Alma Mater Studiorum – Università di Bologna

DOTTORATO DI RICERCA IN
DIRITTO E NUOVE TECNOLOGIE

Ciclo XXIX

Settore Concorsuale di afferenza: 12/H3

Settore Scientifico disciplinare: IUS/20

Dossier sanitario: un approccio traslazionale alla disciplina del trattamento dei dati sanitari in ambito clinico

Presentata da: Luigi Rufo

Coordinatore Dottorato

Prof. Giovanni Sartor

Relatore

Prof.ssa Raffella Brighi

Correlatori

Dott. Michele Martoni
Dott. Stefano Dalmiani

Esame finale anno 2017

“Gran parte del progresso
sta nella volontà di progredire”

(da Lucio Anneo Seneca, *Lettere a Lucilio - 71, 36)*

INDICE

INDICE I

INDICE DELLE FIGURE V

INTRODUZIONE 1

1. Il Contesto 1

2. Gli obbiettivi della ricerca 6

3. Metodologia e struttura della ricerca 7

CAPITOLO I 9

eHealth: le informazioni in una struttura sanitariagestite tramite strumenti elettronici 9

1.1 I percorsi diagnostico-terapeutici ed i sistemi informativi a supporto 10

1.1.1 I sistemi informativi sanitari 13

1.1.2 I modelli informativi: relazioni vs documentali e ad eventi 15

1.1.3 I documenti sanitari 17

1.2 La Cartella Clinica Elettronica (CCE) 22

1.3 Il Dossier sanitario (DS) 25

1.3.1 Dossier Sanitario e FSE: tra differenze ed uguaglianza 28

1.4 Personal Health Record (PHR) 30

CAPITOLO II 33

La protezione dei dati personali: Linee guida sul Dossier Sanitario 33

2.1 Codice Privacy: i profili generali 36

2.1.1 I soggetti 39

2.1.2 I dati 41

2.1.3 I presupposti di legittimità: informativa consenso 43

2.1.4 Gli obblighi di sicurezza 46

2.1.5 Il Trattamento dei dati sanitari 48

2.2 Linee guida in materia di Dossier sanitario 50

2.2.1 L'informativa del Dossier sanitario 52

2.2.2 Il consenso al Dossier sanitario 53

2.2.3 I dati a maggior tutela 55

2.2.4 Diritto all'oscuramento 55

2.2.5 Finalità di ricerca scientifica 58

2.2.6 Profili di accesso e di sicurezza dei dati nel Dossier sanitario 59

2.3 Il Regolamento europeo: le principali novità in ambito sanitario 64
2.3.1 Informativa e Consenso 66
2.3.2 I nuovi diritti: diritto all'oblio e alla portabilità dei dati 68
2.3.3 Privacy by design e Privacy by default 70
2.3.4 Privacy Impact Assessment (PIA) 70
2.3.5 Principio di accountability 71
2.3.6 Il Data Protection Officer (DPO) 72
2.3.7 Data Breach 73
2.4 Breve riflessione e prime conclusioni 74
CAPITOLO III 75
La Privacy by Design 75
3.1 Privacy by design: "The 7 foundational principles" 78
3.1.1 Proattivo non reattivo – prevenire non correggere 80
3.1.2 Privacy come impostazione di default 80
3.1.3 Privacy incorporata nella progettazione 81
3.1.4 Massima funzionalità − Valore positivo, non valore zero 81
3.1.5 Sicurezza fino alla fine − Piena protezione del ciclo vitale 81
3.1.6 Visibilità e trasparenza − Mantenere la trasparenza 82
3.1.7 Rispetto per la privacy dell'utente − Centralità dell'utente 82
3.2 Dossier sanitario: un approccio alla *Privacy by design* 82
3.2.1 Analisi e progettazione nella visione Privacy by design 85
CAPITOLO IV 87
Case Study: Progettazione di un Dossier Sanitario 87
4.1 Introduzione all'ambito e Istituzione del case Study: Fondazione G. Monasterio 87
4.1.1 Ricerca tecnologica 91
4.1.2 Approccio multidisciplinare 93
4.1.3 La storia tecnologia della Fondazione G. Monasterio 93
4.1.4 Processi sanitari 95
4.1.5 Obiettivi della Ricerca applicata 98
4.2 Analisi preliminare del Dossier sanitario: l'uso di *UML* 98
4.3 Progettazione del "Dossier Sanitario" con metodologia *Privacy by design* e *UML* 102
4.3.1 SC01 - Consultazione dell'Informativa 107

4.3.2 SC02 - Consenso Apertura Dossier sanitario ... 109
4.3.3 SC03 - Consenso Importazione dati e documenti pregressi ... 112
4.3.4 SC04 - Consenso per dati "a maggior tutela" ... 115
4.3.5 SC05 - Consenso dati finalità di Ricerca ... 118
4.3.6 SC06 - Consenso Consultazione Dossier Sanitario ... 121
4.3.7 SC07 - Consenso consultazione "Console del paziente" ... 124
4.3.8 SC08 - Consultazione del Dossier da parte dell'Operatore sanitario ... 127
4.3.9 SC09 - Alimentazione sistemi informatici ... 130
4.3.10 SC10 - Verifica esistenza dei dati del paziente ... 133
4.3.11 SC11 - Revoca Apertura Dossier ... 135
4.3.12 SC12 – Decesso del Paziente ... 138
4.3.13 SC13 - Annullamento Dossier ... 141
4.3.14 SC14 – Richiesta oscuramento dei dati ... 143
4.3.15 SC15 – Gestione Dati oscurati ... 146
4.3.16 SC16 – Richiesta de-oscuramento Dati ... 150
4.3.17 SC17 - Consenso paziente minore / sottoposto a tutela ... 153
4.3.18 SC18 - Consenso Importazione dati e documenti pregressi paziente minore / sottoposto a tutela ... 156
4.3.19 SC19 – Consenso dati "a maggior tutela" paziente minore/sottoposto a tutela 159
4.3.20 SC20 - Consenso dati finalità di Ricerca paziente minore / sottoposto a tutela 163
4.3.21 SC21 - Scadenza del dossier a seguito della maggiore età del paziente ... 166
4.3.22 SC22 - Riattivazione del dossier a seguito della maggiore età del paziente ... 168
4.3.23 SC23 – Gestione Dati a maggior tutela ... 171
4.3.24 SC24 - Gestione Finalità di ricerca anonima ... 176
4.3.25 SC25 - Gestione Finalità di ricerca aggregata ... 179
4.3.26 SC26 – Rilascio delega per accesso dossier ... 183
4.3.27 SC27 - Gestione visualizzazione dossier con delega ... 185
4.4 Applicazioni degli Use Case in strumenti di gestione del dossier ... 187
4.4.1 Strumenti per i pazienti ... 187
4.4.2 Strumenti per gli operatori sanitari ... 192
CONCLUSIONI ... 195
APPENDICE ... 202
Normativa Nazionale in tema di *"Sanità elettronica"* ... 202
Struttura del Codice Privacy (D. Lgs. 196/2003) ... 206

Modello “Informativa Dossier sanitario” 210
Modello “Consenso trattamento dati con DS” 215
Modello “Oscuramento / Deoscuramento dei dati” 217
Modello “Revoca Alimentazione e consultazione DS” 219
Modello Valutazione del rischio e Check-List delle misure di sicurezza nel DS 221
BIBLIOGRAFIA 222

INDICE DELLE FIGURE

Figura 1. Rappresentazione grafica del concetto di empowerment 4
Figura 2. Supporto dell'ICT nella progettazione, gestione, e valutazione dei PDTA 12
Figura 3. Differenza tra Database SQL vs NoSQL 17
Figura 4. I 7 principi fondanti della Privacy by design 79
Figura 5. Diagramma dell'andamento dei ricoveri degli stabilimenti di Pisa e Massa dal 1992 al 2009 89
Figura 6. Sistema di Valutazione della Performance del Sistema Sanitario Toscano è affidato al Laboratorio Management e Sanità della Scuola Superiore Sant'Anna di Pisa (MeS) – Anno 2014 91
Figura 7. Schema approccio contenuti di ricerca 92
Figura 8. Schema approccio multidisciplinare nell'ambito clinico.....93
Figura 9. Programma Speciale Ministero della salute – art. 12 comma 2, lettera h, D. Lgs 502/92 Regione Toscana.....94
Figura 10. Esempio di un classe.....100
Figura 11. Rappresentazione grafica delle "relazioni di associazioni".....101
Figura 12. Schema generale dei Casi d'uso 103
Figura 13. Schema modello informativo generale.....104
Figura 14 Interaction model Generale 105
Figura 15. Diagramma degli stati del Dossier.....106
Figura 16. UCM D01 "Consultazione dell'informativa".....107
Figura 17. Information Model "Consultazione dell'informativa".....108
Figura 18. Interaction Model "Consultazione dell'informativa".....108
Figura 19. UCM D02 "Consenso Apertura Dossier sanitario" 109
Figura 20. Information Model Generale "Consenso Apertura Dossier sanitario".....110
Figura 21. Information model contenuto minimo "Consenso Apertura Dossier sanitario" 111
Figura 22. Interaction Model "Consenso Apertura Dossier sanitario" 111
Figura 23. UCM D03 "Consenso Importazione dati e documenti pregressi".....112
Figura 24. Information Model Generale "Consenso Importazione dati e documenti pregressi".....113
Figura 25. Information Model contenuto minimo "Consenso Importazione dati e documenti pregressi".....114
Figura 26. Interaction Model "Consenso importazione dati e documenti pregressi" ...114
Figura 27. UCM D04 "Consenso per dati a maggior tutela" 115
Figura 28. Information Model Generale "Consenso per dati a maggior tutela".....116
Figura 29. Information Model contenuto minimo "Consenso per dati a maggior tutela" 117
Figura 30. Interaction Model Dati a maggior tutela 117
Figura 31. UCM D05 "Consenso dati finalità di Ricerca" 118
Figura 32. Information Model Generale "Consenso dati finalità di Ricerca".....119
Figura 33. Information Model contenuto minimo "Consenso dati finalità di Ricerca"120
Figura 34. Interaction Model Consenso finalità di ricerca 120
Figura 35. UCM D06 "Consenso Consultazione Dossier sanitario".....121
Figura 36. Information Model Generale "ConsensoConsultazione Dossier sanitario" 122

Figura 37. Information Model contenuto minimo “Consenso Consultazione Dossier sanitario” 123
Figura 38. Interaction Model “Consultazione Dossier sanitario” 123
Figura 39. UCM D07 “Consenso Consultazione console paziente” 125
Figura 40. Information Model Generale “Consenso Consultazione Console paziente” 125
Figura 41. Information Model contenuto minimo “Consenso Consultazione Console paziente” 126
Figura 42 Interaction Model “Consultazione Console paziente” 126
Figura 43. UCM D08 “Consultazione del Dossier da parte dell’Operatore sanitario” 127
Figura 44. Information Model Generale “Consultazione del Dossier da parte dell’Operatore sanitario” 128
Figura 45. Information Model contenuto minimo “Consultazione del Dossier da parte dell’Operatore sanitario” 129
Figura 46. Interaction Model “Consultazione del Dossier da parte dell’Operatore sanitario” 129
Figura 47. UCM D09 “Alimentazione sistemi informativi” 130
Figura 48. Information Model Generale “Alimentazione sistemi informativi” 131
Figura 49. Interaction Model “Alimentazione sistemi informativi” 132
Figura 50. UCM D10 “Verifica esistenza dei dati del paziente” 133
Figura 51. Information Model Generale “Verifica esistenza dati del paziente” 134
Figura 52. Interaction Model “Verifica esistenza dati del paziente” 134
Figura 53. UCM D11 “Revoca apertura dossier” 136
Figura 54. Information Model Generale “Revoca apertura dossier” 136
Figura 55. Information Model contenuto minimo “Revoca apertura dossier” 137
Figura 56. Interaction Model “Revoca apertura dossier” 137
Figura 57. UCM D12 “Decesso del paziente” 138
Figura 58. Information Model Generale “Decesso del paziente” 139
Figura 59. Information Model contenuto minimo “Decesso del paziente” 140
Figura 60. Interaction Model “Decesso paziente” 140
Figura 61. UCM D13 “Annullamento Dossier” 141
Figura 62 Information Model Generale “Annullamento Dossier” 142
Figura 63. Interaction Model “Annullamento Dossier” 142
Figura 64. UCM D14 “Richiesta accesso e oscuramento dei dati” 144
Figura 65. Information Model Generale “Richiesta oscuramento dei dati” 144
Figura 66. Information Model contenuto minimo “Richiesta oscuramento dei dati” 145
Figura 67. Interaction Model “Richiesta oscuramento dati” 145
Figura 68. UCM D15 “Gestione dati oscurati” 147
Figura 69. Information Model Generale “Gestione dati oscurati” 148
Figura 70. Information Model contenuto minimo “Gestione dati oscurati” 149
Figura 71. Interaction Model “Gestione dati oscurati” 149
Figura 72. UCM D16 “Gestione de-oscuramento dati” 150
Figura 73. Information Model Generale “Gestione de-oscuramento dati” 151
Figura 74. Information Model contenuto minimo “Gestione de-oscuramento dati” 152
Figura 75. Interaction Model “Gestione de-oscuramento dati” 152
Figura 76. UCM D17 “Consenso paziente minore / sottoposto a tutela” 153

Figura 77. Information Model Generale “Consenso paziente minore / sottoposto a tutela”.....154
Figura 78. Information Model contenuto minimo “Consenso paziente minore / sottoposto a tutela”.....155
Figura 79. Interaction Model “Consenso paziente minore / sottoposto a tutela”.....155
Figura 80. UCM D18 “Consenso Importazione dati e documenti pregressi paziente minore / sottoposto a tutela” 156
Figura 81. Information Model Generale “Consenso Importazione dati e documenti pregressi paziente minore / sottoposto a tutela”.....157
Figura 82. Information Model contenuto minimo “Consenso Importazione dati e documenti pregressi paziente minore / sottoposto a tutela”.....158
Figura 83. Interaction Model “Consenso importazione dati e documenti pregressi” ...158
Figura 84. UCM D19 “Consenso per dati “a maggior tutela” paziente minore / sottoposto a tutela”.....159
Figura 85. Information Model Generale “Consenso dati a maggior tutela paziente minore / sottoposto a tutela” 160
Figura 86. Information Model contenuto minimo “Consenso dati a maggior tutela paziente minore / sottoposto a tutela” 161
Figura 87. Interaction Model “Consenso dati a maggior tutela paziente minore / sottoposto a tutela”.....161
Figura 88. UCM D20 “Consenso dati finalità di Ricerca paziente minore / sottoposto a tutela”.....163
Figura 89. Information Model Generale “Consenso finalità di ricerca paziente minore / sottoposto a tutela”.....164
Figura 90. Information Model contenuto minimo “Consenso finalità di ricerca paziente minore / sottoposto a tutela” 165
Figura 91. Interaction Model “Consenso finalità di ricerca paziente minore / sottoposto a tutela” 165
Figura 92. UCM D21 “Scadenza del dossier a seguito della maggiore età del paziente” 166
Figura 93. Information Model Generale “Scadenza del dossier a seguito della maggiore età del paziente” 167
Figura 94 Interaction Model “Scadenza del dossier a seguito della maggiore età del paziente” 167
Figura 95. UCM D22 “Riattivazione del dossier a seguito della maggiore età del paziente” 168
Figura 96. Information Model Generale “Riattivazione del dossier a seguito della maggiore età del paziente” 169
Figura 97. Information Model contenuto minimo “Riattivazione del dossier a seguito della maggiore età del paziente”.....170
Figura 98 Interaction Model “Riattivazione del dossier a seguito della maggiore età del paziente” 170
Figura 99. UCM D23 “Gestione Dati a maggior tutela”.....172
Figura 100. Information Model Generale “Gestione Dati a maggior tutela”.....173
Figura 101. Information Model contenuto minimo “Gestione Dati a maggior tutela” 174
Figura 102. Interaction Model contenuto minimo “Gestione Dati a maggior tutela”...175
Figura 103. UCM D24 “Gestione Finalità di ricerca anonima”.....177
Figura 104. Information Model Generale “gestione finalità di ricerca anonima” 177

Figura 105 Information Model contenuto minimo "gestione finalità di ricerca anonima" 178
Figura 106. Interaction Model contenuto minimo "Gestione Finalità di ricerca anonima" 178
Figura 107. UCM D25 "Gestione Finalità di ricerca aggregata" 180
Figura 108. Information Model Generale "Gestione Finalità di ricerca aggregata" 181
Figura 109. Information Model contenuto minimo "Gestione Finalità di ricerca aggregata" 182
Figura 110. Interaction Model contenuto minimo "Gestione Finalità di ricerca aggregata" 182
Figura 111. UCM D26 "Rilascio delega accesso Dossier" 183
Figura 112. Information Model "Rilascio delega accesso Dossier" 184
Figura 113. Interaction Model "Rilascio delega accesso Dossier" 184
Figura 114. UCM D27 "Gestione visualizzazione dossier con delega" 185
Figura 115. Information Model "Gestione visualizzazione dossier con delega" 186
Figura 116. Interaction Model "Gestione visualizzazione dossier con delega" 186
Figura 117. Interfaccia di accesso e di consultazione del Dossier attraverso *APP* 187
Figura 118. Interfaccia di accesso attraverso sito web 188
Figura 119. Interfaccia Login e Benvenuto via sito web 189
Figura 119. Interfaccia di Ricerca (A) e di consultazione (B) della lista referti 190
Figura 121. Interfaccia di consultazione (A) e di visualizzazione (B) dei referti 191
Figura 122. Accesso ai sistemi senza consenso al Dossier 192
Figura 123. Esempio di acquisizione del consenso alla apertura. 193
Figura 124. Esempio di uso del dossier da parte di un medico radiologo nella refertazione di una indagine TAC. 193
Figura 125. Esempio di visualizzazione sintetica Dossier per la consultazione integrata in una cartella clinica di ricovero. 194

INTRODUZIONE

1. Il Contesto

La grande rivoluzione tecnologica che ha preso il via da pressappoco due decenni si sta conducendo a tappe forzate verso la fase matura della cosiddetta *"era del digitale"*[1], nella quale le informazioni nativamente o in via derivativa digitali costituiranno il principale bene economico e nuovo paradigma socio-tecnologico delle attività umane.

Le tecnologie digitali stanno mutando abitudini, stili di vita, i modi di comunicare degli individui. Per taluni, gli smartphone e i tablet sono oramai da intendersi come una vera e propria appendice del corpo umano: un "corpo esteso"[2] dotato di autonomia evolutiva e costituito da flussi immateriali di informazioni che possono essere elaborate.

Questo nuovo paradigma sta interessando e modificando, tra gli altri, anche il settore della Sanità; d'altronde, la medicina stessa è una scienza che utilizza le informazioni dei pazienti per calibrare al meglio su di loro gli opportuni interventi terapeutici.

In base a tale assunto è interessante notare come anche lo stesso principio del diritto alla salute, tutelato nel nostro ordinamento dalla Carta fondamentale (art. 32)[3] e dalla giurisprudenza della Corte Costituzionale[4], sia nel tempo mutato, crescendo in livelli di tutela e prestazioni accessibili, condividendo oramai poco o nulla con le sue declinazioni di epoca pre-repubblicana[5].

Il diritto alla salute nella sua dimensione oggi, socialmente e costituzionalmente, acquisita si presenta, pertanto, come "*fondamentale diritto dell'individuo e interesse*

---

[1] *Cfr.* G. Pascuzzi, *Il diritto dell'era digitale*, il Mulino, Bologna 2010, pp.14-8.

[2] *Cfr.* M. Mancarella, *eHealth e diritti. L'apporto dell'Informatica giuridica*, Carocci, Roma 2014, p. 15.

[3] "*La Repubblica tutela la salute come fondamentale diritto dell'individuo e interesse della collettività, e garantisce cure gratuite agli ingenti* […]".

[4] v. Corte Costituzionale 12 luglio 1979, n. 88 in cui si afferma: *"il bene salute è tutelato all'art.32 della Costituzione non solo come interesse della collettività, ma anche e soprattutto come diritto fondamentale dell'individuo, sicché si configura come un diritto primario e assoluto, pienamente operante anche nei rapporti tra privati".*

[5] Note sono le parole di Cammeo, nei primi anni del secolo scorso, che identificava *"il fine pubblico della sanità nell'interesse dello Stato ad avere una popolazione sana e numerosa, poiché la sanità e il numero della popolazione è un presupposto necessari della potenza dello Stato"* , pertanto la tutela della salute era in quel periodo per tradizione concepita in senso assai riduttiva, in quanto era il singolo individuo a doversi preoccupare della tutela della propria salute, intesa come assenza di malattie capaci di arrecare danni al proprio fisico. (CAMMEO-VITTA, *Sanità Pubblica, in Trattato di diritto amministrativo italiano,* a cura di V.E. Orlando, IV, 2° parte, Milano, 1905, 213).

della collettività"[6] e incrementa costantemente (coniugato con le varie istanze di natura etica, finanziaria, medica che ad esso si accompagnano) la propria centralità nell'azione politica-amministrativa dei pubblici poteri[7] e nella pianificazione di interventi sul piano tecnologico a relativo supporto, efficaci ed efficienti e capaci di assicurare ad ogni individuo la possibilità di accedere alle prestazioni sanitarie di prevenzione, cura e riabilitazione.

Alla centralità del diritto alla salute nelle attenzioni della collettività e del legislatore fanno però da contraltare disponibilità economiche pubbliche[8] sempre più a stento bastevoli a soddisfare la crescente domanda di cure, in una società che invecchia e che ha visto crescere, quale esito non necessariamente reversibile della crisi economica degli anni scorsi, nuove fasce di povertà. L'applicazione delle tecnologie digitali al mondo della sanità, nel contesto appena descritto, può fungere da importante ausilio che consenta di ridurre la distanza tra due punti di partenza apparentemente tanto inconciliabili.

Così sia a livello Comunitario con l'attuazione del Piano d'azione europeo *eHealth* 2004[9] , rivolto al miglioramento della qualità dell'assistenza sanitaria attraverso l'uso strumenti digitali, sia a livello nazionale con il Piano settoriale *eGov*[10] 2012, con

---

[6] *Cfr.* L. Montuschi, in Commentario della Costituzione a cura di G. BRANCA, *Rapporti etico-sociali (Art. 29-34)*, Bologna Roma, 1975, sub art. 32, pp.146 ss. Sul diritto alla salute si veda: R. Ferrara, *Il diritto alla salute: principi costituzionali*, in Salute e sanità, a cura di R. Ferrara, in Trattato di biodiritto, diretto da S. Rodotà, P. Zatti, Milano, 2010, pp. 3 ss.; R. Balduzzi, voce *Salute* (diritto alla), in Diz. Dir. Pubbl., diretto da S. Cassese, vol. VI, Milano, 2006, p. 2593; P. Vincenti Amato, *Art. 32*, in Commentario alla Costituzione, a cura di G. Branca, Bologna, 1975; M. Luciani, *Brevi note sul diritto alla salute nella recente giurisprudenza costituzionale*, in L. Chieffi (a cura di), *Il diritto alla salute alle soglie del terzo millennio. Profili di ordine etico, giuridico ed economico*, Giappichelli, Torino 2003, pp. 63-71.

[7] Moltitudini di istanze che non devono certo minare la "*Grundnorm"* che secondo Hans Kelsen (esponente del Normativismo) è la norma fondamentale, posta a fondamento di validità di tutto il sistema di norme costruito a gradini, di un ordinamento giuridico e che in senso logico è la Costituzione. Per un approfondimento sul tema si veda H. Kelsen, *Allgemeine Staatslehre*, Berlin 1925.

[8] Il diritto alla salute è un diritto finanziariamente condizionato, sul punto si veda F. Merusi, *Servizi pubblici instabili*, Bologna, 1990 e R. Ferrara, *L'ordinamento della sanità*, in Sistema del diritto amministrativo italiano, diretto da F. G. Scoca, F. A. Roversi Monaco, G. Morbidelli, Torino, 2007, pp. 111 ss. che inquadra precisamente i diritti finanziariamente condizionati in *"posizioni soggettive il cui essere diritti in senso proprio e pieno appare subordinato ai flussi della finanza pubblica, ossia al fatto che vi siano, nel concreto, le disponibilità di bilancio atte a rendere possibili il riconoscimento e la tutela"*.

[9] Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni, del 30 aprile 2004 - http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=URISERV:l24226f&from=IT (ultimo accesso giugno 2017)

[10] Il Piano e-Gov 2012 è stato lanciato nel 2009 e tra i contenuti oggetto d'attuazione per la Sanità digitale troviamo: l'identificazione del cittadino e la rilevazione delle prestazioni sanitarie erogate mediante l'adozione della Tessera Sanitaria; la creazione di un'unica infrastruttura in rete di tutti i soggetti prescrittori (es. medici di base, pediatri, aziende ospedaliere etc); l'invio telematico delle prescrizioni e dei certificati di malattia da parte dei Medici del SSN; il Fascicolo sanitario elettronico (FSE) per l'archiviazione e accesso alle informazioni sanitarie dei singoli cittadini; lo sviluppo del sistema integrato dei Centri Unici di Prenotazione (CUP).

il quale il legislatore ha analizzato e affrontato la tematica dell'informatizzazione dei processi di cura dei pazienti, si è andato via via sviluppando il concetto di *eHealth*.

A tutt'oggi non esiste una chiara e precisa definizione di questo termine. L'Organizzazione Mondiale della Sanità (OMS), che ha costituito il "Global Observatory for e-Health", a fronte di più di una moltitudine di definizioni, ne ha data una molto generica ma certamente semplice da interpretare: "*the use of information and communication technologies for health"*, descrivendo l'*eHealth* come *"a network, global thinking".*

Dal canto suo, G. Eysenbach, autorevole studioso dell'Università di Toronto, ha più volte ribadito che:

l'eHealth è un settore emergente interdisciplinare tra informatica medica, salute pubblica e affari, con riferimento ai servizi sanitari e le informazioni distribuite o elaborate attraverso Internet e le tecnologie correlate. In un senso più ampio, il termine caratterizza non solo lo sviluppo tecnologico, ma anche una scuola di pensiero, un modo di pensare, un atteggiamento, e un impegno al pensiero globale in rete, al fine di migliorare l'assistenza sanitaria a livello locale, regionale, e mondiale utilizzando le tecnologie dell'informazione e della comunicazione[11].

Anche se, è bene precisarlo, sembra abbastanza chiaro che l'*eHealth* è molto di più che un mero sviluppo tecnologico e che come rileva la dottrina ad oggi costituita sul tema[12], esso è un concetto ben diverso da "sanità elettronica" o "sanità digitale", locuzioni affermatesi nel periodo pre-Internet e che quindi sono prive di quel *quid pluris* rappresentato proprio dall'evoluzione telematica della Rete[13].

Alla luce di quanto detto le potenzialità applicative, in parte ancora inesplorate, degli strumenti tecnologici in parola rappresentano un punto di forza, ben potendo essi raccogliere la sfida che propone l'attuale concezione del diritto alla salute fondato sulla centralità del paziente e sulla condivisione e gestione delle informazioni cliniche che lo riguardano, così da favorirne l' em*powerment* (c.d. *patient empowerment*).

---

[11] G. Eysenbach, *What is e-health?, J Med Internet Res 2001* - vedi sito http://www.jmir.org/2001/2/e20/ (ultima consultazione giugno 2017).

[12] Mancarella, *eHealth e Diritti,* cit., p. 16.

[13] T. Schael, *Sanità elettronica e servizi digitali al cittadino. La rivoluzione delle ricette e dei certificati di malattia,* in "E-Healthcare", 3, 2009, p.13.

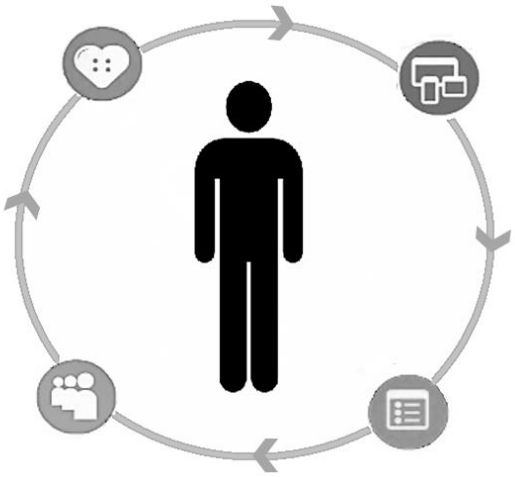


Figura 1. Rappresentazione grafica del concetto di empowerment

Con *patient empowerment*[14] si sottintende, infatti, un processo di sviluppo personale (v. Figura 1) nel quale il paziente, in una relazione di *partnership* con il professionista sanitario, viene dotato di conoscenza, capacità e una maggiore consapevolezza sui trattamenti sanitari che lo interessano. Un flusso informativo non unidirezionale, ma bidirezionale o, ancor più precisamente, circolare.

Si vuole così arrivare a modificare il ruolo del paziente che con l'utilizzo di nuovi strumenti tecnologici (nello specifico: *Podcast, Blog, Social Networks* e *apps),* potrà assumere un ruolo sempre più propositivo, da soggetto e non più da oggetto della relazione medica, e nuovo produttore di proposte terapeutiche[15].

A conferma di ciò, negli ultimi anni, nella letteratura scientifica medica si sta facendo spazio il concetto *P4 Medicine*[16] (più precisamente è la medicina delle quattro P: "predittiva, preventiva, personalizzata e partecipativa")[17], che consente, attraverso un

---

[14] Per maggiore un approfondimento si veda: L. Buccoliero, *E-HEALTH 2.0 - Tecnologie per il patient empowerment*, Mondo digitale n. 4, 2010; G. Ferrando, Diritto alla salute e autodeterminazione, tra diritto europeo e costituzione, in Politica del diritto, XLIII, 1, 2012.

[15] Come emerge dalla pratica, questi strumenti, prevedendo la creazione esplicita di connessioni tra le persone, formando una rete complessa di relazioni che facilitano lo scambio d'informazioni e la collaborazione nei processi di cura tra pazienti. Sul punto si veda Jingquan Li, Privacy policies for health social networking sites, J Am Med Inform Assoc., 2013, 0:1-4. doi:10.1136/amiajnl-2012-001500.

[16] *Cfr.* A.D. Weston, L. Hood, *Systems biology, proteomics, and the future of health care: toward predictive, preventative, and personalized medicine*, J. Proteome Res., 3 (2004), pp. 179-196; P. Cappelletti, *La Medicina Personalizzata fra ricerca e pratica clinica: il ruolo della Medicina di Laboratorio,* RIMeL / IJLaM 2009; 5(Suppl.):26-32; Q. TIAN, *et al. Systems cancer medicine: towards realization of predictive, preventive, personalized and participatory (P4) medicine,* J. Intern. Med., 271 (2012), pp. 111-121.

[17] "Personalizzata", in cui si tiene conto del profilo genetico e corporeo di una persona; "Preventiva" che prevede i problemi di salute e che punta al benessere del paziente; "Predittiva" che riscontra alla malattia con un trattamento adeguato ed evitando così eventuali controindicazioni; "Partecipativa" che abilita i pazienti ad assumersi maggiori responsabilità per la loro salute e cure

coinvolgimento attivo del paziente, di perseguire una doppia funzione di prevenzione, intesa sia come primario tentativo di evitare o rallentare l'evoluzione della malattia, sia di *screening* per contrastare le eventuali complicanze.

Da quanto sinora detto è facilmente comprensibile che la gestione dei servizi di cura attraverso l'impiego di sistemi informativi forniti dall'*eHealth*, sempre opportunamente regolamentati, può migliorare l'accesso alle cure e la collaborazione tra i medici e gli operatori sanitari.

Proprio con riguardo a ciò, il legislatore italiano[18], in quattro tappe – *i)* D.L. 13 settembre 2012, n. 158; *ii)* D.L. 18 ottobre 2012, n. 179 che ha previsto, nella IV sezione, l'art. 12 - Fascicolo sanitario elettronico e sistemi di sorveglianza nel settore sanitario - e l'art. 13 -Prescrizione medica e cartella clinica; *iii)* Decreto del "Fare" approvato a giugno 2013; *iv)* DPR del 29 settembre 2015 n. 17, con cui sono state definite le regole con le quali le Regioni devono predisporre il proprio sistema di Fascicolo sanitario elettronico – ha voluto adottare misure volte ad introdurre concretamente nell'ordinamento strumenti che, oltre a migliorare l'efficienza, l'efficacia e l'appropriatezza delle cure, aiutino i pazienti a gestire e tener aggiornati i propri dati e informazioni in una propria cartella sanitaria in totale autonomia e autodeterminazione.

Il paziente, grazie a queste nuove tecnologie, da utilizzare con le opportune cautele, non sarà più, sperabilmente, prigioniero di un'asimmetria informativa cieca e tacita, ma si troverà inserito in un "mondo virtuale" in grado di garantirgli maggior consapevolezza del proprio stato di salute e il perseguimento di un miglior percorso terapeutico.

In tale prospettiva, nel corso degli ultimi anni è stata avviata una significativa attività di innovazione ed implementazione dei sistemi informativi sanitari da parte del Ministero della Salute e delle Regioni con le strutture sanitarie, pubbliche e private convenzionate, per valorizzare una partecipazione attiva e consapevole del paziente "digitale"[19].

Un mezzo agile e il cui impiego è particolarmente indicato per raggiungere le auspicate finalità dell'*eHealth* è il Dossier sanitario (DS), considerato oggi, in Italia, insieme al già noto Fascicolo sanitario elettronico (FSE), lo strumento migliore per

---

mediche. *Cfr.* L. Hood, *Systems Biology and P4 Medicine: Past, Present, and Future,* in Rambam Maimonides Med J. 2013 Apr 30;4(2):e0012. doi: 10.5041/RMMJ.10112.

[18] *Infra, Norme in tema di sanità digitale,* in Appendice, pp. 203-206.

[19] *Cfr.* M. G. Virone, *Il Fascicolo Sanitario Elettronico. Sfide e bilanciamenti fra Semantic Web e diritto alla protezione dei dati personali*, Aracne, 2015, p. 145.

permettere a più organismi sanitari e professionisti di archiviare e condividere tra loro i dati e le informazioni sulla salute di un medesimo individuo.

Il Garante per la Protezione dei Dati Personali, chiamato ad esprimersi sul DS, lo ha definito come una delle *"numerose iniziative in atto volte a migliorare l'efficienza del servizio sanitario attraverso un ulteriore sviluppo delle reti ed una più ampia gestione informatica e telematica di atti, documenti e procedure"*.[20]

Tuttavia, a livello nazionale vi è stato fin dal principio, e tuttora perdura, un deficit normativo con riguardo ad esso, soprattutto di norme cogenti sulle modalità di strutturazione e di impiego del Dossier, mancando quindi le coordinate "di sistema" che ne consentano uno sviluppo omogeneo; in quanto strumento di titolarità delle singole strutture sanitarie, esso è stato quindi implementato con modalità diverse nelle varie realtà in cui è operativo, rispondendo cionondimeno alle esigenze degli specifici contesti di impiego.

Essendo variegate le esperienze e le modalità applicative di partenza, neanche il sopraggiungere delle Linee guida del Garante sul Dossier sanitario[21] nel giugno 2015 non ha sortito un effetto di armonizzazione, queste sono state infatti diversamente interpretate dalle singole Direzioni sanitarie aziendali e implementate attraverso l'uso di applicativi spesso non interoperabili tra loro.

Non è, inoltre, di secondaria importanza sottolineare che recenti accertamenti ispettivi del Garante Privacy sul Dossier sanitario hanno evidenziato un rilevante numero di criticità legate alla sua implementazione, sul piano della non conformità alla disciplina sul trattamento dei dati personali e sensibili.

2. Gli obiettivi della ricerca

Obiettivo generale della presente ricerca è stata la ricostruzione sistematica dello stato dell'arte in materia di Dossier sanitario, con primaria attenzione ai percorsi diagnostici terapeutici assistenziali, alla documentazione sanitaria, alla protezione dei dati personali, nonché alle interrelazioni tra tale strumento e il Fascicolo sanitario elettronico e i Personal Health Record (PHR).

Obiettivo specifico è stato fornire, alla luce delle criticità esistenti e dei ripetuti provvedimenti dell'Autorità Garante per la protezione dei dati personali, indicazioni interpretative ed applicative delle Linee guida sul Dossier sanitario del 2015 e del

[20] Sul punto si veda Garante Privacy, consultazione pubblica in materia di "*Linee guida in tema di Fascicolo sanitario elettronico e dossier sanitario*". [doc. web n. 1598313].

[21] Sul punto si veda Garante Privacy, Registro dei provvedimenti n. 331 del 4 giugno 2015, [doc. web n. 4084632].

recente Regolamento Europeo in materia di protezione dei dati personali, in modo da proporre una soluzione applicativa di Dossier sanitario in grado di migliorare l'efficacia delle cure, l'efficienza dei processi sanitari e la qualità complessiva del servizio offerto dai vari operatori sanitari coinvolti, indipendentemente dalla localizzazione fisica del paziente all'interno della struttura, grazie alla condivisione tra loro delle informazioni fondamentali.

Il percorso d'analisi compiuto ha così permesso di addivenire - attraverso la modellazione UML (*unified modeling language*), linguaggio che in ambito informatico serve a specificare le caratteristiche di un nuovo sistema, oppure a documentarne uno già esistente - al concreto sviluppo di un sistema Dossier integrato per la gestione informatizzata, uniforme, aggiornata e integrata dei dati anagrafici, clinici e sanitari del paziente all'interno di una determinata struttura sanitaria pubblica o privata, cercando di sopperire, ove necessario, alle carenze normative che riguardano tale strumento e tenendo conto del diritto di autodeterminazione alle cure espresso dal paziente.

3. Metodologia e struttura della ricerca

Il presente lavoro, redatto a conclusione XXIX ciclo del dottorato di ricerca in "Diritto e nuove tecnologie" presso il CIRSFID dell' Università di Bologna, si colloca in un contesto multidisciplinare (informatica giuridica, diritto dell'informatica, diritto amministrativo, diritto costituzionale, scienza medica, ingegneria medica) caratterizzato da un impiego fortemente complementare alle materie citate in una prospettiva di analisi unitaria e completa rispetto al fenomeno oggetto di indagine, che ha consentito di definire, attraverso l'analisi delle norme vigenti, le pronunce dell'Autorità Garante, lo studio tecnico di progetti DS attualmente in fase di sviluppo e un'attività di ricerca applicata di 18 mesi presso la sede di Pisa della Fondazione del CNR e Regione Toscana "Gabriele Monasterio", le caratteristiche architetturali di un Dossier sanitario e le relative potenzialità.

L'elaborato è stato suddiviso in quattro parti, di cui: la prima, dedicata agli aspetti della diffusione dell'innovazione tecnologica in ambito sanitario e, più in particolare, sui sistemi informativi in uso presso le strutture sanitarie, con uno sguardo a quelli che possono essere gli scenari futuri; la seconda, incentrata sui principali diritti e strumenti contenuti nelle Linee guida del Dossier sanitario emanate dal Garante, con un chiaro richiamo alle più recenti evoluzioni normative nazionali e comunitarie, da ultimo il recente Regolamento EU 2016/679 in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali; la terza, volta ad approfondire i principi della *Privacy by design* utilizzati per costruire un Dossier sanitario adeguato sul piano della

sicurezza informatica e “paziente-centrico” e infine l’ultima parte, elaborata durante il lavoro di analisi e di progettazione di un Dossier sanitario, svolto presso la Fondazione G. Monasterio del CNR di Pisa, che ha permesso, attraverso la modellazione UML di “Casi d’uso”, una descrizione puntuale delle “modalità” di utilizzo del sistema informativo da parte di un utilizzatore (attore), secondo modelli tra loro in relazione e rappresentati da peculiari diagrammi che, “ritagliati” in base alle specifiche esigenze dei progettisti e dei progetti, focalizzano solo ciò che serve nello specifico contesto. Infatti, partendo da informativa e consenso – elementi imprescindibili di un lecito trattamento dei dati – è stata ipotizzata una sequenza di azioni, comprensiva di alcune varianti, che il sistema deve prevedere per produrre un risultato osservabile e dal valore segnaletico per un attore.

Da ultimo, in appendice sono stati riportati alcuni schemi e relativa documentazione privacy necessaria per un corretto trattamento dei dati attraverso il Dossier sanitario.

CAPITOLO I

eHealth: le informazioni in una struttura sanitaria gestite tramite strumenti elettronici

"E' dal volume di dati di cui l'uomo dispone che la nostra epoca trae un sentimento immotivato di superiorità e il vero criterio poggia sulla misura in cui l'uomo sa plasmare e padroneggiare le informazioni che possiede"

J.W. Goethe

La domanda di accesso ai dati e alle informazioni sulla salute è sempre più sentita dai pazienti ed anche all'interno delle strutture sanitarie da parte del personale medico e infermieristico.

Dati e informazioni chiare, attendibili e aggiornate rappresentano un *asset* strategico per consentire alle aziende sanitarie di ottimizzare i propri processi di cura e fornire ai propri pazienti servizi sempre migliori evitando, altresì, errori.

Per dare una risposta organica ed ampia, il presupposto per l'implementazione dell'*eHealth* è proprio la disponibilità e l'organizzazione dell'enorme massa dei dati e delle informazioni, intese sia in senso soggettivo (derivanti dal paziente) che oggettivo (derivanti da indagini strumentali), in un sistema informativo[22].

Un sistema informativo può essere definito, tecnicamente, come un insieme di elementi interconnessi che raccolgono (o ricercano), elaborano, memorizzano e distribuiscono informazioni per supportare le attività decisionali e di controllo di un'azienda.[23]

Così che, se prima dell'introduzione di strumenti elettronici la gestione delle informazioni avveniva attraverso il supporto cartaceo, richiedendo quindi un lavoro di registrazione, archiviazione di documenti e ricerca degli stessi, con conseguenti limiti sotto il profilo dell'efficienza, con l'avvento delle tecnologie dell'informazione e della comunicazione (ICT), la situazione è sensibilmente migliorata e i dati possono essere

---

[22] Per approfondimenti v. P. Guarda, *Fascicolo sanitario elettronico e protezione dei dati personali,* Trento 2011,p. 12; sul punto si veda anche U. Izzo, *Medicina e diritto nell'era digitale: i problemi giuridici della cybermedicina*, Danno e Responsabilità, 8, 9/2000, pp. 807-18.

[23] *Cfr.* K. Laudon, *Management dei sistemi informativi,* Pearson, Milano 2006, p. 17-19; per approfondimenti si veda anche N. Agabiti, M. Davoli, D. Fusco, M. Stafoggia, C. A. Perucci, *Valutazione di esito degli interventi sanitari*, Epidemiologia & Prevenzione2011; 35(2) Suppl 1: 1-80, Cap. 3.8 (Sistemi Informativi Sanitari).

già *ab origine* provvisti di quella "forma" significativa[24], utile a ricavarne informazioni, che permetta di avere quale *outcome* in ambito sanitario un miglioramento delle prestazioni a tutela della salute del singolo e della collettività.

Ovviamente, nella progettazione di un sistema informativo un ruolo determinante è svolto dallo sviluppo dell'architettura *software* ed *hardware*; nondimeno, per una maggior aderenza del sistema alla realtà per la quale esso è concepito devono essere interessati anche i soggetti coinvolti nei processi di assistenza, così da mettere a punto prassi operative corrette e uniformi, tecniche per lo scambio e l'archiviazione di documenti, regole comuni per la gestione della privacy e della sicurezza.

Solo così tali sistemi potranno dirsi funzionali e adeguati per garantire continuità di assistenza sanitaria al paziente[25].

1.1 I percorsi diagnostico-terapeutici ed i sistemi informativi a supporto

La strutturazione di processi di cura in un sistema sanitario contemporaneo, calata all'interno di un contesto tecnologico come quello dell'*eHealth*, comporta un'elevata complessità di sviluppo; basti pensare al fatto che il trattamento di un problema di salute richiede frequentemente il contributo di più attori e più specialità mediche.

La complessità di un sistema così pianificato, può creare condizioni che facilitano la mutevolezza, i difetti di congruità, le continue integrazioni delle cure: tutte condizioni, queste, con la conseguente la possibilità di errori medici.

Tuttavia un approccio per processi, connaturato nella strutturazione di un "Percorso Diagnostico Terapeutico Assistenziale" (PDTA), permette di valutare la congruità delle attività svolte rispetto agli obiettivi, alle linee guida operative di riferimento ed alle risorse disponibili, conducendo al miglioramento dell'efficacia e dell'efficienza di ogni intervento[26].

---

[24] I termini "dati" ed "informazioni" sono spesso utilizzati come sinonimi, ma in campo informatico possiedono un significato differente. Il dato è un elemento conosciuto e fine a se stesso, mentre l'informazione è un elemento che deriva dall'elaborazione di un insieme di dati e che permette di venire a conoscenza di qualcosa. *Cfr.* R. Brighi, *Il ruolo dei dati informatici nella costruzione della realtà. Tra vulnerabilità e esigenze di trasparenza*, Aracne editrice, Roma 2016.

[25] Per maggiori informazioni si veda C. Caccia, *Management dei sistemi informativi in sanità*, McGraw-Hill, Milano2008; C. Caccia, G. Nasi, *Il sistema informativo automatizzato nelle aziende sanitarie*, McGraw-Hill, Milano 2002; L. Buccoliero, C. Caccia, G. Nasi, e-*He@lt: percorsi di implementazione dei sistemi informativi in sanità*, McGraw-Hill, Milano 2005; A. Teti, G. Festa, *Sistemi informativi per la sanità*, APOGEO, Milano 2009.

[26] G. Casati, la gestione dei processi in sanità, QA vol. 13 n. 1, 2002.

In particolare il PDTA è uno strumento finalizzato sia all'organizzazione dei processi clinici ed organizzativi di una struttura sanitaria, sia a migliorare e rendere più facilmente fruibile il percorso di cura che il paziente compie.

Si tende infatti a considerare i PDTA come un nuovo approccio metodologico[27] delle organizzazioni sanitarie, sempre più propense a focalizzarsi, in luogo dei finora comuni modelli basati in prevalenza sulla "medicina d'attesa", su nuovi modelli imperniati sulla "medicina d'iniziativa" e organizzati avendo riguardo al "percorso", agli obiettivi, ai ruoli e agli ambiti di intervento, con conseguenti maggiori garanzie di chiarezza delle informazioni per l'utente e dei compiti per gli operatori; tali nuovi modelli permetterebbero altresì di migliorare la costanza, la riproducibilità e l'uniformità delle prestazioni erogate e, al contempo, prevedendo e quindi riducendo l'evento straordinario, di facilitare la flessibilità e l'adattamento ai cambiamenti.

Proprio in tale contesto vanno cristallizzati e tenuti ben presenti alcuni prerequisiti di sostenibilità di tale architettura:

- non si tratta di un nuovo sistema informativo sanitario, i professionisti coinvolti nel PDTA continueranno ad usare il sistema informativo che utilizzano già nella loro attività quotidiana;
- non si tratta di creare una sorta di "cartella clinica di PDTA" da compilare, con conseguente ulteriore gestione di un documento da sottoporre a firma digitale e processo di dematerializzazione;
- si tratta invece, di produrre un *report* "intelligente" sulla base di informazioni già disponibili nei sistemi informativi in uso, aggregandole non soltanto per un singolo episodio ospedaliero o di un'unica prestazione specialistica ambulatoriale o di servizio sociale, ma associando l'insieme dei servizi e delle prestazioni riferiti ad uno specifico fabbisogno[28].

La realizzazione di un PDTA passa attraverso specifiche fasi che si richiamano il noto ciclo di Deming[29]: analisi/pianificazione (*plan*), progettazione (*do*), monitoraggio (*check*), gestione del cambiamento (*act*).

---

[27] *Cfr. Innovazione Digitale a supporto dei Percorsi Diagnostico Terapeutici Assistenziali*, a cura di AISIS, ottobre 2015, pp. 50-1.

