RIVISTA ITALIANA DI MEDICINA LEGALE
ISSN 1124-3376
Anno XL Fasc. 1 - 2018

Denise Amram - Giovanni Comandé

SUL NON FACILE COORDINAMENTO DEGLI OBBLIGHI IMPOSTI DAL REGOLAMENTO EUROPEO SULLA PROTEZIONE DEI DATI PERSONALI UE/679/2016 E DALLA LEGGE N. 24/2017

Estratto

MVLTA PAVCIS AG

Milano • Giuffrè Editore

EDITORIALE

SUL NON FACILE COORDINAMENTO DEGLI OBBLIGHI IMPOSTI DAL REGOLAMENTO EUROPEO SULLA PROTEZIONE DEI DATI PERSONALI UE/679/2016 E DALLA LEGGE N. 24/2017

ON THE DIFFICULTIES TO COMBINE ALL DUTIES EMERGING FROM THE EU GENERAL DATA PROTECTION REGULATION EU/679/2016 AND THE ACT N. 24/2017

Denise Amram * e Giovanni Comandé **

RIASSUNTO

Il contributo mira ad individuare alcune problematiche di coordinamento rispetto agli adempimenti emergenti per le strutture sanitarie in ragione della nuova legge n. 24/2017 e il Regolamento Europeo sulla Protezione dei Dati Personali UE/679/2017.

ABSTRACT

This paper aims at identifying some issues emerging from the combination of duties which the healthcare services have to deal with in order to comply with the new Act n. 24/2017 and the General Data Protection Regulation EU 679/2017.

Parole chiave: sicurezza delle cure - trasparenza dei dati - protezione dei dati.
Keywords: healthcare safety - transparency - data protection.

* Assegnista di ricerca presso Scuola Superiore Sant'Anna (Pisa) e avvocato del Foro di Pisa, denise.amram@gmail.com.

** Professore ordinario diritto privato comparato presso Scuola Superiore Sant'Anna Pisa, g.comande@santannapisa.it.

SOMMARIO:

1. Premessa. Le nuove fonti del diritto in campo sanitario; 2. La trasparenza dei dati e coordinamento con la tutela dei dati personali; 3. Adempimenti delle strutture sanitarie sulla base del Regolamento UE/679/2016; 4. Qualche considerazione conclusiva, in attesa delle prassi.

1. Premessa. Le nuove fonti del diritto in campo sanitario.

Il diritto in campo sanitario italiano è stato recentemente riformato attraverso la Legge n. 24/2017, recante, come noto, "*Disposizioni in materia di sicurezza delle cure e della persona assistita, nonché in materia di responsabilità professionale degli esercenti le professioni sanitarie*" [1].

L'art. 1, comma 2, della nuova legge stabilisce che "*la sicurezza delle cure si realizza anche mediante l'insieme di tutte le attività finalizzate alla prevenzione e alla gestione del rischio connesso all'erogazione di prestazioni sanitarie e l'utilizzo appropriato delle risorse strutturali, tecnologiche e organizzative*" [2].

In questa prospettiva, rientrano nella tutela al diritto alla salute tutti quei requisiti organizzativi volti a garantire trasparenza ed efficienza delle risorse e che coinvolgono, inevitabilmente, visto il progresso scientifico, l'utilizzo delle tecnologie: "*la sicurezza emerge, infatti, dall'interazione tra tutte le componenti del sistema e non dipende solo dalle persone, dalle tecnologie, dall'organizzazione, ma dall'interazione tra loro*" [3].

In tale contesto, occorre verificare l'impatto che l'imminente entrata in vigore (prossimo 25 maggio 2018) del Regolamento Europeo sulla Protezione dei Dati Personali n. Reg. UE/679/2016 avrà sul nuovo assetto normativo, anche in ragione del *favor* rispetto alla riorganizzazione e digitalizzazione dei servizi sanitari.

L'integrazione dei principi enunciati dalla Legge n. 24/2017 con quelli di matrice europea in materia di protezione dei dati personali delinea, dunque, una serie di obblighi e responsabilità per le strutture sanitarie, quali titolari di trattamento di dati personali e sensibili, che implicano una indispensabile attività di coordinamento al livello aziendale.

