ., sez. VI, sent. del 11 gennaio 2016, n. 222;
- Cass. civ., sez. I, sent. del 7 ottobre 2014, n. 21107;
- Cass. civ., sez. I, sent. 1 agosto 2013, n. 18443;
- Cass. civ., sent. 8 luglio 2005, n. 14390;
- Cass. Pen. Sez. V, n. 1098/1997 e, in analogia: Cass. Pen. Sez. V, n. 23324/2004; Cass. Pen. Sez. V, n.13989/2004, Cass. Pen. Sez. V, n. 35167/2005;
- Cass. Civ. 12.11.1992, n. 12189;
- Cass. Civ., sez. III, ordinanza 23/03/2018 n° 7250, Cass. Civ. III, n. 9290 dell'8.6.2012. Cass. Civ, sez. II, n. 22639 del 8.11.2016;
- Cass. Civ. 18.9.1980, n. 5296;
- Tar Sicilia – Catania – Sez. IV – con sentenza n. 879 del 7 maggio 2009;
- Cons. Stato, Sez. VI n. 1882/2001; Cons. Stato, Sez. VI n. 2542/2002;
- TAR Emilia-Romagna-Bologna sent. n. 1207/2001, Corte di Giustizia (Grande Sezione), 29 giugno 2010, procedimento C-28/08 P, Bavarian Lager c. Commissione europea, Consiglio di Stato, 12/8/2016, n. 3631.

4. Articoli

- "*Manuale Sui Principi, Sulle Caratteristiche, Sulle Specifiche Normative In Materia Di Protezione Dei Dati Da Applicare In Italia All'erogazione Di Servizi Sanitari Con*

Tecnologia Cloud Computing", Avv. Luca Bolognini – Avv. Enrico Pelino, Nuova Versione – 2016;

- La rivista statunitense "*Newsweek*" nel rapporto "World Best Hospitals 2022:
- "*Codice privacy: tutte le novità del D.lgs. 101/2018*" di L. Bolognini, E. Pellino – IL CIVILISTA – Giuffrè Francis Lefebvre S.P.A, 2019;
- "*GDPR, l'informativa privacy: a cosa serve e come farla*" – P. Calvi – Network Digital 360 – 24 marzo 2020;
- "*Cloud in Sanità: Vademecum essenziale sulla tutela della privacy. Manuale sui principi, sulle caratteristiche, sulle specifiche normative in materia di protezione dei dati da applicare in Italia all'erogazione di servizi sanitari con tecnologia cloud computing"* - Avv. Luca Bolognini1 – Avv. Enrico Pelino- 2016;
- "*Sanità digitale, il ruolo dei dati per l'innovazione del settore: lo scenario ed i risvolti privacy*" – V. Giardino, Avv. R. Zani – Network Digital 360 - 22 aprile 2021;
- *"Fascicolo sanitario elettronico (fse) e dossier sanitario elettronico (dse) cosa sono e alcuni profili privacy"* – Avv. Stefania Calosso – 22 settembre 2020*;*
- *"Trattamento dei dati sanitari, alla luce del GDPR: il quadro normativo"* - 18 dicembre 2019 – Avv. Chiara Rauccio - *Network Digital 360*;
- "*I dati sanitari, in i dati personali nel diritto europeo",* P. Guarda, a cura di V. Cuffaro, R. D'Orazio, V. Ricciuto, Giappichelli, 2019;
- "*Fascicolo Sanitario Elettronico, cos'è, a che serve e come attivarlo*" - Anna Francesca Pattaro –16 settembre 2021- *Network Digital 360*;
- "*Il nuovo Fascicolo Sanitario Elettronico ed i rischi per la privacy degli assistiti"* - Cristina Criscuoli – 27 aprile 2022 - *Diritto al Digitale;*
- *"Il complesso bilanciamento tra il principio di trasparenza e il diritto alla privacy: la disciplina delle diverse forme di accesso e degli obblighi di pubblicazione"* – Carlo Colapietro - *Federalismi.it – Rivista di diritto pubblico italiano, comparato, europeo* – 13 maggio 2020;
- M. LIPARI, "*Il diritto di accesso e la sua frammentazione dalla legge n. 241/1990 all'accesso civico: il problema delle esclusioni e delle limitazioni oggettive" - Federalismi.it – Rivista di diritto pubblico italiano, comparato, europeo* – 18 settembre 2019.

5. Altre tipologie di fonti

- "*Immagini, suoni e biosegnali – Manuale per i percorsi di cura*", approvato dalla Giunta di Regione Lombardia con DGR n. X/3001 del 9 gennaio 2015;
- "*Le registrazioni dei pazienti. Audio e video effettuati in occasione di contatti con personale o strutture della sanità e apporti informativi direttamente",* approvato dalla Giunta di Regione Lombardia con DGR n. X/5765 del 8 novembre 2016;
- "*Manuale della documentazione sanitaria e sociosanitaria*", approvato dalla Giunta di Regione Lombardia con DGR n. IX/ 4659 del 9 settembre 2013;
- "*Approvazione del Manuale del Fascicolo di ricovero 3A Edizione – 2019"* da parte della Giunta di Regione Lombardia con DGR n. XI/2393 del 11.11.2019;
- *"Linee guida Regionali per la Cartella Clinica Elettronica Aziendale*" - 19.02.2012- Regione Lombardia.