[28] M. Biroli, *Process Analysis o Process Management*, Milano, Sistemi & Impresa, n. 9, 1992.

[29] Sul punto si veda A. L. Fazzari, Sistemi di gestione per la qualità, Giappichelli, Torino 2012; J. Ovretveit, *Valutazione degli interventi in sanità*, Centro Scientifico Editore, Torino, 1998.

Figura 2. Supporto dell'ICT nella progettazione, gestione, e valutazione dei PDTA[30]

Più precisamente (v. Figura 2) la *Fase Plan* prevede la ricognizione delle attuali modalità di gestione, all'interno delle strutture organizzative, dei pazienti trattati, e riferite ad una determinata patologia, allo scopo di identificare "chi, fa cosa, dove e quando" e di creare un workflow operativo dei flussi informativi disponibili e della banche dati aziendali esistenti (CUP, PS, LIS, RIS, Cartelle Cliniche Ospedaliere, ecc.); la *Fase Do* definisce i contenuti, in termini di appropriatezza clinico-assistenziale, di un determinato PDTA e la relativa definizione di standard, procedure e protocolli; revisionando, ove necessario, i processi aziendali, definendo nuove matrici organizzative (chi, fa cosa, dove e quando) con lo scopo di costruire una piattaforma che consenta, a tutti gli *stakeholder* coinvolti, di gestire e monitorare il workflow di processi e di consultare i dati ad esso correlati; la *Fase Check* verifica i risultati complessivamente raggiunti dalle strutture organizzative e dai professionisti coinvolti nell'implementazione del PDTA e permette la valutazione degli eventuali scostamenti tra i percorsi effettivi e quelli di riferimento; la *Fase Act* analizza, sulla base degli scostamenti dai percorsi effettivi e di riferimento, eventuali necessità di modifica del percorso nell'ottica di un miglioramento continuo.

Se, come già accennato nelle considerazioni introduttive[31], l'innovazione digitale nella sanità è davvero, oggi, un *driver* fondamentale per il miglioramento ulteriore delle

[30] Fonte: AISIS, *Innovazione Digitale a supporto dei Percorsi Diagnostico Terapeutici Assistenziali*, cit., p. 25.

prestazioni che essa può erogare, la pluralità degli ambiti disciplinari, medici e non, coinvolti nella loro implementazione configura i modelli PDTA come un ottimo banco di prova per dare concretezza all'informatizzazione dei processi organizzativi e alle attività assistenziali.

Tuttavia per poter modellare un processo clinico adattandolo agli strumenti propri dell'*eHealth*, la gestione dei dati comporta sia l'esigenza di uniformare il linguaggio ad un livello standard di comprensione e riproducibilità per tutti gli operatori, sia una strategia condivisa e strutturata per l'organizzazione del dato clinico che sia incentrato sul paziente.

In altre parole, la realizzazione di un PDTA pone la necessità di scegliere e adottare sistemi informativi flessibili e diffusi nel contesto operativo sanitario (regionali, nazionali ed europei), nonché interoperabili.

1.1.1 *I sistemi informativi sanitari*

Come ricordato nel paragrafo precedente, le caratteristiche essenziali che costituiscono un sistema informativo sono: *i dati* (componente essenziale del sistema ed inizialmente non ancora elaborati); *le informazioni* (insieme di dati elaborati); *le persone* (i destinatari delle informazioni trattate); *gli strumenti* (l'insieme delle apparecchiature in grado di trasferire le informazioni da un soggetto all'altro); *i procedimenti* (insieme di criteri che permettono di capire il modo in cui vengono raccolti ed elaborati i dati).

In ambito sanitario i sistemi informativi tipicamente adottati sono classificati come:

- il sistema informativo ospedaliero (SIO);
- il sistema informativo di gestione Accettazioni di corsia (ADT);
- il sistema informativo di radiologia (RIS);
- il sistema per l'archiviazione e comunicazione delle immagini (PACS);
- il sistema informativo di laboratorio (LIS).

Si deve sottolineare che esistono anche diversi altri sistemi informativi più specialistici, a seconda dei contesti e dei livelli di informatizzazione.

---

[31] Si rinvia *supra*, Intro par. 1.

Naturalmente, i sistemi informativi che ci apprestiamo a studiare, se pur indipendenti, possono, grazie ad appositi protocolli standardizzati[32], scambiarsi informazioni ed alcuni tipi di dati strutturati.

Nello specifico *il sistema informativo ospedaliero (SIO)* è caratteristico e indipendente per ogni struttura sanitaria ed ha lo scopo principiale di regolare la circolazione delle informazioni riguardanti i singoli pazienti e necessarie per gestire la vita di un ospedale; solitamente in un SIO esistono tre classi principali di dati, quelli relativi al paziente (anagrafica del paziente, storia clinica ecc.), quelli relativi alle attività (servizi che l'ospedale fornisce, giorni di ricovero, esami, prestazioni terapeutiche) e quelli relativi alle risorse (personale, attrezzature, risorse finanziarie).

Il Sistema Accettazione/Dimissione/Trasferimento (ADT) è un sistema informativo su cui vengono registrate tutte le operazioni riguardanti la gestione amministrativa legata alla degenza del paziente all'interno di un sistema ospedaliero. In particolare si tratta di un programma per la gestione informatizzata:

- di accettazione del paziente; la struttura sanitaria memorizza i dati anagrafici, i recapiti e le caratteristiche peculiari del paziente;
- di aggiornamento delle informazioni relative all'anagrafica del paziente già presente nel Database della struttura;
- di dimissione del paziente con la compilazione della scheda di dimissione (SDO)
- dell'eventuale fase di trasferimento da un reparto all'altro della struttura ovvero verso una struttura sanitaria esterna.

Il sistema informativo di radiologia (RIS) è sostanzialmente un sottoinsieme del SIO, dal momento che ha il compito di gestire le informazioni generate dalla struttura sanitaria, più precisamente nel reparto di radiologia, e provvede alla conservazione dell'informazione testuale raccolta e generata nel corso del processo diagnostico.

Il sistema informativo PACS è un sistema indipendente dal RIS pur conservandone la parte di diagnostica per immagine. Esso si basa su una rete in grado di connettere le apparecchiature di acquisizione delle immagini, le stazioni di visualizzazione e l'archivio digitale.

Con riguardo ai sistemi RIS e PACS va specificato che il RIS, se pur sistema a sé stante, deve essere in grado di interfacciarsi con il PACS e per tale motivo negli ultimi anni le

[32] Per la gestione di dati clinici e di immagini mediche, gli standard più significativi e specifici sono: HL7 (Health Level Seven), HL7-CDA (Clinical Document Architecture), DICOM (Digital Imaging and Communications in Medicine).

aziende produttrici di soluzioni radiologiche stanno sviluppando prodotti che offrono la più una completa integrazione tra questi due sistemi[33].

Il sistema informativo LIS è utilizzato per gestire le richieste dei pazienti e per ricevere, elaborare e memorizzare le informazioni generate dai macchinari del laboratorio di analisi.

1.1.2 *I modelli informativi: relazioni vs documentali e ad eventi*

In funzione dello stato di informatizzazione dei processi assistenziali possono essere previste varie strategie e modelli di organizzazione del dato clinico.

Fra i sistemi di registrazione/archiviazione elettronica dei dati clinici di un determinato paziente si possono distinguere: la Cartella Clinica Elettronica (CCE), l'equivalente dell'Electronic Medical Record (EMR); il Dossier sanitario (DS), l'equivalente del *Electronic Health Record* (EHR); il *Personal Health Record* (PHR) e altri sistemi ausiliari quali CPOE, CDSS, ePrescribing, ecc.

Il modello finora più conosciuto è il c.d. *Electronic Health Record (EHR)*[34], che si caratterizza per la sua fisionomia organizzativa costruita su un "*data repository*" clinico aziendale unitario, nel quale confluiscono tutte le informazioni sulla salute prodotte nei diversi processi terapeutici, che vedono il paziente come un attore primario, a cui hanno accesso i diversi professionisti sanitari che operano all'interno della struttura.

Si è passati così, negli ultimi decenni, dalla progettazione di cartelle "aziendali di episodio" (*Electronic Medical Record* - EMR) alla realizzazione di cartelle "aziendali di sistema" (EHR), in grado di offrire una visione longitudinale[35] della salute dell'individuo.

Questo modello raccoglie ed archivia il dato clinico e le informazioni riguardanti il percorso terapeutico di un singolo paziente in un *Data Base* (DB)[36].

---

[33] Per maggiori informazioni v. A. Carriero, M. Centonze, T. Scarabin, Management in radiologia, Springer 2010, pag. 191-201.

[34] *Cfr*. Guarda, *Fascicolo sanitario elettronico e protezione dei dati personali*, cit., p. 27.

[35] L. Buccoliero, *E-HEALTH 2.0 -Tecnologie per il patient empowerment*, Mondo digitale n. 4, 2010.

[36] Collezione di dati gestita tramite un Data Base Management System (DBMS). I dati sono strutturati e collegati tra loro, a livello logico, nel rispetto del modello di rappresentazione (es. relazionale) adottato dal DBMS e, a livello fisico, risiedono su dispositivi di memoria organizzati in particolari strutture. Gli utenti si interfacciano con la base di dati attraverso un Query Language (es. SQL). Per maggiori informazioni *Cfr*. P. Atzeni, S. Ceri, S. Paraboschi, R. Torlone. *Basi di Dati: modelli e linguaggi di interrogazione* - Quarta Edizione. McGraw-Hill Italia, 2013; R. Ramakrishnan. *Database Management Systems*, McGraw-Hill, 2004; R.A. Elmasri, S.B. Navathe. *Sistemi di basi di dati Fondamenti* - Prima edizione italiana. Addison Wesley, 2004.

Alla luce di ciò si deve far rilevare che il classico paradigma relazionale di un DB basato su SQL[37] (Structured Query Language), ad oggi in uso nella maggior parte dei sistemi informativi, rischia però per il futuro, alla luce dell'evoluzione dei "*big data*"[38] ed anche dei recenti database NoSQL[39] (Not Only SQL), di essere poco adatto per l'ambito sanitario.

Infatti, in un database relazionale tutto ruota attorno al concetto di tabella, e ne esisterà una per ogni tipo di informazione da trattare, colonna e riga; inoltre, tra le tabelle di un database relazionale possono esistere alcune relazioni[40]. Ebbene, questa strutturazione rigida dei contenuti è invece un elemento che manca nei database NoSQL, in cui le informazioni non troveranno più posto in una struttura di righe elencate in tabelle, ma in oggetti completamente diversi e sequenziali.

Questo fa sì che in un prossimo futuro attraverso DB basati su NoSQL orientati al documento, si possa disporre di sistemi informativi che saranno in grado sia di dar vita ad una memorizzazione strutturata, sia di essere molto più adatti e flessibili nella gestione di dati sanitari sempre più eterogenei (v. Figura 3).

Naturalmente si deve precisare che NoSQL non è sicuramente indicato per tutti gli utilizzi ma può sostituire i DB SQL tradizionali, o in parte affiancarli, in alcune e specifiche occasioni.

---

[37] Linguaggio standard di interrogazione dei database che permette la consultazione e modifica dei dati indipendentemente dal software e dal sistema operativo con il quale è stato creato. E' stato elaborato dall'ANSI. Non è un vero linguaggio di programmazione, in quanto non consente di creare applicazioni indipendenti, ma solamente di richiamare, stampare, scrivere o modificare i dati presenti in un database che sia stato costruito con un software compatibile con SQL. Fonte: http://www.pc-facile.com/glossario/sql.

[38] Il termine è usato per descrivere una raccolta di dati così estesa in termini di volume, velocità e varietà da richiedere tecnologie e metodi analitici specifici per l'estrazione di valore. *Cfr*. A. De Mauro, M. Greco e M. Grimaldi, *A Formal definition of Big Data based on its essential Features*, in *Library Review*, vol. 65, n. 3, 2016, pp. 122-135. Sul punto per maggiore approfondimento si veda M. Keith - M. Katina, *Big Data New Opportunities and new Challenges*, IEEE Computer Society, 2013; T.B. Murdoch, A.S. Detsky, *The inevitable application of big data to health care* JAMA 2013; 309: 1351-2; T.K. Prasad, *Big Data and Smart Healthcare*, slides Symposium "Visions of the Future", marzo 2014.

Sulla complessa tematica dei big data e sulle sfide che questa pone alla protezione dei dati personali, si veda lo *Statement* adottato nel 2014 dal Gruppo di lavoro articolo 29 intitolato: *"Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU"* (WP n. 221).

[39] Il termine NOSQL fu introdotto da Carlo Strozzi nel 1998 per indicare il suo database relazionale open-source che non aveva una interfaccia SQL standard. Il termine indica i database che sono: non relazionali, distribuiti, open-source e scalabili orizzontalmente. Fonte: http://www.strozzi.it/cgi-bin/CSA/tw7/I/en_US/NoSQL/Home%20Page (Ultimo accesso giugno 2017).

[40] Una riga di una tabella A può fare riferimento ad un'altra riga di un'altra tabella B, e ciò può essere espresso inserendo la chiave primaria della riga di B tra i dati di quella di B. Sul punto v. http://www.html.it/articoli/sql-e-nosql-a-documenti-il-confronto-2 (ultima accesso giugno 2017).

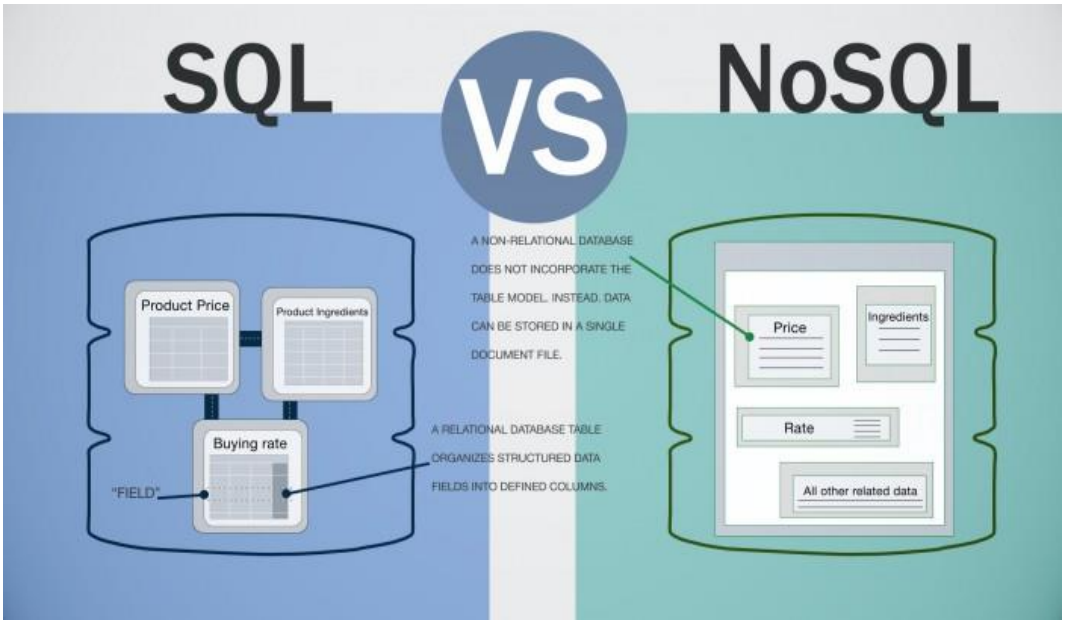


Figura 3. Differenza tra Database SQL vs NoSQL[41]

Come avremo modo di vedere approfonditamente *infra*, un recente modello informativo che si sta facendo sempre più spazio in ambito sanitario è il *Personal Health Record* (PHR)[42].

Tale sistema si connota per un approccio orientato alla gestione, in modalità condivise con il paziente, dei soli eventi e informazioni rilevanti. Infatti i vari dati generati nel tempo dalle singole strutture sanitarie sono qui resi integralmente disponibili al paziente, il quale decide la modularizzazione dei livelli di accesso ad essi. Così che, a differenza di altre piattaforme informative di dati sanitari che privilegiano l'accesso e il controllo nelle mani dei gestori del servizio sanitario e dedicano così all'utente una posizione del tutto marginale e limitata, questo nuovo modello è caratterizzato da una struttura "paziente-centrica" che lo elegge a punto centrale del sistema di gestione delle informazioni idonee a rivelare il suo stato di salute.

1.1.3 *I documenti sanitari*

Procedendo oltre nell'affrontare le questioni "definitorie" necessarie per un corretto inquadramento dei fenomeni di cui ci si occupa in tale sede e, quindi, per il prosieguo dell'esposizione nei capitoli successivi, si deve mettere a fuoco il concetto di "documentazione sanitaria". Per essa si intende l'insieme di ogni rappresentazione

[41] Fonte: https://www.dbbest.com/blog/database-decisions.
[42] Si rinvia *supra*, cap. I par. 1.4.

informatica, grafica, iconografica, elettromagnetica che contenga informazioni volte a certificare un fatto o una situazione legata allo stato di salute di un soggetto[43].

La predisposizione di un documento sanitario all'interno di un percorso sanitario gioca sicuramente un ruolo fondamentale, in quanto primo strumento di lavoro per il personale sanitario su cui si basa il processo di diagnosi e cura del paziente.

In particolare i documenti vengono prodotti secondo l'evidenza di tre diversi contesti di accesso alle cure.

Un primo contesto è il *Pronto soccorso*, dedicato alle urgenze e alle emergenze sanitarie, ad esso il paziente può accedere direttamente a fronte di una prima valutazione da parte di personale sanitario opportunamente formato, il quale, attraverso la metodologia denominata "TRIAGE", stabilisce l'urgenza con cui potrà accedere alle cure.

La classe di urgenza, a seguito della valutazione oggettiva dei "Parametri vitali" e della "Glasgow Coma scale", è espressa mediante un codice di colore: ROSSO (Paziente molto critico; priorità massima); GIALLO (Paziente in potenziale pericolo di vita, priorità alta); VERDE (Paziente che necessita di una prestazione che può essere ritardabile, priorità bassa); BIANCO (Paziente non urgente).

Un secondo contesto è il *Ricovero* che generalmente, può avere una doppia natura: urgente o programmato. Il ricovero urgente avviene attraverso il Pronto Soccorso oppure anche su richiesta del Medico di Medicina Generale o di altro specialista del Servizio Sanitario Regionale. Il ricovero programmato (Day Hospital, Day Surgery, Lungodegenza) avviene invece su richiesta di uno specialista ospedaliero e avviene direttamente al reparto.

Solitamente nei percorsi terapeutici standardizzati si accettano:

i. *ricoveri in urgenza* con le seguenti modalità:

- richiesta di ricovero dal 118;
- richiesta di ricovero da Pronto Soccorso di Dipartimento Emergenza Urgenza;
- richiesta di trasferimento da reparti di altri ospedali, da cui i pazienti giungono per cure urgenti e indifferibili;
- ricovero disposto dal medico di guardia su indicazione del medico di famiglia o dello specialista per cure urgenti e indifferibili.

---

[43] La documentazione sanitaria è la prima fonte "testimoniale" delle attività e degli eventi che si verificano durante i processi di assistenza. Costituisce un bene di straordinaria importanza sul piano clinico, scientifico e didattico, oltre che giuridico, sia per il cittadino che se ne può servire per far valere i propri diritti, sia per la tutela dell'operato professionale degli operatori sanitari. *Cfr. Manuale della documentazione sanitaria*, a cura della Regione Lombardia. http://www.sitilombardia.it/wp-content/uploads/2015/04/Manuale-Documentazione-Sanitaria-gennaio-2013.pdf.

ii. *ricovero programmato in degenza ordinaria:*

viene disposto dal medico responsabile del reparto interessato che ne accerta la reale necessità (appropriatezza del ricovero), definisce il livello assistenziale adeguato, valuta la priorità clinica[44], e quindi provvede:

a) all'inserimento nella lista dei ricoveri programmati;
b) al successivo ricovero, in relazione ai posti letto disponibili.

iii. *ricovero programmato in degenza diurna (Day Hospital, Day Surgery):*

la prenotazione di prestazioni diurne è possibile solamente su richiesta di un medico interno alla struttura dopo visita specialistica o ricovero. E solitamente il Day Hospital è riservato ai malati che hanno bisogno di prestazioni sanitarie complesse non eseguibili in ambulatorio e che hanno di norma una durata inferiore alle 12 ore, non necessitando quindi di pernottamento. Il Day Surgery riguarda invece tutti gli interventi chirurgici che comportano di norma un ricovero di durata inferiore alle 12 ore. Il ricovero in Day Surgery è disposto da un medico specialista della Unità Operativa ospedaliera.

Un ultimo contesto è quello *Ambulatoriale*. Solitamente, presso le strutture ospedaliere vengono effettuate prestazioni specialistiche ambulatoriali: visite, prestazioni strumentali diagnostiche, prestazioni di laboratorio, piccola chirurgia. Importante è sottolineare come alle prestazioni ambulatoriali si può accedere sia in regime istituzionale (a carico del Servizio Sanitario Nazionale, salvo l'eventuale compartecipazione alla spesa), che in Libera Professione.

Alla luce dei contesti di accesso alle cure sopra menzionate, un titolario[45], con annesso elenco esemplificativo e non esaustivo, del flusso documentale di una struttura sanitaria, con vista ed operatività lato paziente potrebbe essere:

[44] Per assicurare un accesso alle cure tempestivo ed adeguato e in ossequio ai principi di trasparenza ed equità garantiti dal Servizio Sanitario Nazionale, il paziente ha diritto a conoscere il Suo livello di priorità clinica e la Sua posizione nella lista di attesa, facendone apposita richiesta alla Direzione Sanitaria.

[45] *Il titolario è il sistema precostituito di partizioni astratte, gerarchicamente ordinate (dal generale al particolare), fissate sulla base dell'analisi delle funzioni dell'ente, al quale deve ricondursi la molteplicità dei documenti prodotti, per organizzarne la sedimentazione ordinata. Il titolario si sviluppa su più livelli, denominati dalla dottrina: titolo, classe, sottoclasse, categoria, sottocategoria.* Fonte: Agenzia per l'Italia Digitale (AgID)

Titolo - Area Sanitaria		
Classe	**Sottoclasse**	**Descrizione**
Direzione ospedaliera		
1	01	Aspetti generali, organizzativi e gestionali
1	02	Rapporti con l'autorità giudiziaria
Pronto soccorso		
2	01	Gestione organizzativa P.S.
2	02	Attività emergenza-urgenza
Assistenza ospedaliera		
3	01	Ricovero (ordinario, day hospital, day surgery)
3	02	Day service
Assistenza ambulatoriale		
4	01	Prestazioni ambulatoriali

CLASSE	COD. SOTTO CLAS.	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE
1. Direzione ospedaliera	01	Aspetti generali, organizzativi e gestionali	Pagamento ticket, ricevute	5 anni
	01	Aspetti generali, organizzativi e gestionali	Richieste copie di cartelle cliniche ed ambulatoriali, schede di P.S., certificati di ricovero, referto esami di laboratorio, ecc.	1 anno
	01	Aspetti generali, organizzativi e gestionali	Deleghe per il ritiro dei referti	1 anno
	01	Aspetti generali, organizzativi e gestionali	CUP, Prenotazione per prestazioni	1 anno
	01	Aspetti generali, organizzativi e gestionali	Registrazioni informatiche di monitoraggio di parametri biologici	Tempo di conservazione correlato al documento principale, massimo 10 anni.
	02	Rapporti con l'autorità giudiziaria	Documentazione relativa a segnalazioni / denunce all'Autorità Giudiziaria	ILLIMITATO

CLASSE	COD. SOTTO CLAS.	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE
2. Pronto Soccorso	01	Gestione organizzativa P.S.	Verbale di Pronto Soccorso (Registri, schede triage, schede di pazienti accolti in PS e trasferiti in altro ospedale, Schede di pazienti entrati in PS, che rifiutano il ricovero)	ILLIMITATO
	02	Attività emergenza - urgenza	Verbale di Pronto Soccorso (Referti)	ILLIMITATO
3.Assistenza Ospedaliera	01	Ricovero (ordinario, day hospital, day surgery)	Cartella clinica di ricovero comprensiva di tutti i documenti costitutivi, es.: richiesta di ricovero, documentazione diagnostica strumentale e di laboratorio, consensi, SDO, lettera di dimissione, referti, tracciati, documenti inerenti la valutazione del dolore ai sensi della legge 38 del 2010.	ILLIMITATO
	01	Ricovero (ordinario, day hospital, day surgery)	Cartella clinica di ricovero (documentazione radiologica e di medicina nucleare)	ILLIMITATO per i referti; ILLIMITATO per le immagini Rx archiviati nel dossier rad. 10 anni per la documentazione non consegnata al paziente.
	01	Ricovero (ordinario, day hospital, day surgery)	Verbale - registro operatorio	ILLIMITATO
	01	Ricovero (ordinario, day hospital, day surgery)	Cartella clinica di ricovero diurno. Comprensiva di tutti i documenti costitutivi.	ILLIMITATO
	01	Day service Attività Ambulatoriali complesse	Documentazione inerente le attività ambulatoriali complesse che prevedono la redazione di fascicolo clinico	30 anni solo per il Day service chirurgico; 10 anni dalla chiusura del fascicolo per gli altri, assimilabili a documentazione ambulatoriale

CLASSE	COD. SOTTO CLAS.	SOTTOCLASSE	TIPO DOCUMENTO	TEMPO CONSERVAZIONE
4.Assistenza Ambulatoriale	01	Prestazioni ambulatoriali	Referti di singole prestazioni ambulatoriali se costituiti in fascicoli ambulatoriali con relativa documentazione a supporto, quando non consegnati in originale ai pazienti	30 anni per attività chirurgica; 10 anni dalla chiusura del fascicolo
	01	Prestazioni ambulatoriali	Prescrizione - proposta - ricetta per richieste di prestazioni sanitarie	ILLIMITATO se in cartella clinica; 5 anni altri esemplari
	01	Prestazioni ambulatoriali	Referti esami di laboratorio	5 anni
	01	Prestazioni ambulatoriali	Referti esami citologici e istologici	ILLIMITATO
	01	Prestazioni ambulatoriali	Referti Radiologici	ILLIMITATO
	01	Prestazioni ambulatoriali	Referti di medicina nucleare	ILLIMITATO

Tabella 1. Titolario e Massimario di scarto documenti saniari

1.2 La Cartella Clinica Elettronica (CCE)

La cartella clinica costituisce il documento ufficiale e legalmente riconosciuto per la raccolta organica e funzionale dei dati sulla storia clinica di un paziente[46].

In ambito europeo, la Raccomandazione della Commissione europea del 2 luglio

[46] B. Primicerio, *La cartella clinica e la documentazione sanitaria ad essa collegata: evoluzione, utilizzazione e responsabilità*, in Il Diritto sanitario moderno, 2004, p. 207; V. Vaccaro, *La cartella clinica* (Nota a TAR VE sez. III 7 marzo 2003, n. 1674), in Trib. am. reg., 2003, 180; G. Rocchietti, *La documentazione clinica. Compilazione, conservazione, archiviazione, gestione e suo rilascio da parte della direzione sanitaria. Trattamento dei dati sanitari e privacy*, in Minerva medicolegale, 2001, fasc. 1, p. 15; O. Bucci, *La cartella clinica. Profili strumentali, gestionali, giuridici ed archivistici*, Santarcangelo di Romagna, 1999; GUARDA, *Fasciolo sanitario elettronico e protezione dei dati personali*, cit., pp. 93-5.

2008 sull'interoperabilità transfrontaliera dei sistemi di cartelle cliniche elettroniche[47], all'art. 3, lettera c, definisce la cartella clinica elettronica come:

una documentazione medica completa o documentazione analoga sullo stato di salute fisico e mentale, passato e presente di un individuo in forma elettronica, che consenta la pronta disponibilità di tali dati per cure mediche e altri fini strettamente collegati.

In ambito nazionale, pur non avendo una definizione precisa, dottrina e giurisprudenza concordano che la CCE è "*un atto pubblico che esplica la funzione di diario dell'intervento medico e dei relativi fatti clinici rilevanti, sicché i fatti devono essere annotati conformemente al loro verificarsi*".[48]

Quanto detto trova riscontro anche all'art. 26 del nuovo Codice di deontologia medica[49] che dispone:

La cartella clinica delle strutture pubbliche e private deve essere redatta chiaramente, con puntualità e diligenza, nel rispetto delle regole della buona pratica clinica e contenere, oltre ad ogni dato obiettivo relativo alla condizione patologica e al suo decorso, le attività diagnostico-terapeutiche praticate. La cartella clinica deve registrare i modi e i tempi delle informazioni nonché i termini del consenso del paziente, o di chi ne esercita la tutela, alle proposte diagnostiche e terapeutiche; deve inoltre registrare il consenso del paziente al trattamento dei dati sensibili, con particolare riguardo ai casi di arruolamento in un protocollo sperimentale.

Alla luce di ciò, l'informatizzazione della cartella clinica, nella prospettiva di rendere i processi sanitari maggiormente efficienti, flessibili e rispondenti ai bisogni delle persone, si inserisce in un contesto ampio di riorganizzazione interna alle strutture ospedaliere, consentendo altresì di introdurre importanti migliorie nella gestione dei dati, rispettandone i requisiti di completezza e di integrità.

La Cartella Clinica Elettronica (CCE) viene dai più vista come una mera evoluzione della Cartella Clinica Cartacea (CCC)[50]. Ma si deve rilevare come essa rappresenti uno degli strumenti dell'*eHealth* per la gestione organica e strutturata dei dati riferiti alla storia clinica di un paziente in regime di ricovero o ambulatoriale,

---

[47] Raccomandazione della Commissione del 2 luglio 2008 sull'interoperabilità transfrontaliera dei sistemi di cartelle cliniche elettroniche, (2008/594/CE) in http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32008H0594 (ultimo accesso giugno 2017).

[48] *Cfr.* Cass., Sez. V Pen., sent. 16 giugno 2005, n. 22694.

[49] Testo attualmente vigente e approvato il 23 gennaio 2007.

[50] *Cartella clinica elettronica ospedaliera*, a cura di AISIS, novembre 2012.

garantendo il supporto dei processi clinici (diagnostico-terapeutici) e assistenziali nei singoli episodi di cura e favorendo la continuità di cura del paziente all'interno della stessa struttura ospedaliera mediante la condivisione e il recupero dei dati clinici in essi registrati; tutte finalità alle quali la CCC, per ovvi limiti "strutturali", non sempre è riuscita a rispondere appieno.
Il valore aggiunto della CCE rispetto alla CCC viene ben lumeggiato in un passaggio testuale delle Linee Guida della Regione Lombardia, nei termini di seguito riportati:

La CCE si configura quindi come un sistema informatico integrato aziendale, da intendersi come strumento trasversale ai vari processi di cura, in sostituzione della cartella clinica cartacea, che da un lato ne rispetti i requisiti e le funzioni, e dall'altro risolva alcune criticità ad essa legate, offrendo opportunità di aumentare il valore attraverso l'integrazione con altri strumenti informatici. È importante riconoscere allo strumento elettronico una sua dignità che ne determina anche una forte differenza nel modo di assolvere alle sue funzioni rispetto allo strumento cartaceo. Lo strumento elettronico oggi è in grado di assolvere a tutti i compiti formalmente definiti per la cartella clinica cartacea ma è necessario e auspicabile che lo faccia in modo diverso, ovvero secondo la logica di una efficace ed efficiente gestione elettronica del dato. Per questo motivo, una visione dello strumento di cartella clinica elettronica come il mero "digitalizzatore" del cartaceo, da implementare senza un'adeguata revisione dei processi interni è riduttiva - se non errata - e non permette di valorizzare il potenziale in termini di gestione integrata delle informazioni, tempestività, automazione, semplificazione offerte dall'ergonomia dello strumento digitale[51].

Solitamente una CCE si costituisce di diversi blocchi funzionali come ad esempio la documentazione amministrativa; il consenso informato; l'inquadramento clinico iniziale medico e infermieristico; la gestione clinica (rilevazioni parametri vitali, documentazione procedure invasive, fogli di assistenza infermieristica, referti ecc.); la gestione della terapia farmacologica (spesso delegata a un applicativo esterno integrato a livello aziendale); la documentazione di trasferimento e dimissione.

Nella definizione specifica di ciascun blocco occorre effettuare un necessario richiamo al ciclo di vita della Cartella Clinica tradizionale, con particolare riferimento agli aspetti qui di seguito riepilogati:
- La CCE si "*apre*" con l'accettazione del paziente. Ad essa viene attribuito un numero identificativo univoco;

[51] *Cfr. Linee guida per la Cartella Clinica Elettronica Aziendale,* a cura della Regione Lombardia, V.02.1, 2012.

- La CCE si "*chiude*" con la refertazione dell'episodio e la chiusura della documentazione relativa nel caso dell'episodio ambulatoriale, con la produzione del referto ambulatoriale firmato digitalmente; invece, nel caso del ricovero, con la compilazione della Scheda di dimissione ospedaliera (SDO).

La CCE deve essere pertanto vista come un supporto informatico[52] per la gestione di dati e processi nel percorso di cura di un paziente e non come una semplice collezione di documenti che, nei fatti, sono solo uno dei prodotti della gestione stessa del processo.

Un importante aspetto che riguarda il suo processo di implementazione è che in Italia i sistemi di cartelle cliniche elettroniche sono stati classificati come Dispositivo Medico, ai sensi del D. Lgs n. 37 del 25/01/2010, e come tali devono essere certificati con il marchio CE dai produttori o distributori, secondo la direttiva della Comunità Europea 2007/47/CE, in cui si afferma che: "*occorre chiarire che un software è di per sé un dispositivo medico quando è specificamente destinato dal fabbricante ad essere impiegato per una o più delle finalità mediche stabilite nella definizione di dispositivo medico*".

La certificazione appena richiamata dà garanzia sulle metodologie produttive dei sistemi informatici e sul monitoraggio del funzionamento degli stessi, garantendo così che eventuali soluzioni di CCE "fai da te", seppure eccellenti dal punto di vista ergonomico e funzionale, non mettano a rischio la vita di un paziente oppure siano fonte di diffusione illecita di informazioni tutelate dalla normativa in materia di trattamento dei dati personali[53].

1.3 Il Dossier sanitario (DS)

Sin dal 2009, pur nell'assenza (a tutt'oggi perdurante) di una definizione normativa a livello nazionale, l'Autorità Garante per la protezione dei dati personali aveva già avvertito l'esigenza di puntualizzare specifiche garanzie, responsabilità e diritti in gioco con riferimento ai sistemi informativi idonei a realizzare, tra i vari professionisti sanitari operanti presso una medesima struttura la condivisione di informazioni assistenziali che ricostruiscono la storia sanitaria di un individuo. In tale

[52] E' oramai noto da tempo che il nostro ordinamento riconosce efficacia giuridica e valore probatorio al documento informatico. Tali disposizioni infatti sono state recepite nel Codice dell'Amministrazione digitale (D. Lgs. 7 marzo 2005 n. 82) che ha raccolto e integrato le disposizione sulla materia.

[53] *Cfr*. *Sviluppo di un modello di cartella paziente integrato*. Fonte: Ministero della Salute.

ottica furono adottate le Linee guida in tema di Fascicolo sanitario elettronico (FSE) e di Dossier sanitario[54].

Il dossier sanitario veniva definito, da tali Linee guida, nei termini seguenti:

lo strumento costituito presso un organismo sanitario in qualità di unico titolare del trattamento (es., ospedale, azienda sanitaria, casa di cura) al cui interno operino più professionisti, attraverso il quale sono rese accessibili informazioni, inerenti allo stato di salute di un individuo, relative ad eventi clinici presenti e trascorsi (es., referti di laboratorio, documentazione relativa a ricoveri, accessi al pronto soccorso), volte a documentarne la storia clinica.

Il dossier sanitario, in altri termini, veniva inteso dal Garante Privacy come raccolta degli eventi clinici presenti e trascorsi erogati per il singolo assistito ed elaborati esclusivamente presso un'unica struttura sanitaria, nella prospettiva di documentarne l'intera storia.

Come si evince dal titolo, le citate linee guida non affrontano soltanto il tema del dossier sanitario, ma anche quello del Fascicolo sanitario elettronico. La trattazione unitaria dei due strumenti in un unico provvedimento ha tuttavia generato nei commentatori una serie di fraintendimenti che hanno a volte erroneamente indotto ad identificare il Dossier con il Fascicolo e viceversa. Premesso questo, va subito chiarito che il DS si differenzia dal FSE per il fatto che i documenti e le informazioni sanitarie accessibili tramite tale strumento sono state generate *da un solo titolare* del trattamento e non da più strutture sanitarie in qualità di autonomi titolari, come avviene nel caso del FSE.

Il notevole incremento nell'utilizzo di sistemi informativi per la gestione della documentazione sanitaria da un lato e le risultanze degli accertamenti ispettivi effettuati dal Garante Privacy con riguardo al trattamento dei dati personali a mezzo di dossier sanitari dall'altro hanno tuttavia indotto il Garante Privacy a varare, nel 2015, nuove e specifiche Linee guida sul Dossier Sanitario, che dovrebbero aver fugato i rischi di confusione tra i due oggetti.[55]

Andando anche oltre la definizione data dal Garante, il Dossier può essere opportunamente inquadrato come uno strumento digitale proprio dell'*eHealth* attraverso cui è possibile non soltanto conservare l'intera storia clinica del paziente con riferimento

[54] G.U. n. 178 del 3 agosto 2009, consultabile sul sito www.gpdp.it [doc. web n. 1634116] (ultimo accesso giugno 2017).

[55] G.U. n. 164 del 17 luglio 2015, consultabile sul sito www.gpdp.it [doc. web 4084632] (ultimo accesso giugno 2017).

alle prestazioni erogate in suo favore all'interno di una data struttura sanitaria, ma anche tener traccia del percorso diagnostico terapeutico e assistenziale seguito.

Proprio con riguardo a questo ultimo aspetto, il Dossier costituisce uno strumento di enorme potenzialità, giacché il professionista, durante il percorso d'indagine e di cura, avrà accesso diretto al dossier e potrà consultare le informazioni sanitarie in esso contenute, così da avere un quadro il più possibile completo prima e durante l'esecuzione di qualsiasi tipo di intervento.

L'utilità del Dossier è indubbia, in varie declinazioni applicative: basti pensare alle risultanze degli esami – a volte invasivi e non ripetibili nel breve periodo - già svolti sull'interessato e ai quali il medico potrà aver accesso, senza necessariamente dover procedere ad una ripetizione degli stessi, con enorme risparmio altresì e di tempo e di denaro; o, ancora, si pensi al vantaggio derivante dall'implementazione del dossier con riferimento ai soggetti affetti da patologie croniche, delle quali il medico potrà così venire immediatamente a conoscenza adottando tutti i dovuti accorgimenti volti a ridurre e/o eliminare il rischio di errore nell'erogazione di trattamenti sanitari specifici.

Tuttavia, come evidenziato anche dal Garante, affinché i dossier sanitari in uso presso le strutture sanitarie possano essere di effettivo ausilio nei processi di diagnosi e cura dei pazienti è necessario che gli stessi siano realizzati con modalità tali da garantire la certezza dell'origine e della correttezza dei dati, nonché l'accessibilità degli stessi solo da parte di soggetti legittimati.

Da ciò, ossia dalla natura non incontrovertibilmente finalizzata ai soli fini medici del Dossier sanitario, discende che la relativa costituzione viene prospettata dal Garante come facoltativa, il che comporta, in assenza di una esplicita volontà dell'interessato alla creazione dello stesso, l'impossibilità di procedere all'apertura del Dossier. In ogni caso, il mancato consenso alla costituzione del dossier non può in alcun modo pregiudicare l'accesso alle cure mediche, che costituisce un diritto costituzionalmente sancito.

Al contrario, in caso di rilascio del consenso alla costituzione e alimentazione del DS, le finalità da perseguire devono essere ricondotte, a garanzia dell'interessato, esclusivamente alla prevenzione, alla diagnosi, alla cura e alla riabilitazione dell'interessato medesimo, senza poter contemplare differenti eventuali impieghi.

Tuttavia, il Garante ha in realtà consentito che qualora attraverso il Dossier si intendessero perseguire anche finalità amministrative (ad esempio la prenotazione attraverso il CUP oppure il pagamento di una prestazione sanitaria) questo sia possibile, ma esso deve essere strutturato in modo che i dati amministrativi siano separati da quelli sanitari e che siano previsti diversi profili di abilitazione dei soggetti che hanno accesso al Dossier, in ragione della funzione delle operazioni che gli stessi possono compiere.

In conclusione, pare opportuno spendere qualche ulteriore considerazione su un aspetto del Dossier molto dibattuto negli ultimi tempi. Infatti, la complessità, più volte richiamata, di sviluppare sistemi informativi che riescano ad integrarsi sul territorio regionale, e più in generale in quello nazionale, ha portato in singole realtà aziendali a configurare impropriamente questi sistemi come Dossier sanitari, il che non deve poter accadere.

L'assoggettamento, di un applicativo dipartimentale in uso, in sistema di Dossier sanitario può infatti correttamente dirsi eseguita soltanto in presenza di due specifiche condizioni:

- accesso al sistema da parte di una pluralità di soggetti, operatori sanitari, afferenti a specialità anche diverse da quelle che hanno generato le informazioni in esso archiviate;
- accesso non limitato al solo episodio di cura.

Un esempio di un sistema dipartimentale che spesso oggi si configura come Dossier è il sistema informativo RIS/PACS che consente a tutti i medici di una struttura di accedere, senza limitazioni temporale e svincolata dalla presa in carico del paziente, a tutti i referti radiologici dello stesso.

Così che, al fine di evitare qualificazioni di supporti informatici improprie alle finalità di Dossier, sarebbe particolarmente opportuno, per non dire necessario, che vengano rispettate in modo capillare le indicazioni del Garante Privacy, che limitano l'accesso ai sistemi applicativi dipartimentali ai soli professionisti della specifica area di competenza e alle sole informazioni relative all'episodio in fase di cura.

1.3.1 *Dossier Sanitario e FSE: tra differenze ed uguaglianza*

Come già affermato, le Linee guida in tema di Fascicolo sanitario elettronico (FSE) e di Dossier sanitario del 2009, trattavano non soltanto del Dossier sanitario, ma anche del Fascicolo sanitario elettronico, cosa che ha portato spesso a confondere i due strumenti.

Sulla base di tale atto del Garante Privacy, nonché prendendo in esame quanto disposto dal DPCM sul Fascicolo sanitario elettronico [56] e le recenti e specifiche Linee guida del 2015 sul Dossier sanitario, attraverso la tabella riportata sotto vengono messe a confronto i principali aspetti che caratterizzano il Dossier sanitario e il Fascicolo sanitario elettronico.

[56] Decreto del Presidente del consiglio dei Ministri del 29 settembre 2015, n. 178, *Regolamento in materia di fascicolo sanitario elettronico* (GU Serie Generale n. 263 del 11-11-2015).

	Dossier Sanitario	**FSE**
Titolarità del Trattamento	Organismo sanitario presso cui è costituito il Dossier (Ospedale, casa di cura ecc)	La titolarità Dipende dalla Finalità: Cura: SSN e servizi socio sanitari regionali, Ricerca: Regioni, Province autonome e Ministero della salute, Governo: Regioni, Province autonome e Ministero della salute e Ministero del Lavoro.
Informativa	Obbligatoria	Obbligatoria
Consenso	Obbligatorio per costituzione, alimentazione e consultazione	Obbligatorio per costituzione, alimentazione e consultazione
Finalità	Prevenzione, diagnosi, cura, riabilitazione e ricerca	Cura, ricerca, Governo
Costituzione	Non obbligatoria, consenso libero e specifico	Non obbligatoria, consenso libero e specifico
Alimentazione	Non obbligatoria	Non obbligatoria
Informazioni pregresse	Ammissibili, inserimento con ulteriore e specifico consenso	Ammissibili, inserimento con ulteriore e specifico consenso
Accesso Informazioni	Accesso modulare	Accesso modulare
Oscuramento	Deve essere garantito e previsto in duplice modalità: - Oscuramento del dato - Oscuramento dell'oscuramento del dato	Deve essere garantito e di default impostato con singola modalità: - Oscuramento dell'oscuramento del dato
Dati a maggior tutela	Garantito inserimento solo con specifico consenso dell'interessato	Garantito inserimento solo con specifico consenso dell'interessato
Soggetti abilitati all'accesso	Abilitati esclusivamente i soggetti operanti sul paziente. Esclusi sono i periti, compagnie di assicurazione, datori di lavoro, associazioni o organizzazioni scientifiche, organismi amministrativi.	Tutti i soggetti del SSN e dei servizi socio-sanitari regionali che prendono in cura l'assistito.
Elenco dei Dati ammessi	Facoltà del titolare di prevedere un contenuto minimo	Il contenuto del FSE è regolato all'art.2 del DPCM sul FSE
Tempistiche di accesso	L'accesso al Dossier deve essere circoscritto al periodo di tempo indispensabile per espletare le operazioni di cura per le quali il soggetto che accede è abilitato.	Le informazioni sono trattate in base ai principi di indispensabilità, necessità, pertinenza e non eccedenza.
Comunicazione al Garante	Non Prevista	Prevista nell'allegato n.1 paragrafo 9 delle Linee guida del 2009.
Misure di sicurezza	Rinvio agli art. 31 e 33 del Codice Privacy.	Rinvio agli art. da 21 a 25, Capo V, del DPCM sul FSE
Data Breach	Previsto obbligatoriamente nel testo delle Linee guida 2015.	Non espressamente previsto nel testo delle Linee guida del 2009. Previsto nel DPCM sul FSE (art. 23, comma 9)

Tabella 2. Differenza tra il Dossier sanitario e il Fascicolo sanitario elettronico

1.4 Personal Health Record (PHR)[57]

Nel campo dei sistemi informativi sanitari la continua evoluzione di questi strumenti va nella direzione dello studio e dell'implementazione dei PHR.

Ad oggi non è agevole ricavare per tale sistema una definizione condivisa, anche se occorre precisare che nella letteratura informatica, dove questa espressione ha preso forma e sostanza, è possibile definirlo come un sistema di registrazione elettronica delle informazioni costituito da un insieme di strumenti *web-based*[58], governato dal cittadino/utente e accessibile agli operatori sanitari per le finalità di diagnostica e cura.

Questo innovativo sistema di "Cartella Clinica Personale"[59] si caratterizza pertanto per un "approccio paziente-centrico"[60] che permette agli utenti di archiviare, di gestire e di condividere *online* i dati e le informazioni sanitarie che li riguardano, rendendoli protagonisti della propria salute e mettendo contemporaneamente al servizio del medico le informazioni socio-sanitarie non direttamente riscontrabili negli esami di laboratorio (es.: abitudini alimentari, dolori cronici, stili di vita, etc.), per una diagnosi più accurata. Tutto ciò, naturalmente, lasciando all'utente piena autonomia[61] nell'amministrare le proprie informazioni in sicurezza e nel rispetto della sua riservatezza[62].

---

[57] Ripreso da L. Rufo, *Profili giuridici del Personal Health Record: tra diritto all'autodeterminazione e tutela della privacy*, in C. Faralli, R. Brighi, M. Martoni (a cura di) *Strumenti, diritti, regole e nuove relazioni di cura: il paziente europeo protagonista nell' eHealth*, Giappichelli, 2015, pp. 321-333.

[58] In termini informatici si parla di un *software Web-based* intendendo un programma in cui tutte le funzioni sono accessibili con un normale *web-browser* (es.: *Firefox*, *Chrome* etc.), non essendo così necessario alcun *software* di installazione sul computer degli utenti. Attraverso le applicazioni *Web-based* l'utente ha il grande vantaggio di poter interagire con il sistema da qualsiasi sede e in qualsiasi momento. Sul punto: *Cfr.* E. Santoro, *web 2.0 e medicina*, Pensiero, Roma, 2009.