1) F. Gelli-M. Hazan-D. Zorzit (a cura di), *La nuova responsabilità sanitaria e la sua assicurazione*, Giuffrè, Milano, 2017; M. Lovo-L. Nocco (a cura di), *La nuova responsabilità sanitaria. Le novità introdotte dalla Legge Gelli*, Il Sole 24 Ore, Milano, 2017.

2) R. Tartaglia et. Al., *La sicurezza delle cure e il rischio clinico*, in AA.VV., *Sicurezza delle cure e responsabilità sanitaria. Commentario alla legge 24/2017*, Quotidiano Sanità Edizioni, Roma, 2017, 13 ss. Gli Autori, richiamando il saggio di C. Vincent, *Sicurezza del Paziente,* Springer Veerlag, 2012 ed. Italiana, definiscono sicurezza delle cure "*quel processo che porta a evitare, prevenire e mitigare effetti avversi o danni derivanti dal processo di assistenza sanitaria*".

3) *Ibidem*, 16.

2. La trasparenza dei dati e coordinamento con la tutela dei dati personali.

L'art. 4 della Legge n. 24/2017, rubricato "Trasparenza dei dati" compie un primo riferimento alla necessità di coordinare le attività connesse alle prestazioni sanitarie con la tutela dei dati personali.

Il primo comma della citata norma enuncia, in via di principio, la necessità che le prestazioni sanitarie, erogate nelle strutture sanitarie pubbliche o private, siano soggette all'obbligo di trasparenza, con il "limite" del rispetto del codice dei dati personali (d.lgs. n. 196/2003). Quest'ultimo, come noto, all'art. 83 prevede una serie di misure volte a garantire la tutela della riservatezza del paziente nella fruizione della prestazione sanitaria, anche in sede di documentazione di anamnesi [4)].

Un primo profilo di criticità riguarda il futuro del d.lgs. n. 196/2003 all'indomani dell'entrata in vigore del Regolamento europeo che, ispirato al principio di *accountability*, ha introdotto, come vedremo a breve, un sistema di obblighi e responsabilità per il titolare del trattamento dei dati, cui le strutture sanitarie, pubbliche e private, sono chiamate ad adeguarsi.

Il richiamo, pertanto, al rispetto dei principi del codice per la protezione dei dati personali è destinato a doversi intendere – estensivamente, seppur in maniera scontata – al Regolamento UE/679/2016: dal 25 maggio 2018, infatti, non è più sufficiente osservare la normativa nazionale sul trattamento dei dati personali, essendo necessario per i titolari del trattamento dimostrare la conformità al Regolamento europeo.

Un ulteriore profilo di criticità per le strutture sanitarie emerge rispetto alle novità introdotte in materia di diritto di accesso del paziente alla documentazione sanitaria e in materia di informativa sul trattamento dei dati. Il processo di digitalizzazione delle risorse documentali, incentivato sia per le strutture sanitarie pubbliche che per quelle private dalla Legge n. 24/2017, è volto ad assicurare al paziente una più efficiente risposta alle richieste, ad esempio, di accesso alle cartelle cliniche.

L'art. 4, comma 2, della Legge n. 24/2017 riduce a sette giorni il termine per evadere la richiesta "*da parte degli interessati aventi diritto, in conformità alla disciplina sull'accesso ai documenti amministrativi e a quanto previsto dal codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196*" e fornire la documentazione sanitaria [5)] relativa al paziente, specificando che la stessa si provveda "*preferibilmente in formato elettronico*". Eventuali ulteriori integrazioni possono, invero, essere fornite dalla struttura sanitaria nel termine di trenta giorni.

4) Così Art. 83, comma 2, lett. *d*), d.lgs. n. 196/2003. Per un approfondimento, L. Benci, *La trasparenza dei dati e la documentazione sanitaria*, in AA.VV., *Sicurezza delle cure e responsabilità sanitaria. Commentario alla legge 24/2017*, cit., 48.