[59] C. Pagliari et al., *Potential of electronic personal health records*, British Medical Journal, 2007, pp. 335-333; N. Archer et al, *Personal health records: a scoping review*, J Am Med Inform Assoc, 2011, pp. 515-522.

[60] E' un paradigma che focalizza l'attenzione del sistema sanitario sul paziente e il suo vissuto prendendo in considerazione le sue tradizioni culturali e preferenze, i suoi valori personali, la situazione familiare e il suo stile di vita così da far diminuire il disagio e l'ansia per la malattia. *Cfr.* S. Simi, *Dalla medicina basata sulle prove alla medicina basata sul paziente*, in AA.VV. *Quale salute per chi. Sulla dimensione sociale della salute*, Franco Angeli, 2010, p. 107.

[61] L. De Panfilis, S. Zullo, *Aspetti etici delle applicazioni eHealth,* in C. Faralli, R. Brighi, M. Martoni (a cura di) Strumenti, diritti, regole e nuove relazioni di cura: il paziente europeo protagonista nell' eHealth, Giappichelli, 2015, pp. 55-67.

[62] M. Martoni, *Social "Sanitary" Network per l'eHealth: fra condivisione della conoscenza e protezione dei dati personali*, in C. Faralli, R. Brighi, M. Martoni (a cura di) Strumenti, diritti, regole e nuove relazioni di cura: il paziente europeo protagonista nell' eHealth, Giappichelli, 2015, pp. 85-107.

Alla luce di quanto sin qui detto il sistema PHR[63] non coincide, senza dubbio, con l'*Elettronic Health Records*[64] (EHR) – nella versione italiana corrisponde al Fascicolo sanitario elettronico[65] (FSE) o al Dossier Sanitario (DS) che contengono, nello specifico, solo documenti sanitari e socio-sanitari – sistema informativo sanitario che ha come obiettivo il fornire ai medici, e più in generale ai clinici, una visione globale e unificata dello stato di salute dei singoli cittadini, e che rappresenta il punto di aggregazione e di condivisione delle informazioni e dei documenti clinici afferenti al cittadino, controllati dai vari attori del Sistema Sanitario[66].

Ciò nondimeno il PHR, a differenza dell'EHR, è un ottimo strumento, utilizzabile non solo in "lettura" come valido supporto informatico alle decisioni mediche, ma anche in "scrittura" come repository per i dati elaborarti, in quanto rappresenta un'efficace soluzione alla frammentazione dei dati sanitari dei pazienti sparsi nei sistemi delle varie strutture sanitarie.

Si deve anche sottolineare come tale strumento possa includere, come già accennato, a differenza dell'EHR, al di là dei dati sanitari riferiti in senso stretto al paziente, anche informazioni relative ai familiari (es.: condividendo informazioni su eventuali malattie ereditarie), dati degli operatori sanitari nonché eventuali informazioni sull'ambiente di lavoro importanti per la salute dell'individuo. Infatti tali informazioni possono essere a loro volta, senza difficoltà, rielaborate e/o aggregate ai risultati di laboratorio così da condurre verso facili soluzioni in caso di ricadute cliniche o necessità sociali[67].

Se, come si è detto, il *quid novi* di un PHR, rispetto ai sistemi ad oggi in uso, è rappresentato dalla centralità e dalla autonomia che offre al paziente[68], è tuttavia anche

---

[63] R. Ducato, P. Guarda, *Profili giuridici dei "personal health records": l'autogestione dei dati sanitari da parte del paziente tra "privacy" e tutela della salute*, in Rivista critica del diritto privato, 2014, fasc. 3, pp. 389-419.

[64] R.D. Kush et al. *Electronic Health Records, Medical Research, and the Tower of Babel,* N Engl J Med 2008 358: 1738-1740; GUARDA, *Fasciolo sanitario elettronico e protezione dei dati personali*, cit., p. 31.

[65] Il Fascicolo sanitario elettronico è «*l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito*», previsto dall'art. 12 del Decreto legge 18 ottobre 2012, n. 179 recante "Ulteriori misure urgenti per la crescita del Paese", convertito con emendamenti nella legge 17 dicembre 2012, n. 221.

[66] *Il fascicolo sanitario elettronico - Linee guida nazionali*, in G.U. 2 marzo 2011 n. 50, S.O.

[67] P. C. Tang, *Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption*, J Am Med Inform Assoc. 2006 Mar-Apr; 13(2): 121-126. doi: 10.1197/jamia.M2025.

[68] Per un maggior approfondimento: C. Maioli, E. Sánchez Jordán, *Big Data e capacità informativa per l'autodeterminazione del paziente,* in C. Faralli, R. Brighi, M. Martoni (a cura di) Strumenti, diritti, regole e nuove relazioni di cura: il paziente europeo protagonista nell' eHealth, Giappichelli, 2015, pp. 155 ss.

doveroso citare quali "forme" il PHR può assumere per essere creato, alimentato e gestito dallo stesso[69].

Un primo supporto utile per un paziente è l'installazione di un software PHR, in locale, sul proprio *Personal Computer*, così da poter inserire, aggiornare, scaricare, scansionare e stampare i propri dati e documenti sanitari comodamente da casa[70].

Un secondo supporto è *Internet,* infatti la maggior parte dei prodotti PHR sono accessibili *online* permettendo così di gestire, di aggiornare e trasmettere i dati sanitari ovunque ci si trovi[71].

Un ulteriore sistema è rappresentato dalle applicazioni cosiddette "*App* mediche*"*[72] per *Smartphone,* che si stanno diffondendo molto rapidamente e presentano una varietà di caratteristiche tecniche differenti ed in grado di adattarsi alle varie esigenze degli utenti, dando la possibilità di condividere i propri dati anche attraverso i *social media*[73].

---

[69] I. Genitsaridia et al., *Evaluation of personal health record systems through the lenses of EC research projects, Computers in Biology and Medicine*, 2013; J. S. Kahn al., *What It Takes: Characteristics Of The Ideal Personal Health Record*, Health Affairs, 28, no.2 (2009).

[70] v. Intelichart - www.intelichart.com; myPHR – www.myphr.com (servizi attivi alla data di giugno 2017).

[71] v. Health Vault - www.healthvault.com; Dossia - www.dossia.org; webMD - www.webmd.com (servizi attivi alla data di giugno 2017).

[72] Le applicazioni mediche per smartphone e tablet sono moltissime e per fare ordine in questo campo sono stati creati siti *web* che le raccolgono, catalogano per utilità e valutano in termini di affidabilità. Es.: www.imedicalapps.com; http://myhealthapps.net; www.medicapp.info; www.mobimed.it (servizi attivi alla data di giugno 2017).

[73] *Cfr.* L. Jingquan, *Privacy policies for health social networking sites*, cit., pp. 1-4.

CAPITOLO II

La protezione dei dati personali: Linee guida sul Dossier Sanitario

"La tecnologia sta cambiando non solo i modelli di organizzazione sociale e la vita degli individui, ma anche il quadro istituzionale. Si pensi a come il computer e le tecnologie informatiche incidano sulla vita privata"

Stefano Rodotà, Tecnologie e diritti[74]

La possibilità, propria delle tecnologie ICT, di trattare rilevanti quantità di dati[75] a velocità elevata e spesso senza un controllo capillare, arrivando persino a tracciare profili dettagliati dei soggetti interessati, ha prodotto una conseguente accelerazione anche nell'elaborazione normativa del diritto alla protezione della sfera personale delle persone.

Come noto, la tradizionale nozione di "diritto alla privacy" (*The right to privacy*) compare per la prima volta in uno scritto di due avvocati statunitensi del 1890, Samuel Warren e Louis Brandeis, che nella loro originaria concezione dello stesso coglievano la necessità di un diritto di proteggere le persone dalle interferenze altrui (*The right to be let alone*)[76].

Tuttavia, dal XIX secolo ad oggi la nozione di privacy è mutata, passando dal generico "diritto passivo" di essere lasciati soli al "diritto attivo" dell'interessato di controllare come vengono trattati i propri dati[77].

---

[74] S. Rodotà, *Tecnologie e diritti*, il Mulino, Bologna 1995.

[75] Dati in grado di generare informazioni legate alla sfera privata, alla salute, al pensiero politico, al credo religioso di un individuo.

[76] *"The right to be let alone is like the right not to be assaulted or beaten, the right not to be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed. In each of these rights, as indeed in all other rights recognized by the law, there inheres the quality of being owned or possessed -and (as that is the distinguishing attribute of property) there may be some propriety in speaking of those rights as property".* Cfr. S. Warren, L. Brandeis, *The right to privacy*, Harvard Law Review, Boston (MA), 1890, p. 205.

[77] Secondo la definizione presente sul glossario dell'Autorità Garante, *"privacy è un termine inglese che evoca significati a volte mutevoli, accostabile ai concetti di* "riservatezza", "privatezza". Nella realtà contemporanea, con il concetto di *privacy* non si intende soltanto il diritto di essere lasciati in pace o di proteggere la propria sfera privata, ma soprattutto il diritto di controllare l'uso e la circolazione dei propri dati personali che costituiscono il bene primario dell'attuale società dell'informazione.
Il diritto alla privacy e, in particolare, alla protezione dei dati personali costituisce un diritto fondamentale delle persone, direttamente collegato alla tutela della dignità umana, come sancito anche dalla Carta dei diritti fondamentali dell'Unione Europea". Fonte: Glossario Autorità Garante – www.gpdp.it.

Complice proprio il progresso tecnologico, il già presidente dell'Autorità Garante Stefano Rodotà ha affermato proprio che

la tutela della privacy si è sempre più strutturata come diritto di ogni persona al mantenimento del controllo sui propri dati, ovunque essi si trovino, così riflettendo la nuova situazione nella quale ogni persona cede continuamente, e nelle forme più diverse, dati che la riguardano[78].

Pertanto, a seguito della sua evoluzione storica, il riconoscimento del diritto alla privacy ha preso due diverse direttrici: da una parte il "diritto alla riservatezza", il cui contenuto nasce come possibilità per l'individuo di preservare una particolare sfera intima e personale, proteggendo i propri fatti privati (es. convinzioni ideologiche, religiose, stato di salute) dalla divulgazione, in altre parole una sorta di diritto al riserbo[79], dall'altra la "protezione dei dati personali"[80] che tiene conto della tutela dell'identità dei soggetti interessati e anche di tutte le tecniche a mezzo delle quali si garantiscono la sicurezza e la protezione dei dati personali[81].

I fondamenti costituzionali o sovracostituzionali delle due declinazioni della privacy sono tuttavia comuni: l'art. 8 della "Convenzione europea dei diritti dell'uomo"[82] (CEDU), afferma il diritto di ogni individuo "*al rispetto della propria vita personale e familiare, del proprio domicilio e della propria corrispondenza* […]"; l'art. 8 della "Carta dei diritti fondamentali dell'Unione europea", sancisce che "*Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano*"; a livello nazionale, l'art. 2 della Costituzione che, nell'interpretazione dello stesso quale "fattispecie aperta"[83], consente al diritto alla riservatezza di trovare posto tra i diritti

---

[78] S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, Roma-Bari, 2014.

[79] Per maggiore approfondimento *Cfr.* L. Califano, *Privacy e Sicurezza*, Democrazia & Sicurezza, 2013, pp. 1-18.

[80] Come afferma un'autorevole dottrina (Pizzetti), *"l'espressione "diritto alla protezione dei dati personali" non è come spesso si usa nel linguaggio, un poco gergale, dei giornalisti e del pubblico, solo "diritto alla privacy" come protezione della diffusione delle informazioni che riguardano una persona. Esso riguarda il diritto a che ogni informazione, di qualunque genere, che sia direttamente o indirettamente riferibile ad una persona , non sia illecitamente raccolta, trattata, conservata e diffusa", in* F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento Europeo*, Giappichelli, Torino, 2016, p. 45, nota.

[81] G. M. Salerno, *La protezione della riservatezza e l'inviolabilità della corrispondenza*, in P. Ridola, R. Nania (a cura di), *I diritti costituzionali*, Giappichelli, Torino, 2006, vol. II, pp. 617 ss.

[82] Firmata nel 1950 dal Consiglio d'Europa, la convenzione è un trattato internazionale volto a tutelare i diritti umani e le libertà fondamentali in Europa. http://eur-lex.europa.eu/summary/glossary/eu_human_rights_convention.html?locale=it (ultimo accesso giugno 2017).

[83] Si vuole così definire una norma che non intende fare riferimento a una serie tassativa, determinata e chiusa di diritti, la quale non potrebbe essere ampliata o modificata se non con legge costituzionale, ma che postulerebbe la possibilità di ricomprendere nella stessa ogni diritto che

fondamentali della persona, in particolare nella sua accezione di vero e proprio diritto della personalità[84] (e, nondimeno, può trovarvi "ospitalità" anche il diritto alla protezione dei dati personali).

La Direttiva "madre" 95/46/CE[85], che disciplinava la raccolta e l'utilizzazione dei dati personali all'interno dell'Unione europea e recepita nel nostro ordinamento dalla Legge n. 675/1996, nasce in un quadro evidentemente antecedente la Carta di Nizza ma già orientato (Considerando n. 1) alla promozione della democrazia "*basandosi sui diritti fondamentali sanciti dalle costituzioni e dalle leggi degli Stati membri nonché dalla convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali*", di cui il diritto alla riservatezza costituiva evidentemente già un dato più che consolidato.

Sempre i considerando di tale Direttiva, ed in particolare il Considerando n. 2, lasciavano emergere il rilevante principio secondo cui:

i sistemi di trattamento dei dati sono al servizio dell'uomo; (...) essi, indipendentemente dalla nazionalità o dalla residenza delle persone fisiche, debbono rispettare le libertà e i diritti fondamentali delle stesse, in particolare la vita privata, e debbono contribuire al progresso economico e sociale, allo sviluppo degli scambi nonché al benessere degli individui.

Quindi, pur nel contesto di una Direttiva fondata sulla base normativa dell'art. 100 dell'allora vigente Trattato istitutivo della Comunità europea, e quindi fondata sull'esigenza di ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri aventi per oggetto l'instaurazione ed il funzionamento del mercato interno, era già allora ben presente al legislatore europeo il rilievo costituzionale (e CEDU) dei diritti in questione.

---

potesse ritenersi "inviolabile" in considerazione dell'evoluzione storica. Sul punto per maggior approfondimento cfr. A. Barbera, *Sub art. 2*, in G. BRANCA (a cura di) *Commentario della Costituzione*, Bologna, Zanichelli editore, Roma, 1975.

[84] Cass., 27 maggio 1975, n. 2129, in Foro it.,1976, I, c. 2895.

[85] La direttiva 95/46/CE, del Parlamento europeo e del Consiglio del 24 ottobre 1995, definisce un quadro normativo volto a stabilire un equilibrio fra un livello elevato di tutela della vita privata delle persone e la libera circolazione dei dati personali all'interno dell'Unione europea (UE). A tal fine, la direttiva fissa limiti precisi per la raccolta e l'utilizzazione dei dati personali e chiede a ciascuno Stato membro di istituire un organismo nazionale indipendente incaricato della sorveglianza di ogni attività associata al trattamento dei dati personali. http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=URISERV%3Al14012 (ultimo accesso giugno 2017).

Sullo stesso solco si muovono, a seguire, il D. Lgs. 196/2003[86] (Codice Privacy a tutt'oggi in vigore) e il nuovo Regolamento Europeo 2016/679[87].

La lenta ma inesorabile evoluzione in tema di *data protection*, con l'acquisizione di un ruolo preponderante da parte di questo "lato della medaglia" del tema privacy, si è avuta in parallelo con il progredire dell'innovazione tecnologica, che non può evidentemente rimanere priva di un quadro giuridico al passo con i tempi, pena il rischio di un'"obsolescenza giuridica"[88] dei riferimenti normativi relativi al trattamento di dati personali. Questa riflessione acquisisce maggior evidenza se si pensa alle note rivelazioni di Edward Snowden[89] che hanno contribuito a farci riflettere sul concetto di diritto alla privacy e portano a domandarci se oggi ha ancora senso parlare di privacy e di riservatezza in un mondo globalizzato e sempre più sorvegliato[90].

2.1 Codice Privacy: i profili generali

ll D. Lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali (di seguito "Codice")[91], che all'art. 1 recita: *"chiunque ha diritto alla protezione dei dati personali che lo riguardano",* è ad oggi il *corpus* normativo che nell'ordinamento italiano disciplina compiutamente il diritto alla protezione dei dati personali.

In particolare il legislatore interno, attraverso l'adozione del Codice (Testo Unico che si compone di 186 articoli e suddiviso in tre parti tese a razionalizzare e semplificare la materia[92]) ha voluto garantire, esclusivamente alle persone fisiche[93], che

---

[86] Codice in materia di protezione dei dati personali. http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248 (ultimo accesso giugno 2017).

[87] http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ITA (ultimo accesso giugno 2017).

[88] Intesa come perdita di efficienza della "norma" rispetto all'incalzante progresso tecnologico.

[89] Edward Joseph Snowden è un tecnico informatico Statunitense, ex contractor della CIA (Central Intelligence Agency) ed ex collaboratore di una società informatica di assistenza tecnica della NSA (National Security Agency). Nel giugno del 2013 ha rivelato al giornale The Guardian un programma segreto (denominato prisma) della NSA finalizzato a raccogliere metadati riferiti alle comunicazioni domestiche negli USA per finalità di sorveglianza.

[90] G. Ziccardi, *Internet, controllo e libertà*, Raffaello Cortina Editore, Milano, 2015.

[91] Per maggiori informazioni sul tema Cardarelli-Sica- Zeno Zencovich, *Il codice dei dati personali. Temi e problemi*, Milano, 2004; R. Imperiali, *Il Codice della privacy*, Milano, 2004; P. Perri, *Privacy, Diritto e sicurezza informatica*, Milano, 2007.

[92] v. *"La struttura del Codice Privacy"* con le norme attualmente in vigore in Italia, in Appendice, pp. 207-210.

[93] Il D. Lgs. 196/2003, nella sua prima formulazione, tutelava anche le persone giuridiche, scelta priva di precedenti nelle esperienze degli altri Paesi europei. Tuttavia, nel 2011 con l'art. 40 del decreto legge 6 dicembre 2011, n. 201 (convertito, con modificazioni, dalla legge 22 dicembre 2011, n. 214), è

"*il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali*" (art. 2, comma 1).

"Trattamento" che, secondo l'art. 4, è definibile come

qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

Alla luce di ciò appare doveroso sottolineare che, perché ricorra un'ipotesi di trattamento di dati personali, non è necessario che gli stessi siano organizzati e/o memorizzati in un archivio o in una banca dati, ma è sufficiente che sia svolta una qualsiasi operazione avente ad oggetto un dato personale.

Presupposti della legittimità del trattamento sono alcuni principi fondamentali fissati dal Codice, la cui presenza segnala il corretto operare da parte di chi lo esegue, nello specifico abbiamo:

- il *Principio di necessità:* "*I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità*" (articolo 3).

Attraverso tale principio il codice vuole sancire l'obbligo della minimizzazione dei dati trattati attraverso sistemi informativi o software, imponendo l'utilizzo di dati anonimi o "codificati"[94], arrivando così ad identificare direttamente l'interessato solamente in casi eccezionali e laddove non sia possibile perseguire determinate finalità in altri modi meno invasivi.

- *Il Principio di liceità:* I dati personali oggetto di trattamento sono "*trattati in modo lecito e secondo correttezza*" (articolo 11, comma 1, lett. a).

---

stato rimosso dall'impianto normativo ogni riferimento alla tutela della persona giuridica (imprese, enti ed associazioni).

[94] L'identificazione del soggetto interessato è mediata dall'utilizzo di un codice precedentemente classificato. Es. un numero di matricola, progressivo elimina coda.

Il trattamento è pertanto lecito quando conforme alla legge, ai regolamenti e alla normativa comunitaria e deve essere effettuato senza che l'interessato sia indotto a fornire informazioni con artifici o raggiri ovvero riceva indebite pressioni che ne condizionino il rilascio del consenso.

- *Il Principio di finalità:* I dati personali oggetto di trattamento sono "*raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi*" (articolo 11, comma 1, lett. b).

In base a tale principio l'interessato deve essere messo a conoscenza delle finalità effettive oggetto del trattamento. Nello specifico devono essere finalità chiare, univoche, legittime e di sola pertinenza del titolare del trattamento. Ed infatti, qualora il titolare ritenesse di voler aggiungere ulteriori finalità rispetto a quelle originariamente comunicate, è necessario che informi tempestivamente l'interessato e, ove obbligatorio, acquisisca un nuovo consenso.

Importante è notare che la norma distingue la raccolta dalla registrazione, potendo le due operazioni essere svolte in momenti e con supporti diversi. Accade spesso, infatti, che la raccolta del dato abbia luogo a mezzo di un supporto cartaceo, con successiva registrazione e trasposizione su supporto magnetico.

- *Il Principio di qualità ed esattezza dei dati:* I dati personali oggetto di trattamento sono: "*esatti e, se necessario, aggiornati*" (articolo 11, comma 1, lett. c).

Tale principio implica che il titolare debba sempre garantire l'esattezza dei dati raccolti e, ove necessario, provvedere al relativo aggiornamento. Ne discende, quale necessaria conseguenza, che al verificarsi di situazioni di dubbia esattezza del dato vadano intraprese azioni volte a ripristinare il fisiologico livello di affidabilità o, ove ciò non sia possibile, occorra valutarne la cancellazione.

- *Il Principio di proporzionalità:* I dati personali oggetto di trattamento sono: "*pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati*" (articolo 11, comma 1, lett. d).

In base a tale principio tutti i dati personali oggetto del loro trattamento devono essere pertinenti, completi e non eccedenti rispetto alle finalità dichiarate e che si intendono perseguire. Infatti, l'interessato verrebbe leso nella sua identità personale nel caso di trattamento di dati in cui mancasse il nesso logico tra l'informazione raccolta e la finalità perseguita[95].

- *Principio della giusta durata:* "I dati personali oggetto di trattamento sono: *conservati in una forma che consenta l'identificazione dell'interessato per un periodo di*

[95] G. Buttarelli, *Banche dati e tutela della riservatezza*, Giuffrè, Milano, 1997.

tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati" (articolo 11, comma 1, lett. e).

Questo principio prevede la conservazione dei dati per un periodo di tempo limite non superiore a quello strettamente necessario a svolgere le finalità per i quali sono stati raccolti. Cosicché, quando il dato non sarà più necessario, è preferibile che esso venga cancellato, o quantomeno, se utile per finalità statistiche, reso anonimo.

Ultimo, ma non meno importante, è il principio previsto dal comma 2 dell'art. 11 (articolo che riveste nel suo complesso un ruolo centrale all'interno del Codice), che impone l'inutilizzabilità dei dati nel caso sia disattesa la disciplina rilevante in materia di trattamento dei dati personali.

2.1.1 *I soggetti*

I principali soggetti protagonisti del trattamento dei dati sono: Titolare, Responsabile e Incaricato.

Il codice considera "titolare" del trattamento:

la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo, cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza"(art. 4, comma 1, Lett. f).

Da questa definizione si può evincere che il titolare è una qualifica "di fatto" dal momento che non è attribuita attraverso atti costitutivi di designazione. Egli esercita un potere decisionale completamente autonomo rispetto alle finalità e alle modalità del trattamento ed assume la funzione di primario centro d'imputazione, attivo e passivo, in caso di violazione delle norme in materia di privacy.

Nella definizione sopra richiamata viene dato rilievo normativo, oltre che alla figura del titolare del trattamento, anche a quella del "contitolare"[96], che viene ad aversi qualora il trattamento sia comune a più titolari e questi assumano congiuntamente, su di esso, le decisioni circa le modalità, le finalità di trattamento e la sicurezza dei dati.

Tuttavia, eventuali esigenze organizzative del titolare del trattamento possono comportare la necessità di affidare anche ad altri soggetti talune responsabilità. Per tale

[96] Sul punto si veda: F. Modafferi, *Lezioni di diritto alla protezione dei dati personali, alla riservatezza e all'identità personale*, Lulu, 2015, pp.197 ss.; A. Del Ninno, *La tutela dei dati personali. Guida pratica al Codice della privacy (d.lgs. 30.6.2003. n. 196)*, Cedam, 2006, pp. 23-34.

ragione il codice prevede la possibilità di designare uno o più responsabili del trattamento. Il "responsabile" è inteso come *"la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali"* (art. 4, comma 1, Lett. g).

A questa definizione della figura del responsabile si affianca, all'art. 29 del Codice, una disciplina dei requisiti soggettivi e delle modalità della sua designazione.

Esso è designato dal titolare facoltativamente ed è individuato tra i soggetti con più esperienza, capacità e affidabilità. È possibile procedere alla designazione di più soggetti con la qualifica di responsabili, anche mediante la suddivisione dei compiti da svolgere. L'atto di designazione dovrà essere redatto per iscritto e contenere le istruzioni precise e chiare da compiere.

Responsabile del trattamento può essere anche, come già evidenziato dall'art. 4, comma 1, Lett. g, una società esterna che naturalmente agisce in nome e per conto del titolare-delegante.

Accanto alle figure sopra richiamate, un ruolo, meno rilevante sul piano gerarchico ma fondamentale per assicurare le corrette operazioni di un trattamento di dati, è svolto dall'incaricato.

"L'incaricato" è *"la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile"* (art. 4, comma 1. Lett. *h*).

La designazione degli incaricati è disciplinata dall'art. 30, ove si stabilisce che essi operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite. Si rende così necessario l'obbligo di provvedere ad effettuare la designazione scritta nei confronti di tutti i soggetti che compiano operazioni di trattamento su dati personali, configurando una cosiddetta "delega di esecuzione". Da sottolineare che, a differenza del responsabile che può essere anche una persona giuridica, l'incaricato può essere solo una persona fisica.

Per mera completezza, tra i soggetti coinvolti in un trattamento (su un versante "contrapposto" a quello di titolare, responsabile e incaricato) va menzionata la figura dell'interessato, che è intendersi come *"la persona fisica cui si riferiscono i dati personali"* (art. 4, comma 1, Lett. i).

All'interessato, alla luce dell'art. 7 del Codice, sono garantiti specifici diritti, e in particolare: l'aggiornamento, la rettifica ovvero, quando vi abbia interesse, l'integrazione dei dati; la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati; l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati

comunicati o diffusi, eccettuato il caso in cui tale adempimento si riveli impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

2.1.2 *I dati*

Il Codice, secondo le definizioni contenute nell'art. 4, prevede varie tipologie di dati che possono essere oggetto di un trattamento.

La grande categoria che li raggruppa è quella di "dato personale"[97].

Più precisamente un dato personale è «*qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*».

Analizzando tale definizione si può senza dubbio affermare che dato personale[98] è una qualunque informazione riferibile ad un interessato e costituito da quattro elementi fondamentali[99] strettamente connessi tra loro e che sono:

- "Qualunque informazione": i dati personali includono quindi informazioni soggettive (opinioni o valutazioni personali dell'interessato) ed oggettive (informazioni ricavate empiricamente). Sono pertanto comprese in questa categoria le informazioni sulla vita privata e familiare del soggetto.
- "relativa a": questo secondo elemento indica la necessità di una stretta relazione tra l'informazione e la persona fisica ad essa riferita.
- "persona fisica": le informazioni oggetto di trattamento devono riguardare la persona fisica e non anche le persone giuridiche.
- "identificata o identificabile": questo ultimo elemento indica chiaramente che per avere un dato personale ci devono essere informazioni che, anche aggregate tra loro, comportano l'identificazione diretta (es. attraverso il nome e/o il cognome) o indiretta (es. attraverso il codice fiscale, numero di telefono) dell'interessato.

Tra le tipologie di dati previste dal codice, all'interno della *species* del *genus* "dati personali", troviamo i dati identificativi, che permettono l'identificazione diretta dell'interessato, e i dati anonimi, che non possono essere associati ad un interessato

---

[97] Il 29 luglio 2015 è stato presentato il testo della "Dichiarazione dei diritti in internet" dove il dato personale è definito all'interno dell'art. 5 "[…] *Tali dati sono quelli che consentono di risalire all'identità di una persona e comprendono anche i dati dei dispositivi e quanto da essi generato e le loro ulteriori acquisizioni e elaborazioni, come quelle legate alla produzione di profili*".

[98] Sul punto anche Gruppo articolo 29, Parere n. 4/2007 "sul concetto di dato personale" (WP29 n.136) adottato il 20 giugno 2007.

[99] *Cfr.* Modafferi, *Lezioni di diritto alla protezione dei dati personali,* cit., pp. 115 ss.; M. Soffientini, (a cura di), *Privacy, Protezione e trattamento dati*, Wolters Kluwer, 2016, pp. 70-1.

specifico e quindi possono essere trattati liberamente, prescindendo dalla normativa privacy.

Ulteriore *species* è quella dei "dati sensibili". Si considerano in essa ricompresi i dati personali idonei a rilevare: l'origine razziale ed etnica; le convinzioni religiose, filosofiche o di altro genere; le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale; lo stato di salute e la vita sessuale.

Il Codice assoggetta ad una disciplina rigorosa il trattamento di questa tipologia di dati, dal momento che tratta la sfera più intima della persona[100].

Importante è sottolineare che la locuzione "idonei a rivelare", nell'introdurre ad un'elencazione "tassativa nei fini" non è suscettibile, sotto tale aspetto, di integrazione, sia in realtà idonea a far rientrare in questa tipologia non soltanto i dati "per definizione" sensibili (es. i dati relativi alla salute di un interessato), ma anche quelli che possono acquisire questa connotazione in rapporto al contesto specifico nel quale sono utilizzati (ad es. le scelte alimentari effettuate in una mensa aziendale).

I dati inerenti lo stato di salute di un soggetto sono, tra i dati sensibili, probabilmente i più "appetibili", ad oggi, da parte di soggetti che per finalità commerciali potrebbero avere interesse ad accedervi, ad analizzarli e a utilizzarli. A questa categoria di dati sensibili, per la quale si impiega anche frequentemente la denominazione di "dati sanitari", è opportunamente dedicata una disciplina *ad hoc*. Sovente essi vengono definiti anche come "dati sensibilissimi", dal momento che un loro illecito trattamento potrebbe procurare grave nocumento al soggetto interessato.

Un'ultima *species* di dato personale espressamente prevista dal Codice è quella dei "dati giudiziari".

In questa tipologia rientrano:

i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.p.r. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Da ultimo, per completare la parte definitoria, è opportuno soffermarsi brevemente sulle nozioni di "comunicazione" e di "diffusione".

---

[100] La delicatezza e l'importanza dei trattamenti dei dati sensibili per finalità di prevenzione, diagnosi, cura e riabilitazione emerge anche dalla lettura della Relazione 2013 dell'Autorità Garante.

Come avremo modo di vedere anche più avanti per i dati sanitari contenuti nel Dossier sanitario, il legislatore, visti i rischi che l'interessato può correre a causa della circolazione dei dati e delle informazioni che lo riguardano, ha utilizzato a tal proposito delle definizioni alquanto rigorose e estese nella loro portata applicativa.

Per "comunicazione" si intende "*il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione*"; per "diffusione" invece "*il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione*".

La distinzione tra comunicazione e diffusione rileva però soprattutto, più che per il novero dei soggetti destinatari della divulgazione del dato, per la possibilità di controllo dell'interessato dell'accesso ai dati stessi e al loro utilizzo, che può avere impatti significativamente lesivi dell'identità personale. In tale prospettiva, il Garante ha previsto il divieto di *diffusione* per i dati sensibili, permettendone la *comunicazione* soltanto previo espresso consenso dell'interessato[101].

2.1.3 *I presupposti di legittimità: informativa consenso*

Il Codice in materia di protezione dei dati personali pone in capo ai titolari del trattamento, nei confronti dell'interessato, alcuni adempimenti che prescindono dalla natura pubblica o privata del soggetto titolare del trattamento[102].

Ancora prima della raccolta o alla prima comunicazione dei dati il primario strumento attraverso cui garantire il diritto dell'interessato di controllare la circolazione delle informazioni che lo riguardano è costituito dall'informativa sul trattamento dei dati personali[103].

L'informativa è stata sempre al centro di accessi dibattiti dottrinali[104] e giurisprudenziali[105] e al riguardo un'autorevole dottrina ha affermato che "*se si vivono*

---

[101] *Cfr.* G. Finocchiaro, *Privacy e protezione dei dati personali*, Zanichelli, 2012, pp. 73-76.

[102] Sul punto F. Bravo, *Le condizioni di liceità del trattamento dei dati*, in J. Monducci, G. Sartor (a cura di), Il Codice in materia di protezione dei dati personali, Cedam, Padova, 2004, nonché J. Monducci, *Diritti della persona e trattamento dei dati particolari*, Giuffrè, Milano, 2003.

[103] In materia di informativa e consenso. *Cfr.* le pronunce dell'Autorità Garante del 19 giugno 1997, in Boll. n. 1, 21, [doc. web n. 1161215]; 28 luglio 1997, in Boll. n. 1, 24-25 [doc. web. n. 40057]; 8 settembre 1997, in Boll. n. 2, 13-14 [doc. web n. 1055101]; 21 ottobre 1997, in Boll. n. 2, 21-22 [doc. web n. 40855]; 22 ottobre 1997, in Boll. n. 2, 25-27 [doc. web. n. 1055346].

[104] Buttarelli, attuale Garante europeo, etichettò l'informativa come: *"uno stanco e formale adempimento, che deve caratterizzare sempre più una relazione leale e corretta con l'interessato. v. http://www.interlex.it/675/buttarelli2.htm (Ultimo accesso giugno 2017)*

le norme sulla tutela dei dati personali come un'autentica conquista civile, si perdona quel tanto di burocrazia che portano nella nostra vita".[106]

L'informativa, disciplinata dall'art. 13 del Codice, costituisce un adempimento generale a cui, salvo casi eccezionali, sono sottoposti tutti i titolari di trattamento ed ha la finalità di chiarire in modo semplice e completo quale utilizzo verrà fatto dei dati personali. Infatti, proprio nell'ottica del consenso informato, l'interessato deve avere la possibilità di sapere, per liberamente orientare le proprie scelte, quali siano le conseguenze del suo rifiuto di conferire i dati.

Secondo l'art. 13, l'informativa deve contenere obbligatoriamente:

a) le finalità e le modalità del trattamento cui sono destinati i dati;

b) la natura obbligatoria o facoltativa del conferimento dei dati;

c) le conseguenze di un eventuale rifiuto di rispondere;

d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;

e) i diritti di cui all'articolo 7;

f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.

È opportuno porre mente alla circostanza che, molto spesso, i dati vengono raccolti presso soggetti terzi diversi dall'interessato. In tale circostanza, non potendo il titolare fornire l'informativa all'interessato stesso, l'art. 13, comma 4, impone che questa, con l'indicazione delle categorie di dati trattati, venga fornita all'interessato a cui i dati si riferiscono all'atto della registrazione o non oltre la prima comunicazione, quando questa sia prevista.

Infine, si rammenta che la norma prevede che l'informativa possa essere resa sia in forma scritta che orale; non è pertanto richiesto uno specifico onere di forma. La

---

[105] Per trattamenti particolarmente invasivi nella sfera personale dell'interessato, l'obbligo dell'informativa è stato rimarcato più volte dalla giurisprudenza. Ad esempio il Consiglio di Stato, in materia di dati sensibili, ha statuito che *"il regolamento per la disciplina del trattamento dei dati informativi da inserire nelle schede relative ai pazienti dimessi dagli istituti di cura pubblici e privati deve prevedere anche modalità atte a garantire l'informativa ai pazienti da parte del medico titolare del trattamento terapeutico"*. Consiglio di Stato, Sez. I, 18 settembre 2000, n. 146.

[106] S. Rodotà, Affari e finanza, suppl. Repubblica, 10 dicembre 2002.

scelta è tuttavia rimessa al titolare, che sceglierà sulla base del tipo di strumento utilizzato per la raccolta dei dati presso l'interessato.

L'informativa, come noto, non esaurisce gli obblighi del titolare per quanto concerne il trattamento dei dati personali. Un ulteriore e necessario presupposto di legittimità è dato dall'art 23 del Codice, che richiede al titolare di munirsi di un apposito *consenso* al trattamento.

Nello specifico il consenso rappresenta una libera espressione e dichiarazione di volontà dell'interessato, è un elemento essenziale, dunque, dal momento che proprio in forza di esso l'interessato può esercitare l'effettivo potere di controllo sull'uso dei propri dati personali[107].

La volontà di acconsentire al trattamento deve essersi formata dopo un'esatta rappresentazione delle circostanze rilevanti: il consenso deve, quindi, essere "informato"[108]: l'interessato, in altri termini, deve avere previamente ricevuto informazioni complete e adeguate, contenute nell'informativa, tali da consentirgli di validamente decidere se prestare o meno il proprio consenso[109].

Forti analogie sono riscontrabili tra tale consenso e il consenso informato in ambito medico, che è espressione del diritto del paziente di scegliere, accettare o anche eventualmente rifiutare i trattamenti che gli vengono proposti, con *"profili interconnessi di rilevanza giuridica, etico-filosofica e medico-legale"*[110].

Il Codice Privacy all'art. 23 non si limita a prevedere la mera necessità del consenso, ma stabilisce anche quelli che sono i suoi i suoi requisiti di validità.

Il codice infatti dispone che il consenso è valido solo se:

- è espresso liberamente e specificamente in riferimento ad un trattamento ben definito (laddove la libertà di espressione dello stesso implica l'assenza condizionamenti dell'interessato al momento in cui questo viene reso);
- è documentato per iscritto, quando il trattamento riguarda dati sensibili;

---

[107] Concetto approfondito da Acciai che afferma *"dalle notizie in tal modo acquisite l'interessato può effettivamente decidere l'an e il quomodo della circolazione dei propri dati personali, finendo, così, anche tale requisito, per incidere sulla libertà di controllare i propri dati personali da parte del soggetto cui gli stessi si riferiscono"*. v. Acciai R. (a cura di), *Il diritto alla protezione dei dati personali. La disciplina sula privacy alla luce del nuovo Codice*, Maggioli editore, Santarcangelo di Romagna, 2004, p. 123.

[108] In tema di "Consenso informato" si veda: F. Ciciliano, *La disciplina giuridica del consenso informato*, Arnus University Books, Pisa, 2013; G. Casciaro, *Il consenso informato*, Giuffré, 2012.

[109] Da specificare che il consenso prestato per un determinato trattamento non può legittimare il medico ad eseguirne uno diverso, per natura od effetti, salvo sopraggiunga una situazione di necessità ed urgenza – non preventivamente prospettabile – che determini un pericolo serio per la salute o la vita del paziente.

[110] C. Faralli, Introduzione, in Id. (a cura di), *Consenso informato in medicina. Aspetti etici e giuridici*, Franco Angeli, 2012.

- sono state rese all'interessato le informazioni di cui all'art. 13 (in un'ottica di trasparenza dell'operato del titolare nei confronti dell'interessato).

Il consenso, a pena di nullità, deve essere prestato prima dell'inizio del trattamento e comunque dopo aver avuto conoscenza dell'informativa. Esso può riguardare l'intero trattamento oppure una o più operazioni del medesimo e, comunque, può essere liberamente revocato, ferma restando la legittimità delle attività di trattamento svolte prima della revoca.

Per completezza va inoltre menzionato l'art. 24 del Codice, che prevede tutta una serie di ipotesi di esclusione dell'obbligo del consenso.

Difatti, il trattamento è lecito senza che debba essere richiesto il consenso quando i dati sono:

a) necessari per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;

b) necessari per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;

c) provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati;

d) relativi allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

e) necessari per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2.

2.1.4 *Gli obblighi di sicurezza*

Ai fini della più completa garanzia del diritto alla protezione dei dati personali, il Codice all'art. 31 impone, al titolare del trattamento, l'adozione e il rispetto di "misure di sicurezza", che rappresentano il livello minimo di protezione richiesto in relazione ai

rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta[111].

È chiaro quindi che ai soggetti destinatari degli obblighi di sicurezza sono richiesti interventi di tipo organizzativo, fisico e logico sottoposti a continuo aggiornamento e verifica; oltre a ciò, è necessario che l'adozione di tali misure di sicurezza avvenga adottando accorgimenti idonei e preventivi, suggeriti dalle conoscenze acquisibili in base al progresso tecnologico, alla natura dei dati e alle specifiche caratteristiche del trattamento[112].

Il legislatore dedica alle misure minime di sicurezza gli artt. 33 e seguenti. Più precisamente afferma che i titolari dei trattamenti, salvo eventuali ulteriori obblighi, debbono in ogni caso rispettare le misure minime descritte agli artt. 34-36 del Codice e il disciplinare tecnico contenuto nell'Allegato B del Codice stesso; al di sotto di tali standard minimi non è possibile ritenere sussistente un adeguato livello di protezione sui dati personali trattati.

Per maggior completezza, va detto che le norme del Codice distinguono le misure in parola in relazione alla natura degli strumenti utilizzati per il trattamento.

Così che all'art. 34 troviamo regolati gli accorgimenti da tenere presenti in caso di trattamenti con strumenti elettronici; all'art. 35 vengono invece regolamentati i trattamenti compiuti con strumenti diversi da quelli elettronici.

Tuttavia, entrambe le norme non entrano nei dettagli degli accorgimenti da adottare con riferimento ad entrambi, rinviando invece all'Allegato B che specifica analiticamente tutte le misure richieste, quali ad esempio, per i primi (strumenti elettronici):

- prevedere un Sistema di autenticazione informatica (es. attraverso l'uso di User e Password o di un *Token* o anche di dispositivi biometrici);
- creare un sistema di autorizzazione (es. creare gruppi di utenti per determinati categorie dati o per determinate mansioni che questi svolgono);
- provvedere all'aggiornamento periodico dei sistemi e al controllo dei soggetti legittimati a trattare i dati;
- provvedere ad adottare procedure per la custodia di copie di sicurezza per l'eventuale ripristino dei dati e dei sistemi.

---

[111] Per maggiori informazioni sul punto Finocchiaro, *Privacy e protezione dei dati personali*, cit., p. 253; Modafferi, *Lezioni di diritto alla protezione dei dati personali,* cit., pp. 204-206.

[112] D. D'Agostini, A. Piva, A. Rampazzo, La sicurezza delle informazioni in ambito sanitario, In Mondo Digitale, AICA, Milano 2010, 2, pp.59-66.

Analizzando gli obblighi di sicurezza è, a questo punto, doveroso introdurre la figura dell' "Amministratore di sistema"[113]. Questi è una figura essenziale per la sicurezza delle banche dati e per la corretta gestione delle reti telematiche; in considerazione di ciò il Garante Privacy, con il provvedimento "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratori di sistema"*[114] del 27 novembre 2008 (successivamente modificato nel 2009), ha richiamato l'attenzione su questa figura che, per lo svolgimento delle sue funzioni, deve possedere particolari requisiti di esperienza, capacità e all'affidabilità[115].

Tutte le funzioni tipiche dell'amministrazione di un sistema sono richiamate nel menzionato Allegato B: queste spaziano in un campo alquanto ampio, dalla realizzazione di copie di sicurezza (operazioni di *backup* e *recovery* dei dati) alla custodia delle credenziali alla gestione dei sistemi di autenticazione e di autorizzazione.

La mancata adozione delle misure minime di sicurezza comporta, oltre che sanzioni amministrative, anche conseguenze di natura penale, che possono giungere fino ai due anni di arresto (art. 169 del Codice Privacy).

2.1.5 *Il Trattamento dei dati sanitari*

La grande tematica della normativa in materia di protezione dei dati personali connessa all'ambito sanitario è *ab origine* singolare e molto discussa.

Sin dalla Legge n. 675/96 la previsione di norme e principi specifici posti a tutela della riservatezza del paziente è stata per lo più percepita come un mero vincolo burocratico tale da creare un ostacolo alle esigenze di urgenza, velocità e appropriatezza delle prestazioni sanitarie da erogare.

Tuttavia, con il passare del tempo e con il maturare della consapevolezza diffusa di una normativa meno burocratica e orientata piuttosto all'effettiva tutela del paziente e del rispetto della sua dignità, si è finalmente giunti, con il Codice Privacy del 2003, ad un ripensamento complessivo del rapporto tra diritto alla privacy e sanità, che si è tradotto sul testo normativo in questione nel passaggio da una disciplina confinata entro

---

[113] La figura dell'Amministratore di Sistema era già stata disciplinata dalla previgente normativa e, in particolare, dall'art. 1, comma 1, lett. c) del D.P.R. n. 318/1999, che aveva definito questa figura professionale come *"il soggetto a cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione".*

[114] Provvedimento reperibile sul sito www.gpdp.it [doc. web. n. 1577499] (ultimo accesso giugno 2017).

[115] Risposta alla FAQ n. 20 del Provvedimento "Amministratori di sistema" del Garante Privacy del 27 novembre 2008.

un unico articolo[116] (Legge n. 675/96) ad un'articolata serie di previsioni che vanno a occupare un intero Titolo, il quinto, della Parte II del nuovo Codice, dedicato appunto al "trattamento dei dati personali in ambito sanitario" (articoli da 75 a 94).

Nello specifico, questo titolo regola in maniera esaustiva le modalità di trattamento delle informazioni idonee a rivelare lo stato di salute che devono essere rispettate dagli esercenti le professioni sanitarie e dagli organismi sanitari pubblici.

Come già accennato in precedenza[117], alla luce di questo titolo V viene individuata una "nuova" tipologia di dato, quello "sanitario", che assume così una precisa connotazione giuridica, rinvenibile nelle seguenti caratteristiche:

- essere riferito ad un interessato identificato o identificabile;
- essere trattato da un soggetto esercente la professione sanitaria;
- essere raccolto per la finalità di diagnosi, prevenzione e cura di un paziente, di un terzo o della collettività.

Proseguendo oltre nell'analisi del Titolo V del Codice, appare sin da subito rilevante il richiamo che viene fatto ai due elementi basilari del trattamento in ambito sanitario: l'informativa e il consenso. Come già evidenziato, tali requisiti di legittimità del trattamento sono entrambi indefettibili.

L'art. 76, comma 1, individua le casistiche di trattamento considerate legittime dal legislatore, e più precisamente:

a) con il consenso dell'interessato e anche senza l'autorizzazione del Garante, se il trattamento riguarda dati e operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica dell'interessato;

b) anche senza il consenso dell'interessato e previa autorizzazione del Garante, se la finalità di cui alla lettera a) riguarda un terzo o la collettività.

---

[116] Art. 23 Legge 675/96 rubricato "Dati inerenti alla salute" che prevedeva: - *Gli esercenti le professioni sanitarie e gli organismi sanitari pubblici possono, anche senza l'autorizzazione del Garante, trattare i dati personali idonei a rivelare lo stato di salute, limitatamente ai dati e alle operazioni indispensabili per il perseguimento di finalità di tutela dell'incolumità fisica e della salute dell'interessato. Se le medesime finalità riguardano un terzo o la collettività, in mancanza del consenso dell'interessato, il trattamento può avvenire previa autorizzazione del Garante.*
- I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato solo per il tramite di un medico designato dall'interessato o dal titolare.
- L'autorizzazione di cui al comma 1 è rilasciata, salvi i casi di particolare urgenza, sentito il Consiglio superiore di sanità. E' vietata la comunicazione dei dati ottenuti oltre i limiti fissati con l'autorizzazione.
- La diffusione dei dati idonei a rivelare lo stato di salute è vietata, salvo nel caso in cui sia necessaria per finalità di prevenzione, accertamento o repressione dei reati, con l'osservanza delle norme che regolano la materia.

[117] Si rinvia *supra,* par. 2.1.2

A queste due ipotesi vanno aggiunte le fattispecie enunciate all'art. 82, tutte essenzialmente accomunate dalla circostanza di prevedere l'acquisizione del consenso in un momento successivo rispetto all'erogazione della prestazione sanitaria, ancorché "senza ritardo": si tratta, com'è evidente, di fattispecie aventi come comune denominatore il sussistere di condizioni di emergenza per la salute.

Sulla base dei principi generali, già illustrati, in caso di trattamento dei dati sanitari la manifestazione del consenso richiederebbe di norma la forma scritta, avendo ad oggetto il trattamento dei dati sensibili. Ciò nonostante, il Codice prevede alcune semplificazioni. Infatti, secondo l'art. 81 del Codice, fornita l'informativa ai sensi degli artt. 78, 79 ed 80, "*il consenso al trattamento dei dati idonei a rivelare lo stato di salute, può essere manifestato con un'unica dichiarazione, anche oralmente*" ed in tal caso il consenso, anziché con atto scritto dell'interessato, deve essere "*documentato con annotazione dell'esercente la professione sanitaria o dell'organismo sanitario pubblico*".

È opportuno sottolineare come l'annotazione del consenso possa avvenire anche con modalità informatiche, purché nel rispetto delle norme previste dal Codice dell'Amministrazione digitale.

Specifiche modalità di semplificazione sono previste anche per l'informativa (articoli da 77 a 81 del Codice). In particolare, le modalità di semplificazione consistono per lo più nella possibilità di prevedere un'unica informativa a vantaggio di più titolari ovvero anche nel caso in cui l'interessato debba compiere più prestazioni medico-assistenziale erogate da unità e reparti diversi o da parte di più strutture.

Si deve tuttavia tener presente che le semplificazioni previste non riguardano il contenuto minimo dell'informativa ex art. 13 del Codice; difatti essa, anche se resa in forma sintetica, deve sempre contenere gli elementi previsti come obbligatori.

A chiusura del titolo V troviamo l'art. 94, che legittima il trattamento di dati idonei a rivelare lo stato di salute che sono contenuti in banche di dati, schedari, archivi o registri tenuti in ambito sanitario, purché effettuato nel rispetto del principio di necessità (art. 3 del Codice).

Con tale articolo si legittima così anche l'utilizzo del Dossier sanitario oggetto, come già detto, di apposite previsioni in ambito di protezioni dei dati personali e rintracciabili nelle Linee guida che ci apprestiamo ad analizzare.

2.2 Linee guida in materia di Dossier sanitario

In assenza di norme cogenti, attraverso il documento in esame si analizzeranno le Linee guida in materia di Dossier sanitario del 4 giugno 2015.

Le presenti Linee guida, a fronte dell'incremento dell'uso di tali strumenti, sono frutto di un lungo percorso vissuto "in negativo" da parte del Garante Privacy e di alcune aziende e strutture sanitarie oggetto di provvedimenti sanzionatori[118]. Infatti, sono emerse nel corso dei vari accertamenti ispettivi irregolarità ricorrenti che riguardavano, in particolare, l'informativa (carente e priva degli elementi essenziali per consentire una scelta consapevole sulla costituzione o meno del dossier), la costituzione del dossier senza il consenso del paziente, gli accessi indiscriminati al sistema informatico (ogni medico della struttura poteva consultare i referti sia dei propri pazienti sia di qualsiasi altra persona che avesse effettuato un esame clinico presso l'Azienda) e da ultimo l'impossibilità di esperire il diritto di oscuramento dei dati che lo riguardavano.

Come si evince dallo stesso titolo, i dati sanitari oggetto delle Linee guida sono quelli salvati nel dossier sanitario, ivi definito come:

l'insieme dei dati personali generati da eventi clinici presenti e trascorsi riguardanti l'interessato, messi in condivisione logica a vantaggio dei professionisti sanitari che presso lo stesso titolare del trattamento lo assistono, rappresenta un trattamento di dati personali specifico, volto a documentare parte della storia clinica dell'interessato attraverso la realizzazione di un sistema integrato delle informazioni sul suo stato di salute accessibile da parte del personale sanitario che lo ha in cura.

L'Autorità ha altresì affermato che:

affinché i dossier sanitari in uso presso le strutture sanitarie siano effettivamente degli strumenti di ausilio nei processi di diagnosi e cura dei pazienti è necessario che gli stessi siano realizzati con modalità tali da garantire in primo luogo la certezza dell'origine e della correttezza dei dati e l'accessibilità degli stessi solo da parte di soggetti legittimati.

[118] Sul punto si veda: il provvedimento del Garante del 10 gennaio 2013 nei confronti dell'Azienda ospedaliero-universitaria Ospedali Riuniti di Trieste e delle altre aziende sanitarie della regione Friuli Venezia Giulia [doc. web n. 2284708]; il provvedimento del Garante del 3 luglio 2014 nei confronti dell'Azienda sanitaria dell'Alto Adige [doc. web n. 3325808]; il provvedimento del Garante del 23 ottobre 2014 nei confronti dell'Azienda ospedaliero-universitaria S. Orsola Malpighi di Bologna [doc. web n. 3570631]; il provvedimento del Garante del 18 dicembre 2014 nei confronti dell'Azienda Policlinico Umberto I di Roma [doc. web n. 3725976]; il provvedimento del Garante del 22 ottobre 2015 nei confronti dell'Azienda dall'Azienda USL 11 di Empoli [doc. web n. 4449114]; il provvedimento del Garante del 22 giugno 2016 nei confronti dell'Azienda Ospedaliera Sant'Andrea di Roma [doc. web. 5410033].

Dall'analisi di questi profili generali si può senza dubbio ricavare che il DS rappresenta un trattamento ulteriore rispetto alla cura del singolo evento clinico, e come tale necessita di una specifica informativa e di specifici consensi.

2.2.1 *L'informativa del Dossier sanitario*[119]

Dal momento che il professionista, nel consultare le informazioni contenute nel DS ed elaborate nell'ambito dell'intera struttura sanitaria, non soltanto quindi del suo reparto/ambulatorio (quindi, da professionisti diversi), anche in occasione di altri eventi clinici occorsi in passato all'interessato, pone in essere un "ulteriore trattamento"[120], si rende necessaria una distinta informativa – da fornire all'interessato prima dell'acquisizione del consenso – che contenga, oltre al contenuto minimo previsto dal già citato art. 13 del Codice, anche:

- *la descrizione del Dossier sanitario:* nell'informativa deve essere evidenziata l'utilità, per la struttura e per il paziente, dell'attivazione del Dossier, quale strumento fondamentale per il miglioramento della qualità e della personalizzazione del percorso terapeutico, nonché per la fruibilità immediata delle informazioni cliniche al fine di avere un quadro clinico quanto più completo durante la diagnosi;
- *le conseguenze per il mancato consenso:* il paziente deve essere informato che il suo mancato consenso alla costituzione e successiva alimentazione del Dossier non incide sulla possibilità di accedere alle cure mediche, dal momento che per sua natura questo strumento è meramente facoltativo;
- *il trattamento dei "dati a maggior tutela":* deve essere riportata specifica menzione per l'eventuale intenzione del titolare del trattamento di rendere accessibili i dati soggetti a maggiore tutela dell'anonimato (es. informazioni relative a soggetti affetti da HIV, soggetti che hanno subito atti di violenza sessuale o di pedofilia, ecc.);
- il divieto di diffusione dei dati: deve essere precisato che tali dati, essendo idonei a rivelare le condizioni di salute, non possono essere oggetto di diffusione (art. 22 comma 8 del Codice, secondo cui "*i dati idonei a rivelare lo stato di salute non possono essere diffusi*»"*);*
- *lo stato di emergenza:* deve essere resa nota all'interessato anche la circostanza che, qualora acconsenta al trattamento dei suoi dati personali mediante il Dossier sanitario, questo potrà essere consultato, nel rispetto dell'Autorizzazione generale del Garante,

---

[119] *Infra, Fac-simile Modulo Informativa Dossier sanitario*, in Appendice, pp. 211-215, elaborato durante la ricerca applicata presso la Fondazione G. Monasterio.

[120] Va ben specificato che in assenza del Dossier sanitario il professionista ha accesso alle sole informazioni sintomatologiche riferite dal paziente e a quelle elaborate in relazione all'evento clinico.

anche qualora ciò sia ritenuto indispensabile per la salvaguardia della salute di un terzo o della collettività;

- *la consultazione da parte di liberi professionisti:* l'interessato deve essere informato sull'eventualità che il dossier sia consultato anche da parte di professionisti che agiscono in libera professione *intramoenia*, ossia nell'erogazione di prestazioni al di fuori del normale orario di lavoro utilizzando le strutture ambulatoriali o diagnostiche della struttura sanitaria a fronte del pagamento da parte del paziente di una tariffa *ad hoc*;
- *l'ambito di conoscibilità:* l'interessato deve essere informato in merito ai soggetti o alle categorie di soggetti ai quali i dati possono essere comunicati; il Dossier potrà essere infatti consultato solo da parte dei medici che forniranno nel tempo e a vario titolo assistenza sanitaria al paziente;
- *i diritti dell'interessato:* nell'informativa deve essere indicata la modalità con cui rivolgersi al titolare per l'esercizio dei diritti di cui all'art. 7 del Codice, per revocare il consenso, per esercitare la facoltà di oscurare alcuni eventi clinici e per visionare gli accessi che sono stati effettuati al proprio dossier sanitario.

Sotto questo aspetto assume particolare rilievo anche il diritto riconosciuto all'interessato di poter ottenere l'indicazione della logica applicata a tale trattamento (art. 7, comma 2, lett. c), del Codice), ovvero l'indicazione dei criteri utilizzati nell'elaborazione elettronica dei dati.

A conclusione di questo elenco, va infine sottolineato che, vista la particolare delicatezza dei dati personali trattati mediante il Dossier, è necessario che l'informativa stessa sia facilmente consultabile dall'interessato anche successivamente alla prestazione del consenso[121].

2.2.2 *Il consenso al Dossier sanitario*

In merito al consenso al trattamento dei dati sanitari attraverso il Dossier, sin da subito va chiarito che l'interessato deve essere lasciato libero di scegliere se le informazioni cliniche che lo riguardano (anche informazioni pregresse, pur singolarmente autorizzate) siano trattate o meno con questo strumento, garantendogli così la possibilità che i dati sanitari restino disponibili solo al professionista sanitario che li ha redatti, senza la loro necessaria inclusione in tale sistema.

[121] In tal senso, si riporta come l'Autorità abbia nel tempo apprezzato l'iniziativa di molte strutture sanitarie di pubblicare l'informativa sul proprio sito Internet o di affiggere la stessa nei locali di attesa delle prestazioni sanitarie.

Importante è, altresì, evidenziare che il consenso al Dossier deve essere autonomo e specifico anche se manifestato unitamente a quello previsto per il trattamento dei dati a fini di cura (artt. 23, 76, 81 e 82 del Codice).

Esso può essere acquisito sia in forma scritta sia in forma orale mediante annotazione, anche informatica, della dichiarazione espressa dal paziente al personale sanitario che lo acquisisce e lo certifica nel pieno delle sue funzioni di incaricato di pubblico servizio.

Titolato a esprimere il consenso è il paziente, ovvero, in caso di sua incapacità di agire o incapacità di intendere e volere, chi ne esercita legalmente la potestà o un prossimo congiunto o un familiare o ancora, in loro assenza, il responsabile della struttura presso cui l'interessato dimori.

Un caso particolare di cui tener conto è quello del minore che diventa maggiorenne. Raggiunta la maggiore età, il sistema sarà infatti, per quanto lo riguarda, "congelato" in automatico, e dovrà essere acquisito nuovamente -al primo contatto utile- il consenso dell'interessato.

Dato l'ampio spettro dei soggetti che possono accedere, a diverso titolo (ad es., prestazione specialistica, nuovo ricovero, attività riabilitativa), al Dossier, un profilo centrale segnalato dal Garante è che "*ai fini dell'accesso al dossier da parte del personale sanitario non è necessario che venga acquisito volta per volta il consenso dell'interessato*". Il dossier sarà così accessibile nel tempo da parte di tutti gli operatori sanitari che prenderanno in cura il paziente sulla base del consenso che avrà inizialmente prestato.

Da rilevare la piena facoltà dell'interessato di revocare il consenso al trattamento tramite Dossier (liberamente manifestabile in qualsiasi momento), comportando conseguentemente la chiusura del Dossier che lo riguarda, che non deve essere ulteriormente implementato. Tuttavia, al fine di consentire l'eventuale operatività terapeutica le informazioni sanitarie già in esso presenti al momento della revoca resteranno disponibili al professionista o alla struttura interna al titolare che le ha redatte (ad es., informazioni relative a un ricovero utilizzabili solo dal reparto di degenza) e soggette ad eventuali conservazioni in osservanza di obblighi di legge (art. 22, comma 5, del Codice), ancorché non più condivisibili con i professionisti degli altri reparti che prenderanno in seguito in cura l'interessato.

Riassuntivamente, dalla lettura combinata delle Linee guida sul Dossier e delle norme del Codice da osservare in materia, si evince che il contegno dell'interessato rispetto alla prestazione del consenso potrebbe articolarsi, a titolo esemplificativo, nelle seguenti modalità:

- nego il consenso alla costituzione del Dossier sanitario;

- acconsento alla costituzione del Dossier sanitario;
- acconsento alla costituzione del Dossier sanitario e ad eventuale storico;
- acconsento all'alimentazione nel Dossier sanitario dei "dati a maggior tutela";
- acconsento al trattamento per finalità di ricerca.

2.2.3 *I dati a maggior tutela*

Qualora il titolare del trattamento volesse inserire nel dossier sanitario informazioni in ordine alle quali l'ordinamento nazionale ha posto specifiche tutele di riservatezza, per ragioni di dignità personale, con riferimento a particolari categorie di interessati, deve acquisire una specifica e autonoma manifestazione di volontà, contestuale alla costituzione del Dossier ovvero all'atto dell'esecuzione della prestazione stessa in favore degli interessati che rientranti in dette categorie, i cui dati, per le ragioni anzidette, sono soggetti a maggiore tutela dell'anonimato:

- vittime di atti di violenza sessuale o di pedofilia (L. 15 febbraio 1996, n. 66; L. 3 agosto 1998, n. 269 e L. 6 febbraio 2006, n. 38);
- persone sieropositive (L. 5 giugno 1990, n. 135);
- soggetti che fanno uso di sostanze stupefacenti, di sostanze psicotrope e di alcool (d.p.r. 9 ottobre 1990, n. 309);
- donne che si sottopongono a un intervento di interruzione volontaria della gravidanza o che decidono di partorire in anonimato (L. 22 maggio 1978, n. 194; D.M. 16 luglio 2001, n. 349);
- servizi offerti dai consultori familiari (L. 29 luglio 1975, n. 405).

È convinzione diffusa degli operatori che tale elenco sia destinato ad essere ampliato, dal momento che ci sono oggi pazienti affetti da malattie che hanno una rilevante ricaduta sociale, come ad esempio le malattie mentali, le malformazioni congenite, ecc., i cui dati non hanno certo minore rilevanza di quelli attualmente previsti come oggetto di maggior tutela.

In riferimento ai dati oggetto di maggior tutela va comunicato all'interessato che egli può legittimamente richiedere che tali informazioni siano consultabili solo da parte di alcuni soggetti dallo stesso individuati (ad es., solo dallo specialista presso cui è in cura), fermo restando la possibilità che agli stessi possano sempre accedere i professionisti che li hanno elaborati.

2.2.4 *Diritto all'oscuramento*

Un'importante garanzia a tutela della riservatezza dell'interessato, in merito al trattamento mediante il dossier sanitario, consiste nella possibilità di oscurare alcuni dei documenti sanitari in esso contenuto[122]. Ciò anche nel rispetto della legittima volontà dell'interessato di richiedere una *second opinion*[123] di un altro specialista, senza che quest'ultimo possa essere influenzato da quanto già espresso da un collega.

Tuttavia, anche nel caso in cui l'interessato richieda l'oscuramento delle informazioni e/o dei documenti oggetto del Dossier, questi restano comunque disponibili al professionista sanitario o alla struttura interna e al titolare che li ha raccolti o elaborati (ad es., referto accessibile tramite Dossier da parte del professionista, che lo ha redatto, cartella clinica accessibile da parte del reparto di ricovero).

Per "oscuramento" s'intende, precisamente, quel procedimento che introduce restrizioni all'accesso – con approccio modulare – rendendo non visibili, ai singoli operatori, i dati dall'interessato.

Sin da subito si deve precisare che, quando si parla di oscuramento, non si deve assolutamente cadere nell'errore di ritenere oscurabile un dato all'interno di un documento che lo contiene, in quanto, trattandosi di documentazione sanitaria comparabile ad atto pubblico, l'eliminazione di una sua parte risulterebbe un'alterazione (dando luogo ad un illecito penale), ma si deve ritenere occultabile l'intera documentazione riferita ad un episodio/evento di cura.

L'oscuramento può configurarsi come *volontario*, su richiesta dell'interessato, oppure *per legge*, rientrano in tale circostanza quelle informazioni che per espresse previsioni normative sono oscurate di *default*.

---

[122] Si tratta di un'importante garanzia a tutela della riservatezza dell'interessato già indicata dal Garante nelle Linee guida del 2009, che è stata riproposta dal Legislatore anche con riferimento al FSE (cfr. art. 12, comma 3-bis, D.L. 18 ottobre 2012, n. 179 e art. 9 dello schema di Decreto del Presidente del Consiglio dei ministri in materia di Fascicolo sanitario elettronico; *Cfr*. Linee guida nazionali sul Fascicolo sanitario elettronico adottate dal Ministero della salute l'11 novembre 2010).

[123] Il secondo parere (nel mondo anglosassone: "second opinion") non è un concetto recente, ma proclamato ed invocato fino dagli anni 70 negli ospedali americani, allo scopo di ridurre il costo (assicurativo, privato) della salute dei pazienti, migliorando il target di diagnosi e terapia e, per quanto possibile, i tempi di guarigione. Una ricerca su banche dati mediche ci ha consentito di constatare che second opinion è particolarmente richiesta su casi di diagnostica istopatologica, oltre che su pazienti neurologici e neuroradiologici, oncologici, ginecologici, urologici, gastroenterologici, internistici, maxillo-facciali e odontoiatrici. Per maggiori informazioni sul punto K. Sikora, *Second opinions for patients with cancer*, BMJ 1995, 311: 1179-80; 2. D. Wijers, L. Wieske, M.D. Vergouwen, E. Richard, J. Stam, EM. Smets, *Patient satisfaction in neurological second opinions and tertiary referrals*, J Neurol 2010, 257: 1869-74; E. Zan, D.M. Yousem, M. Carone, J.S. Lewin, *Second-opinion consultations in neuroradiology*, Radiology 2010, 255: 135-41; K. Jones, R.C. Jordan, *Patterns of second-opinion diagnosis in oral and maxillofacial pathology*, Oral Surg Oral Med Oral Pathol Oral Radiol Endod 2010, 109: 865-9; L. Cifaldi, V. Felicetti, G. Cristina, *La richiesta di un secondo parere in oncologia: sfiducia o bisogno?* Med 2010, 101: 299-302.

Come già affermato in precedenza, l'oscuramento introduce regole restrittive di consultazione sui documenti archiviati nel Dossier. Tuttavia, il Garante Privacy ha previsto un'ulteriore garanzia in capo all'interessato: difatti, è previsto che "*l'oscuramento dell'evento clinico (revocabile nel tempo) deve avvenire con modalità tali da garantire che i soggetti abilitati all'accesso non possano venire automaticamente a conoscenza del fatto che l'interessato ha effettuato tale scelta (oscuramento dell'oscuramento)*", rafforzando così il diritto di autoderminazione già ben saldo in capo al paziente.

In questo "obbligo", per gli operatori sanitari, vi è chi individua un'applicazione del generale diritto all'oblio[124]. Ma si deve constatare che lo stesso diritto di oscuramente non detiene assolutamente un legame chiaro con il diritto all'oblio: al contrario, esso è distinto per caratteristiche e applicabilità.

Detto ciò, si deve sottolineare come l'oscuramento sia suscettibile di revoca, a seguito della quale le informazioni "sensibili" già oscurate saranno de-oscurate, fermo restando che nel caso dei dati oscurati «per legge» l'autorizzazione di de-oscuramento dell'interessato indicherà anche quale medico può accedere ai dati (es. autorizza i dati HIV solo per il medico del reparto di Malattie Infettive).

È, inoltre, importante evidenziare che l'esercizio del diritto all'oscuramento potrebbe comportare, per i medici, la disponibilità di informazioni non complete; non aggiornate; non aderenti ad un processo terapeutico già in atto.

In considerazione di ciò, anche se per sua natura il Dossier non certifica lo stato di salute del paziente, in quanto in quanto esso è soltanto un ausilio per il medico in vista della migliore e più celere individuazione del percorso terapeutico da attuare, è indubbia l'utilità di un dossier il più possibile completo, onde per cui è doveroso informare compiutamente l'interessato sulle conseguenze dell'oscuramento.

A causa delle criticità appena descritte il Garante prescrive al titolare del trattamento di informare i soggetti abilitati ad accedere ai Dossier in ordine alla possibilità che gli stessi possono non essere completi in quanto l'interessato potrebbe aver esercitato il diritto di oscuramento.

Infine, per quanto riguarda l'eventuale modalità di gestione del diritto all'oscuramento, il titolare deve mettere a disposizione un apposito modulo per il suo esercizio, che può essere compilato e presentato all'ufficio competente a riceverlo tanto al momento dell'erogazione della prestazione quanto successivamente[125].

---

[124] C. Rabbito, *Sanità elettronica e diritto Problemi e prospettive*, Società Editrice Universo, 2010, p.79.

[125] *Infra, Fac-simile "Modulo richiesta oscuramento*", in Appendice, pp. 218, elaborato durante la ricerca applicata presso la Fondazione G. Monasterio.

2.2.5 *Finalità di ricerca scientifica*

Quando parliamo di finalità di ricerca si devono intendere "*le finalità di studio e ricerca scientifica in campo medico, biomedico ed epidemiologico*".[126]

Infatti, i dati sanitari raccolti attraverso il Dossier sanitario possono essere trattati, al pari di ogni altra informazione clinica, anche per fini di ricerca nel rispetto di quanto previsto dal Codice per tali tipi di trattamenti, ovvero, in via generale, previa acquisizione del consenso informato del paziente (art. 110 del Codice)[127].

Questo consenso è da intendersi come generico ma preventivo, dal momento che per ogni protocollo di ricerca il comitato etico di competenza della struttura che svolge la studio è chiamato ad intervenire giudicando l'appropriatezza delle finalità e dei dati raccolti per la finalità di ricerca, e per ogni protocollo di analisi viene quindi previsto uno specificato consenso da sottoporre al paziente, in sostituzione del consenso generico espresso per il Dossier.

Tuttavia nei casi di ricerche istituzionali (es. quelle promosse dal Ministero) meriterebbe una più attenta analisi la valutazione della validità del solo consenso generico già espresso.

Come esempi di finalità di ricerca si può citare:

- un'organizzazione di sanità pubblica che avanza la richiesta per accedere ai dati dell'EHR in forma anonima per verificare i tassi di mortalità per pazienti/persone che vivono in una data area geografica;
- un organismo di ricerca sanitaria che avanza la richiesta di accedere ai dati dell'EHR in forma anonima per verificare lo stato di salute di tutti le pazienti/persone che hanno subito operazioni a cuore aperto per l'applicazione di dispositivi di valvola cardiaca durante gli ultimi 10 anni;
- il Ministero della Salute che avanza la richiesta di accedere ai dati dell'EHR in forma anonima per identificare tutti gli effetti secondari potenziali di un dato protocollo farmaceutico;

---

[126] *Cfr*. artt. 4, comma 4, lett. c) e 110 del Codice; art. 12, comma 2, lett. b), D.L. 18 ottobre 2012, n. 17 e art. 1, comma 1, lett. e), del citato schema di decreto del Presidente del Consiglio dei ministri in materia di Fascicolo sanitario elettronico

[127] Al riguardo, è necessario che siano ben distinti i trattamenti effettuati a fini di ricerca medica, biomedica ed epidemiologica relativi anche alla sperimentazione clinica (art. 110 del Codice) da quelli effettuati per fini di cura (art. 78, comma 5 del Codice). Ciò, con particolare riferimento alle indicazioni relative alla facoltatività del conferimento dei dati personali a fini di ricerca e a quelle relative alle conseguenze in ordine al mancato conferimento dei dati personali. Sul punto si veda il *Provvedimento del Garante del 22 giugno 2016 nei confronti dell'Azienda Ospedaliera Sant'Andrea di Roma* [doc. web. 5410033].

- un'amministrazione sanitaria provinciale richiama, dall'EHR, una lista di tutti gli uomini sopra 45 anni di età che vivono nella provincia che non hanno avuto un esame della prostata per iniziare una campagna specifica di promozione della salute.

2.2.6 *Profili di accesso e di sicurezza dei dati nel Dossier sanitario*

Uno dei rischi che desta maggiore preoccupazione, per una struttura sanitaria che si appresta a costituire un sistema di Dossier sanitario, è rappresentato dagli accessi compiuti dal personale, sia sanitario che amministrativo, che ha la facoltà di consultare/implementare le informazioni contenute all'interno dello stesso.

Negli ultimi anni, il Garante ha ravvisato non poche violazioni in relazione agli accessi "indiscriminati" a tale strumento. Come già sottolineato, l'accesso al dossier è consentito soltanto alle unità di personale che, operanti all'interno della struttura sanitaria, prendono in cura l'interessato e «*limitatamente al tempo in cui si articola la presa in carico del paziente*».

Si precisa che sono di *default* escluse dall'accesso al Dossier due macro categorie di soggetti: il "*personale medico nell'esercizio di attività medico-legale (ad es., visite per l'accertamento dell'idoneità lavorativa o per il rilascio di certificazioni necessarie al conferimento di permessi o abilitazioni)*", e i "*periti, compagnie di assicurazione, datori di lavoro, associazioni o organizzazioni scientifiche, organismi amministrativi anche operanti in ambito sanitario*".

Le segnalazioni ricevute dal Garante palesano l'impiego, in talune strutture, di sistemi informativi inidonei a garantire il pieno rispetto di tali limitazioni d'uso: si sono difatti ravvisati accessi ai dossier anche da parte di professionisti che, benché operanti all'interno dell'azienda ospedaliera, non avevano alcun contatto con i soggetti interessati. Tali accessi, per lo più giustificati da interessi personali prescindenti dalle finalità di cura a cui il Dossier è preordinato, costituiscono a tutti gli effetti degli accessi abusivi.

A fronte di tale situazione Il Garante si è premurato nelle Linee guida di assicurare idonee garanzie agli interessati, in particolare prescrivendo che:

i titolari del trattamento forniscano all'interessato, che abbia manifestato il proprio consenso al trattamento dei dati personali mediante il dossier sanitario, un riscontro alla richiesta avanzata dallo stesso o da un suo delegato, volta a conoscere gli accessi eseguiti sul proprio dossier con l'indicazione

della struttura/reparto che ha effettuato l'accesso, nonché della data e dell'ora dello stesso[128]

e che i soggetti autorizzati ad accedere al Dossier debbano essere informati di tale diritto esercitabile dagli interessati, così da determinare, auspicabilmente, un effetto sufficientemente dissuasivo rispetto alle pratiche censurate.

In particolare, al fine di garantire che l'accesso al Dossier sia in concreto possibile per i soli operatori autorizzati, il titolare deve adottare le opportune restrizioni sul piano tecnico effettuando una preliminare ricognizione delle ipotesi nelle quali il personale possa avere necessità di consultare il dossier e successivamente, sulla base di questa, individuare i diversi profili di autorizzazione, graduandone il livello di "profondità".

Posta la regola generale dell'accesso finalizzato alle attività di prevenzione, diagnosi, cura e riabilitazione, ciò non implica però che il solo personale medico e paramedico che ha in cura l'interessato possa avere lecito accesso al Dossier; difatti, anche "*il personale amministrativo operante all'interno della struttura sanitaria in cui viene utilizzato il dossier*" può, "*in qualità di incaricato del trattamento*", consultarlo, al solo scopo di ricavarne "*le informazioni indispensabili per assolvere alle funzioni amministrative cui è preposto (ad es., il personale addetto alla prenotazione di esami diagnostici o visite specialistiche può consultare unicamente i soli dati indispensabili per la prenotazione stessa)*".

A titolo esemplificativo, in relazione al contenuto del Dossier, è possibile articolare le visibilità e/o i diritti di scrittura dei singoli profili operatore secondo la griglia che segue.

Ruolo	**Documentazione**
Medici	anagrafica paziente, copia di documenti personali del paziente, consensi informati e dichiarazioni di volontà, dati di accettazione (diagnosi all'ingresso o motivo, provenienza, trasferimenti, ecc), anamnesi, esame obiettivo, diari, pianificazione delle attività, esami di laboratorio (ivi inclusi quelli a c.d. maggior tutela), dati e parametri bioumorali, scale di valutazione, indagini strumentali, visite e consulenze

[128] *Il titolare del trattamento o un suo delegato devono fornire riscontro alla suddetta richiesta dell'interessato entro 15 giorni dal suo ricevimento. Se le operazioni necessarie sono di particolare complessità, ovvero ricorre altro giustificato motivo, il titolare o un suo delegato ne danno comunicazione all'interessato. In tal caso, il termine per l'integrale riscontro è di 30 giorni dal ricevimento della richiesta medesima. Cfr.* "Linee guida in materia di Dossier sanitario".

	specialistiche, prescrizioni e somministrazioni farmaci e terapie, procedure chirurgiche, procedure interventistiche, procedure riabilitative, dieta, dati di dimissione (Scheda MinSal SDO), diagnosi, decorso, terapia alla dimissione, lettera di dimissione.
Infermieri	anagrafica paziente, copia di documenti personali del paziente, consensi informati e dichiarazioni di volontà, dati di accettazione (diagnosi all'ingresso o motivo, provenienza, trasferimenti, ecc), anamnesi, esame obiettivo, diari, pianificazione delle attività, esami di laboratorio (ivi inclusi quelli a c.d. maggior tutela), dati e parametri bioumorali, scale di valutazione, indagini strumentali, visite e consulenze specialistiche, prescrizioni e somministrazioni farmaci e terapie, procedure chirurgiche, procedure interventistiche, procedure riabilitative, dieta, dati di dimissione (Scheda MinSal SDO), diagnosi, decorso, terapia alla dimissione, lettera di dimissione.
Tecnici sanitari	anagrafica paziente, consensi informati e dichiarazioni di volontà, dati di accettazione (diagnosi all'ingresso o motivo, provenienza, trasferimenti, ecc), anamnesi, esame obiettivo, diari, pianificazione delle attività, esami di laboratorio (ivi inclusi quelli a c.d. maggior tutela), dati e parametri bioumorali, scale di valutazione, indagini strumentali, visite e consulenze specialistiche, prescrizioni e somministrazioni farmaci e terapie, procedure chirurgiche, procedure interventistiche, procedure riabilitative, dieta, dati di dimissione (Scheda MinSal SDO), diagnosi, decorso, terapia alla dimissione, lettera di dimissione.
Amministrativi di reparto	anagrafica paziente, copia di documenti personali del paziente, consensi informati e dichiarazioni di volontà, dati di accettazione (diagnosi all'ingresso o motivo, provenienza, trasferimenti, ecc), anamnesi, esame obiettivo, diari, pianificazione delle attività, esami di laboratorio (ivi inclusi quelli a c.d. maggior tutela), dati e parametri bioumorali, scale di valutazione, indagini strumentali, visite e consulenze specialistiche, prescrizioni e somministrazioni farmaci e terapie, procedure chirurgiche, procedure interventistiche, procedure riabilitative, dieta, dati di dimissione (Scheda MinSal SDO), diagnosi, decorso, terapia alla dimissione, lettera di dimissione.
Tecnici informatici	anagrafica paziente, copia di documenti personali del paziente, consensi informati e dichiarazioni di volontà, dati di accettazione (diagnosi all'ingresso o motivo, provenienza, trasferimenti, ecc), anamnesi, esame obiettivo, diari, pianificazione delle attività, esami di laboratorio (ivi inclusi quelli a c.d. maggior tutela), dati e parametri bioumorali, scale di valutazione, indagini strumentali, visite e consulenze specialistiche, prescrizioni e somministrazioni farmaci e terapie, procedure chirurgiche, procedure interventistiche, procedure riabilitative, dieta, dati di

	dimissione (Scheda MinSal SDO), diagnosi, decorso, terapia alla dimissione, lettera di dimissione.

Tabella 3. Ruoli e visibilità dei documenti nel Dossier sanitario

Strettamente connessa alla problematica dei permessi di lettura/scrittura sul Dossier da parte del personale autorizzato è la necessità di stabilire un "periodo di latenza" di accesso alle informazioni.

Tuttavia, nella consapevolezza che non è possibile prevedere in modo rigido ed esaustivo tutta la casistica dei percorsi terapeutici e delle informazioni che potrebbero essere consultate/caricate, è lasciata alle singole aziende sanitarie, motivando ovviamente le scelte compiute, la facoltà di definire preventivamente tempi e modi, da implementare nel Dossier, dei vari accessi da effettuare durante il periodo della presa in carico del paziente.

In tale quadro si rende necessario individuare anche i presupposti in presenza dei quali un medico diverso da quello che ha in carico l'interessato può, mediante accesso, durante un processo di cura già attivo, visualizzare la documentazione sanitaria di tale paziente "non suo". Potrebbero, questi, essere qualificati come "accessi giustificati"[129].

Presupposti legittimanti l'accesso potrebbero essere:

- *l'espletamento di attività di consulenza:* Il medico non ha in carico il paziente ma gli viene chiesta una consulenza da parte di un'altra unità operativa;
- *l'attività legata a prelievi e trapianti:* il medico accede al sistema centralizzato dei donatori per valutare l'eventuale idoneità del paziente per l'espianto e il successivo trapianto;
- *l'attività di prevenzione/diagnosi/cura/riabilitazione:* il medico ha in carico il paziente ma è non registrato nei percorsi informatizzati previsti;
- *la salvaguardia di un terzo o della collettività:* Il medico può utilizzare il Dossier quando si ritiene indispensabile per la tutela di un terzo o della collettività.

Tornando agli accorgimenti di natura organizzativa e tecnica, è opportuno ricordare che le Linee guida del Garante impongono, al titolare del trattamento, l'adozione di idonei sistemi di autenticazione e autorizzazione che, come già ricordato, devono consentire un accesso selettivo al Dossier sanitario fondato sul principio di indispensabilità del dato trattato. È inoltre necessario che vengano individuate apposite procedure per la verifica periodica della qualità e della coerenza delle credenziali di

[129] Concetto espresso, nelle memorie difensive, dalla Dott.ssa Federica Banorri (DPO Azienda Ospedaliera Policlinico S. Orsola Malpighi di Bologna) a seguito del provvedimento sul Dossier sanitario del Garante del 23 ottobre 2014 presso l'Azienda Ospedaliera Policlinico S. Orsola Malpighi di Bologna. Provvedimento visibile sul sito www.gpdp.it [doc. web. n. 3570631] (ultimo accesso giugno 2017).

autenticazione e dei profili di autorizzazione per gli incaricati, come previsto dall'Allegato B del Codice[130].

In secondo luogo, il titolare deve realizzare sistemi di controllo delle operazioni effettuate sul dossier, mediante la previsione di registrazione di file di *log* degli accessi e di tutte le operazioni compiute.

In particolare, i file di *log* che sono conservati per un periodo non inferiore a 24 mesi dalla data di registrazione, onde consentire agli interessati di venire a conoscenza degli eventuali accessi ai propri dati, nonché delle motivazioni che li abbiano giustificati, devono registrare, per ogni operazione di accesso al Dossier, almeno le seguenti informazioni: il codice identificativo del soggetto incaricato che ha posto in essere l'operazione di accesso; la data e l'ora di esecuzione; il codice della postazione di lavoro utilizzata; l'identificativo del paziente il cui dossier è interessato dall'operazione di accesso da parte dell'incaricato e la tipologia dell'operazione compiuta sui dati.

Da ultimo, si devono predisporre sistemi di *audit log*.

Al fine di scongiurare il verificarsi di trattamenti non consentiti o di accessi non autorizzati viene inoltre introdotto l'obbligo, per il titolare, di prevedere specifici "*alert"* di sistema che individuino eventuali comportamenti anomali o "a rischio" relativi alle operazioni eseguite dagli incaricati del trattamento (ad es., relativi al numero degli accessi eseguiti, alla tipologia o all'ambito temporale degli stessi).

Come vedremo nel paragrafo successivo, in caso di violazione dei dati (*data breach*) o di incidenti informatici, che possono esporre a rischi di violazione i dati contenuti nel Dossier, deve essere data immediata comunicazione al Garante.

2.2.6.1 Il Data Breach

Il significato della locuzione "Data Breach" (letteralmente "violazione dei dati") trova pressoché perfetta corrispondenza in quella che il Codice Privacy individua quale:

violazione della sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico (Art. 4, comma 3, lett. g-bis).

---

[130] *Infra, Fac-simile "Scheda Valutazione del rischio nel DS" e "Check-List delle misure di sicurezza nel DS"*, in Appendice, p. 222.

Il nostro ordinamento giuridico in materia di protezione dei dati personali conosce già la *data breach notification* in alcuni ambiti specifici. Infatti, il l'Autorità Garante ha parlato per la prima volta espressamente di "*data breach"* nel 2013, in relazione al settore delle comunicazioni elettroniche[131], poi anche successivamente, in ambito pubblico, con un provvedimento del 2015 stabilì, per le Amministrazioni pubbliche, l'obbligo di comunicare al Garante le violazioni dei dati personali che si verificano nell'ambito delle banche dati (qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti, art. 4, comma 1, lett. p), del Codice), di cui sono titolari[132].

Con riguardo invece al data breach in ambito sanitario il Garante ha introdotto apposite specificazioni con le Linee guida in commento.

In particolare, ai sensi dell'art. 154, comma 1, lett. c), del Codice, il titolare ha l'obbligo di comunicare all'Autorità Garante, entro quarantotto ore dalla conoscenza del fatto, tutte le violazioni dei dati o gli incidenti informatici che possano avere avuto un impatto significativo sui dati personali trattati attraverso il Dossier sanitario.

Tali comunicazioni devono essere redatte secondo lo schema riportato nell'"Allegato B" al provvedimento in analisi, e inviate tramite posta elettronica o posta elettronica certificata alla casella pec dedicata: databreach.dossier@pec.gpdp.it.

Inoltre, in ragione della particolare delicatezza del trattamento dei dati effettuato mediante il Dossier sanitario, è necessario che il titolare individui una procedura per comunicare senza ritardo all'interessato le operazioni di trattamento illecito effettuate dagli incaricati o da chiunque sui dati personali trattati mediante il relativo Dossier. Tale tempestiva informazione, infatti, in termini generali, può consentire all'interessato di minimizzare i rischi connessi alla violazione della disciplina di protezione dei dati personali.

Come si vedrà nel prossimo paragrafo, la recente normativa europea sulla protezione dei dati personali ha apportato novità sullo strumento in parola.

2.3 Il Regolamento europeo: le principali novità in ambito sanitario

A conclusione di questo secondo capitolo, analizzeremo brevemente le principali novità del Regolamento (UE) 2016/679 che costituirà, da qui a poco meno di un anno

---

[131] *"Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (cd. data breach)"*, 4 aprile 2013, in www.gpdp.it [doc. web 2388260] (ultimo accesso giugno 2017).

[132] "*Misure di sicurezza e modalità di scambio dei dati personali tra Amministrazioni pubbliche*", 2 luglio 2015, , in www.gpdp.it [doc. web n. 4129029] (Ultimo accesso giugno 2017).

(25 maggio 2018), la nuova fonte primaria di riferimento in materia di protezione dei dati personali delle persone fisiche[133].

Questo nuovo testo normativo[134] sostituirà nei Paesi UE le attuali discipline nazionali in materia di protezione dei dati già emanate sulla base della precedente Direttiva comunitaria.

Esso introduce regole più chiare e stabilisce criteri più rigorosi con l'obiettivo di assicurare una maggiore garanzia all'interessato rispetto al trattamento dei dati attraverso le nuove tecnologie della società dell'informazione e una migliore armonizzazione e allineamento normativo nel contesto europeo.

In particolare all'art. 1 si definisce l'ambito soggettivo di applicazione del Regolamento dichiarando la sua finalità alla protezione dei diritti e delle libertà fondamentali delle persone fisiche (art. 1, comma 2), escludendo così la tutela per il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto (considerando n. 14).

Ai fini del presente studio, quel che ovviamente più interessa è l'impatto di tale Regolamento nell'ambito sanitario.

Una delle prime e più significative novità è già possibile riscontrarla nelle definizioni di cui all'art. 4, arricchite per quanto concerne: i *dati genetici* che sono "*i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione*"; e *i dati relativi alla salute,* in altri termini, "*i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute*".

Questi ultimi possono senz'altro essere definiti anche, più sinteticamente, quali "dati sanitari". Il Considerando 35 del Regolamento, con riferimento alla nozione di salute, esplicita che essa ricomprende sia quella fisica che quella mentale, passata, presente o futura. Questa tipologia di dati ingloba altresì informazioni sulla persona

---

[133] Per un prima analisi sul Regolamento *Cfr.* F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento Europeo*, Giappichelli, Torino, 2016**;** L. Bolognini, E. Pelino, C. Bistolfi, *ll Regolamento Privacy Europeo*, Giuffrè, 2016; A. Messina, N. Bernardi, *Privacy e Regolamento Europeo*, IPSOA, 2015.

[134] I regolamenti comunitari a differenza delle direttive non necessitano di alcun atto di recepimento o di attuazione. Vengono per questo definiti: "self-executing", sul punto *Cfr.* Corte di Giustizia CE 25 maggio 1993, in causa 193/91; Corte Costituzionale, sentenza 2 febbraio 1990, n. 64; Corte Costituzionale, sentenza 18 aprile 1991, n. 168.

fisica raccolte durante la sua registrazione al fine di ricevere servizi di assistenza sanitaria, quali ad esempio un numero, un simbolo o un elemento specifico attribuitole per identificarla in modo univoco.

Sono inoltre classificabili, sempre ai sensi dello stesso Considerando, quali dati sanitari (a titolo meramente esemplificativo e non tassativo), le informazioni riguardanti «una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro».

2.3.1 *Informativa e Consenso*

Tra le principali novità introdotte dal Regolamento europeo troviamo anche regole più precise in materia di informativa e consenso.

L'informativa, disciplinata agli artt. 13 e 14, diventa sempre più lo strumento cardine capace di assicurare trasparenza riguardo al trattamento dei dati personali e all'esercizio dei diritti.

In particolare, dall'attenta lettura di queste due norme è possibile rilevare tre diverse tipologie di informativa privacy, distinguibili sulla base della modalità di rilascio, fermo restando la loro applicazione a qualsiasi trattamento. Così che avremo:

- *l'informativa standard:* il titolare al trattamento la rilascia in occasione del primo contatto diretto con l'interessato (art. 13);
- *l'informativa posticipata:* il titolare, avendo raccolto i dati presso terzi, successivamente ed "*entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese*" la rilascia all'interessato (art. 14);
- *l'informativa ulteriore:* il titolare, mutando o integrando le finalità del trattamento, provvederà in pieno spirito di trasparenza e in un tempo ragionevole a rilasciarla all'interessato (art. 13 comma 3 e 14 comma 4).

Giova, per mera completezza, riassumere in modo schematico le indicazioni da rendere nell'informativa:

- l'identità del titolare e dell'eventuale rappresentante;
- la finalità del trattamento;
- l'ambito di circolazione e gli eventuali destinatari dei dati;
- la durata del trattamento;
- il processo decisionale utilizzato per il trattamento;
- i diritti dell'interessato;
- (eventualmente) l'origine dei dati se arrivano da terzi.

Da ultimo è interessante precisare che, proprio in un'ottica di praticità e chiarezza dell'informativa, questa potrà recare l'uso di icone, identiche in tutta l'Unione Europea, che siano identificative dell'informazione completa e più estesa che deve essere comunicata all'interessato.

Un esempio ne è ravvisabile in materia di videosorveglianza, in occasione dell'affissione delle "informative brevi" che contengono l'immagine di una videocamera per segnalare la presenza, nelle immediate vicinanze, di un dispositivo ottico di ripresa.

Alla luce di ciò è auspicabile e opportuno che i Titolari del trattamento verifichino la rispondenza delle informative attualmente utilizzate a tutti i criteri sopra delineati, in modo da apportare le modifiche o le integrazioni eventualmente necessarie prima di maggio 2018.

Con riguardo al consenso, al Considerando 32 del Regolamento si dice che esso deve *"essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano"*[135].

Pertanto per essere valido, rispetto all'attuale art. 23 del Codice, esso deve essere:

- libero (senza condizionamenti o vincoli di qualsivoglia natura);
- specifico (che tenga conto delle varie finalità per cui si raccoglie);
- informato (preceduto da un informativa);
- inequivocabile (il titolare deve essere certo di averlo ricevuto);
- espresso (non vale il consenso ex silentio).

Doveroso è precisare che, in caso di dati inerenti lo stato di salute, il Regolamento prevede che il consenso debba essere anche "esplicito". Pertanto è assolutamente vietata, in tale ambito, l'acquisizione del consenso "per fatti concludenti" e naturalmente il consenso potrà essere revocato in qualsiasi momento, fermo restando che i trattamenti già effettuati sulla base di un consenso legittimamente acquisito rimarranno comunque legittimi.

Infine si deve rilevare come, nel contesto del Regolamento europeo, non sia richiesta una forma specifica per il consenso. Infatti, in linea di principio, può considerarsi perfettamente valido (al di fuori dell'ambito poc'anzi richiamato) anche un consenso espresso per fatti concludenti, purché rispetti il requisito dell'inequivocabilità.

Non vanno tuttavia trascurate le possibili implicazioni e criticità sul piano probatorio del consenso acquisito in ambito sanitario: fondare su di esso un trattamento

---

[135] Sul concetto di "Consenso" nel sistema europeo si veda anche quanto contenuto nel Parere del Gruppo articolo 29 *"sulla definizione di consenso"* del 13 luglio 2011 (WP n.187).

di dati sensibili è, pertanto, una scelta che va adeguatamente ponderata, tanto più che l'operatività che si è fino ad oggi consolidata, sulla base dell'ancora vigente Codice privacy, è quella di un'acquisizione del consenso con forma scritta *ad probationem* (art. 23, comma 3) e le procedure di acquisizione in essere sono già allineate a tale "standard". Si ritiene infatti che la "forma scritta" sia una modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati sensibili) che potrebbe essere, altresì, risolta con l'annotazione del consenso in modo informatico attraverso un *flag* sul sistema informativo in uso.

Tuttavia, occorrerà attendere maggiori precisazioni dei regolatori per comprendere come il sistema di acquisizione del consenso tramite comportamenti concludenti potrà legittimamente essere implementato; posto che le finalità per le quali il consenso è richiesto sono le medesime, quale che sia la modalità di acquisizione, sarebbe sorprendente se il consenso ottenuto con tale "nuova" modalità si attestasse su uno standard meno rigoroso di garanzie per l'interessato.

Da ultimo, va sottolineato come il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutte le caratteristiche sopra individuate. In caso contrario, è opportuno adoperarsi per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il regolamento, se si vuole continuare a fare ricorso a tale base giuridica[136].

2.3.2 *I nuovi diritti: diritto all'oblio e alla portabilità dei dati*

Il Regolamento del 2016 pone altresì le basi per l'esercizio di nuovi diritti in ambito privacy, il principale e più innovativo dei quali è sicuramente è il c.d. "Diritto all'oblio"[137], grazie al quale l'interessato potrà ottenere la cancellazione dei propri dati personali e sensibili che lo riguardano e senza ingiustificato ritardo da parte del titolare del trattamento[138].

Si configura così un diritto dell'individuo ad essere dimenticato, o più precisamente, a non essere più ricordato per fatti che lo riguardano.

---

[136] *Cfr. "Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali"* del 28 aprile 2017, http://www.garanteprivacy.it/fondamenti-di-liceita-del-trattamento (ultimo accesso giugno 2017).