5) Si osserva che la nuova legge si riferisce alla "documentazione sanitaria", ricomprendendo "*tutta la documentazione sanitaria e non solo la cartella clinica intesa come cartella medica*", così L. Benci, cit., 49.

La *ratio* della norma risiede nel diritto del paziente di essere messo nelle condizioni di ottenere, attraverso una migliore strategia aziendale, pronte risposte alle richieste di accesso ai documenti sanitari. Anche in questo caso, la norma richiama il codice dei dati personali.

Orbene, a ciò si aggiunga che ai sensi degli artt. 12, 13, 14 del Regolamento UE/679/2016 il titolare del trattamento deve assicurare una pronta risposta rispetto anche ai cc.dd. diritti di informativa degli interessati [6)].

Il paziente della struttura sanitaria ha, altresì, il diritto di chiedere al titolare del trattamento (la struttura sanitaria) di ricevere in forma scritta (salva espressa richiesta dell'interessato di ricevere le stesse in forma orale, previa identificazione dell'istante) le informazioni relative al trattamento (anche attraverso strumenti elettronici) [7)]. Il Regolamento stabilisce che il titolare debba evadere la richiesta di informativa entro trenta giorni, salva la richiesta di proroga per un massimo di due mesi.

Le informazioni circa il trattamento devono essere fornite gratuitamente (l'obbligo di informativa costituisce, pertanto, un costo a carico del titolare), salvo che le richieste dell'interessato siano considerate infondate o eccessive: in tal caso l'interessato è obbligato a contribuire e il titolare può rifiutarsi di evadere la richiesta qualora le informazioni richieste siano già state fornite. L'onere della prova grava in ogni caso sul titolare.

Nuovi termini e adempimenti, pertanto, sono imposti alle strutture sanitarie al fine di evadere le richieste di accesso alla documentazione sanitaria e all'informativa sui dati personali: per tale ragione occorre che le strutture sanitarie affrontino un processo di rinnovamento rispetto alla gestione delle richieste e delle risorse coinvolte.

L'ultimo comma dell'art. 4 della legge n. 24/2017 impone alle strutture sanitarie obblighi di pubblicazione di tutti i dati di risarcimento erogati nell'ultimo quinquennio dall'azienda.

In questo caso, il coordinamento con la tutela della riservatezza e dei dati personali non deve essere sottovalutato sotto il profilo organizzativo.

6) S. Calzolaio, *Protezione dei dati personali*, *Dig. Giuffrè*, 2017, 1-44; F. Piraino, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, *Nuova giur. civ. comm.*, 2017, 369 ss.

7) La risposta deve essere intellegibile, concisa, trasparente e facilmente accessibile: il linguaggio utilizzato deve essere semplice e chiaro. Sono ammesse icone purché accompagnate da una informativa estesa.

L'oggetto dell'informativa varia a seconda che i dati personali siano raccolti (art. 13) o meno (art. 14) presso l'interessato. Le informazioni devono essere fornite anche in caso di modifica delle finalità di un trattamento in corso.L'informativa, in ogni caso, deve contenere: 1) i dati di contatto del responsabile della protezione dei dati (Data Protection Officer, DPO); 2) l'indicazione espressa dell'obbligo di tenere a disposizione dell'interessato l'elenco dei responsabili del trattamento; 3) l'indicazione espressa dell'obbligo di indicare il responsabile del trattamento per il riscontro all'interessato in caso di esercizio dei diritti; 4) l'indicazione espressa dell'obbligo di indicare le modalità del trattamento; 5) l'indicazione della base giuridica del trattamento (se da contratto, o su base volontaria); 6) l'indicazione specifica del legittimo interesse ad effettuare il trattamento; 7) l'indicazione espressa della possibilità del trasferimento all'estero nonché delle relative condizioni legittimanti; 8) l'indicazione del periodo di conservazione dei dati (tempi dettati per legge (1-5-10 anni) oppure in base alla necessità di adempiere alla motivazione del trattamento); 9) l'obbligo di indicazione espressa della possibilità di revoca del consenso; 10) l'indicazione espressa della possibilità di reclamo all'Autorità di controllo (Garante Privacy); 11) l'indicazione espressa delle notizie sui trattamenti automatizzati (anche parzialmente).

Si pensi alla recente sentenza del Tribunale di Palermo del 5.10.2017, con cui è stato risarcito il danno non patrimoniale, nella misura di 2.000 euro per ciascun ricorrente, in ragione del fatto che sulla banca dati della giurisprudenza della Sezione Giurisdizionale per la Regione Sicilia della Corte dei Conti erano presenti numerose sentenze relative a procedimenti finalizzati al conseguimento di trattamenti pensionistici, che contenevano riferimenti alle condizioni di salute dei ricorrenti. Si legge in motivazione che "*risulta acclarata la diffusione di alcuni dati concernenti lo stato di salute dei ricorrenti e, in particolare, determinate condizioni patologiche dalle quali gli stessi risultavano affetti* (...) [cui] *ordinariamente si accompagni uno stato di comprensibile disagio e tensione interiore: stato pregiudizievole, questo, che appare munito di connotati di "serieta" e "non futilita" tali da renderlo meritevole di ristoro per equivalente pecuniario*" [8].

In tale prospettiva appare quanto mai opportuno un coordinamento al livello aziendale tra gli uffici destinati alla gestione della piattaforma web per la pubblicazione dei dati relativi ai risarcimenti erogati nell'ultimo quinquennio con le figure di riferimento per la protezione dei dati personali (su cui *infra*).

3. Adempimenti delle strutture sanitarie sulla base del Regolamento UE/679/2016.

Abbiamo sin qui visto che, al fine di garantire trasparenza e sicurezza in materia di documentazione sanitaria, le strutture sanitarie sono chiamate a riordinare e/o rinnovare alcuni aspetti relativi ai processi gestionali in adempimento a specifici obblighi emergenti dalla Legge n. 24/2017 e che ciascun intervento, in ogni caso, non possa prescindere da una lettura della normativa in materia di protezione di dati personali. A ciò si deve aggiungere che il Regolamento UE/679/2016 ha introdotto nuovi adempimenti cui le organizzazioni, nella specie le strutture sanitarie pubbliche e private, sono obbligate a rispettare, onde evitare di incorrere in sanzioni e/o responsabilità.

In virtù del principio di *accountability*, infatti, spetta al titolare del trattamento porre in essere misure tecniche e organizzative adeguate (se del caso modificare e/o aggiornare quelle pre-esistenti) al fine di garantire, in ragione della natura, del contesto e delle finalità del trattamento, nonché della valutazione dei rischi per i pazienti, il rispetto della normativa europea in materia di protezione di dati personali.

Ai sensi dell'art. 30 del Regolamento, ad esempio, occorre che le strutture sanitarie con più di 250 dipendenti si dotino di un registro [9] delle attività in cui vengono enucleate

8) Trib. Palermo, 5 ottobre 2017, *inedita*.

9) Il registro deve contenere le seguenti informazioni ai sensi dell'art. 30 del Regolamento: il nome e i dati di contatto del titolare del trattamento e dell'eventuale DPO designato, le finalità del trattamento, una descrizione delle categorie di dati personali trattati e delle categorie di interessati, le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, gli eventuali trasferimenti di dati verso paesi terzi con l'indicazione delle

le modalità di esecuzione per ogni trattamento effettuato. Sulla base della mappatura dei trattamenti, sarà elaborata l'analisi dei rischi collegati.

Ancora, il titolare del trattamento di una struttura sanitaria è tenuto a procedere ad una valutazione d'impatto sulla protezione dei dati prima di iniziare il trattamento, analizzando in particolare il livello di rischio di violazione di diritti e le libertà delle persone fisiche interessate mediante il trattamento automatizzato / a mezzo di nuove tecnologie, ad esempio dei dati contenuti nelle cartelle cliniche dei pazienti.