[137] F. Pizzetti, (a cura di), *Il caso di Diritto all'oblio*, Giappichelli, 2013.

[138] *Cfr.* V. Mayer-Schonberger, *Delete. Il diritto all'oblio nell'era digitale*, Egea, Milano 2013.

Tuttavia si deve constatare come secondo la dottrina (Pizzetti), in ambito sanitario, il diritto all'oblio, non è da considerarsi un diritto assoluto, ma limitato. Un diritto cedevole che soggiace a libertà e diritti di rango superiore[139].

Nel testo del Regolamento tale diritto è regolato all'art. 17 e, oltre alla richiesta di cancellazione espressa dall'interessato, prescrive anche che:

il titolare del trattamento si deve attivare nel cancellare i dati personali, se sussiste uno dei motivi seguenti:

a) i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b) l'interessato revoca il consenso su cui si basa il trattamento e non sussiste altro motivo legittimo per trattare i dati;

c) l'interessato si oppone al trattamento dei dati personali e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;

d) i dati sono stati trattati illecitamente;

e) i dati devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento;

f) i dati sono stati raccolti relativamente all'offerta di servizi della società dell'informazione.

Tuttavia, si può derogare a questa previsione al ricorrere di una delle seguenti ipotesi[140]:

- *per l'esercizio del diritto alla libertà di espressione e di informazione;*
- *per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;*
- *per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;*
- *a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o*
- *per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.*

---

[139] Pizzetti (a cura di), *il caso del diritto all'oblio*, cit., p. 56.

[140] E' stato infatti sottoposto al Garante il ricorso di una persona che contestava la decisione di Google di non deindicizzare un articolo che riferiva di un'inchiesta giudiziaria in cui risultava implicata, il Garante della Privacy italiano, ha stabilito che gli utenti non possono ottenere dal motore di ricerca la cancellazione dai risultati di ricerca di una notizia che li riguarda se si tratta di un fatto recente e di rilevante interesse pubblico: il diritto all'oblio, infatti, deve essere bilanciato con il diritto di cronaca. Visibile sul sito www.gpdp.it [doc. web n. 3736353] (ultimo accesso giugno 2017).

Accanto al diritto all'oblio, il Regolamento introduce quello alla portabilità dei dati. Tale diritto, previsto all'art. 20, rafforza il controllo dell'interessato sui dati personali che lo riguardano, quando questi sono trattati con mezzi automatizzati.

L'articolo stabilisce, in particolare, che:

l'interessato debba poter ricevere da un titolare del trattamento tutti i dati personali che lo riguardano in un formato strutturato, di uso comune, leggibile da dispositivo automatico e interoperabile tutti i dati personali, in modo da poterli all'occorrenza trasmettere agevolmente ad un altro fornitore di servizi o comunque ad altro titolare del trattamento.

Nonostante ciò resta, però vietato il trasferimento dei dati personali verso Paesi situati fuori dall'Unione Europea e che non rispondono agli standard di adeguatezza in materia di tutela dei dati.

2.3.3 *Privacy by design e Privacy by default*

Previsto all'art. 25 del Regolamento, quello della privacy by design e by default è un principio chiave di tutto il processo di adeguamento e sviluppo dei sistemi informativi rispetto alla normativa privacy. Su di esso si tornerà approfonditamente *infra* (capitolo 3).

2.3.4 *Privacy Impact Assessment (PIA)*

La necessità di assicurare che le operazioni di un trattamento di dati personali siano adeguate e legittime, secondo quanto emerge dall'art. 35 del Regolamento, comporta il dovere, e l'obbligo in alcuni casi, in capo al Titolare del trattamento di effettuare precise e preliminari valutazioni di impatto privacy.

In particolare, l'analisi preliminare dell'impatto privacy (c.d. PIA) consente di valutare in anticipo quale criticità possano sorgere rispetto ad un attività sui dati, prima che questi vengano trattati.

In altri termini, il titolare attraverso questa approfondita analisi potrà identificare misure appropriate per minimizzare i rischi e adottare ogni necessaria misura tecnica, giuridica e organizzativa.

La necessità di una corretta valutazione dell'impatto privacy è ancora più evidente quando il trattamento dei dati avviene attraverso l'uso nuove tecnologie, che evolvono quotidianamente in termini tanto di *hardware* quanto di *software*, basti pensare in sanità

alla proliferazione dei dispositivi indossabili che registrano tutti i parametri vitali dell'interessato.

Come ebbe modo di affermare Rodotà:

è ormai evidente che, insieme a grandissimi vantaggi, le nuove tecnologie, anche per la loro diffusione planetaria, stanno creando rischi di inquinamento dell'ambiente delle libertà civili e politiche. Bisogna passare a tecnologie "pulite", anche attraverso una costante valutazione dell'impatto privacy, soprattutto perché il rischio di inquinamento si è accentuato negli ultimi tempi per effetto delle pressioni determinate dalle esigenze di sicurezza interna e internazionale e delle spinte a subordinare i diritti delle persone ad esigenze di mercato[141].

Da ultimo è doveroso segnalare che Il titolare del trattamento, allorquando svolga una valutazione d'impatto sulla protezione dei dati, debba consultarsi con il responsabile del trattamento e il DPO, figura che vedremo approfonditamente più avanti. In particolare la valutazione deve contenere almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, se del caso, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati;
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

2.3.5 *Principio di accountability*

L'art. 5, comma 2, del Regolamento sancisce il principio di responsabilizzazione (c.d. accountability[142]), sulla base del quale il titolare del trattamento dovrà dimostrare l'adozione di misure tecniche e organizzative adeguate che tengano conto, proattivamente e costantemente, di eventuali rischi che un determinato trattamento di dati può comportare per i diritti e le libertà degli interessati.

Tutto questo deve avvenire a monte, quindi prima di procedere al trattamento dei dati vero e proprio, mediante l'elaborazione di un idoneo sistema documentale di

[141] S. Rodotà, *Libera Circolazione e protezione dei dati personali*, a cura di Rocco Panetta, Tomo I, Milano 2006,

[142] "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ("accountability")", cfr. art. 5 Regolamento (EU) 679/2016.

gestione della privacy, anche attraverso l'elaborazione di specifici modelli organizzativi, analoghi a quelli utilizzati nell'applicazione della disciplina *ex* D. Lgs. n. 231/2001[143].

In particolare, si deve sottolineare come in ambito pubblicistico il concetto di accountability[144] è strettamente collegato a quello di trasparenza inteso come accessibilità alle informazioni senza privativa, allo scopo di favorire forme diffuse di controllo.

2.3.6 *Il Data Protection Officer (DPO)*

Nel regolamento viene introdotta negli articoli da 37 a 39 la figura del Responsabile della protezione dei dati o "Data Protection Officer" (DPO), incaricato di assicurare una gestione corretta dei dati personali nelle imprese e negli enti.
Tale figura sarà obbligatoria per tutte le pubbliche amministrazioni ed enti pubblici, eccetto le autorità giudiziarie, nonché per tutti i soggetti (enti e imprese) che trattano su larga scala dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici, oppure che svolgono attività in cui i trattamenti richiedono il controllo regolare e sistematico degli interessati.

Ai sensi dell'art. 37, i Titolari o il Responsabile del trattamento dovranno quindi designare un soggetto che possieda un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, che sia in grado di adempiere alle proprie funzioni in piena indipendenza e in assenza di conflitti di interesse, operando come dipendente, oppure anche sulla base di un contratto di servizi.

Va sottolineato che per quanto concerne la designazione del DPO, all'interno delle linee guida, recentemente emendate, dal Gruppo di lavoro dei Garanti *ex* art. 29[145], viene specificato che tale figura può essere ricoperta esclusivamente da una persona fisica, supportata, laddove necessario, da un team. In quest'ultimo caso, è essenziale che ogni membro dell'organizzazione esercitante la funzione del DPO soddisfi tutti i relativi

---

[143] Soffientini, (a cura di), *Privacy, Protezione e trattamento dati*, cit., pp. 133 ss.

[144] Termine che potrebbe essere tradotto in *"responsabilizzazione e obbligo di rendicontazione*" e che si compone di tre elementi principali: 1) "trasparenza" intesa come garanzia della completa accessibilità alle informazioni; 2) "responsività" intesa come la capacità di rendere conto di scelte, comportamenti e azioni compiute; 3) "compliance" intesa come la capacità di finalizzare l'azione pubblica rispetto all'obiettivo stabilito dalle norme.

[145] Linee guida sul responsabile della protezione dei dati, del 13 dicembre 2016, pubblicate sul sito del Gruppo di Lavoro Art. 29 e aggiornate il 5 aprile 2017. La traduzione della versione adottata ad aprile 2017 è possibile visualizzarla al seguente link: http://194.242.234.211/documents/10160/0/Linee-guida+sui+responsabili+della+protezione+dei+dati+%28RPD%29+-+WP+243.pdf (ultimo accesso giugno 2017)

requisiti della Sezione 4 del Regolamento (es. è essenziale che nessuno si trovi in conflitto di interesse).

Tra le sue attività, il DPO ha il compito di informare e consigliare il titolare o il responsabile del trattamento da lui preposto, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento Europeo e dalle altre disposizioni dell'UE o delle normative locali degli Stati membri relative alla protezione dei dati. Dovrà poi verificare che la normativa vigente e le policy interne del titolare siano correttamente attuate ed applicate, incluse le attribuzioni delle responsabilità, la sensibilizzazione e la formazione del personale, ed i relativi audit. Su richiesta, dovrà fornire pareri in merito alla valutazione d'impatto sulla protezione dei dati, potendo manifestare la propria opinione, anche e soprattutto qualora dissenziente, agli alti vertici della società, sorvegliandone poi i relativi adempimenti.

2.3.7 *Data Breach*

Nel richiamare quanto già in precedenza esposto a riguardo, è opportuno ora rilevare in quali punti il Regolamento innova la disciplina sul *data breach*.

La ratio della disciplina si evince già dal considerando 85 che prevede che la violazione dei dati personali vada affrontata e gestita con tempestività al fine di evitare l'insorgenza o l'aggravamento di danni materiali o immateriali alle persone fisiche: perdita del controllo dei dati personali o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

È prevista altresì l'attivazione di un flusso di comunicazione in due direzioni: verso il Garante Privacy e, nei casi più gravi, anche verso l'interessato.

Secondo quanto disposto dall'art. 33 del Regolamento, la comunicazione al Garante deve essere fatta entro 72 ore dal momento in cui si è avuta conoscenza della violazione. Tuttavia, qualora la notifica non sia effettuata entro il termine previsto, deve essere fatta entro un congruo termine e va corredata dei motivi del ritardo. Questo aspetto rappresenta una novità rispetto al passato: infatti, nel contesto normativo italiano erano finora previste delle differenziazioni di tempo rispetto all'ambito di riferimento: 24 ore per i titolari operanti nel settore delle telecomunicazioni, 48 ore per i titolari operanti nel settore sanitario.

Specificatamente la notifica deve:

- *descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;*
- *comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;*
- *descrivere le probabili conseguenze della violazione dei dati personali;*
- *descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.*

Come anticipato, il titolare del trattamento deve attivarsi e informare anche della violazione dei dati personali, senza indebito ritardo, anche l'interessato, non però in ogni caso ma allorquando sussista, *ex* art. 34 del Regolamento, un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie.

2.4 Breve riflessione e prime conclusioni

Al termine di questa analisi, svolta per approfondire lo stretto legame che intercorre tra l'innovazione e il diritto alla privacy in ambito sanitario, non si può far a meno di notare che la protezione dei dati in un contesto fragile ed intimo come la tutela della salute ricopre notevole importanza. Così che si deve ritenere verificata la condizione secondo cui non può esistere diritto alla salute senza diritto alla privacy come non esiste diritto alla privacy in sanità senza diritto alla salute.

Questi diritti, costituzionalmente garantiti, presentano una forte interdipendenza, e si spera che la loro grande carica innovativa trovi nel Regolamento europeo una cornice adeguata ad accompagnarne le evoluzioni verso un prossimo futuro in cui la privacy non sia più vista come un inutile "appesantimento burocratico" ma rappresenti, piuttosto, un imprescindibile supporto per l'adeguato esercizio del diritto di autodeterminazione del paziente; sarà così possibile addivenire alla realizzazione di percorsi terapeutici attenti non solo all'aderenza medica, ma anche alla dignità personale del paziente stesso[146].

[146] Con il Provvedimento 9 novembre 2005, il Garante è tornato sul tema della dignità del paziente, affermando che al cittadino, che entra in contatto con le strutture sanitarie per diagnosi, cure, prestazioni mediche, operazioni amministrative, deve essere garantita la più assoluta riservatezza e il più ampio rispetto dei diritti fondamentali e della dignità. Visibile sul sito www.gpdp.it [doc web n. 1191411] (ultimo accesso giugno 2017).

CAPITOLO III

La Privacy by Design

"Qualsiasi innovazione tecnologica può essere pericolosa: il fuoco lo è stato fin dal principio, e il linguaggio ancor di più; si può dire che entrambi siano ancora pericolosi al giorno d'oggi, ma nessun uomo potrebbe dirsi tale senza il fuoco e senza la parola".

Isaac Asimov [147]

L'avvento delle nuove tecnologie ha senza dubbio migliorato accessibilità e fruibilità dei dati e delle informazioni personali, che rappresentano oggi una fonte inesauribile di sempre nuove applicazioni, nell'ambito del "mercato economico della conoscenza".

Nondimeno, se lo sviluppo dei sistemi informatici di archiviazione e di organizzazione dei dati ha, da un lato, favorito l'attività lavorativa di professionisti e imprese, dall'altro ha però generato nuovi pericoli in materia di affidabilità e sicurezza, determinando il sorgere in capo agli operatori di più stringenti obblighi di custodia, imposti tanto dalla normativa in materia di protezione dei dati personali quanto dagli standard internazionali per la sicurezza informatica[148].

Infatti, tutte le norme e gli standard ad oggi emanati, vincolanti e non, sono accomunati dal loro convergere verso la necessità di garantire, mediante la predisposizione e l'attuazione di misure di sicurezza idonee, la tutela dei dati e delle informazioni che riguardano l'utente.

Già a metà degli anni '90, a seguito di uno studio svolto dalla Dutch Registratierkamer (ora "College Bescherming Persoonsgegevens")[149] in collaborazione

---

[147] I. Asimov, *I robot dell'alba*, Arnoldo Mondadori Editore, 1985, p. 286.

[148] Gli standard per la sicurezza informatica nel dettaglio rappresentano tutte le tecniche e le modalità operative che le aziende dovrebbero seguire per mettere in sicurezza i propri dati. Un esempio è la normativa ISO 27001:2005 che ha introdotto standard e protocolli al fine di protegge i dati e le informazioni da minacce assicurandone l'integrità e la sola disponibilità agli utenti "addetti". http://www.iso.org/iso/home.htm (ultimo accesso giugno 2017).

[149] Autorità per la Protezione dei Dati olandese che consiglia il Governo e si occupa dei ricorsi, delle investigazioni sul rispetto della privacy e dispensa raccomandazioni applicando la Wet Bescherming Persoonsgegevens normativa olandese di riferimento.

con l'Information and Privacy Commissioner of Ontario[150], fu redatto un documento dal titolo "*Privacy Enhancing Technologies: the path to anonymity"*[151] in cui comparve per la prima volta l'espressione *Privacy Enhancing Technologies*[152] *(PET)* per indicare l'insieme di tutti gli strumenti, non particolarmente invasivi, che in ambito ICT sono utili per modellare i sistemi informativi al fine di accrescere la protezione e la sicurezza dei dati personali.

In particolare i principi chiave su cui si basano le PET sono essenzialmente: a) la minimizzazione della raccolta, dell'utilizzo, della divulgazione e della conservazione dei dati identificativi degli utenti; b) la partecipazione e il coinvolgimento attivo degli utenti, tra l'altro, permettendo l'esercizio di poteri di controllo durante il ciclo di vita dei dati personali trattati; c) la maggiore sicurezza delle informazioni sensibili, sia sotto il profilo del diritto alla riservatezza sia sotto il profilo dell'integrità dei dati, ottenuta attraverso tecniche di anonimizzazione e di de-identificazione delle informazioni sensibili nel rispetto dello standard ISO/IEC 15408:1999, dedicato alla definizione dei *"Common Criteria"* per la valutazione della sicurezza dei sistemi informativi.

Appare chiaro che il ruolo delle PET è complementare alle norme in materia di protezione e sicurezza dei dati personali ed altresì lascia la modellazione dei sistemi alla capacità dei tecnici che sono chiamati a tener conto delle infinite variabili legate all'interesse soggettivo dell'utente e all'ambiente di progettazione.

Il valore assunto dalle PET ha fatto si che, successivamente, tale concetto si è evoluto in *"PETs Plus"*[153], la cui novità principale è la realizzazione e la valorizzazione di modelli inclusivi, in cui la tutela dei dati personali e gli interessi economici non siano antitetici, agevolando così la fiducia degli utenti nell'adozione di strumenti informatici.

Rilevante è, a questo punto, notare come un'ulteriore tassello nella evoluzione dell'uso delle PET sia la teorizzazione nel 2009, ad opera di Ann Cavoukian[154], della *Privacy by Design.*

---

[150] Organismo indipendente istituito nel 1987 che sostiene e promuove il tema della protezione dei dati personali in Ontario (Canada).

[151] Il documento riporta un'attenta analisi su come le nuove tecnologia possano essere utilizzate per contenere gli abusi sui dati e informazioni personali degli utenti.

[152] Per approfondimento si veda Information and Privacy Commissioner of Ontario, Dutch Registratierkamer, *Privacy Enhancing Technologies - The Path to Anonymity, Registratiekamer*, The Netherlands, Voll. I-II, 1995; D. Martin, A. Serjantov (edited by), *Privacy Enhancing Technologies, Proceeding of 4° international workshop, PET 2004*, Toronto, May 2004, Berlin.

[153] *Cfr*. A. Cavoukian, *Moving Forward From PETs to PETs Plus: The Time for Change is Now*, Toronto, 2009, p. 4.

[154] Promotrice del concetto della *Privacy by design* è stata dal 1997 al 2014 membro dell'Information and Privacy Commissioner of Ontario. Attualmente ricopre l'incarico di Executive Director of the Privacy and Big Data Institute at Ryerson University.

Riconosciuta formalmente come *global privacy standard* durante la *32nd International Conference of Data Protection and Privacy Commissioners*[155] svolta nel 2010 a Gerusalemme, la *Privacy by design* rappresenta attraverso l'attuazione dei suoi sette principi fondanti un approccio innovativo che garantisce il rispetto della disciplina della protezione dei dati personali. Infatti, attraverso la sua applicazione, che tiene conto fin dal momento della progettazione di tutte le misure tecniche e organizzative adeguate, è possibile salvaguardare *a priori* i dati degli utenti, senza, dunque, la necessità di successivi interventi attivi da parte degli interessati. Va così sottolineato che, in tale prospettiva, l'approccio alla protezione dei dati personali non può essere basato solo su una mera valutazione di conformità normativa, ma presuppone che l'utente diventi il punto di partenza per sviluppare il progetto, realizzando così un approccio *user-centric*[156].

Da ultimo, va preso atto che in ambito europeo l'elaborazione concettuale della *Privacy by design* ha trovato una codificazione – dopo un laborioso iter legislativo iniziato il 25 gennaio del 2012[157] – nell'art. 25[158] del Regolamento EU n. 679/2016, rubricato *Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita*[159], anche se, si deve rilevare come questo articolo pur avendo una carica cogente ed innovativa rispetto al passato richiama in gran parte l'essenza intrinseca del principio di necessità nel trattamento dei dati, già contenuto nell'art. 3 del Codice Privacy ed ampiamente descritto nei provvedimenti del Garante, e che dispone:

---

[155] *Cfr*. 32ND International Conference of Data Protection and Privacy Commissioners, *Resolution on Privacy by Design, Jerusalem - Israel*, 27-29 October 2010.

[156] Filosofia di progettazione nel quale si prendono in considerazione i bisogni dell'utente in ogni passo del processo di progettazione al fine di massimizzare l'usabilità del prodotto stesso.

[157] La riforma della legislazione europea sulla protezione dei dati personali che intende rafforzare oltre al il principio della *privacy by design and by default*, a titolo esemplificativo, il diritto all'oblio, il diritto ad una più facile trasferibilità dei dati tra *service provider*, il principio di accountability, il concetto di *Data breach. Cfr*. COM(2012)11 def. del 25 gennaio 2012, Proposta di regolamento del Parlamento Europeo e del Consiglio concernente la tutela del le persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati.

[158] Al fine di chiarire questi i concetti espressi nell'articolo 25 occorre guardare il Considerando 78 del Regolamento in cui si legge *"La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. […] In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati"*.

[159] Nella versione ufficiale in lingua inglese i concetti della "*privacy by design and by default*" nell'art. 25 del Regolamento (UE) 2016/679 sono stati codificati come "*data protection by design and by default*".

i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Un precetto questo che, anticipando di qualche anno la formalizzazione del più ampio concetto della *Privacy by design,* comporta un'importante conseguenza nell'ambito dei trattamenti di dati svolti con sistemi automatizzati. Infatti, secondo il principio di necessità i sistemi informativi e i programmi informatici devono essere configurati in modo da gestire i dati in modalità de-identificata – ad esempio attraverso l'impiego di un codice alfanumerico – così da non consentire l'identificazione diretta dell'interessato.

Per concludere, ritornando alle peculiarità della *Privacy by design,* particolarmente interessante ai fine della presente ricerca è notare, come si vedrà in dettaglio *infra*, come tale concetto sia di ampio utilizzo anche all'ambito della sanità digitale, con la peculiarità che il suo dispiegarsi in tale settore non è rilegato al solo aspetto tecnologico di progettazione e sviluppo dei sistemi informativi, ma interessa anche la fase di realizzazione e adeguamento dei locali delle strutture: si pensi, ad esempio, alle sale server o agli uffici ove si rischia, con accessi non autorizzati, l'illecita divulgazione dei dati sensibili degli interessati.

3.1 Privacy by design: "The 7 foundational principles"

Privacy by Design refers to the philosophy and approach of embedding privacy into the design specifications of various technologies. This may be achieved by building the principles of Fair Information Practices [come "1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" e "*Global Privacy Standard Privacy Principles" del 2006] into the design, operation and management of information processing technologies and systems*.[160]

Ciò che contraddistingue il concetto della *Privacy by design* sono senza dubbio i sette principi[161] cardine teorizzati dalla Cavoukian (v. figura 1), che per le caratteristiche della loro stessa formulazione sono idonei a trovare piena esplicazione nei seguenti

[160] A. Cavoukian, *Privacy by Design:Take the Challenge*, Information and Privacy Commissioner of Ontario, 2009, p. 361.

[161] A. Cavoukian, *Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices*, Toronto, 2010, p. 12.

ambiti: “1) sistemi IT; 2) implementazione di pratiche commerciali; 3) progettazione strutturale e infrastrutture di rete”.

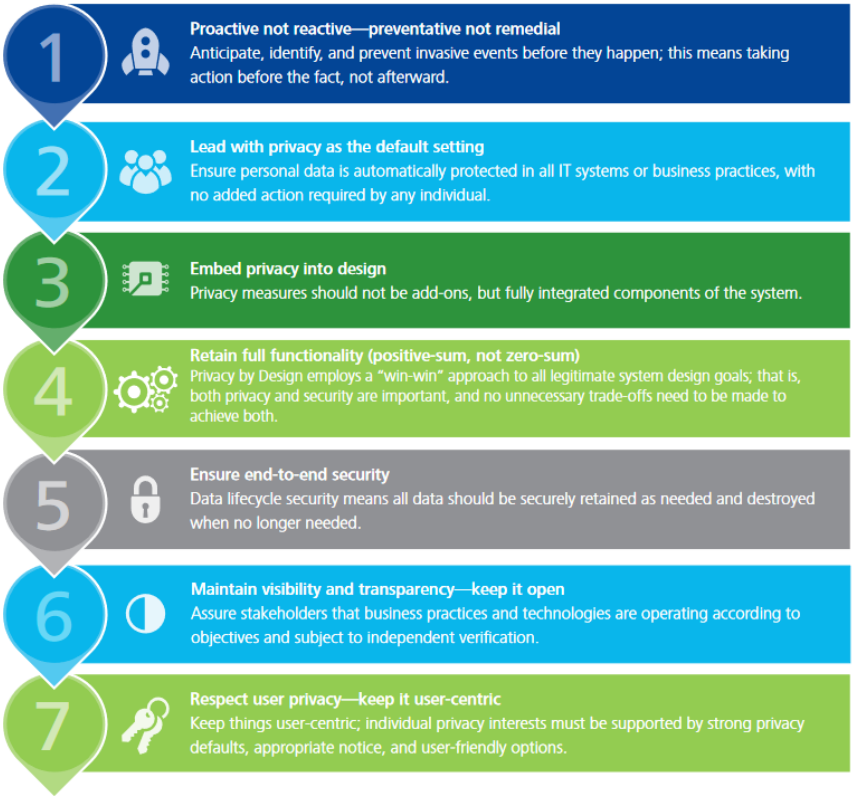


Figura 4. I 7 principi fondanti della Privacy by design[162]

Prima di soffermarci ad analizzarli singolarmente, si deve preliminarmente rilevare come essi possano essere applicati a tutte le tipologie di dati e di informazioni personali, ma sicuramente devono essere utilizzati con particolare vigore per la protezione e sicurezza dei dati sensibili - in particolar modo per i dati sanitari - al fine di poter fronteggiare con maggior efficacia il rischio che le informazioni riferite o riferibili agli interessati vengano accidentalmente rese di pubblico dominio.

Un’ulteriore caratteristica che necessita di menzione è la mancanza di limiti per la loro applicazione: infatti, la *Privacy by design* non ha un'applicabilità limitata soltanto a progetti da costruire *ex novo*, poiché può essere utilizzata anche per progetti già esistenti che, attraverso una preliminare fase di reingegnerizzazione, possono beneficiare di questo approccio senza arrecare alcun pregiudizio a quanto è stato già realizzato.

[162] Fonte: https://www2.deloitte.com/ca/en/pages/risk/articles/Privacybydesign.html.

3.1.1 Proattivo non reattivo – prevenire non correggere

Il primo principio della *Privacy by design* è caratterizzato da azioni con un approccio di tipo proattivo piuttosto che reattivo. Infatti è molto più utile prevenire ed affrontare le criticità prima che si trasformino in un danno reale e attivo. Così che la tempestività nell'agire, prima ancora che il problema possa sorgere, rappresenta un valore aggiunto nella progettazione e caratterizza questo principio favorendo la protezione delle informazioni.

Tuttavia è rilevante sottolineare che quanto detto è valido solo se esiste un monitoraggio costante del progetto e la volontà di definire elevati standard di protezione e sicurezza dei dati.

In ambito sanitario è facile ritenere che questo principio risulti cruciale: la prevenzione e l'anticipazione di possibili violazioni dei dati sanitari permettono di raggiungere una percezione di alta affidabilità delle strutture sanitarie presso i pazienti, oltre a ridurre/eliminare interventi architetturali successivi, con il risparmio così anche di ulteriori costi per un eventuale ripristino.

3.1.2 Privacy come impostazione di default

La *Privacy by Design* attraverso l'impostazione di default di un sistema IT cerca di realizzare il più elevato livello di protezione i dati personali. Sulla base di questo principio l'utente potrà contare sull'impostazione incorporata nel sistema per mantenere il proprio grado di riservatezza senza dover compiere alcuna azione. Per l'utente è un principio importante, essendo lui stesso il primo attore nella gestione delle proprie informazioni.

I concetti su cui si basa la *Privacy by Default* sono "*privacy-protective*" e "*data minimization*"[163]. Il primo concetto riguarda la visione secondo cui la progettazione di un sistema IT tiene conto di uno specifico e efficace scopo che legittima la raccolta dei dati. Il secondo impone il trattamento dei dati solo nei casi strettamente necessari.

Si incoraggia così la realizzazione di un vero e proprio meccanismo di prevenzione che in ambito sanitario potrebbe essere attuato ad esempio con l'utilizzo di

[163] Principio che deriva dall'articolo 6 comma 1, lettera b) e c) della direttiva 95/46/CE e dall'articolo 4 comma 1, lettera b) e c) del Regolamento CE n. 45 del 2001 e prevede che i dati personali devono essere "raccolti per finalità determinate, esplicite e legittime" e devono essere "adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e / o successivamente trattati".

pseudonimi per identificare e/o de-identificare i pazienti oppure prevedere l'oscuramento automatico dei referti caricati nei sistemi informativi aziendali.

3.1.3 Privacy incorporata nella progettazione

Tale principio sostiene l'importanza di considerare la protezione dei dati e la sua gestione una componente essenziale nella progettazione di un sistema, senza diminuire la funzionalità di quest'ultimo.

Per poter attuare in pieno questo principio è necessario il continuo aggiornamento delle buone prassi implementative, degli standard e degli atti normativi - come leggi e regolamenti - tenendo conto del progresso tecnologico.

In sanità questo è realizzabile attraverso l'aggiornamento degli standard e delle Linee guida che sono d'indirizzo per lo sviluppo e implementazione dei sistemi IT.

3.1.4 Massima funzionalità − Valore positivo, non valore zero

La *Privacy by design* attraverso l'elaborazione di questo principio punta ad una visione che mira a conciliare tutti gli interessi e gli obiettivi posti durante lo sviluppo di un sistema IT attraverso un valore positivo, non un valore zero.

In altri termini quello a cui si vuole giungere è la dimostrazione di poter fare coesistere la privacy e la sicurezza senza dover forzosamente scegliere di tutelare un aspetto tralasciando un altro.

Un punto di svolta nell'applicazione di questo principio è la creazione di sistemi non invasivi che mantengono solo le informazioni strettamente necessarie.

3.1.5 Sicurezza fino alla fine − Piena protezione del ciclo vitale

La sicurezza è un concetto chiave e senza di essa non sarebbe possibile attribuire nessuna responsabilità e nessun diritto. Infatti, solamente con l'applicazione degli elementi legati alla sicurezza, la *Privacy by design* assicura fino alla fine l'intero ciclo vitale delle informazioni.

Alla luce di quanto appena detto, il ruolo più delicato è ricoperto dagli sviluppatori e progettisti, il cui compito è quello di applicare le metodologie di sicurezza al fine di eliminare, o quanto meno ridurre, non solo il rischio di furto ma anche la cancellazione completa o parziale dei dati.

3.1.6 Visibilità e trasparenza − Mantenere la trasparenza

La *Privacy by design* cerca di assicurare trasparenza a tutti i soggetti interessati.

Il principio della trasparenza impone che le informazioni destinate al pubblico o all'interessato siano: concise; facilmente accessibili e di facile comprensione e che sia usato un linguaggio semplice e chiaro.

Questo principio rappresenta una caratteristica rilevante e che da vita al concetto dell'*accountability*. In altri termini si chiede al titolare del trattamento di dimostrare, che il trattamento sia stato effettuato conformemente alle norme in materia di protezione dei dati personali. Sono di aiuto a dimostrare tale conformità l'adesione ai codici di condotta o a meccanismi di certificazione.

3.1.7 Rispetto per la privacy dell'utente − Centralità dell'utente

Prima di ogni cosa, la *Privacy by design* richiede ai progettisti e sviluppatori di considerare prioritarie le richieste e gli interessi degli utenti.

Così che il concetto di "centralità dell'utente" assume due diversi significati: il primo, che lo declina come il diritto dell'utente di esercitare il controllo sulle proprie informazioni; il secondo, che lo attua in termini di fattore che forgia un sistema intorno alla figura dell'utente, e quindi intorno alle sue esigenze.

Ne consegue che, se gli utenti devono aver modo di gestire le informazioni che li riguardano in maniera facile e veloce, il sistema dovrà permettere questo risultato.

In ambito sanitario è ormai un dato consolidato quello per cui, attraverso il conferimento del consenso (ai trattamenti medici), il paziente possa pressoché totalmente autodeterminarsi nelle scelte ed essere il fulcro della prestazione sanitaria erogata; in ambito di consenso al trattamento dei dati, dovrebbe operare, a ben vedere, il medesimo approccio.

3.2 Dossier sanitario: un approccio alla *Privacy by design*

L'analisi condotta sino a questo momento ci permette di poter addivenire ad alcune prime riflessioni che riguardano il rapporto tra protezione dei dati sanitari, sicurezza dei sistemi IT, autodeterminazione dei pazienti e Dossier sanitario.

Molteplici risultano gli aspetti di cui bisogna tener conto in fase di sviluppo di un sistema informativo quale è il Dossier sanitario: basti pensare ai bisogni dei pazienti,

agli interessi degli operatori sanitari, alle varie posizioni giuridiche in gioco che spesso finiscono per risultare tra loro confliggenti.

Osservando quanto detto nel paragrafo precedente, si può ritenere che un bilanciamento tra questi aspetti possa essere raggiunto proprio attraverso l'applicazione della *Privacy by design*, efficace strumento di contemperamento delle esigenze di tutti i soggetti coinvolti nell'erogazione delle prestazioni sanitarie e in grado di recare loro indubbi vantaggi, a fronte di pregiudizi sostanzialmente nulli.

Per pervenire ad un simile risultato è però necessario, come auspicato nei principi a fondamento della *Privacy by design*, un quadro giuridico e tecnologico condiviso a livello comunitario, al fine di armonizzare la frammentarietà e di ovviare alle lacune legislative che attualmente esistono, in materia di privacy applicata all'ambito sanitario, nei singoli Paesi europei.

Nello specifico, parlando di Dossier sanitario si deve segnalare come il nostro ordinamento non abbia una disciplina normativa cogente di rifermento e come l'unico testo esistente che provi a dare le linee d'indirizzo sia costituito dalle "Linee guida in materia di Dossier sanitario"[164] del 4 giugno 2015, emanate dal Garante per la protezione dei dati personali.

E' però interessante notare che, sia pur con lo stile "discorsivo" che le caratterizza, le Linee guida sul Dossier sanitario tengono conto delle criticità connesse alla sicurezza e alla protezione dei dati sanitari, dettando, con maglie sufficientemente larghe, delle vere e proprie prescrizioni, laddove statuiscono che:

affinché i dossier sanitari in uso presso le strutture sanitarie siano effettivamente degli strumenti di ausilio nei processi di diagnosi e cura dei pazienti è necessario che gli stessi siano realizzati con modalità tali da garantire in primo luogo la certezza dell'origine e della correttezza dei dati e l'accessibilità degli stessi solo da parte di soggetti legittimati.

Questo apre effettivamente ad uno scenario che vede, come *best practices* operativa auspicabile per lo sviluppo di un Dossier sanitario, l'applicazione della *Privacy by design*, e pone una sfida che è, come affermato dalla stessa Autorità Garante, riservata a tutti gli attori istituzionali a cui è chiesto di garantire il buon funzionamento dei sistemi informativi sanitari, sia in termini di efficacia che di efficienza ed equità nel rispetto dei diritti fondamentali dei pazienti.

[164] Gazzetta Ufficiale n. 164 del 17 luglio 2015, [Doc. web n. 4084632].

Soffermandoci sulle Linee guida[165], si deve constatare come esse diano un espresso rilievo al ruolo del paziente per la creazione e alimentazione dei documenti all'interno del Dossier sanitario, prevedendo il diritto di autodeterminazione in ordine alla visibilità dei dati e delle informazioni archiviate, nonché il diritto alla visione dei log di accesso al dossier.

Tuttavia, la particolare delicatezza dei dati sensibili trattati mediante il Dossier sanitario impone la doverosa adozione di specifici accorgimenti tecnici – che tengano conto dell'evoluzione tecnologica – da utilizzare nel *design* del *dossier* al fine di scongiurare l'accesso abusivo, il furto, lo smarrimento parziale o integrale e di garantire la certezza dell'origine del dato, la sua esattezza, integrità e immodificabilità.

Più specificamente, con l'adozione di tali accorgimenti viene richiesto, al titolare del trattamento, di mettere in atto procedure tecniche e organizzative tali da rendere il sistema conforme sia al Regolamento UE di recente approvazione, sia alle Linee guida e ai provvedimenti emanati del Garante Privacy al fine di assicurare la tutela dei diritti dell'interessato.

Tenuto conto del principio di autodeterminazione dell'interessato, il titolare del trattamento garantisce che siano così trattati, di default, solo i dati personali e sensibili necessari e legati alle specifiche finalità di prevenzione, diagnosi, cura e riabilitazione dell'interessato.

L'analisi condotta sino ad ora consente di rilevare che un ruolo fondamentale, nella fase di progettazione e sviluppo, spetta ai produttori dei sistemi IT, in capo ai quali sorge l'obbligo di sviluppare *software* nei quali la privacy e la sicurezza, elevati al rango di componente essenziali degli stessi, ne siano elementi chiave e integrati, senza che questo ne comporti una diminuzione di funzionalità.

Avviandoci alla conclusione, pare opportuno richiamare la considerazione elaborata in dottrina, secondo cui «*progettare sistemi informativi in un'ottica di "privacy by design" "significa,* (…) *primariamente, permettere all'utente, principale beneficiario delle misure considerate, di essere centro dei flussi di dati*»[166].

Per valutare appieno la portata di questa riflessione, dobbiamo rilevare innanzitutto che nell'ambito sanitario, oggetto del nostro studio, si ritiene che affrontare le problematiche connesse alla protezione dei dati attraverso l'adozione di una politica *"by design and by default"* rappresenti le basi per la creazione di nuove infrastrutture

---

[165] Si rinvia *supra*, cap. II.

[166] R. Brighi; M.G. Virone, *Una tutela "by design" del diritto alla salute. Prospettive di armonizzazione giuridica e tecnologica*, in: *A Matter of Design: Making Society trough Science and Technology*, Milano, Open Access Digital Publication by STS Italia Publishing, 2014, p. 1218.

per la gestione della salute, consentendo così di raggiungere il giusto bilanciamento tra esigenze di cura, tutela di diritti fondamentali del paziente e interessi di salute pubblica.

In questo contesto non è secondario il tema dell'educazione degli utenti – c.d. Privacy by education[167] – sull'impiego delle nuove tecnologie e i rischi privacy. Un utente informato e formato è infatti più propositivo e ben disposto ad utilizzare le nuove infrastrutture e servizi che sempre più quotidianamente si stanno facendo largo tra le corsie delle strutture sanitarie. La centralità del paziente nei sistemi informativi digitali sanitari presuppone in altri termini, per essere davvero compiuta, che l'elevato grado di sicurezza e di garanzia della privacy generi fiducia, e che tale fiducia sia poi il motore che consenta il pieno utilizzo e l'ulteriore sviluppo dei servizi che la sanità digitale può mettere a disposizione del paziente, in un circolo "virtuoso". Essere centro dei flussi di dati significa allora, in quest'ottica, esserne al centro in qualità di soggetto attivo tanto rispetto alla possibilità di azione sui dati stessi e sul loro utilizzo, quanto rispetto alla fruizione dei servizi che grazie a quei dati possono essere erogati.

3.2.1 Analisi e progettazione nella visione Privacy by design

Alla luce di quanto detto sino a questo momento è evidente che le fasi di analisi e di progettazione di un Dossier sanitario devono obbligatoriamente tenere conto di una visione *Privacy by design*.

Particolarmente significativo è in tal senso lo sviluppo del Dossier sanitario – oggetto del nostro studio – che si sta concretizzando presso la Fondazione G. Monasterio[168], nel quale, utilizzando sin dal primo momento una visione *Privacy by design,* si sono potuti costruire degli scenari operativi per il funzionamento del nuovo sistema.

In questo senso va detto che il modello di Dossier è stato concepito seguendo un approccio proattivo e preventivo, in grado quindi di anticipare eventuali rischi al fine di preservare i dati personali e sensibili lungo l'intero ciclo vitale del dato stesso[169]. Tale obiettivo è stato possibile grazie all'implementazione di strumenti di autenticazione e di autorizzazione. Infatti, attraverso il tracciamento, il monitoraggio e la conservazione dei *log* di accesso sul Dossier, è possibile in piena trasparenza tutelare gli interessi del

---

[167] L. Jingquan, *Privacy policies for health social networking sites*, J Am Med Inform Assoc., 2013.

[168] La metodologia, gli obiettivi e le fasi di sviluppo del Dossier sanitario, progettato presso la Fondazione G. Monasterio ed oggetto del Tirocinio di 18 mesi, troveranno maggior definizione nel capitolo IV.

[169] Si rinvia *supra,* par. 3.1.5.

paziente che potrà visualizzare, anche in autonomia, chi abbia avuto accesso alle sue informazioni e in quale momento specifico.

Inoltre, con riguardo alla figura del paziente si deve segnalare come questa nella creazione, e successiva alimentazione, del modello di Dossier in analisi assume un ruolo centrale. Infatti, proprio nel rispetto da quanto teorizzato dalla *Privacy by design,* il paziente non trae, come utente, solo benefici dal suo utilizzo, ma insieme al personale sanitario ha un ruolo di vero e proprio artefice di tutte le attività che avvengono sul Dossier e attraverso il Dossier.

A tal proposito, è rilevante sottolineare come il ruolo attivo e centrale del paziente, più volte ricordato, trova la sua primissima applicazione proprio nella scelta, attraverso il rilascio – o la revoca – del consenso, di creazione del Dossier presso la struttura sanitaria che lo accoglie al fine di prestargli le cure necessarie.

Soffermandosi su questo dato[170], un ulteriore aspetto che pone in risalto la centralità dell'utente è l'implementazione nel sistema sviluppato di appositi filtri di oscuramento e de-oscuramento che il paziente può in piena libertà e autonomia decidere di applicare ai documenti caricati nel sistema informativo.

Pensare e sviluppare un sistema informativo sanitario in termini di *Privacy by design* si è rivelato non semplice; anzi, più volte è stato necessario uno sforzo operativo non privo di criticità sotto i profili tecnici, etici e giuridici. Infatti, come rilevato in dottrina[171] è impossibile pensare di gestire i profili giuridici legati alla privacy e alla sicurezza dei dati in un sistema IT in modo totalmente automatico, senza quindi l'intervento umano che, attraverso la programmazione di nuove variabili, è invece in grado di *bypassare* l'eventuale blocco.

Per concludere, si segnala che la progettazione del Dossier in analisi è stata possibile anche grazie all'aver tenuto conto, *step by step,* di tutte le norme comunitarie e nazionali vincolanti e all'aver cercato, altresì, un'efficace armonizzazione del *design* del sistema e un buon bilanciamento di tutti i diritti in gioco[172], così da rendere le finalità del progetto Dossier un fattore di beneficio per tutti[173] i soggetti coinvolti nella sua implementazione.

---

[170] Si rinvia *supra*, par. 3.1.7.

[171] Per maggior approfondimenti, si rinvia a U. Pagallo, *On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law*, in S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?*, Springer Science+Business Media B.V, 2012, pp. 331-346. U. Pagallo, *Privacy e Design*, in M. Pietrangelo (a cura di), *Diritti di libertà nel mondo virtuale della rete*, Fascicolo monografico di *Informatica e diritto*, 2009, 1, pp. 123-134 nonché U. Pagallo, *Designing Data Protection Safeguards Ethically*, in Information, 2011, 2, pp. 247-265 e U. Pagallo, E. Bassi, *The Future of EU Working Parties' "The Future of Privacy" and the Principle of Privacy by Design*, in M. Bottis (eds.), An Information Law for the 21st Century, Atene, Nomiki Bibliothiki, 2011, pp. 286-305.

[172] Si rinvia *supra*, cap. II.

[173] Si rinvia *supra*, par. 3.1.4.

CAPITOLO IV

Case Study: Progettazione di un Dossier Sanitario

"Il passaggio dalla dimensione materiale a quella digitale rappresenta una delle sfide più importanti per la sanità (non solo) italiana, per la sua efficienza e, quindi, per la garanzia dell'unico diritto che la nostra Costituzione espressamente qualifica, ad un tempo, come diritto fondamentale e interesse della collettività".

Antonello Soro[174]

4.1 Introduzione all'ambito e Istituzione del case Study: Fondazione G. Monasterio

La medicina, come più volte detto, negli ultimi decenni ha fatto grandi progressi clinici, tecnologici ed organizzativi e tutto questo è strettamente connesso a esperienze positive e casi di successo.

Un esempio concreto legato alla ricerca Medica e alla Sanità Pubblica è sicuramente la Fondazione Toscana "Gabriele Monasterio", che ha avuto origine come Istituto di Fisiologia Clinica del C.N.R. nel 1968 dalla Regione Toscana e il Consiglio Nazionale delle Ricerche (CNR).

L'istituto di Fisiologia Clinica del C.N.R. fin dalla sua costituzione ha incorporato una unità clinica per la ricerca sui pazienti, combinando clinica, ricerca e formazione principalmente in campo cardiovascolare, adulto e pediatrico, e ponendosi come centro per l'integrazione, l'innovazione e lo sviluppo nella ricerca clinica, tecnologica, biologica ed epidemiologica.

Nel tempo, vista la crescente importanza ed attrazione delle attività svolte si rese evidente la primaria necessità di passare da un regime convenzionale ad uno stabile assetto istituzionale. Nel 1995 venne inquadrato dal Ministero della Salute l'attività di IFC come "Centro di Ricerca ad Alta Specializzazione" (CREAS), convenzionando l'attività con il SSR Toscano ed inglobando l'Ospedale Pediatrico Apuano nella struttura di cura di IFC, che già era dotata di 2 corsie di cardiologia all'interno dell'Azienda Ospedaliera "Santa Chiara" di Pisa.

[174] Intervento di Antonello Soro al convegno "La smaterializzazione dei documenti e il suo impatto sul sistema salute", 6 maggio 2016, Roma. [Doc. web. 4984096] (Ultimo accesso giugno 2017).

Ulteriori incrementi di attività resero necessaria la creazione di una nuova sede ospedaliera interamente dedicata a IFC, con la costituzione nel 2000 dell'Area della Ricerca del CNR "San Cataldo", a cui afferiranno poi gli altri istituti del CNR a Pisa.

Nel 2006 IFC rappresentava il più grande istituto del CNR in Italia, con una dotazione di personale di circa 800 unità e con sedi a Milano, Roma, Brindisi, Palermo.

Nel 2007 la Regione Toscana ed il CNR decisero di dare vita alla Fondazione "Gabriele Monasterio", al fine di istituzionalizzare e rendere stabile il ruolo dei servizi di cura erogati da IFC all'interno del SSR Toscano, passando alla Fondazione i servizi di cura, di ricerca applicata ai pazienti e di formazione.

Da qui con la Legge Regione Toscana n. 25/2006 la Fondazione fu inquadrata come "Presidio specialistico" equiparandola alle Aziende Ospedaliero Universitaria. Successivamente ai sensi della Legge Regione Toscana n. 85/2009 la Fondazione viene convertita in un ente pubblico specialistico del Servizio Sanitario Regionale.

La Fondazione Monasterio nel settore si caratterizza per l'alto profilo delle competenze disponibili, per le tecnologie avanzate per la diagnostica funzionale, d'immagine e di laboratorio di cui dispone e per un livello avanzato di gestione informatica integrata dei processi sanitari e gestionali.

Con l'attività assistenziale posta in essere dalla Fondazione, il paziente è al centro del sistema multidisciplinare che offre percorsi diagnostico-terapeutici moderni e particolareggiati in base al regime di cura che può essere di degenza, ambulatoriale, di day-hospital e day-service.

Più specificatamente nel settore e-Health, presso la Fondazione, sono attive aree di ricerca con progetti di cartella clinica digitalizzata (incluso il Fascicolo Sanitario Elettronico (FSE) e Dossier Sanitario (DS)), telemonitoraggio / teleassistenza e lo sviluppo di *apps* orientate al rapporto interattivo medico-paziente di supporto alla diagnostica.

Ad oggi la Fondazione Gabriele Monasterio opera su due sedi: a Pisa presso l'Area della Ricerca CNR e a Massa presso l'Ospedale del Cuore "G. Pasquinucci".

In particolare presso lo stabilimento di Pisa la Fondazione dispone di n. 46 posti letto, di cui 6 di terapia intensiva e 40 di sub intensiva, e svolge attività di ricovero in degenza ordinaria e *diday-hospital* / *day-service* di cardiologia, medicina cardiovascolare, pneumologia, attività ambulatoriale attività di lipoaferesi e di imaging ECO, TC, RM, PET, MNS.

Invece, presso lo Stabilimento di Massa ci sono n. 71 posti letto, di cui 11 di terapia intensiva, 30 di sub intensiva e 30 di degenza ordinaria e viene svolta attività di ricovero in degenza ordinaria e di day hospital adulto, pediatrico, cardiologico e cardiochirurgico, attività ambulatoriale adulto, pediatrico e prenatale.

Nel suo complesso l'attività clinica, in continua evoluzione (v. figura 5), erogata per il solo anno 2014[175] nei due Stabilimenti Ospedalieri di Pisa e di Massa può essere sintetizzata in: 4.679 ricoveri in ambito cardiologico e cardiochirurgico, dal neonato all'anziano: il 60% di essi è definibile come di alta e il 37% come altissima specialità; 1.404 interventi cardiochirurgici**,** di cui 1.133 nell'adulto (oltre un terzo dei quali con approccio mini-invasivo) e 271 in ambito pediatrico e del congenito adulto; 4.774 procedure cardiointerventistiche di cui 4.055 di emodinamica (3.826 nell'adulto e 229 pediatriche e in congeniti adulti), e 719 di elettrofisiologia e cardiostimolazione; 108.715 accessi ambulatoriali (3.277 pediatrici) con una notevole crescita delle attività di day service con percorsi personalizzati per specifiche patologie, finalizzati alla riduzione dei ricoveri inappropriati ed, insieme a garantire la completezza dell'indagine diagnostica.

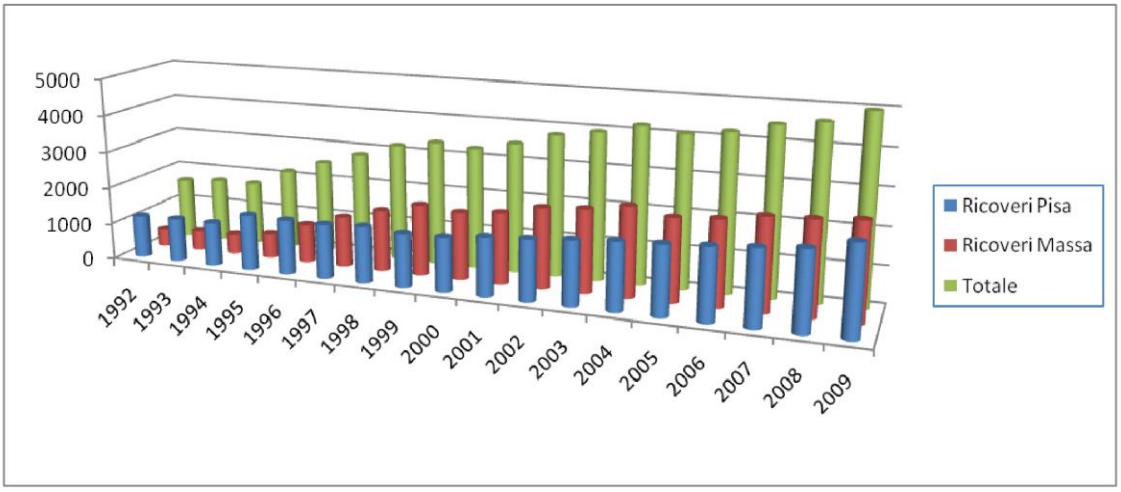


Figura 5. Diagramma dell'andamento dei ricoveri degli stabilimenti di Pisa e Massa dal 1992 al 2009[176]

Tutto ciò producendo un resoconto medio economico annuo, in Keuro che si può sintetizzare in:

- totale valore della produzione 68.252K€, di cui il 77.63% per valorizzazione delle attività sanitarie erogate ed il 20,82 % per contributi in conto esercizio e capitale; il residuo (circa 1,56% per altre entrate tra cui preminenti le attività di ricerca e sperimentazione clinica);
- totale costi della produzione 64.238K€ di cui circa il 23,06% per acquisto di beni, il

[175] Dati elaborati dalla Fondazione G. Monasterio.
[176] Fonte: Fondazione G. Monasterio.

39,33% per sevizi (rientrandovi anche il rimborso degli oneri per il personale funzionalmente assegnato), il 13,97% oneri di personale e il 4,75% per altri oneri.

Si deve sottolineare come le attività cliniche, sopra menzionate, si caratterizzano per l'elevata incidenza e complessità dei ricoveri in regime di urgenza con la gestione della sindrome coronarica acuta e di patologia acuta cardiovascolare che richiede l'approccio interventistico e cardiochirurgico urgente. Interventi questi che a volte sono eseguiti anche grazie all'integrazione con le strutture sanitarie del territorio (ASL 1 di Massa Carrara, ASL 12 Versilia e ASL 5 Pisa).

La Fondazione, inoltre, si caratterizza per la diagnosi e la cura di malattie cardiovascolari rare e/o con caratteristiche di complessità ed urgenza di approccio (amiloidosi cardiaca, cardiomiopatie esotossiche, genetiche, miopericarditi, endocardite, etc.). È inoltre centro di riferimento regionale per la diagnosi e cura delle dislipidemie ereditarie e per il trattamento con LDL aferesi; in tale ambito costituisce centro all'avanguardia per l'assistenza e ricerca integrata bedside-bench e di studi clinici internazionali sulle nuove terapie farmacologiche partecipando a network nazionali ed europei.

Altresì si deve far rilevare come secondo i risultati nel trattamento dello scompenso cardiaco congestizio, certificati dall'AGENAS, la Fondazione è tra i centri leader in Italia: nel 2013 (ultimo dato certificato) infatti si è registrata una mortalità a 30 giorni pari all'1,8 % a fronte di una media nazionale del 10,5%.

Sono di assoluta eccellenza anche i risultati, certificati, riferibili all'attività chirurgiche; sempre nel 2013 la mortalità a 30 giorni per gli interventi di by-pass aortocoronarico isolato è stata pari allo 0,8%, contro una media nazionale del 2,4%, mentre per gli interventi di valvuloplastica o sostituzione di valvole cardiache, la mortalità a 30 giorni si è attestata all'1,1%, a fronte di una media nazionale del 2,9%. Ma vi è di più, infatti, in ambito pediatrico, nel triennio 2012 – 2014 la mortalità a 30 giorni è rimasta al di sotto dell'1% (la media dei centri europei si attesta intorno al 3,5%).

Alla luce di quanto detto nel settore della cardiologia e della cardiochirurgia, secondo i dati elaborati dal Laboratorio MeS della Scuola Sant'Anna, l'attività della Fondazione rappresenta circa il 30% del totale della attività delle Aziende Ospedaliere della Regione Toscana Toscane (Careggi, Siena, Pisa, Meyer, Monasterio) con Performance elevate (v. figura 6).

Ma oltre agli ottimi successi legati all'attività clinica, si deve segnalare che la Fondazione collabora con i maggiori produttori di apparecchiature biomedicali, in particolare nel campo dell'imaging (G.E., Philips, Toshiba, ecc.), è iscritta nell'Osservatorio Nazionale sulla Sperimentazione Clinica e ha moltissime

collaborazioni sono in atto con IFC-CNR, con IN-CNR, con le Università di Pisa, Firenze, Siena, con la Scuola Sant'Anna, e la Scuola Normale Superiore.

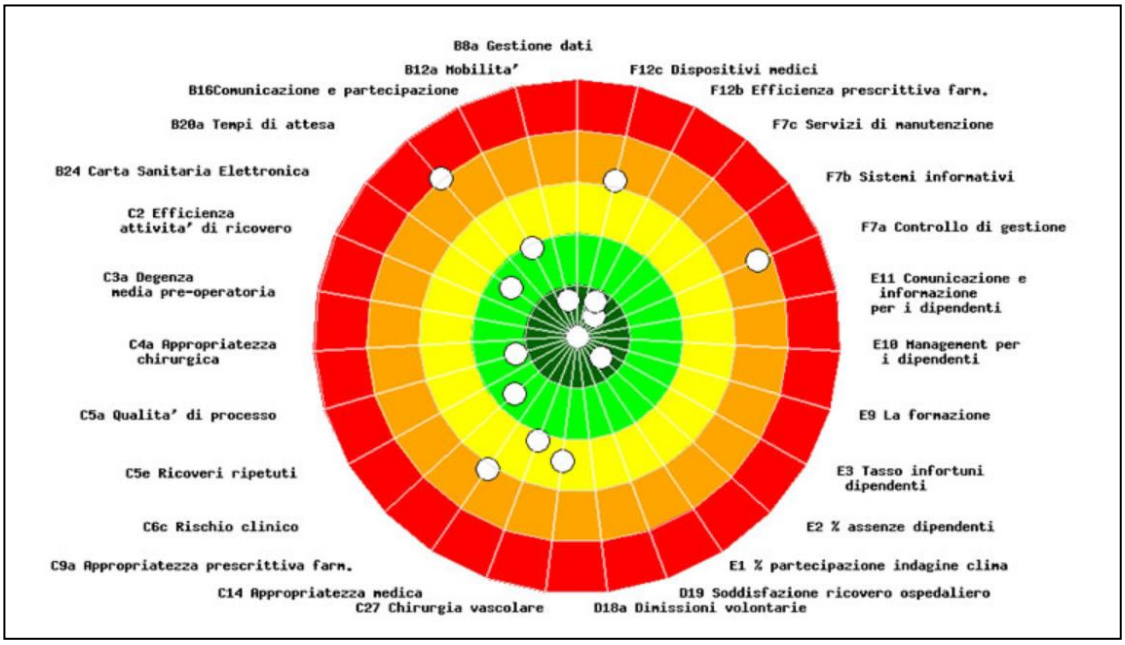


Figura 6. Sistema di Valutazione della Performance del Sistema Sanitario Toscano è affidato al Laboratorio Management e Sanità della Scuola Superiore Sant'Anna di Pisa (MeS) – Anno 2014

Altresì, la completa informatizzazione delle sue strutture fa della Fondazione anche una struttura sanitaria paperless, così che con tale approccio tecnico e gestionale oltre a costituire un fondamentale ausilio per le attività cliniche e di ricerca, a totale beneficio degli operatori sanitari e dei pazienti i cui dati clinici relativamente ad esami, visite e precedenti ricoveri sono immediatamente e costantemente disponibili.

4.1.1 Ricerca tecnologica

Nell'ambito della scienza medica vi sono tendenze ed evoluzioni in atto sin da quando la medicina è nata e gli aspetti che storicamente, anche in FTGM, sono oggetto di continui mutamenti riguardano principalmente la fisiologia e la clinica medica.

Infatti, sia per la fisiologia, scienza che studia le funzioni degli organismi viventi – animali e vegetali – per conoscere le cause, le condizioni e le leggi che determinano e regolano i fenomeni vitali, sia per la clinica medica, metodologia medica basata sull'esame diretto del paziente e sulla cura non chirurgica delle varie patologie, l'ICT, con la sua carica evolutiva, rappresenta un ottimo strumento collaborativo a supporto della gestione del paziente e che affiancata alle tecnologie diagnostiche (CT, RM, RX digitale, ecc), interventistiche (endoscopia, chirurgia robotizzata, ecc) e terapeutiche

(dispositivi medici elettronici, protesi, ecc) permette, altresì, di rendere immediate le evidenze cliniche.

In particolar modo, le linee d'azioni, prettamente mediche, di quanto appena detto possiamo rappresentarle in una evoluzione su tre assi (v. figura 7).

Così che, partendo da una maggiore conoscenza dei meccanismi fisiologici degli esseri umani è possibile ritagliare azioni specifiche creando modelli standardizzati di paziente, in considerazione di una media generale, che conducano il più possibile verso l'istanza specifica del paziente su cui si sta effettivamente lavorando (asse rosso).

Interessante è notare come la linea d'azione dell'asse rossa incroci la linea dalle scienze di base, in cui si applica il concetto di "traslazionalità" che si focalizza sullo studio delle metodologie e degli interventi che consentono la selezione di nuove proposte terapeutiche, e attraverso l'incontro di questi due assi si cerca di applicare quanto studiato direttamente sul paziente, attraverso i percorsi di sperimentazione clinica, e successivamente completando il ciclo traslazionale "*from bench to bed and from bed to bench*" dal paziente vengono rilevati gli scostamenti rispetto ai valori attesi e riportati in ambito di ricerca, (asse marrone).

In questo scenario, alla luce di quanto sinora rappresentato, ricopre altresì un ruolo fondamentale l'asse che rappresenta il passaggio dalla terapia per classi biologiche alla terapia personalizzata che tiene conto dei fattori genetici dei pazienti, l'efficacia delle molecole sul singolo paziente, le interazioni ed intolleranze ecc. (asse blu).

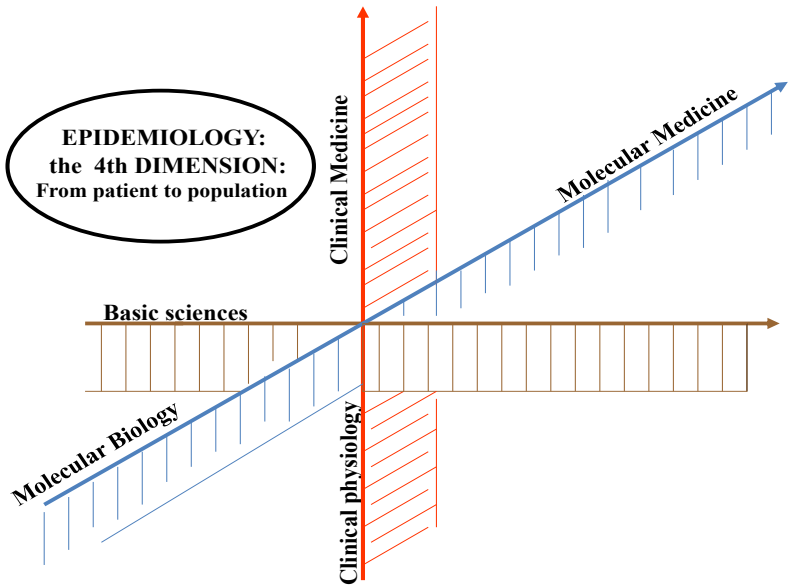


Figura 7. Schema approccio contenuti di ricerca[177]

[177] Fonte: Fondazione G. Monasterio.

4.1.2 Approccio multidisciplinare

Nel tempo FTGM ha sempre favorito un approccio multidisciplinare (v. figura 8) che nell'ambito della salute e, in particolare, nel momento della diagnosi mette in evidenza il fatto che con una maggiore compliance si possa produrre un modello di cura centrato sul paziente e sul suo vissuto personale.

Nella evoluzione della scienza medica, a cui i sistemi ICT sono di supporto, è infatti basilare un approccio globale che consideri le potenzialità di ogni prospettiva, indicata come branca specialistica (Epidemiologia, biotecnologie, Clinica, laboratorio, ecc).

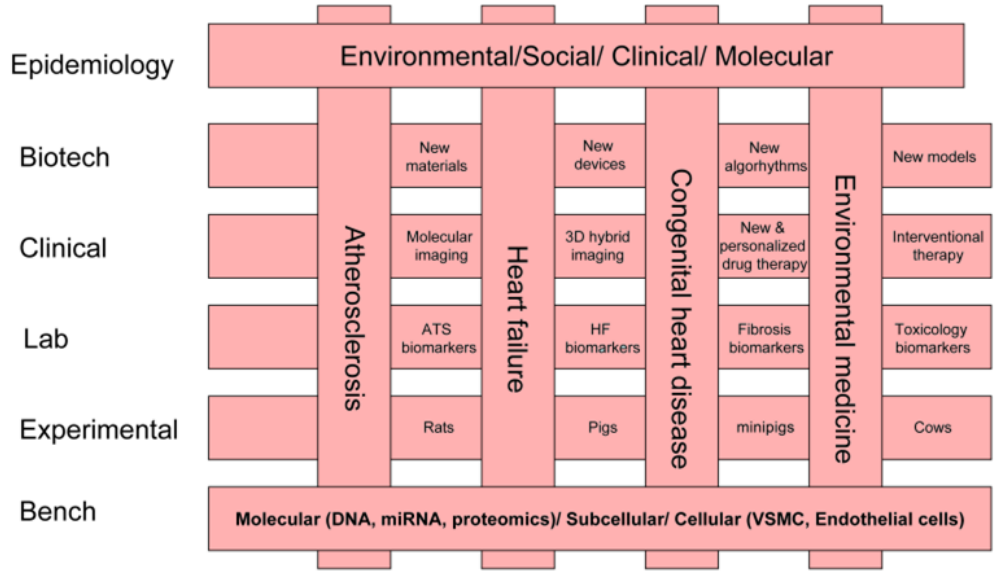


Figura 8. Schema approccio multidisciplinare nell'ambito clinico[178]

4.1.3 La storia tecnologia della Fondazione G. Monasterio

In FTGM l'uso delle tecnologie è particolarmente invasivo a causa della lunga storia di evoluzioni e progetti di ricerca applicata che parte sin dagli anni '80 in Istituto di Fisiologia Clinica. Questo ha condotto ad una scelta di campo molto importante, infatti, dal 1999 i prototipi informatici sviluppati presso la Fondazione vengono messi in uso ospedaliero per tutti i pazienti ricoverati, costituendo la prima cartella clinica cardiologica sviluppata in Java in ambito di ricerca.

[178] Fonte: Fondazione G. Monasterio.

Figura 9. Programma Speciale Ministero della salute – art. 12 comma 2, lettera h, D. Lgs 502/92 Regione Toscana[179]

In particolare, riguardo ai sistemi di gestione dei dati di cartelle cliniche una esperienza significativa è quella condotta a partire dal 1995 con il progetto "Sperigest" del Ministero della Sanità[180].

In detto progetto si considerava un sistema virtualmente unico che metteva a disposizione, secondo profilature diverse, i dati clinici, amministrativi e di governo, come nella figure sopra (v. figura 9).

Per la prima volta in Italia un'AUSL ed un'Azienda Ospedaliera comunicarono tra loro attraverso la presenza di un'unica cartella clinica consultabile da entrambe le strutture sanitarie, creando importanti sinergie ed efficienza nei servizi offerti ai cittadini. Attraverso l'analisi dei risultati emersi nel tempo è stato evidente, altresì, che il Progetto Sperigest è divenuto un supporto capace di integrare ed elaborare le informazioni, indispensabile sia nella gestione amministrativa sia nel rafforzamento delle capacità di governo e programmazione della struttura sanitaria,

Negli anni successivi diversi altri progetti di ricerca hanno fatto crescere il livello di gestione informatizzata delle informazioni cliniche fino a giungere nel 2007 ad un sistema unico integrato di ricerca.

Tuttavia con la nascita della Fondazione Monasterio nel 2007 e la sua partenza operativa nel 2008 detti sistemi furono reingegnerizzati per un uso più affidabile ed efficiente, costituendo una base per l'EHR aziendale che negli ultimi anni sta conducendo verso ad una ristrutturazione dei processi sanitari tramite l'ausilio dell'ICT.

[179] Fonte: Fondazione G. Monasterio.
[180] http://www.cnr.it/documenti/Innovazione/BRAVAR_2011.pdf

4.1.4 Processi sanitari

Ad oggi, secondo il modello di gestione integrata, oramai il più consono per la cura ed assistenza dei pazienti affetti da multi patologie soprattutto croniche, gli elementi di base per una strutturazione adeguata dei processi sanitari sono rappresentabili come:

- stratificazione delle malattie/problemi del paziente
- adozione di un protocollo diagnostico terapeutico per malattia/problema (condiviso da tutti i soggetti interessati ricavato dalle linee guida internazionali e/o nazionali ed integrato dalla conoscenza delle risorse utilizzabili), fondati su mattoni base di attività (e.g. esecuzione, decisione, confronto);
- adozione di interventi educazionali e di coinvolgimento attivo per malattia/problema del paziente nel percorso di cura (patient engagement), fondati su mattoni base di attività (e.g. esecuzione, autocontrollo, follow-up);
- integrazione dei mattoni base dell'insieme di protocolli e interventi educazionali attivati sul paziente, attraverso l'individuazione di attori, task distinti per fase della malattia, ed attraverso la mappatura delle funzioni ICT della piattaforma che si intende utilizzare/bisogni.

Così che, appare chiaro come un'analisi dei processi deve essere in grado di rappresentare le singole fasi in cui i processi siano scomponibili, al fine di determinarne gradi di interazione tra di esse e fornire indicazioni utili ad esempio su fattori prognostici, indici di efficienza, aderenza a linee guida, oltre che al rispetto delle normative locali che regolamentano i processi sanitari ed il loro governo (si pensi in Italia alla Scheda di Dimissione Ospedaliera, che non è presente in altri paesi in quanto tale).

Alla luce di ciò, l'obiettivo del programma della Fondazione Monasterio è quello di analizzare gli attuali processi e svilupparne una ri-strutturazione caratterizzata dal supporto ICT e dall'interoperabilità semantica tra domini diversi, ponendo attenzione ai tre seguenti aspetti:

- *aspetto tecnico:* per garantire l'interoperabilità tra sistemi, basata sui Web Services e architetture SOA. Questo necessita della modellazione dei concetti sanitari, anche di specialità, che vengono trasmessi da un dominio ad un altro;
- *aspetto clinico:* per garantire un corretto e non ambiguo passaggio di informazioni tra specializzazioni diverse, permettendo una multidisciplinarietà clinica efficace;
- *aspetto organizzativo e di governo:* per garantire l'accoglimento di linee guida cliniche, gold standard, principi di efficienza ed appropriatezza, che nei processi gestiti da un sistema EHR possano fornire una valutazione di efficienza ed efficacia, oppure

definire uno scostamento da percorsi definiti da regolamenti interni o recepiti da normative nazionali o regionali.

Per l'aspetto tecnico, i sistemi sanitari seguiranno un approccio "paziente centrico": il paziente, nel sistema a regime, verrà seguito nei suoi percorsi di cura in forma centralizzata. Il sistema fornisce la possibilità di raccogliere tutti gli elementi che caratterizzano la storia clinica del paziente e di "archiviarli" per renderli poi disponibili secondo diversi profili di accesso. L'orientamento al problema e la gestione dei piani di assistenza e dei protocolli di assistenza – potenziati dalla logica di *workflow*, consentono poi un costante monitoraggio e valutazione della qualità dell'assistenza erogata ed un progresso continuo nella definizione dei protocolli di cura stessa. L'interazione con il sistema BPM rappresenta un valore aggiuntivo di monitoraggio e guida dei processi sanitari, non impedendo, in sua assenza, un corretto funzionamento del dossier sanitario secondo schemi liberi di cura dei singoli pazienti.

Per l'aspetto clinico viene data particolare enfasi al management clinico, in cui i requisiti clinici sono definiti a partire dalle esigenze espresse dal personale sanitario ed investono la sfera relativa alla documentazione intesa come elementi di diagnostica, la cartella clinica, la cartella ambulatoriale, la cura ed il *follow up*. Esempio di implementazione di requisiti clinici su percorsi informatizzati è la possibilità di svolgere le azioni cliniche ordinarie, come la lettura di esiti di indagini o scrittura di diari/valutazioni mediche ed infermieristiche, direttamente al letto del paziente, ivi comprese la rilevazione dei parametri fisiologici e la prescrizione e somministrazione della terapia farmacologica.

Il sistema gestisce sia la documentazione a validità medico legale sia le comunicazioni strutturate e formali (richieste di prestazioni, ordini, etc.) che la comunicazione informale. Per comunicazione formale si intende la capacità di gestire lo scambio di documentazione "codificata" ossia lo scambio informatico di richieste di servizio (esami radiologici piuttosto che ematochimici, etc.) lo scambio della documentazione (referti, documentazione del caso, etc.) e la possibilità quindi di usufruire in tempo reale di tutti i dati clinici del paziente. Per sistema di comunicazione informale si intende lo scambio di informazioni "veloci", o messaggistica, tra operatori (la notifica verso un utente della disponibilità di un referto, l'ok all'idoneità operatoria di un paziente, etc.), in breve a quei meccanismi di comunicazione che sono alla base della gestione del *workflow* clinico. Tale meccanismo risulta spesso di grande utilità per comunicazioni trasversali rapide e per utilizzare propriamente risorse interne.

Per l'aspetto organizzativo e di governo viene data particolare enfasi al governo sanitario, in cui la raccolta del dato clinico ed amministrativo è strutturata all'interno di un più ampio concetto organizzativo. I dati infatti non solo rispettano i requisiti clinici

ritenuti indispensabili dal personale sanitario sia per la documentazione (cartella clinica, cartella ambulatoriale, etc.) che per l'elaborazione (statistiche, report, etc.), ma rispettano anche le normative ed i percorsi di lavoro vigenti nell'intera Azienda Ospedaliera. Da questi dati è possibile estrapolare le elaborazioni del caso in termini di monitoraggio e statistiche utili alla ricerca medica. Ad esempio si prevede che il sistema esegua automaticamente in ambito clinico i controlli di qualità relativi alla consistenza del dato inserito, verificando che siano stati riempiti tutti i campi necessari per generare flussi a validità amministrativa, quale la Scheda di Dimissione Ospedaliera (SDO), che sia stata inserita la diagnosi principale, che sia stato indicato il motivo del ricovero, etc.

Il sistema fornisce inoltre il supporto per l'identificazione del legame tra l'assorbimento di risorse e l'ottenimento di risultati, misurati sia in termini di risorse usate che di benefici per i pazienti (outcome). Ciò grazie al fatto che il sistema proposto è in grado di seguire informaticamente il percorso clinico del paziente ed implementare contemporaneamente strumenti quali le Linee Guida e *l'Evidence Based Medicine*.

L'opportunità di disporre dell'informazione costo di processo è di estrema utilità al fine di programmare l'attività e controllare il livello di raggiungimento degli obiettivi fissati, sviluppando intorno allo strumento "percorso del paziente" l'intero ciclo di programmazione e controllo di gestione.

Infine, il sistema opera nel pieno rispetto delle normative, consentendo di avvalersi della codifica regionale e nazionale standard per la quantificazione dei DRG e la codifica delle diagnosi e delle prestazioni.

Il raggiungimento degli obiettivi prima espressi presuppone di utilizzare una logica di informatizzazione orientata al paziente e quindi di organizzare la raccolta dati in funzione del percorso dell'assistito, in un'ottica di risultati di efficacia ed efficienza gestionale e di qualità clinica (outcome). Questo ad indicare che informatizzare la gestione clinica dei dati non si riconduce ad una semplice riproduzione nel sistema elettronico della modulistica cartacea esistente nelle unità organizzative, ma implica una profonda analisi ed eventualmente una revisione dei processi interni ed esterni alle unità per razionalizzare i processi in un'ottica sistemica e tenendo presente per la *"Gestione clinica"*:

- valutazione clinica, indagini strumentali;
- Accessi paziente e degenza;
- Diagnosi, terapia, riabilitazione;
- Procedure chirurgiche e mediche;
- Documentazioni a validità medico-legale;

invece per la *"Gestione amministrativa e governo"* :

- personale e contabilità;

- schematizzazione delle attività e consuntivi;
- magazzino materiali, strumentazioni;
- previsioni di attività, pianificazioni;
- rendicontazioni verso regione e ministero.

4.1.5 Obiettivi della Ricerca applicata

L'obiettivo generale posto alla base della ricerca applicata è stato analizzare e implementare, in modo sistematico ma funzionale, l'impianto generale del Dossier sanitario già in fase di sviluppo presso la Fondazione G. Monasterio.

In modo particolare gli obiettivi specifici sono stati: delineare i contenuti da registrare nel Dossier, analizzare i vincoli legati alla normativa sulla protezione dei dati personali, redigere la documentazione necessaria alla sua operatività.

La ricerca applicata è stato svolto attraverso l'analisi del contesto reale di generazione e utilizzo delle informazioni sanitarie in corsia e negli ambulatori, tenendo incontri con medici e infermieri secondo la metodologia lean[181] semplificata.

La ricerca ha avuto inizio a luglio 2015 terminando a dicembre 2016 per una durata complessiva di diciotto mesi.

4.2 Analisi preliminare del Dossier sanitario: l'uso di *UML*

L'analisi preliminare per l'implementazione del Dossier sanitario è stata compiuta attraverso l'uso del UML (*unified modeling language*, "linguaggio di modellizzazione unificato")[182], linguaggio che descrive l'architettura di un sistema IT nel suo dettaglio, documentando, altresì, le caratteristiche tecniche che dovranno essere implementate. Il principale punto di forza dell'UML consiste nel fatto che il processo di sviluppo del sistema può essere effettuato in modo tale che gli analisti, i programmatori e chiunque

[181] Metodologia - ideata nei primi anni '90 da due ricercatori del MIT Womack e Jones - che interviene sui processi, li osserva, li analizza e li modifica per poterli far tendere verso le effettive necessità poste dai soggetti interessai e arrivando anche ad eliminare eventuali sprechi. Per un maggior approfondimento: *Cfr.* J.P. Womack, D.T. Jones, D. Roos, *The Machine That Changed the World: The Story of Lean Production*, Harper Perennial, 1990; Womack J.P., Jones D.T., *Lean Thinking. Per i manager che cambieranno il mondo*, 2008; A. Rosa, La metodologia Lean e la riduzione degli sprechi, Il sole 24 ore, 14 ottobre 2015 http://www.sanita24.ilsole24ore.com/art/aziende-e-regioni/2015-10-14/la-metodologia-lean-e-riduzione-sprechi-095941.php?uuid=AC3BB0FB (ultimo accesso giugno 2017).

[182] A. Watson, *"Visual Modelling: past, present and future", http://www.uml.org/Visual_Modeling.pdf (*ultimo accesso giugno 2017).

altro interessato possa capire ed esaminare in modo efficiente il sistema e prendere parte alla sua costruzione in modo attivo.

I benefici centrali derivanti dall'utilizzo di questo linguaggio sono che:

- si potrà conoscere in anticipo il risultato finale del progetto su cui si sta lavorando dal momento che il sistema IT è disegnato e ben documentato ancor prima che venga sviluppato da parte dei programmatori;
- la scrittura del codice sorgente è resa più agevole ed efficiente visto che, come detto, la fase di disegno del sistema precede la fase di scrittura del codice;
- il sistema si comporterà esattamente come ci si aspetta prevedendo e anticipando eventuali *bag*;
- chiunque sia coinvolto nello sviluppo potrà avere una chiara idea di tutto l'insieme che costituisce il sistema. In tal modo, si potranno sfruttare al meglio anche le risorse hardware;
- grazie alla documentazione dettagliata diviene ancora più facile effettuare eventuali modifiche future al codice sorgente.

Il linguaggio UML[183] trova la sua operatività nell'utilizzo di diagrammi che hanno come obiettivo la costruzione di molteplici viste[184] di un sistema IT, tutte correlate tra loro.

In particolare, il nostro studio ha affrontato la progettazione di un Dossier sanitario attraverso la costruzione di tre diagrammi: Use Case Model (c.d. Casi d'uso, oppure UCM), Class Diagram (c.d. Diagrammi delle classi), Sequence Diagram (c.d. Diagrammi d'Interazione).

Infatti, attraverso un caso d'uso è possibile descrivere testualmente un comportamento particolare di un sistema dal punto di vista dell'utente e senza timore – da parte degli sviluppatori – di non recepire bene lo scopo finale. E' in altri termini una tecnica efficace per catturare ed esprimere in modo specifico e dettagliato il comportamento di un sistema IT e l'interazione con gli utenti del sistema stesso (detti attori).

Altresì, questo tipo di diagramma – in cui abbiamo detto che un attore fornisce l'*input* e il sistema esibisce un risultato osservabile – può prevedere "l'inclusione" – rappresentando una dipendenza tra casi d'uso, in cui il caso incluso fa parte del

---

[183] *Cfr.* G. Booch et al. *"The Unified Modeling Language User Guide 2/E"*, Addison -Wesley, 2005; sul tema vedere anche J. Rumbaugh et al. *"The Unified Modeling Language Reference Manual 2/E"*, Addison -Wesley, 2004; C. LARMAN. *"Applying UML and Patterns",* Addison -Wesley, 2004.

[184] Una vista è una porzione di un modello orientata alla rappresentazione di un particolare aspetto di un sistema IT. Sul punto v. *G.* Booch, J. Rumbaugh, I. Jacobson, *Unified Modeling Language User Guide,* Addison Wesley, 1998.

comportamento di quello che lo include – oppure "l'estensione" – consistendo in un incremento di comportamento, supplementare ed opzionale che gestisce casi particolari o non standard – di altri *use case model*.

Un UCM è composto da varie sezioni:

i. *Nome:* titolo del caso d'uso e che riflette il suo scopo, od obiettivo.
ii. *ID:* idealmente un numero progressivo ed automatico che permette di mantenere la sua tracciabilità durante l'intero processo.
iii. *Descrizione degli obiettivi:* semplice dichiarazione che riassume l'obiettivo dell'intero caso d'uso.
iv. *Attori:* tipicamente vengono indicati i soggetti primari e secondari che ne prendo parte.
v. *Pre-condizioni:* condizioni che devono essere soddisfatte prima di attivare il caso d'uso.
vi. *Scenario:* descrizione testuali dei vari passi che compongono il caso d'uso.
vii. *Post-condizioni:* condizioni che devono essere soddisfatte prima che il caso d'uso sia completato.

La descrizione testuale di un caso d'uso è rappresentato graficamente da un ovale (ellisse) con il nome del caso d'uso scritto all'interno o al di sotto di questo. Un attore è rappresentato dalla figura di un omino stilizzato (*stick figure*).

Con riguardo, invece, ai diagrammi *Class Diagram* attraverso la loro costruzione è possibile rappresentare il flusso narrativo delle varie istanze di uno *Use case model.*

Ogni classe è corredata da un insieme di attributi (che descrivono le caratteristiche o lo stato della classe) e operazioni (che descrivono il comportamento della classe).

Il simbolo grafico che rappresenta le classi è un rettangolo suddiviso in tre scomparti (v. figura 10), rispettivamente dedicati al nome della classe, agli attributi e alle operazioni.

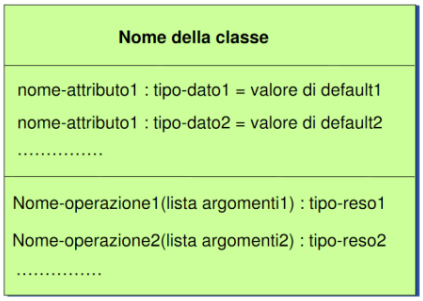


Figura 10. Esempio di un classe

Le classe possono essere legate concettualmente tra loro attraverso “relazioni di associazioni” (v. figura 11) che possono essere: semplici, di aggregazione, di composizione.

Semplici: definite come relazioni uno a uno che uniscono le varie classi parte. Graficamente rappresentate con una linea retta.

Di aggregazione: definita come una relazione non forte ovvero una relazione nella quale le classi parte hanno un significato anche senza che sia presente la classe tutto. Graficamente rappresentata con una linea e un rombo finale vuoto;

Di composizione: definita come una relazione forte cioè una relazione nella quale le classi parte hanno un reale significato solo se sono legate alla classe tutto. Graficamente rappresentata con una linea e un rombo finale pieno.

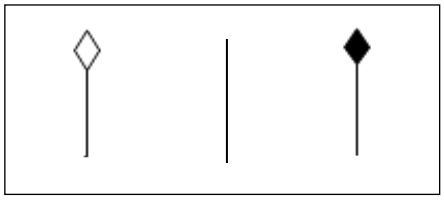


Figura 11. Rappresentazione grafica delle “relazioni di associazioni”

Da ultimo, la costruzione dei Diagrammi d’Interazione permette di rappresentare la descrizione temporale di uno scenario, inteso come determinata sequenza di azioni che vanno da un tempo T1 (d’inizio) e un tempo T2 (di fine).

I componenti essenziali di questo tipo di diagramma sono: gli oggetti, un messaggio e il tempo.

Gli oggetti sono gli elementi rappresentati dal diagramma e sono disposti su un asse verticale (rappresenta la dimensione del tempo) in sequenza da sinistra verso destra. Da ogni blocco iniziale (rappresentato da un elemento grafico) parte una linea tratteggiata verso il basso, denominata “linea della vita” (*lifeline*). Lungo la *lifeline* si trovano piccoli rettangoli chiamati “attivazione” (*activation*) e rappresentano l’esecuzione di un’operazione di cui l’oggetto si fa carico. La lunghezza del rettangolo, invece, rappresenta la durata dell’attivazione.

Un messaggio è l’elemento che viaggia da un oggetto ad un altro, viene disegnato a partire dalla *lifeline* dell’oggetto da cui parte il messaggio e arriva sulla *lifeline* dell’oggetto a cui il messaggio è diretto.

Si può anche verificare il caso in cui un oggetto mandi un messaggio a se stesso, cioè un messaggio che parte dalla sua *lifeline* e arriva alla stessa *lifeline*. Tale tipo di comportamento viene definito Ricorsione.

Il tempo che viene fatto partire graficamente alla base di ogni oggetto e proseguire fino in basso. Così che un messaggio che si trovi più vicino ad un oggetto rispetto ad un altro (in direzione verticale), si verificherà prima nel tempo.

Importante è segnalare che le interazioni rappresentate, in questo diagramma, sono sostanzialmente dei messaggi inviati da un oggetto[185] a un altro e le risposte del sistema sono raffigurate con delle frecce che tornano indietro dall'asse del sistema verso l'asse dell'attore che da avvio allo scenario.

4.3 Progettazione del "Dossier Sanitario" con metodologia *Privacy by design* e *UML*

In questo paragrafo verranno descritti i cosiddetti *casi d'uso* per la creazione e l'utilizzo del Dossier sanitario in un contesto assistenziale di base e secondo quanto descritto nell'allegato A delle Linee guida in materia di Dossier sanitario emanate dall'Autorità Garante della Privacy. Infatti, proprio da un'attenta analisi delle presenti linee guida e con un approccio *Privacy by design* è stato possibile individuare e descrivere i casi d'uso e le altre tipologie di diagrammi UML di seguito rappresentati.

Preme evidenziare che l'attività di analisi e di elaborazione dei casi d'uso tiene, altresì, conto di un'eventuali necessità di adattamento a realtà specifiche e, peraltro, facendo attenzione che i vari modelli non venissero snaturati dei loro elementi essenziali.

Tuttavia, prima di affrontare nello specifico la trattazione dei singoli casi d'uso, è doveroso osservare che essi sono stati concepiti e rappresentati tenendo conto del principio sulla "centralità del Paziente" descritto dalla metodologia *Privacy by design*, facendo così ruotare tutto il sistema di Dossier Sanitario intorno alla necessità del "Consenso per la creazione del Dossier sanitario" (v. figura 12).

Alla luce di quanto appena detto è importante mettere in risalto come gli atti sanitari compiuti sul soggetto di cura (Paziente) producono documentazione sanitaria associata che costituisce la fonte di alimentazione del Dossier, *step* successivo al rilascio del consenso e con relativa apertura del Dossier, su cui hanno preso forma i diritti esplicati nei vari UCM che vedremo nel dettaglio nei paragrafi successivi.

Descrizione dei casi d'uso che trovano un sunto organico – delle singole classi dei dati contenuti e gestiti attraverso il Dossier sanitario - nello scema generale del modello informativo sotto rappresentato (v. figura 13).

---

[185] Si ricorda che oltre ai messaggi inviati da un oggetto a un altro, un oggetto può inviare un messaggio a sé stesso.

Da ultimo, al fine di rendere ancora più chiara la lettura va fatto rilevare che essi sono stati elaborati rispettando la scansione temporale di avvenimento (v. figura 14) e ciò ha consentito, altresì, la rappresentazione di un diagramma di stato (v. figura 15) che ha permesso di fornire una visione completa del funzionamento del sistema in riferimento ai specifici e rilevanti momenti di vita del Dossier, in particolare: apertura, revoca e chiusura.

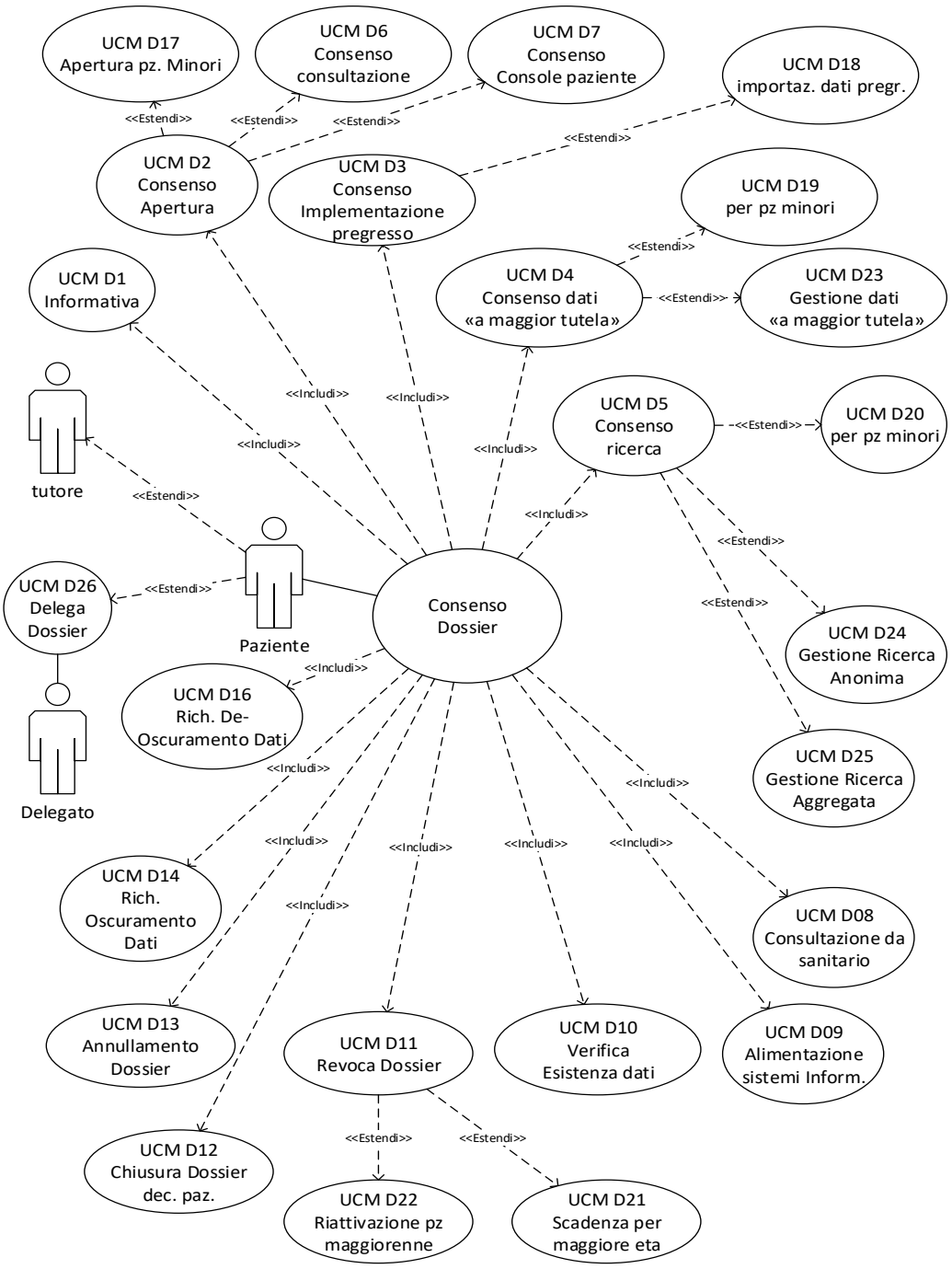


Figura 12. Schema generale dei Casi d'uso

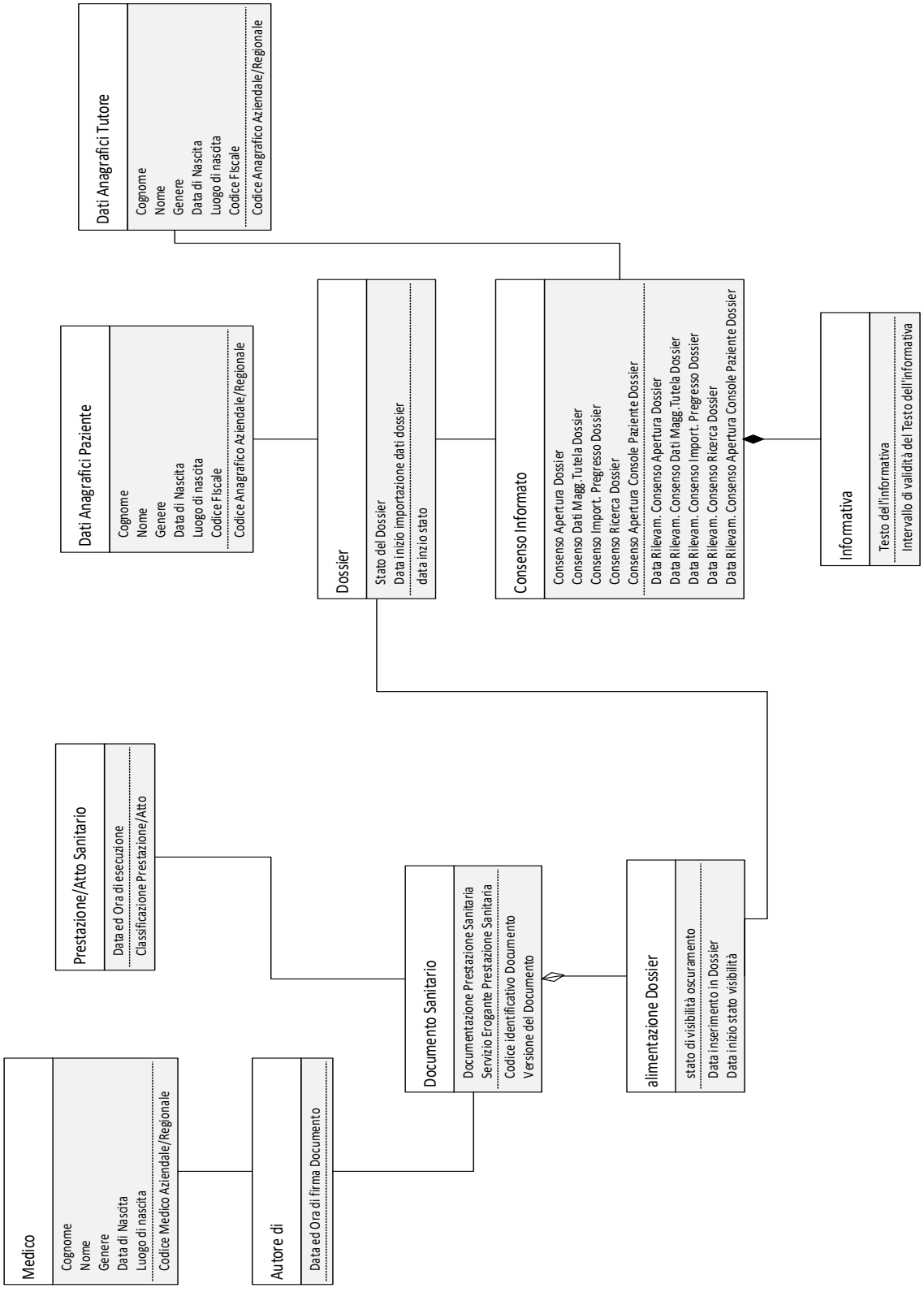


Figura 13. Schema modello informativo generale

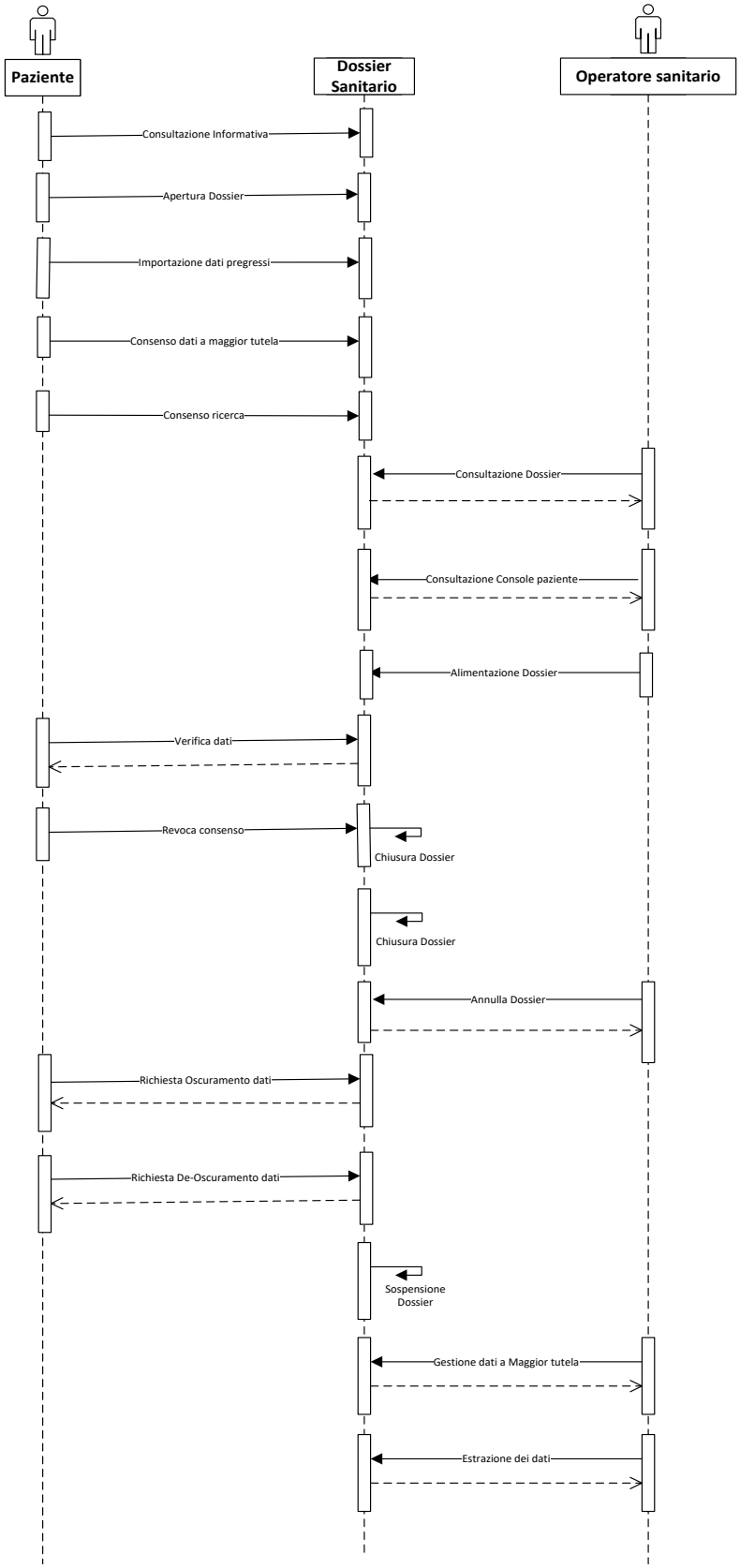


Figura 14 Interaction model Generale

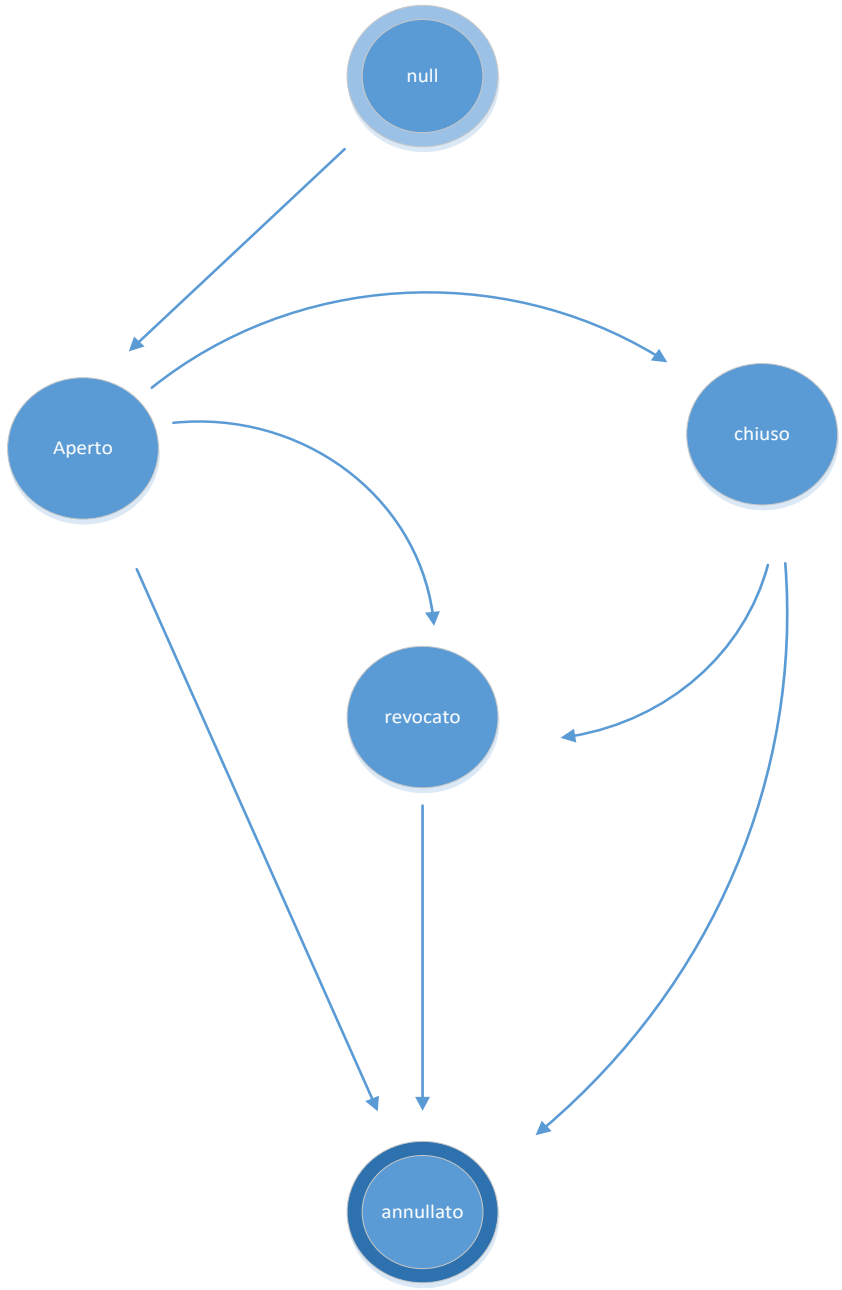


Figura 15. Diagramma degli stati del Dossier

Si riportano nel seguito le analisi dei singoli *Use case*.