La struttura sanitaria pubblica dovrà, inoltre, necessariamente designare un D.P.O. (Data Protection Officer, ovvero un responsabile per la protezione dei dati), una delle principali novità in materia [10], ai sensi dell'art. 37 lett. *a*) del Regolamento UE/679/2016; mentre, le strutture sanitarie private dovranno ragionevolmente dotarsi di un D.P.O. in ragione delle altre due ipotesi previste dall'art. 37: ovvero a norma della lett. *b*) se le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala e *c*) in ragione del trattamento su larga scala di dati appartenenti a speciali categorie (inclusi, ai sensi dell'art. 9 del Regolamento, i dati cc.dd. sanitari). Sebbene, infatti, le due condizioni richiamate possano essere suscettibili di interpretazione diverse, essendo basate su parametri indeterminati quali "attività principali del titolare" e "larga scala", appare – in ogni caso – opportuno includere l'obbligo di nomina di un D.P.O. per le strutture sanitarie [11].

Le strutture sanitarie dovranno, altresì, adeguarsi all'espletamento degli adempimenti necessari in caso di c.d. *data breach*, quali l'obbligo di notifica della violazione all'autorità di controllo senza ritardo, ove possibile entro settantadue ore, nonché l'obbligo di comunicazione all'interessato, sempre senza ritardo, con linguaggio semplice e chiaro.

Il breve e, senza dubbio non esaustivo, elenco degli obblighi cui le strutture sanitarie dovranno adeguarsi nelle prossime settimane in vista dell'entrata in vigore del Regolamento UE/679/2016 mostra le ricadute di quest'ultimo sul piano del buon funzionamento dell'apparato organizzativo-gestionale sanitario.

eventuali garanzie adeguate prescritte, ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati e la descrizione generale delle misure di sicurezza tecniche ed organizzative adottate.

10) L'art. 39 del Regolamento 679/2016 attribuisce al D.P.O. i seguenti compiti: "*a*) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; *b*) sorvegliare l'osservanza del GDPR, e delle altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; *c*) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'art. 35; *d*) cooperare con l'autorità di controllo; e e)fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione".

11) G. Comandè – G. Malgieri, Manuale per il trattamento dei dati personali, Il sole 24ore, 2018, 11 e ss.

4. Qualche considerazione conclusiva, in attesa delle prassi.

Il diritto alla salute, così come costituzionalmente enunciato all'art. 32 Cost., include oggi, oltre la tutela del diritto all'integrità psico-fisica, del diritto ad un ambiente salubre e del diritto alle prestazioni sanitarie, anche quella del diritto alla sicurezza delle cure [12)].

Quest'ultima componente, pilastro della nuova Legge n. 24/2017, si realizza anche attraverso la prevenzione e gestione del rischio derivante dall'erogazione delle prestazioni sanitarie, nonché l'adeguato utilizzo delle risorse strutturali, tecnologiche e organizzative che coinvolgono tutto il personale, indipendentemente dal tipo di rapporto di lavoro con la struttura sanitaria in questione [13)].

In senso lato, dunque, può affermarsi che la sicurezza delle cure si realizza, altresì, allorquando la struttura sanitaria, nell'assicurare ai pazienti il rispetto dei principi enunciati dal Regolamento UE/679/2016 in materia di protezione dei dati personali, adotti tutte le misure strutturali e organizzative volte ad assicurare il corretto adempimento degli obblighi imposti dalla normativa europea.

Il presente contributo ha voluto far emergere qualche interrogativo in ordine al non semplice coordinamento, sul piano pratico-gestionale, di due normative apparentemente distanti per ambito di applicazione e beni giuridici tutelati, ma al contempo simili rispetto all'individuazione di nuovi profili di rischio e responsabilità a carico delle strutture sanitarie.

Si consolideranno, auspicabilmente, delle buone prassi volte a garantire il pieno rispetto dei principi europei nell'ambito dell'erogazione delle prestazioni sanitarie.

12) Sull'evoluzione della tutela del diritto alla salute, per tutti, F.D. Busnelli - U. Breccia (a cura di), *Il diritto alla salute*, Il Mulino, Bologna, 1979; F.D. Busnelli - U. Breccia (a cura di), *Tutela del diritto alla salute e diritto privato*, Giuffrè, Milano 1978.

13) R. Breda, *La responsabilità civile delle strutture sanitarie e del medico tra conferme e novità*, in *Danno e resp.*, 2017, 283 ss.