4.3.1 SC01 - Consultazione dell'Informativa

Descrizione del caso d'uso

La prima attività da compiere per poter dar vita alla creazione di un Dossier Sanitario - ottemperando a quanto disposto al *punto 2* dalle Linee guida sul Dossier Sanitario - è la somministrazione dell'informativa al paziente *ovvero* suo tutore.

Attore Primario

Paziente/Tutore.

Precondizioni

Nessuna.

Scenario

Il paziente *ovvero* il suo tutore, si rivolge alla struttura sanitaria per ottenere una prestazione medica. Accolto dall'Operatore sanitario l'interessato riceve l'informativa che dovrà visionare e con cui verrà reso edotto del significato e peculiarità del Dossier Sanitario.

L'informativa renderà edotto l'interessato: sulle finalità e le modalità del trattamento cui sono destinati i dati; la natura obbligatoria o facoltativa del conferimento dei dati; le conseguenze di un eventuale rifiuto al Trattamento; l'elenco dei soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati; i diritti di cui all'articolo 7 del Codice Privacy; gli estremi identificativi del titolare.

Post-condizione

Viene rilasciato dall'Operatore sanitario al paziente il modulo con l'informativa.

Use Case Model

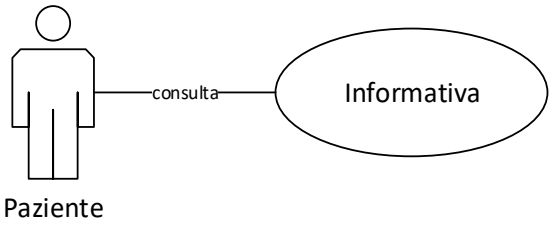


Figura 16. UCM D01 "Consultazione dell'informativa"

Information Model

Lista delle informazioni da trattare:

- Informativa

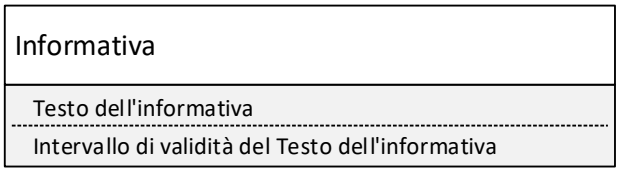


Figura 17. Information Model "Consultazione dell'informativa"[186]

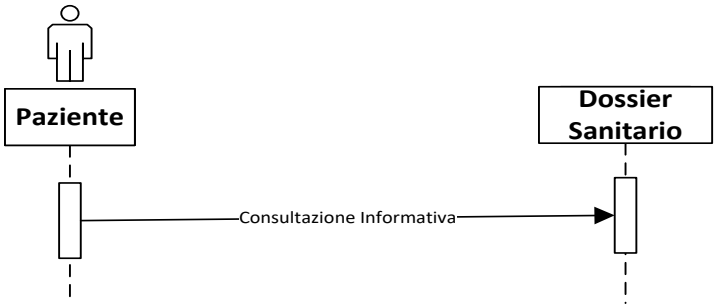


Figura 18. Interaction Model "Consultazione dell'informativa"

[186] Nell'information model si specifica che per "Intervallo di validità del Testo dell'Informativa" si intende la versione del documento che riporta il testo dell'informativa.

4.3.2 SC02 - Consenso Apertura Dossier sanitario

Descrizione del caso d'uso

Il presente caso d'uso, successivamente alla consultazione dell'informativa, permette al Paziente - secondo quanto previsto dal *punto 3* dalle Linee guida sul Dossier sanitario - di esprimere il proprio consenso libero ed informato al fine di concedere agli Operatori sanitari di aprire un suo Dossier sanitario.

Attore Primario

Paziente.

Precondizioni

Al fine di poter esprimere il proprio consenso il paziente dovrà:

- essere identificato con idonei meccanismi che ne garantiscano l'identità,
- essere maggiorenne,
- essere registrato presso l'anagrafe sanitaria,
- SC01, UCM D01 Consultazione dell'Informativa.

Scenario

Il paziente, compilando con i propri dati anagrafici e spuntando il SI/NO nel modulo di consenso cartaceo e firmandolo *ovvero* rilasciandolo oralmente, fornisce alla Struttura sanitaria un consenso esplicito, libero ed informato per la costituzione del Dossier sanitario.

Post-condizione

Il consenso all'alimentazione del Dossier sanitario viene registrato nei sistemi informatici di gestione del dossier da parte del personale addetto.

Use Case Model

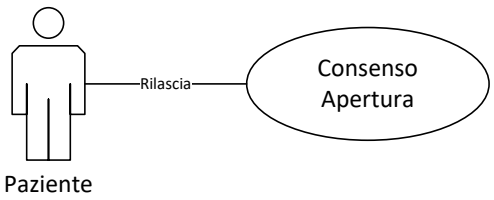


Figura 19. UCM D02 "Consenso Apertura Dossier sanitario"

Information Model

Lista delle informazioni da trattare:

- Dati anagrafici del paziente
- Dati del consenso apertura

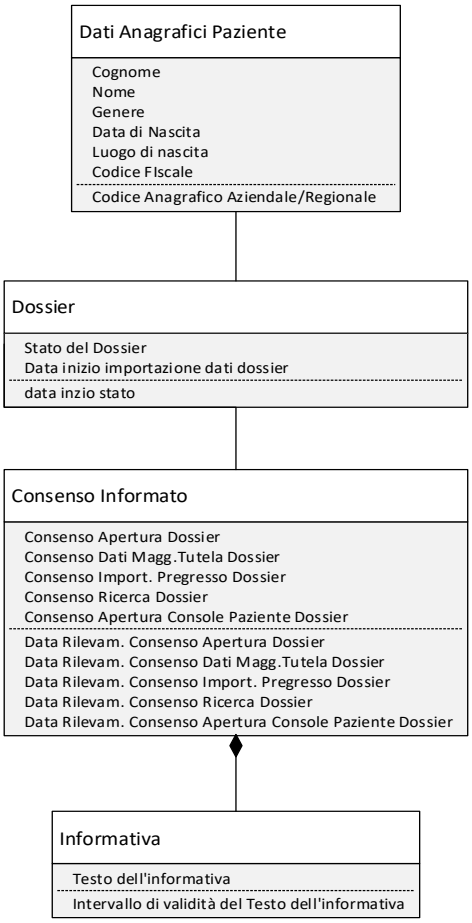


Figura 20. Information Model Generale “Consenso Apertura Dossier sanitario”

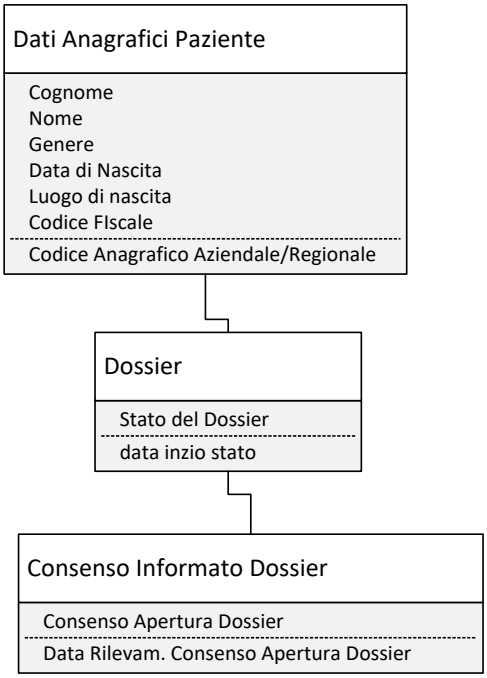


Figura 21. Information model contenuto minimo “Consenso Apertura Dossier sanitario”

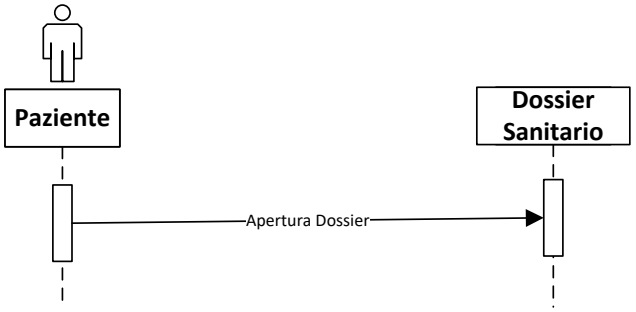


Figura 22. Interaction Model “Consenso Apertura Dossier sanitario”

4.3.3 SC03 - Consenso Importazione dati e documenti pregressi

Descrizione del caso d'uso

Il presente caso d'uso, successivamente all'apertura del Dossier, permette al paziente - secondo quanto previsto dal *punto 3* dalle Linee guida sul Dossier Sanitario - di esprimere il proprio consenso libero ed informato al fine di concedere agli operatori sanitari di popolare il sistema del Dossier Sanitario con i propri dati e documenti sanitari pregressi.

Attore Primario

Paziente.

Precondizioni

Al fine di poter esprimere il proprio consenso il paziente dovrà:

- essere identificato con idonei meccanismi che ne garantiscano l'identità,
- essere maggiorenne,
- essere registrato presso l'anagrafe sanitaria,
- SC02, UCM D02 Consenso Apertura Dossier sanitario.

Scenario

Il paziente, compilando con i propri dati anagrafici e spuntando il SI/NO nel modulo di consenso cartaceo e firmandolo *ovvero* rilasciandolo oralmente, fornisce alla Struttura sanitaria un consenso esplicito, libero ed informato per l'alimentazione nel Dossier sanitario dei dati e documenti creati antecedentemente alla costituzione dello stesso.

Post-condizione

Il Consenso all'alimentazione con dati e documenti pregressi viene registrato nei sistemi informatici di gestione del dossier da parte del personale addetto.

Use Case Model

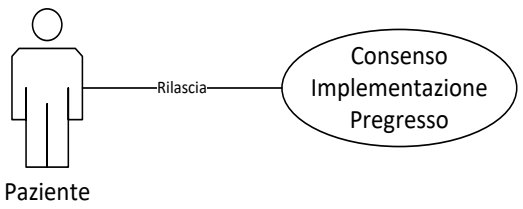


Figura 23. UCM D03 "Consenso Importazione dati e documenti pregressi"

Information Model

Lista delle informazioni da trattare:

- Dati anagrafici del paziente
- Dati del consenso

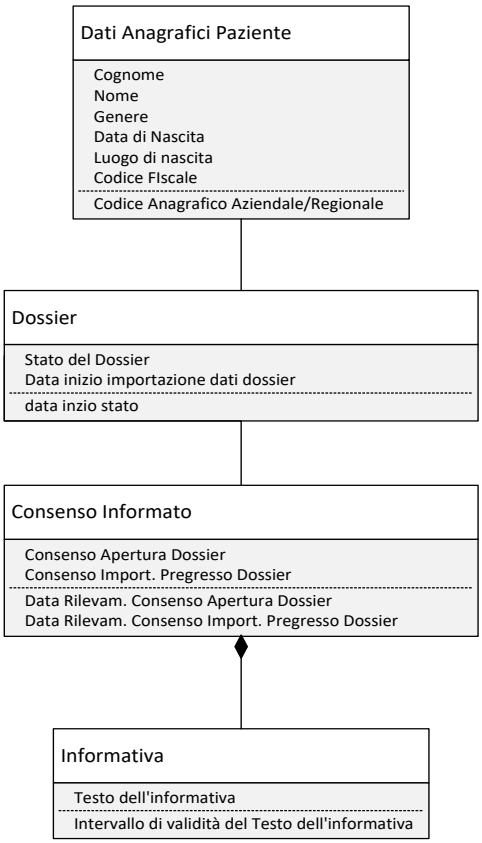


Figura 24. Information Model Generale “Consenso Importazione dati e documenti pregressi”

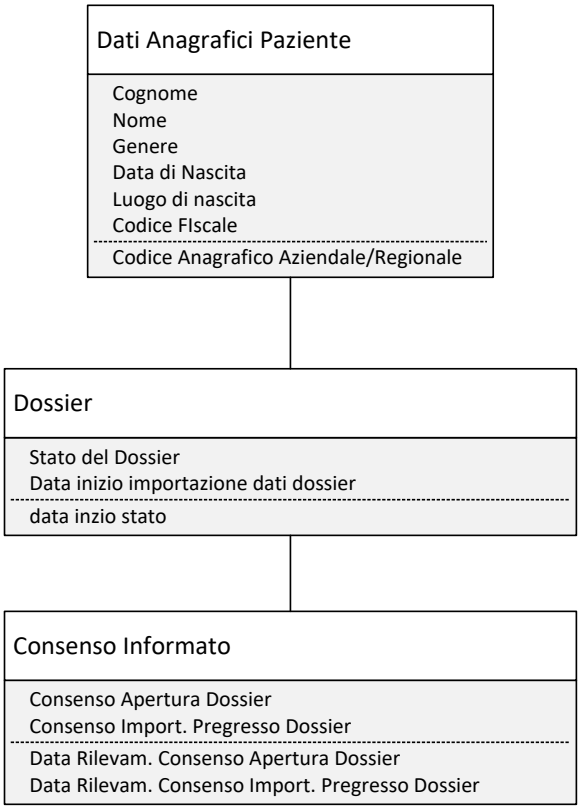


Figura 25. Information Model contenuto minimo “Consenso Importazione dati e documenti pregressi”

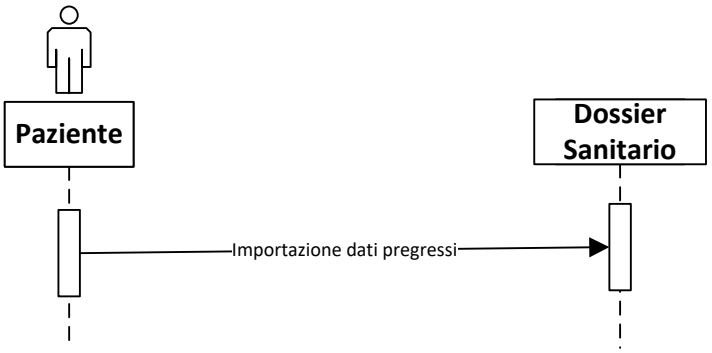


Figura 26. Interaction Model “Consenso importazione dati e documenti pregressi”

4.3.4 SC04 - Consenso per dati "a maggior tutela"

Descrizione del caso d'uso

Il presente caso d'uso, successivamente all'apertura del Dossier, permette al paziente, o al Genitore / Tutore - secondo quanto previsto dal *punto 3.1* dalle Linee guida sul Dossier sanitario - di esprimere il consenso libero ed informato al fine di concedere agli operatori sanitari di popolare il sistema del Dossier sanitario con i propri dati e documenti sanitari "a maggior tutela".

Attore Primario

Paziente.

Precondizioni

Al fine di poter esprimere il proprio consenso il paziente dovrà:

- essere identificato con idonei meccanismi che ne garantiscano l'identità,
- essere maggiorenne o sottoposto a tutela,
- essere registrato presso l'anagrafe sanitaria,
- SC02, UCM D02 Consenso Apertura Dossier sanitario.

Scenario

Il paziente, spuntando il SI nel modulo del consenso cartaceo e firmandolo *ovvero* rilasciandolo oralmente, fornisce alla struttura sanitaria il proprio consenso esplicito, libero ed informato per l'alimentazione del Dossier sanitario con i dati a maggior tutela.

Post-condizione

Il consenso all'alimentazione dei dati a maggior tutela nel Dossier sanitario viene registrato nei sistemi informatici di gestione del dossier da parte del personale addetto.

Use Case Model

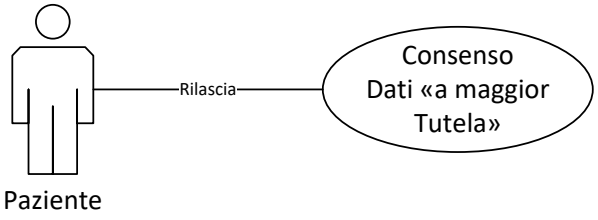


Figura 27. UCM D04 "Consenso per dati a maggior tutela"

Information Model

Lista delle informazioni da trattare:

- Dati anagrafici del paziente
- Dati del consenso

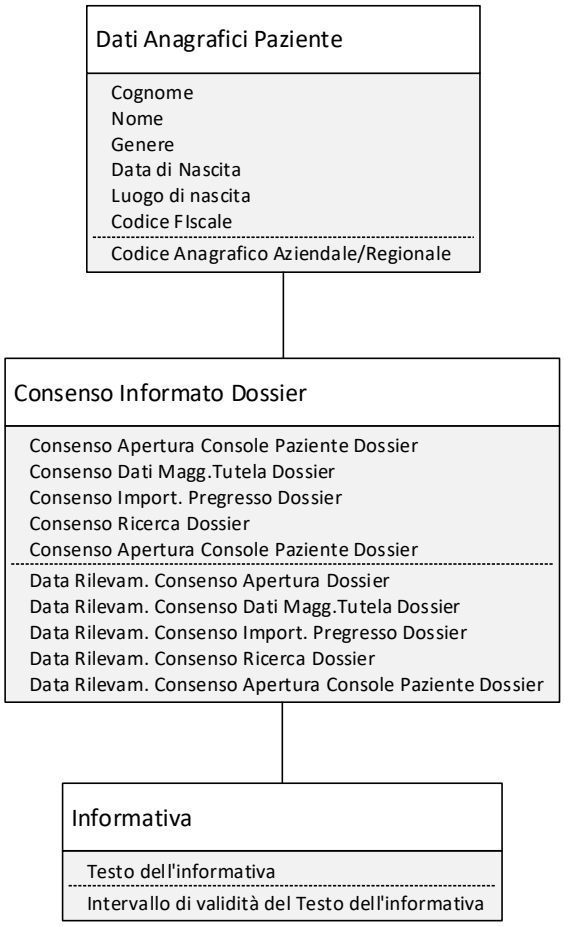


Figura 28. Information Model Generale “Consenso per dati a maggior tutela”

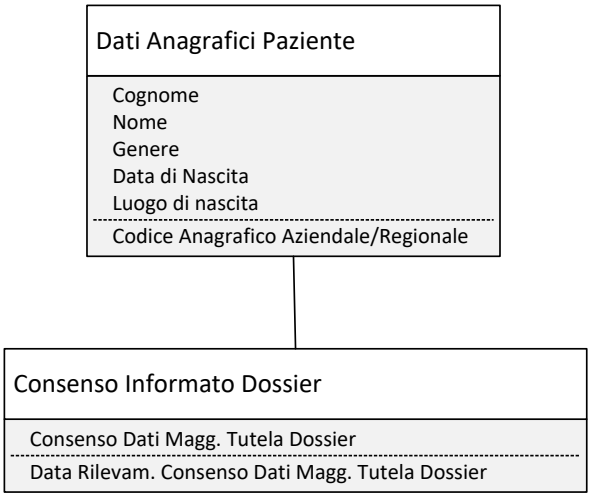


Figura 29. Information Model contenuto minimo “Consenso per dati a maggior tutela”

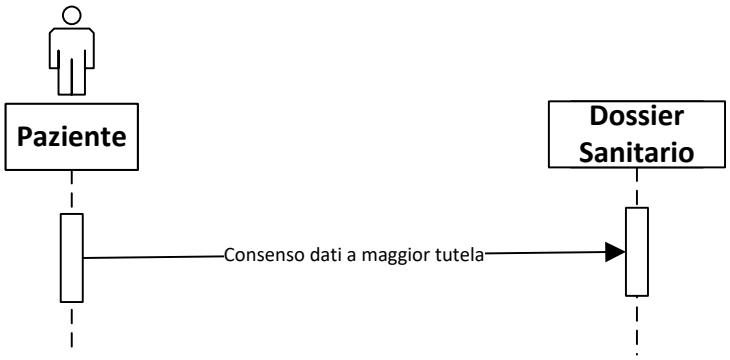


Figura 30. Interaction Model Dati a maggior tutela

4.3.5 SC05 - Consenso dati finalità di Ricerca

Descrizione del caso d'uso

Il presente caso d'uso, successivamente all'apertura del Dossier, permette al paziente – secondo quanto previsto dal *punto 3* dalle Linee guida sul Dossier Sanitario – di esprimere il proprio consenso libero ed informato al fine di concedere agli Operatori di ricerca di utilizzare il sistema del Dossier Sanitario per finalità di ricerca.

Attore Primario

Paziente.

Precondizioni

Al fine di poter esprimere il proprio consenso il paziente dovrà:

- essere identificato con idonei meccanismi che ne garantiscano l'identità,
- essere maggiorenne,
- essere registrato presso l'anagrafe sanitaria,
- SC02, UCM D02 Consenso apertura Dossier Sanitario.

Scenario

Il paziente, spuntando il SI nel modulo di consenso cartaceo e firmandolo *ovvero* rilasciandolo oralmente, fornisce alla struttura sanitaria il proprio consenso esplicito, libero ed informato per utilizzare i dati del Dossier Sanitario per finalità di ricerca.

Post-condizione

Il consenso all'utilizzo dei dati per finalità di ricerca viene registrato nei sistemi informatici di gestione del dossier da parte del personale addetto.

Use Case Model

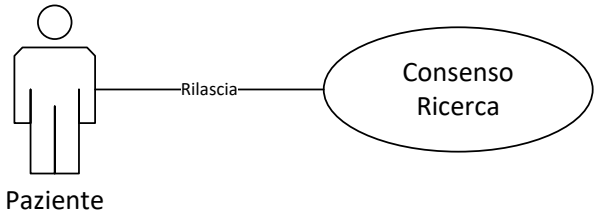


Figura 31. UCM D05 "Consenso dati finalità di Ricerca"

Information Model

Lista delle informazioni da trattare:

- Dati anagrafici del paziente
- Dati del consenso

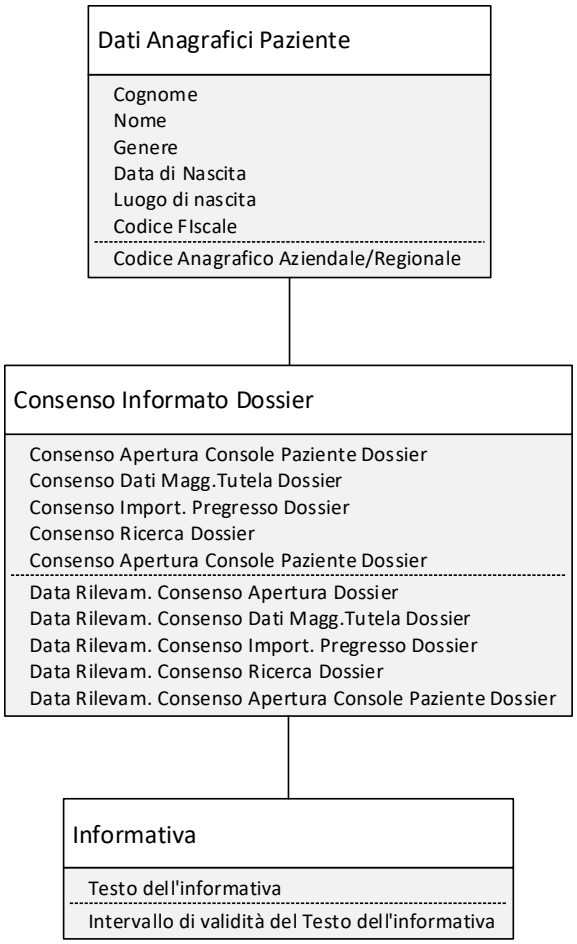


Figura 32. Information Model Generale “Consenso dati finalità di Ricerca”

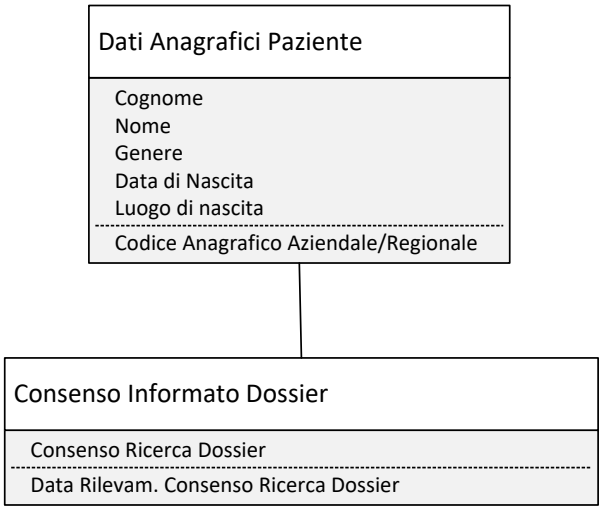


Figura 33. Information Model contenuto minimo “Consenso dati finalità di Ricerca”

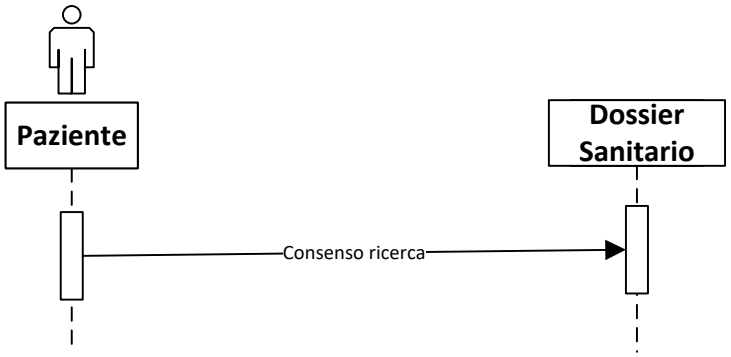


Figura 34. Interaction Model Consenso finalità di ricerca

4.3.6 SC06 - Consenso Consultazione Dossier Sanitario

Descrizione del caso d'uso

Il presente caso d'uso, contestualmente all'apertura del Dossier, permette al paziente – secondo quanto previsto dal *punto 3* dalle Linee guida sul Dossier Sanitario – di esprimere il proprio consenso libero ed informato al fine di concedere agli Operatori sanitari di consultare i propri dati e documenti sanitari presenti sul Dossier sanitario.

Attore Primario

Paziente.

Precondizioni

Al fine di poter esprimere il proprio consenso il paziente dovrà:

- essere identificato con idonei meccanismi che ne garantiscano l'identità,
- essere maggiorenne,
- essere registrato presso l'anagrafe sanitaria,
- SC02, UCM D02 Consenso Apertura Dossier sanitario,
- Essere in possesso del codice fiscale dell'Operatore sanitario da abilitare.

Scenario

Il paziente, compilando con i propri dati anagrafici e spuntando il SI/NO nel modulo di consenso cartaceo e firmandolo *ovvero* rilasciandolo oralmente, fornisce alla Struttura sanitaria un consenso esplicito, libero ed informato per la consultazione del Dossier sanitario da parte di un operatore sanitario indicato nel modulo.

Post-condizione

Il consenso alla consultazione del Dossier sanitario viene registrato nei sistemi informatici di gestione del dossier da parte del personale addetto.

Use Case Model

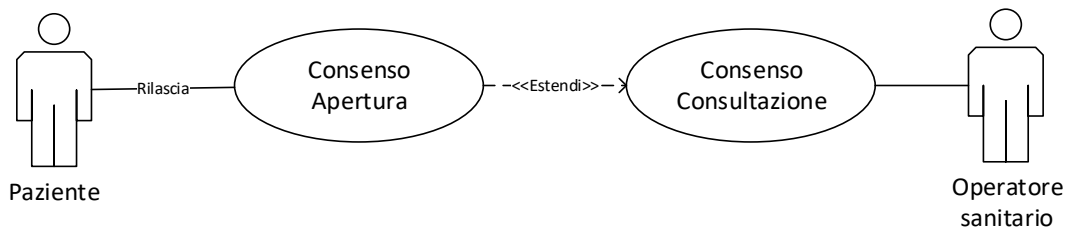


Figura 35. UCM D06 "Consenso Consultazione Dossier sanitario"

Information Model

Lista delle informazioni da trattare:

- Dati anagrafici del paziente
- Dati del consenso
- Dati del medico

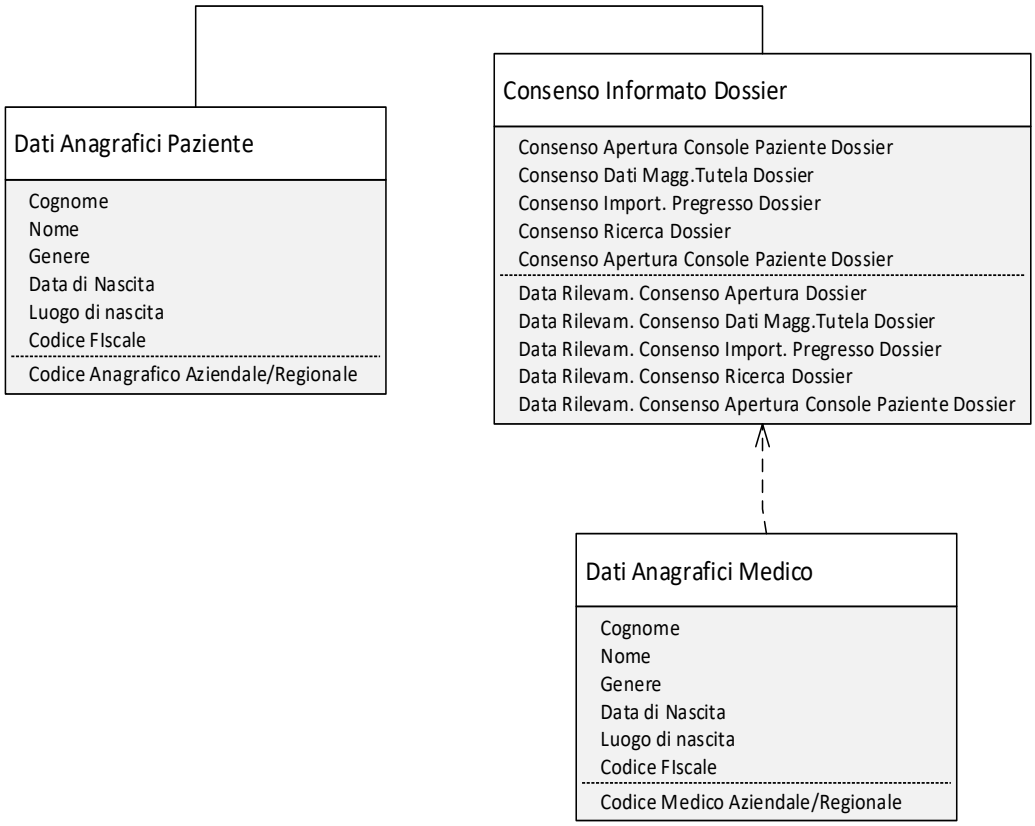


Figura 36. Information Model Generale "Consenso Consultazione Dossier sanitario"

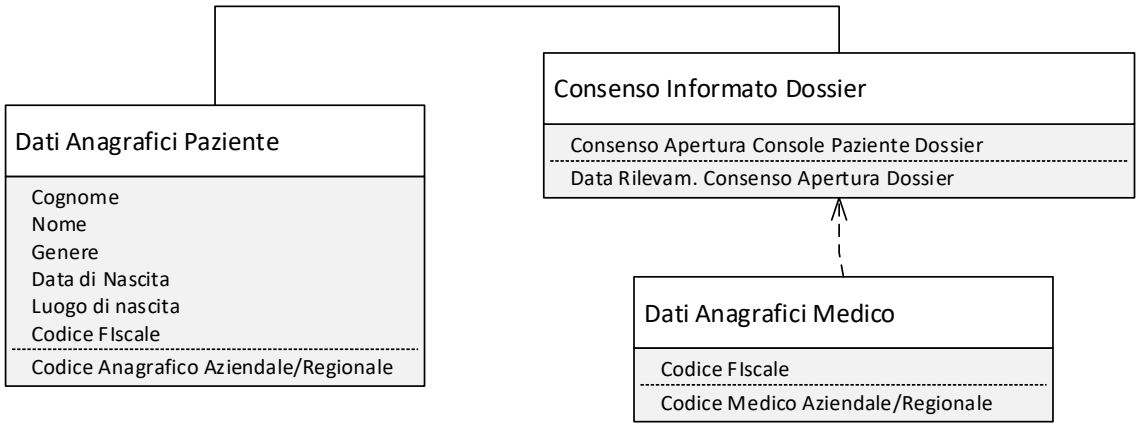


Figura 37. Information Model contenuto minimo “Consenso Consultazione Dossier sanitario”

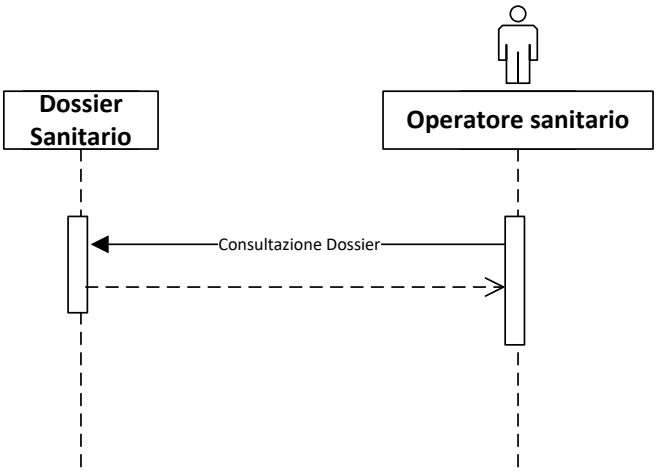


Figura 38. Interaction Model “Consultazione Dossier sanitario”

4.3.7 SC07 - Consenso consultazione "Console del paziente"

Descrizione del caso d'uso

Il presente caso d'uso, contestualmente all'apertura del Dossier, permette al paziente - secondo quanto previsto dal *punto 3* dalle Linee guida sul Dossier Sanitario - di esprimere il proprio consenso libero ed informato al fine di concedere agli Operatori sanitari di consultare i propri dati e documenti sanitari presenti in un area personale *ad hoc*, denominata "Console del paziente", da lui alimentata e presente nel Dossier Sanitario.

Attore Primario

Paziente.

Precondizioni

Al fine di poter esprimere il proprio consenso il paziente dovrà:

- essere identificato con idonei meccanismi che ne garantiscano l'identità,
- essere maggiorenne,
- essere registrato presso l'anagrafe sanitaria,
- SC02, UCM D02 Consenso Apertura Dossier Sanitario.

Scenario

Il paziente, compilando con i propri dati anagrafici e spuntando il SI/NO nel modulo di consenso cartaceo e firmandolo *ovvero* rilasciandolo oralmente, fornisce alla Struttura sanitaria un consenso esplicito, libero ed informato per la consultazione della "console del paziente" contenuta in un area *ad hoc* del Dossier sanitario.

Post-condizione

Il consenso alla consultazione della console del paziente viene riportato nei sistemi informatici di gestione del dossier da parte del personale addetto.

Use Case Model

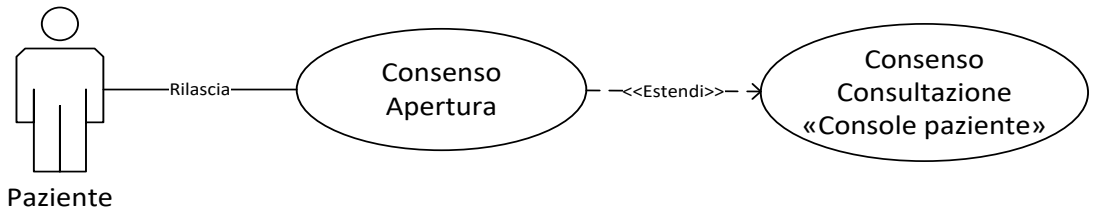


Figura 39. UCM D07 “Consenso Consultazione console paziente”

Information Model

Lista delle informazioni da trattare:

- Dati anagrafici del paziente
- Dati del consenso

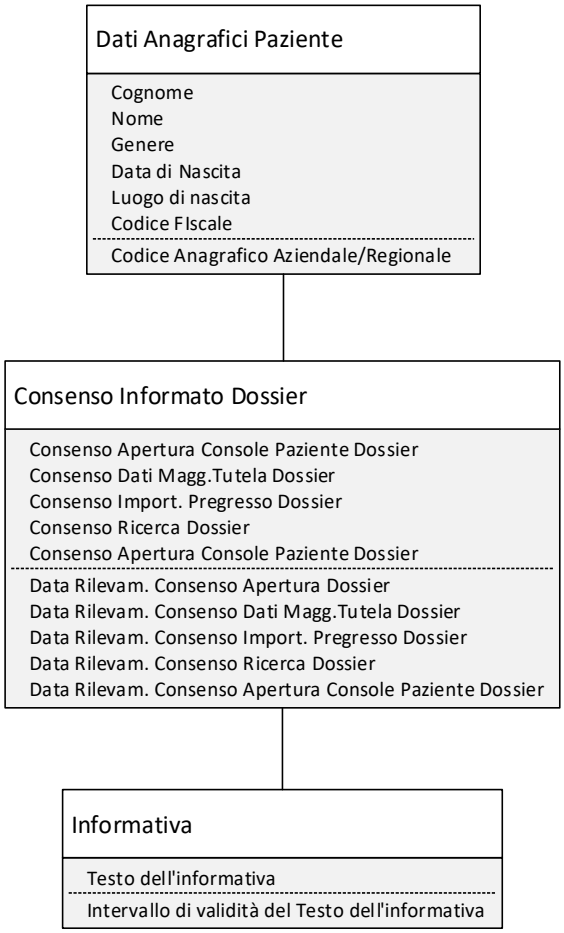


Figura 40. Information Model Generale “Consenso Consultazione Console paziente”

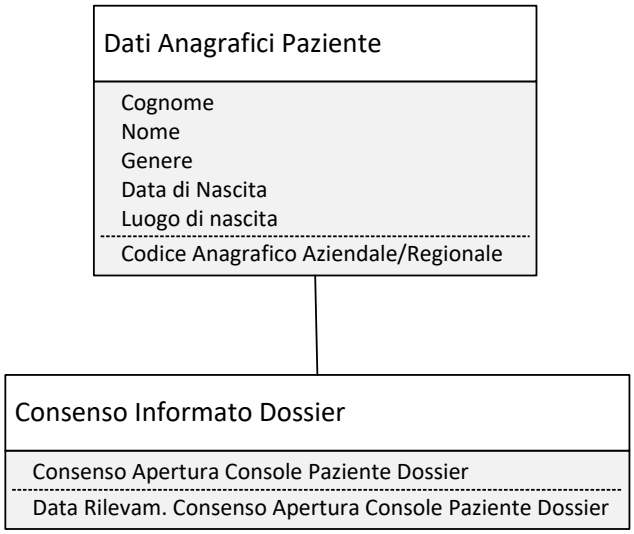


Figura 41. Information Model contenuto minimo “Consenso Consultazione Console paziente”

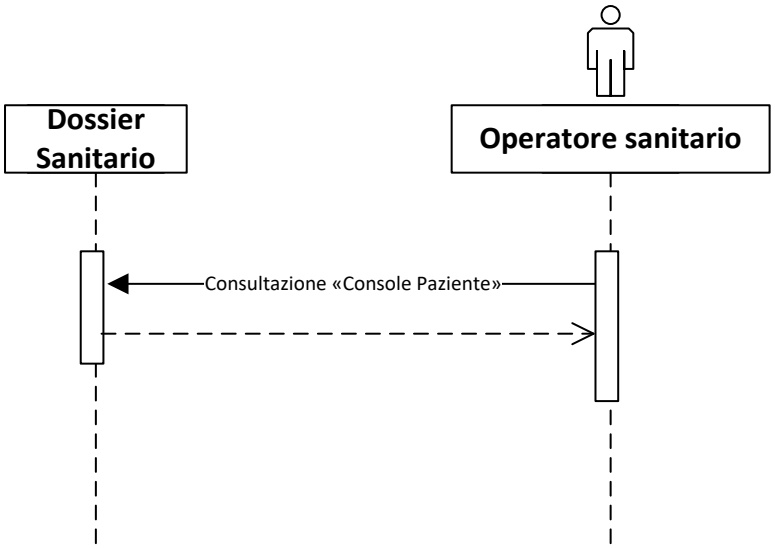


Figura 42 Interaction Model “Consultazione Console paziente”

4.3.8 SC08 - Consultazione del Dossier da parte dell'Operatore sanitario

Descrizione del caso d'uso

Il presente caso d'uso permette ai singoli operatori sanitari (medici, infermieri, tecnici, ecc) coinvolti nel processo di cura del paziente e incaricati dal titolare del Dossier, di consultare i dati e i referti presenti e trascorsi legati allo specifico percorso diagnostico-terapeutico, contenuti nel Dossier sanitario.

Attore Primario

Operatore sanitario.

Precondizioni

Al fine di poter consultare i dati e i documenti il professionista sanitario deve:

- essere incaricato nel trattamento dati Dossier,
- SC02, UCM D02 Consenso Apertura Dossier sanitario.

Scenario

I singoli Operatori sanitari che prenderanno in cura il paziente potranno consultare il Dossier sanitario con i vari referti sanitari in esso contenuti. Tuttavia, avranno a disposizioni le sole informazioni rese in quel momento dal paziente stesso (ad es., raccolta dell'anamnesi e delle informazioni relative all'esame della documentazione diagnostica prodotta) e quelle relative a precedenti prestazioni erogate se resi consultabili dal paziente.

Post-condizione

Nessuna.

Use Case Model

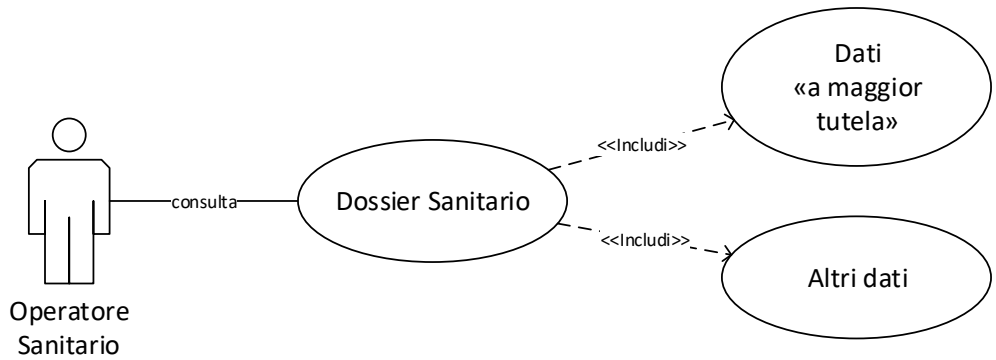


Figura 43. UCM D08 "Consultazione del Dossier da parte dell'Operatore sanitario"

Information Model

Lista delle informazioni da trattare:

- Dati anagrafici del paziente
- Dati del consenso
- Dati del Medico operatore

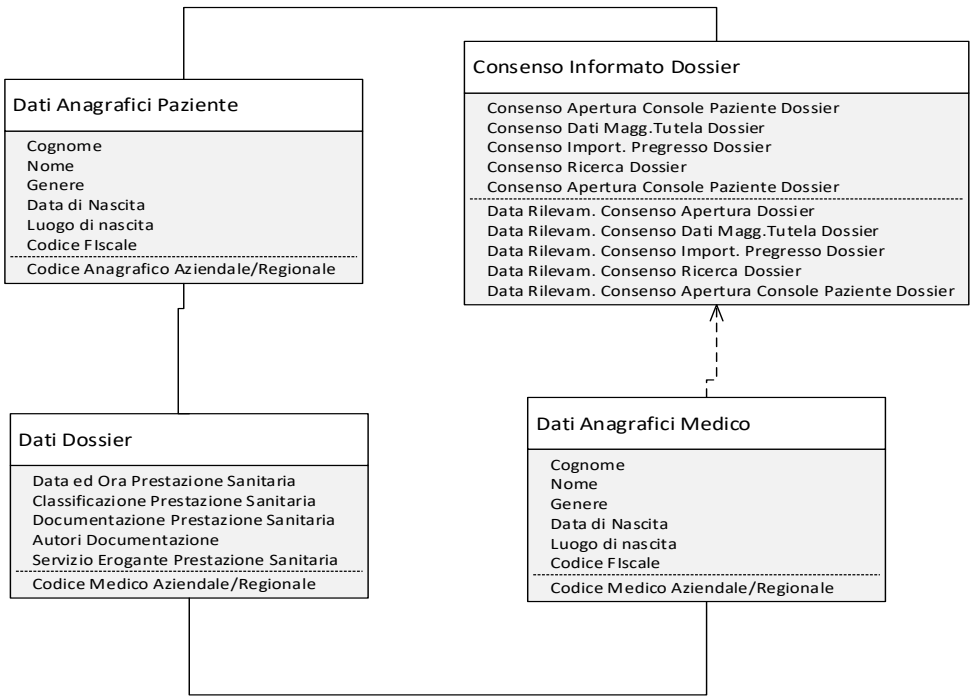


Figura 44. Information Model Generale “Consultazione del Dossier da parte dell’Operatore sanitario”

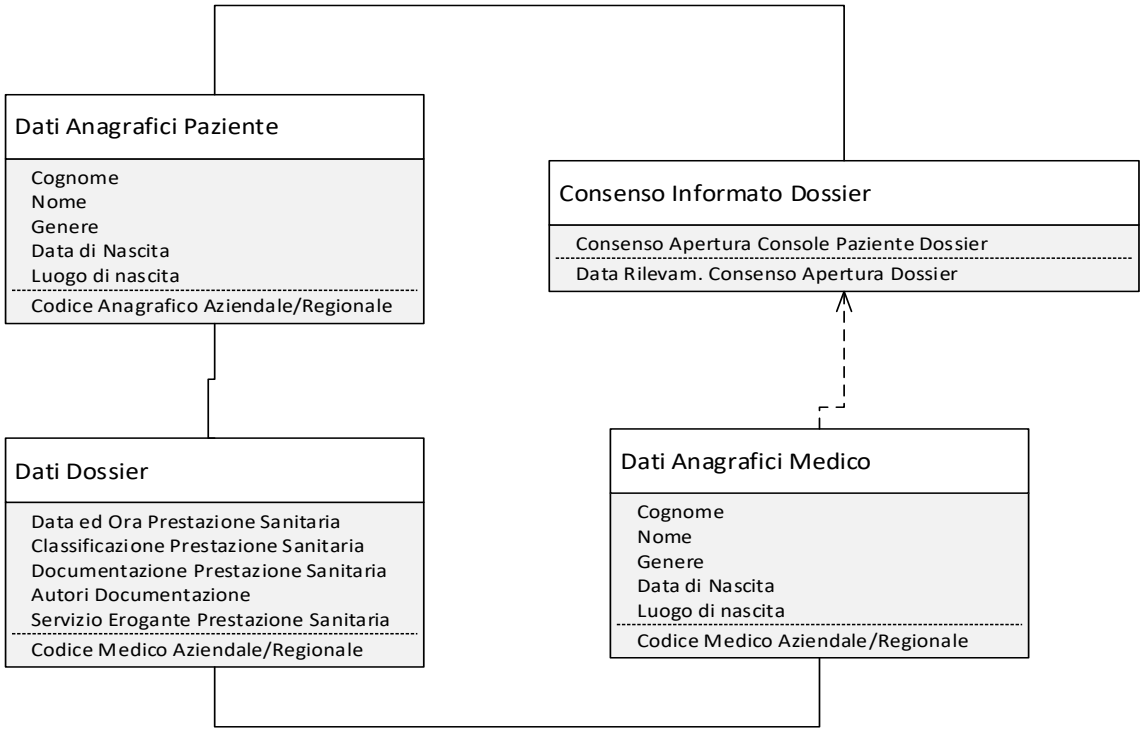


Figura 45. Information Model contenuto minimo "Consultazione del Dossier da parte dell'Operatore sanitario"

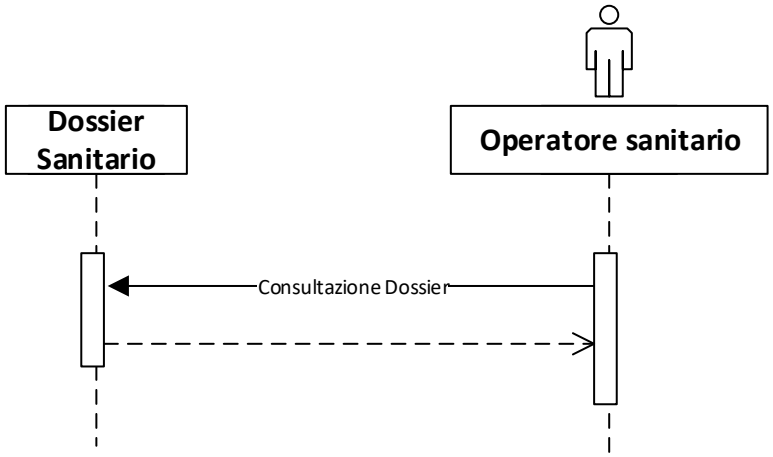


Figura 46. Interaction Model "Consultazione del Dossier da parte dell'Operatore sanitario"

4.3.9 SC09 - Alimentazione sistemi informatici

Descrizione del caso d'uso

Il presente caso d'uso permette all'Operatore sanitario, acquisito il consenso libero ed informato del paziente, di inviare al Dossier sanitario, tramite apposito Sistema informatico clinico-sanitario, i dati e i documenti sanitari dello specifico percorso diagnostico.

Attore Primario

Operatore Sanitario, Sistema informatico clinico-sanitario.

Precondizioni

Al fine di poter procedere all'alimentazione del dossier:

- Il paziente dovrà essere registrato presso l'anagrafe sanitaria,
- la struttura sanitaria dovrà avere appositi sistemi informatici interoperabili con il Dossier sanitario,
- SC02, UCM D02 Consenso Apertura Dossier Sanitario.

Scenario

I singoli medici che prenderanno in cura il paziente potranno alimentare il Dossier con i vari documenti sanitari prodotti tramite il Sistema informatico clinico-sanitario.

Post-condizione

Il Dossier Sanitario è alimentato con tutti i documenti sanitari prodotti durante lo specifico processo di cura e saranno, sulla base di determinate condizioni, consultabili dai medici che hanno in cura il paziente.

Use Case Model

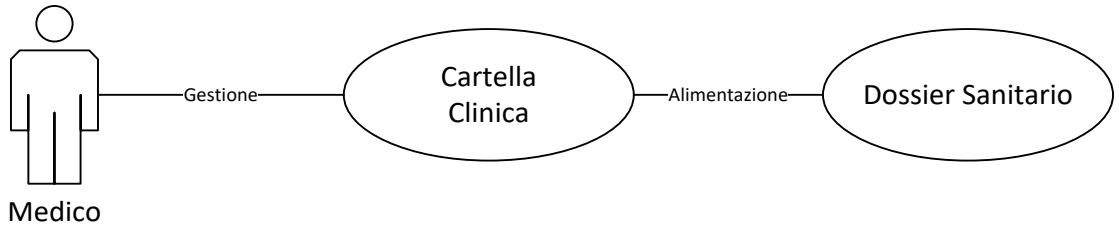


Figura 47. UCM D09 "Alimentazione sistemi informativi"

Information Model

Lista delle informazioni da trattare:

- Dati anagrafici del paziente
- Dati e documenti clinici
- Medico operatore

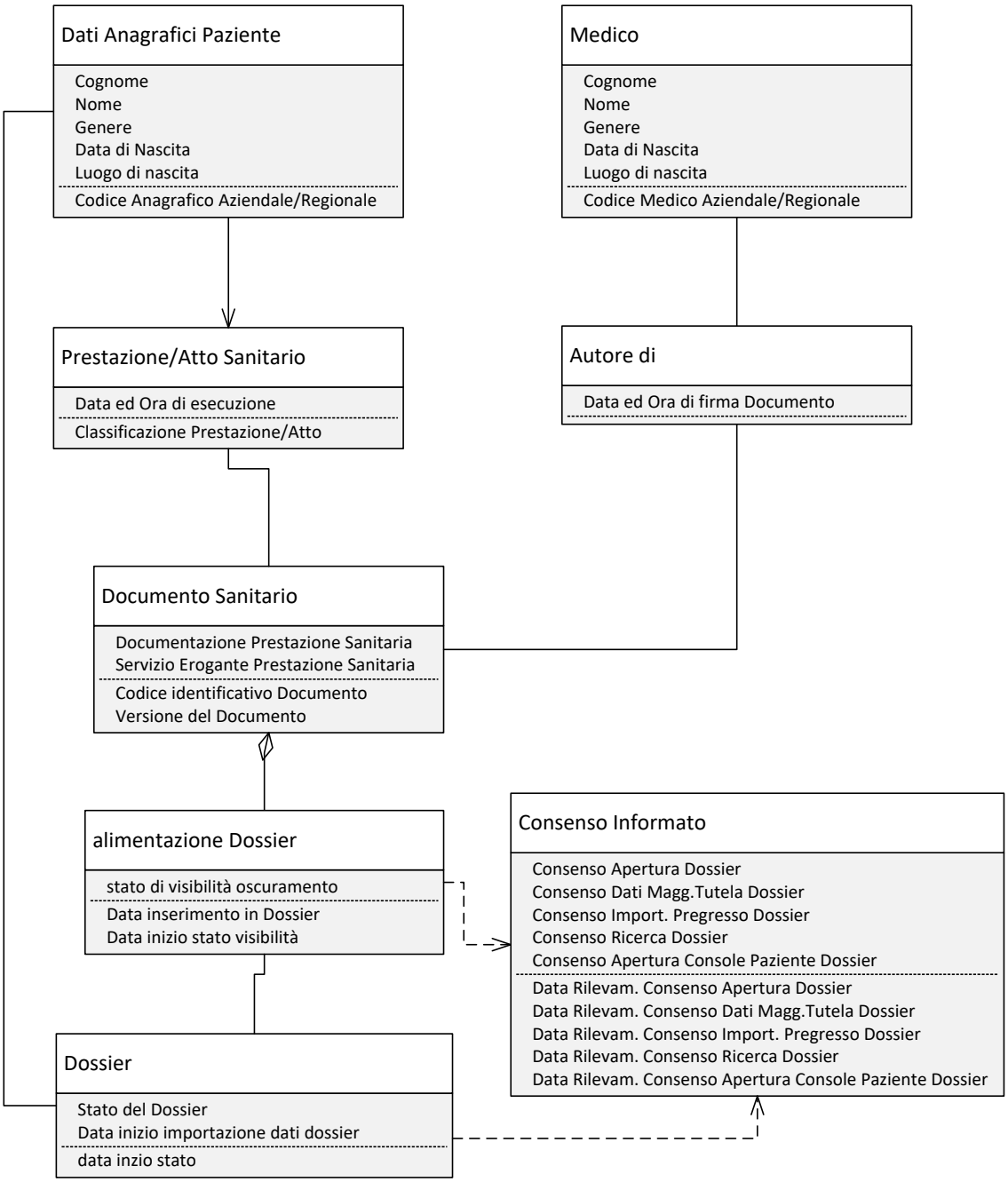


Figura 48. Information Model Generale “Alimentazione sistemi informativi”

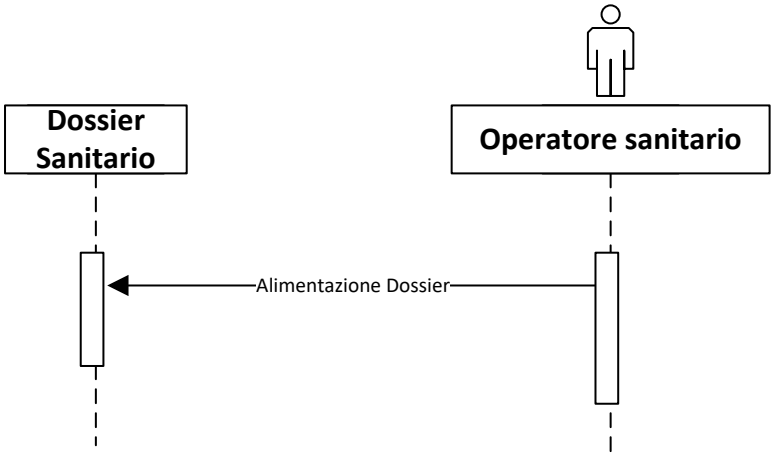


Figura 49. Interaction Model “Alimentazione sistemi informativi”

4.3.10 SC10 - Verifica esistenza dei dati del paziente

Descrizione del caso d'uso

Il presente caso d'uso - secondo quanto previsto dal *punto 5* dalle Linee guida sul Dossier Sanitario - permette al paziente ottenere la conferma circa l'esistenza o meno nel Dossier sanitario di dati che lo riguardano, la loro comunicazione in forma intelligibile, l'indicazione della loro origine, delle finalità e modalità del trattamento (art. 7, comma 1 e 2, lett. a) e b), del Codice).

Attore Primario

Paziente.

Precondizioni

Al fine di poter presentare istanza *ex* art. 7 del Codice privacy, il paziente dovrà:

- il paziente sarà identificato con idonei meccanismi che ne garantiscano l'identità,
- essere maggiorenne,
- essere registrato presso l'anagrafe sanitaria,
- SC02, UCM D02 Consenso Apertura Dossier Sanitario.

Scenario

Il paziente esprime la sua necessità di verificare quali dati e/o documenti sono contenuti nel suo Dossier Sanitario.

Post-condizione

Nessuna.

Use Case Model

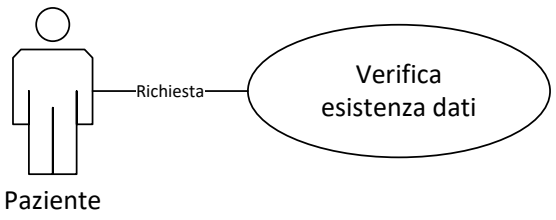


Figura 50. UCM D10 "Verifica esistenza dei dati del paziente"

Information Model

Lista delle informazioni da trattare:

- Dati anagrafici del paziente
- Dati e documenti clinici
- Medico operatore

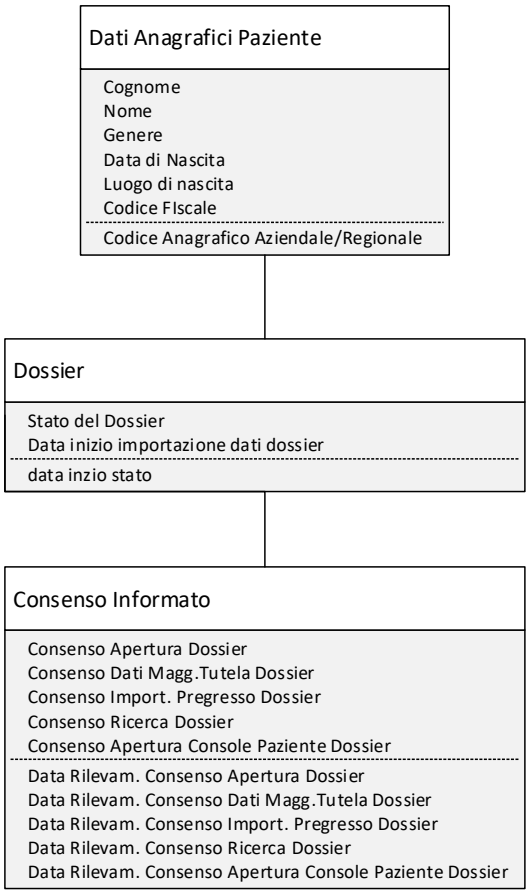


Figura 51. Information Model Generale “Verifica esistenza dati del paziente”

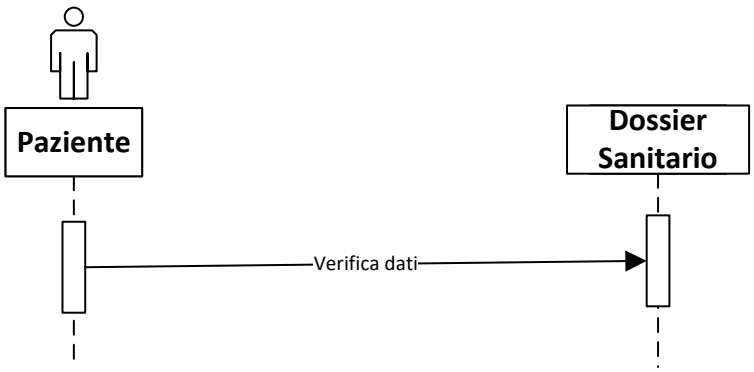


Figura 52. Interaction Model “Verifica esistenza dati del paziente”

4.3.11 SC11 - Revoca Apertura Dossier

Descrizione del caso d'uso

Il presente caso d'uso permette al paziente - secondo quanto previsto dal *punto 3* dalle Linee guida sul Dossier Sanitario - di revocare il proprio consenso libero ed informato all'implementazione da parte degli Operatori sanitari del Dossier Sanitario, interrompendo così il conferimento dei dati e dei documenti sanitari.

Attore Primario

Paziente.

Precondizioni

Al fine di poter revocare il proprio consenso il paziente dovrà:

- essere identificato con idonei meccanismi che ne garantiscano l'identità,
- essere maggiorenne,
- essere registrato presso l'anagrafe sanitaria,
- SC2, UCM D2 Consenso apertura.

Scenario

Il paziente esprime la sua necessità di revocare il consenso al Dossier Sanitario.

Post-condizione

Revocato lo stato del consenso, il sistema automaticamente non sarà più alimentabile con nuove e successive prestazioni sanitarie e consultabile da parte degli Operatori sanitari precedentemente autorizzati. Tuttavia, anche in caso di revoca, il Dossier potrà essere alimentato - da eventuali correzioni dei dati e dei documenti che lo hanno composto fino alla revoca del consenso – e consultato solamente da parte degli organismi sanitari che hanno generato tali dati e documenti e che mantengono la titolarità su di essi.

Use Case Model

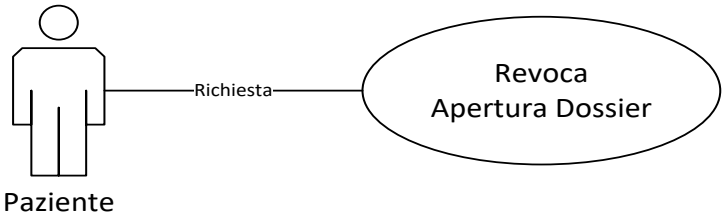


Figura 53. UCM D11 “Revoca apertura dossier”

Information Model

Lista delle informazioni da trattare:

- Dati anagrafici del paziente
- Dati del consenso

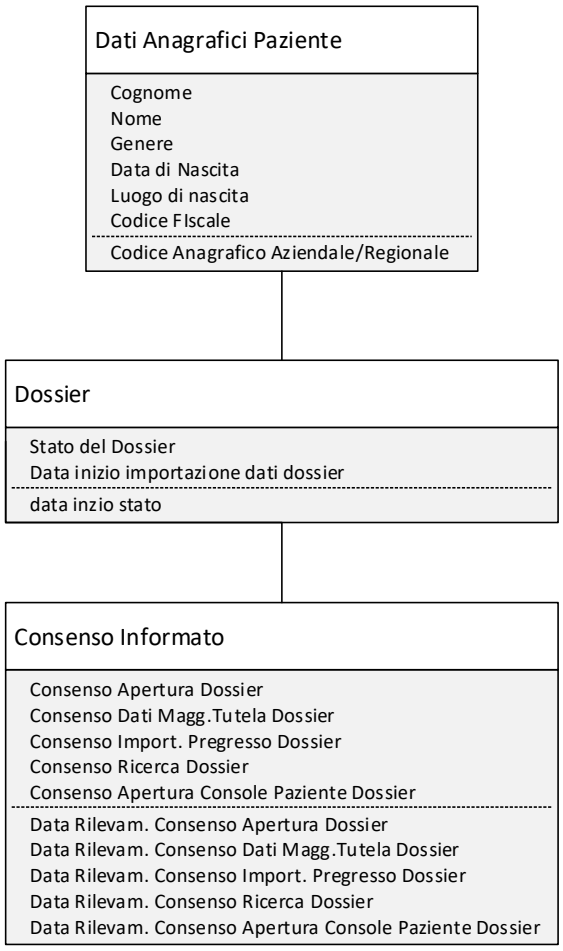


Figura 54. Information Model Generale “Revoca apertura dossier”

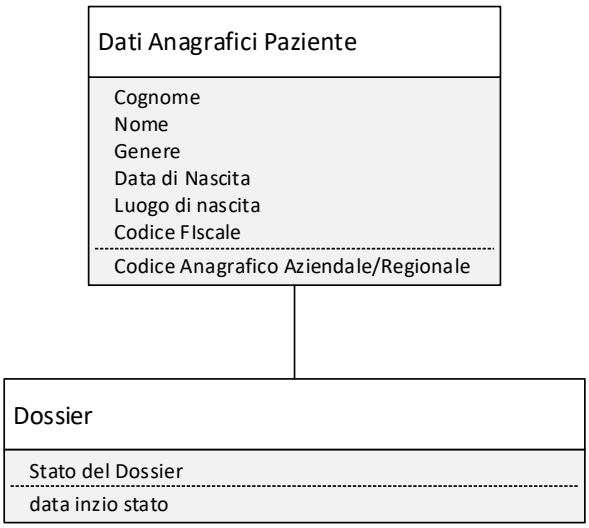


Figura 55. Information Model contenuto minimo “Revoca apertura dossier”

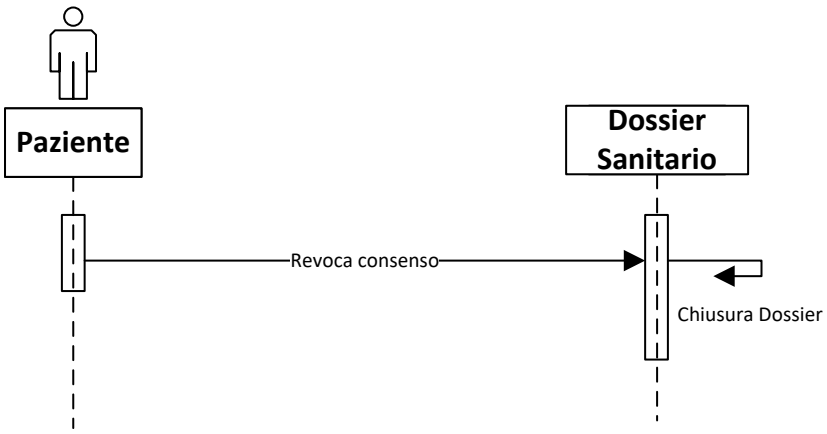


Figura 56. Interaction Model “Revoca apertura dossier”

4.3.12 SC12 – Decesso del Paziente

Descrizione del caso d'uso

Il presente caso d'uso analizza la chiusura del Dossier Sanitario al decesso del paziente.

Attore Primario

Paziente, Titolare del dossier.

Precondizioni

Per poter procedere alla chiusura del Dossier il paziente dovrà:

- Il titolare del dossier viene informato sul decesso del paziente,
- essere identificato con idonei meccanismi che ne garantiscano l'identità,
- SC02, UCM D02 Consenso apertura.

Scenario

Entro 30 giorni dalla ricezione della notizia del decesso, il Titolare del trattamento provvederà a chiudere il dossier del paziente deceduto.

Post-condizione

Il Dossier sanitario automaticamente non sarà più alimentabile dall'Operatore sanitario, ma rimarrà secondo quando previsto dall'art. 9, comma 3, del Codice Privacy: *"consultabile da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione"*.

Use Case Model

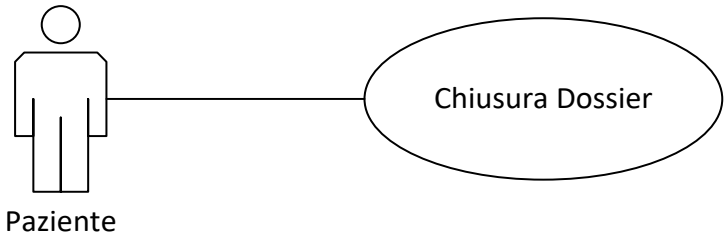


Figura 57. UCM D12 "Decesso del paziente"

Information Model

Lista delle informazioni da trattare:

- Dati anagrafici del paziente
- Dati del consenso

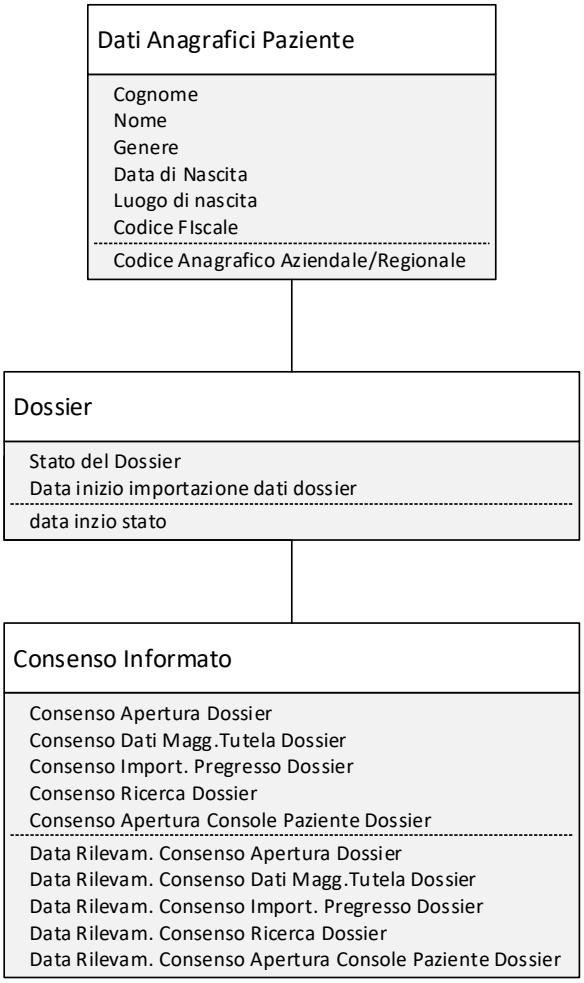


Figura 58. Information Model Generale “Decesso del paziente”

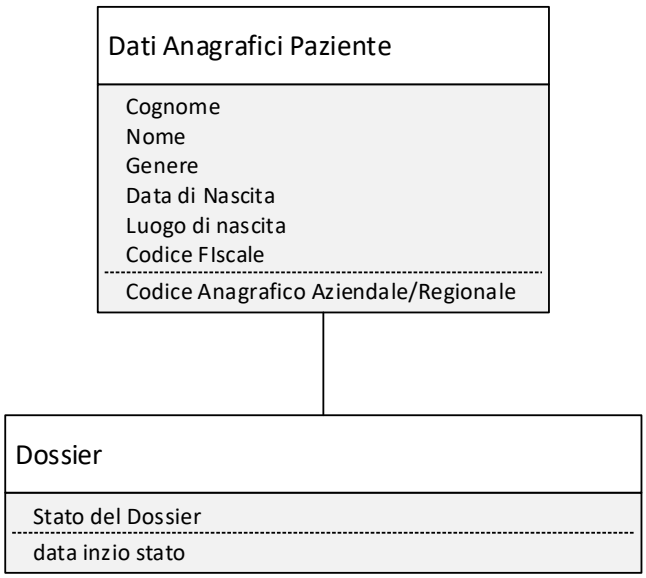


Figura 59. Information Model contenuto minimo “Decesso del paziente”

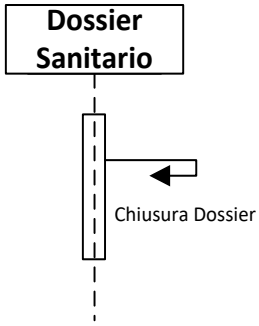


Figura 60. Interaction Model “Decesso paziente”

4.3.13 SC13 - Annullamento Dossier

Descrizione del caso d'uso

Il presente caso d'uso permette di eliminare un Dossier sanitario creato, dall'Operatore sanitario, a causa di una errata identificazione del soggetto interessato o su un paziente di prova.

Attore Primario

Operatore sanitario.

Precondizioni

- SC02, UCM D02 Consenso apertura,
- SC10, UCM D10 Verifica esistenza dei dati del paziente.

Scenario

In seguito a controlli o su segnalazione del paziente si rileva un errore da parte dell'Operatore che ha acquisito il consenso all'apertura del dossier. E' stato, infatti, attivato un dossier sanitario ad un soggetto che non corrisponde alla persona interessata che ha rilasciato il consenso. Pertanto si procede all'annullamento del dossier comprensivo dei contenuti.

Post-condizione

Annullato il dossier il sistema automaticamente non lo renderà più disponibile per usi successivi.

Use Case Model

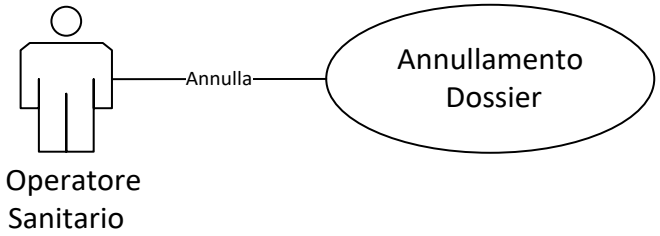


Figura 61. UCM D13 "Annullamento Dossier"

Information Model

Lista delle informazioni da trattare:

- Dati anagrafici del paziente

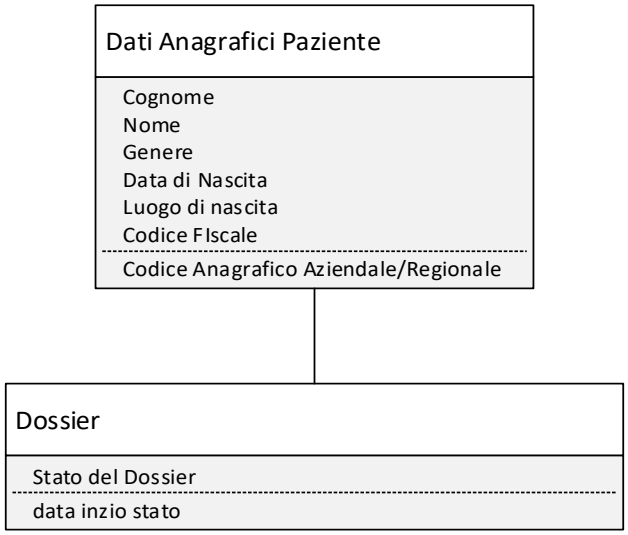


Figura 62 Information Model Generale "Annullamento Dossier"

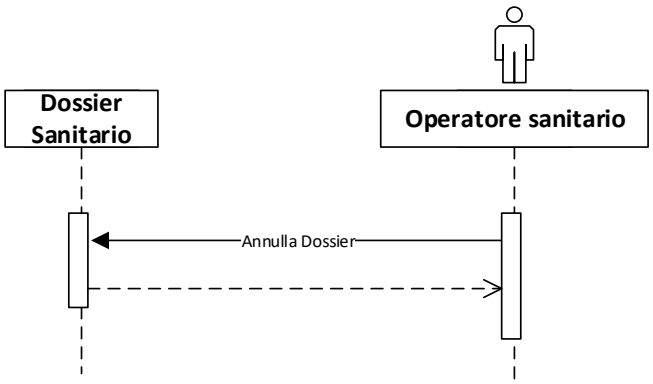


Figura 63. Interaction Model "Annullamento Dossier"

4.3.14 SC14 – Richiesta oscuramento dei dati

Descrizione del caso d'uso

Il presente caso d'uso – secondo quanto previsto dal *punto 5.1* delle Linee guida del Dossier sanitario – permette al paziente di modificare selettivamente il proprio consenso libero ed informato alla consultazione dei dati e dei documenti contenuti nel Dossier. In altri termini il paziente potrà decidere e specificare che un determinato dato o documento sanitario oggetto del trattamento sia "oscurato" e pertanto reso non consultabile ai professionisti che non hanno contribuito a generarlo.

Attore Primario

Paziente.

Precondizioni

Al fine di poter revocare il proprio consenso il paziente dovrà:

- essere identificato con idonei meccanismi che ne garantiscano l'identità,
- essere maggiorenne,
- SC02, UCM D02 Consenso apertura,
- SC09, UCM D09 Alimentazione sistemi informativi.

Scenario

Il paziente esprime tramite modulo cartaceo la sua volontà di oscurare specifici documenti contenuti nel Dossier Sanitario. I documenti vengono indicati dal paziente tramite il tipo di prestazione e la data di effettuazione. L'operatore incaricato del titolare a gestire gli oscuramenti prende in carico il modulo firmato dal paziente e modifica in relazione a questi sul sistema informatico di gestione del Dossier la visibilità dei documenti indicati dal paziente.

Post-condizione

Impostati i criteri selettivi di visibilità dei dati il sistema automaticamente negherà la possibilità di consultare i documenti al professionista che non li ha generati.

Use Case Model

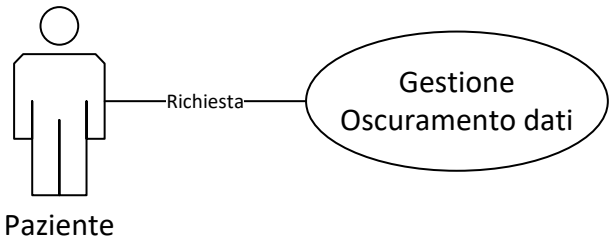


Figura 64. UCM D14 “Richiesta accesso e oscuramento dei dati”

Information Model

Lista delle informazioni da trattare:

- Dati anagrafici del paziente.
- Dati esame/visita/ricovero da oscurare

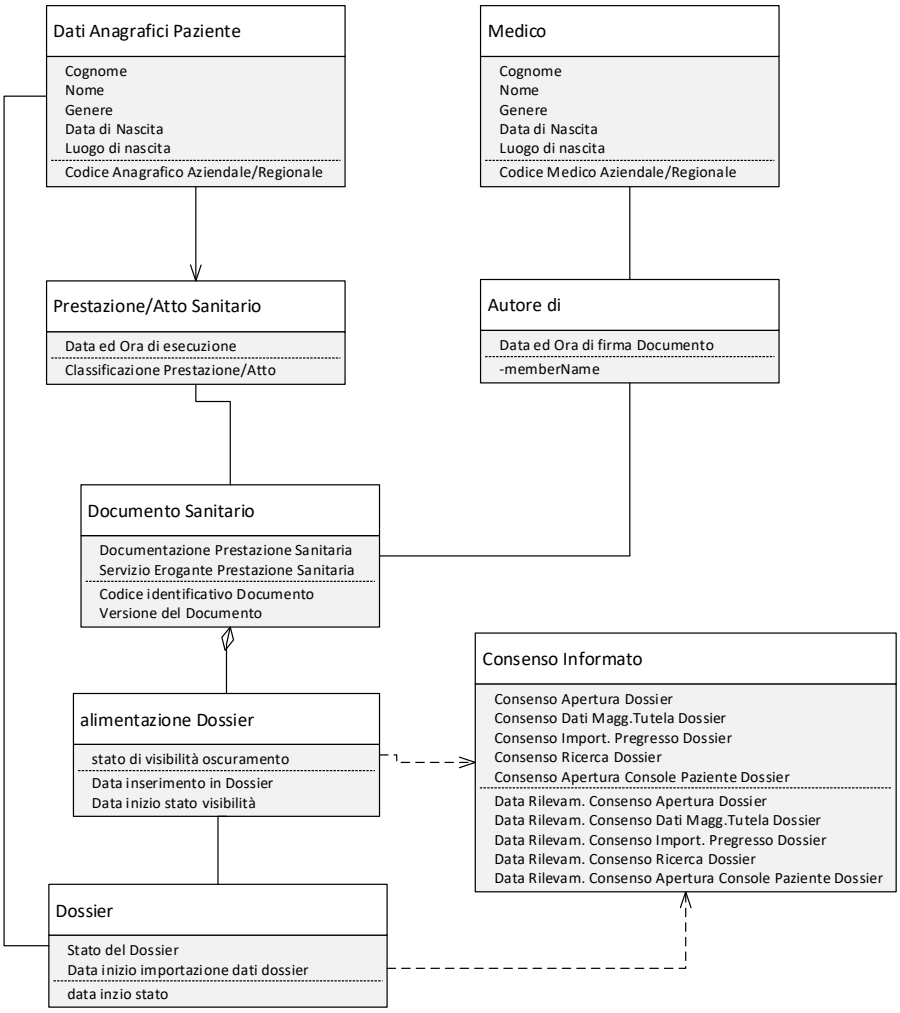


Figura 65. Information Model Generale “Richiesta oscuramento dei dati”

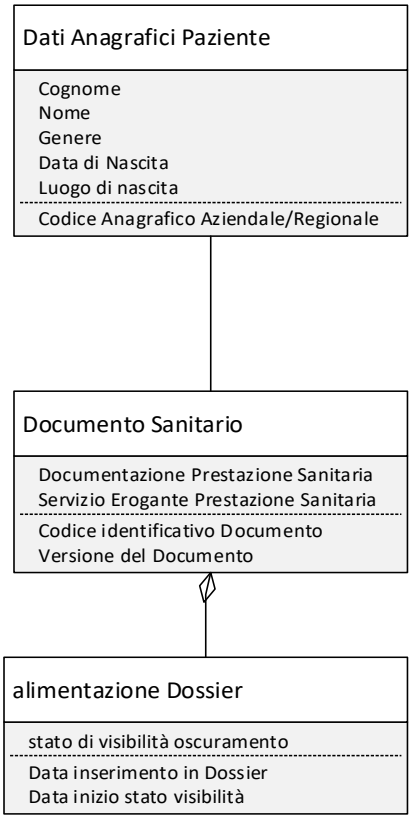


Figura 66. Information Model contenuto minimo “Richiesta oscuramento dei dati”

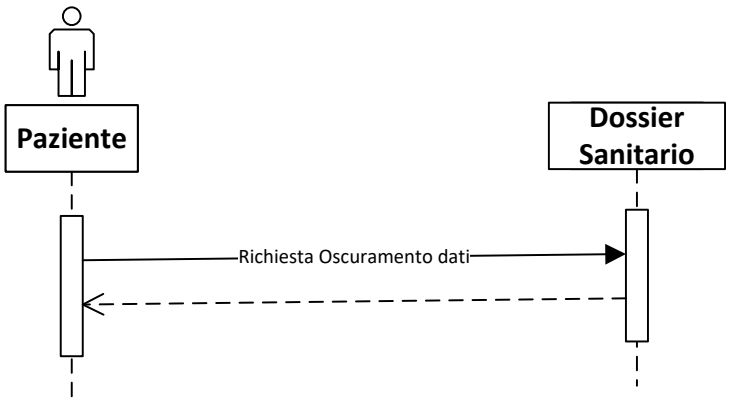


Figura 67. Interaction Model “Richiesta oscuramento dati”

4.3.15 SC15 – Gestione Dati oscurati

Descrizione del caso d'uso

Il presente caso d'uso – alla luce del *punto 5.1* delle Linee guida del Dossier sanitario – obbliga l'Operatore sanitario, a fronte di una specifica e libera manifestazione di volontà del paziente, o dal Genitore / Tutore, ad oscurare i dati o i documenti sanitari non rendendoli, pertanto, consultabili ai soggetti abilitati all'accesso al Dossier sanitario.

Attore Primario

Operatore sanitario.

Precondizioni

Al fine di poter impostare i criteri di visibilità l'Operatore sanitario dovrà:

- SC14, UCM D014 – Richiesta accesso e oscuramento dei dati.

Scenari

Scenario 1:

Il paziente non ha richiesto l'oscuramento di nessun dato.

Scenario 2:

Impostato – secondo la volontà del paziente – l'oscuramento su un referto X, il sistema automaticamente negherà all'Operatore sanitario di consultare tale referto, non presentandolo neppure come oscurato.

Scenario 3:

Impostato – secondo la volontà del paziente – l'oscuramento su un referto X, il sistema automaticamente permetterà la visualizzazione al solo Operatore sanitario che ha elaborato, ovvero prodotto o partecipato alla catena di produzione per trattamenti non anonimizzati, il referto da lui prodotto.

Post-condizione

Nessuna.

Use Case Model

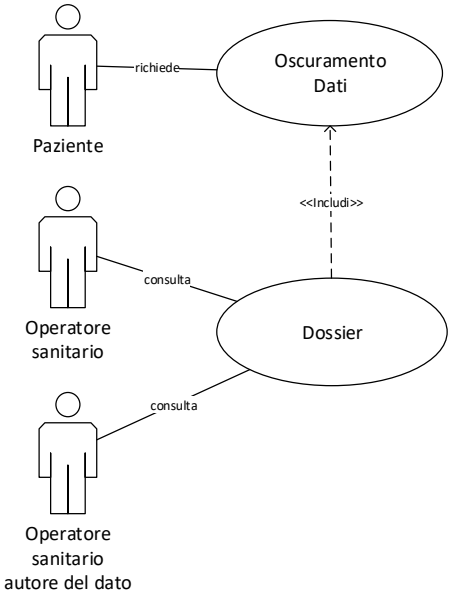


Figura 68. UCM D15 “Gestione dati oscurati”

Information Model

Lista delle informazioni da trattare:

- Dati anagrafici del paziente
- Dati del consenso
- Dati del Medico operatore

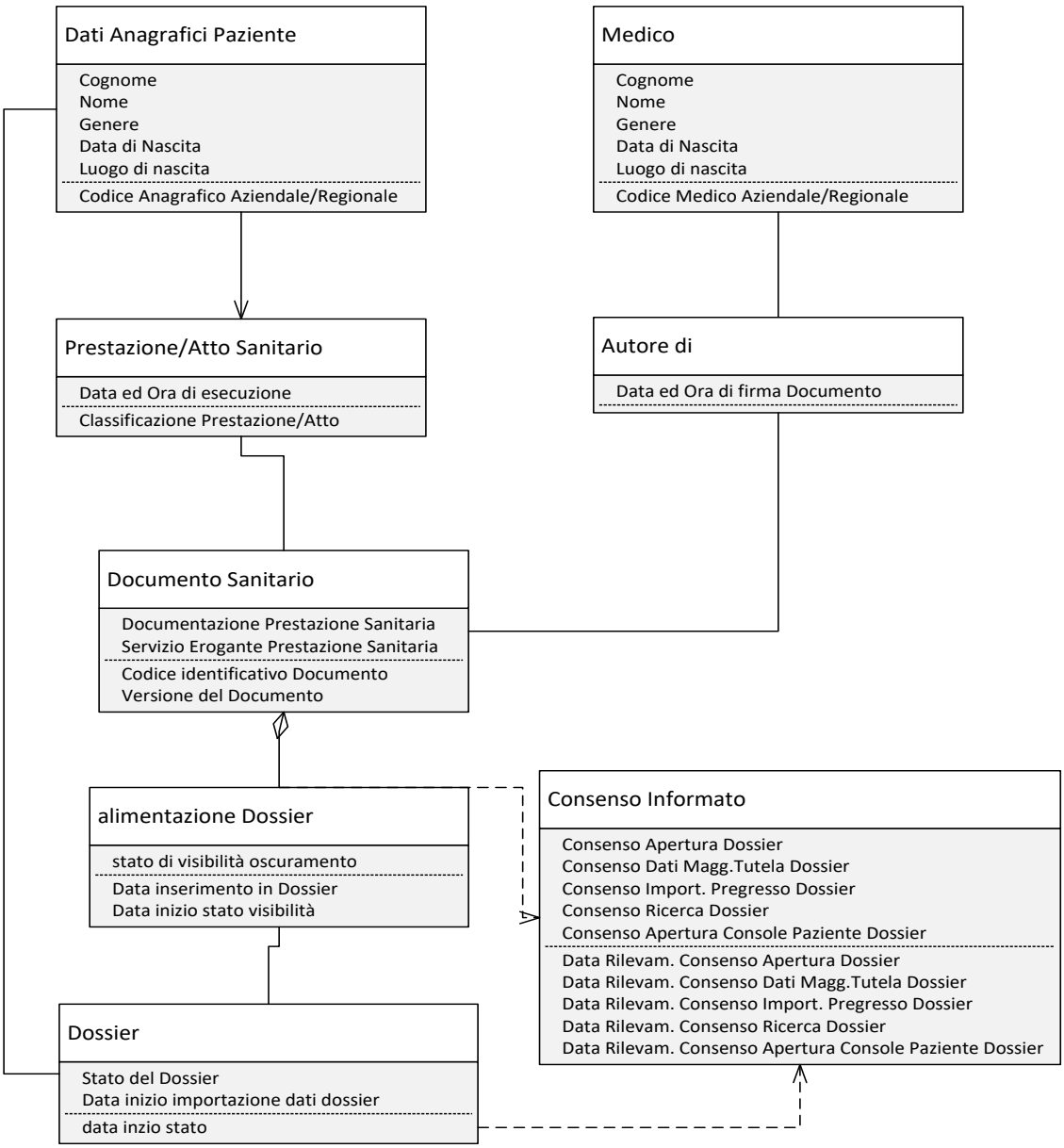


Figura 69. Information Model Generale “Gestione dati oscurati”

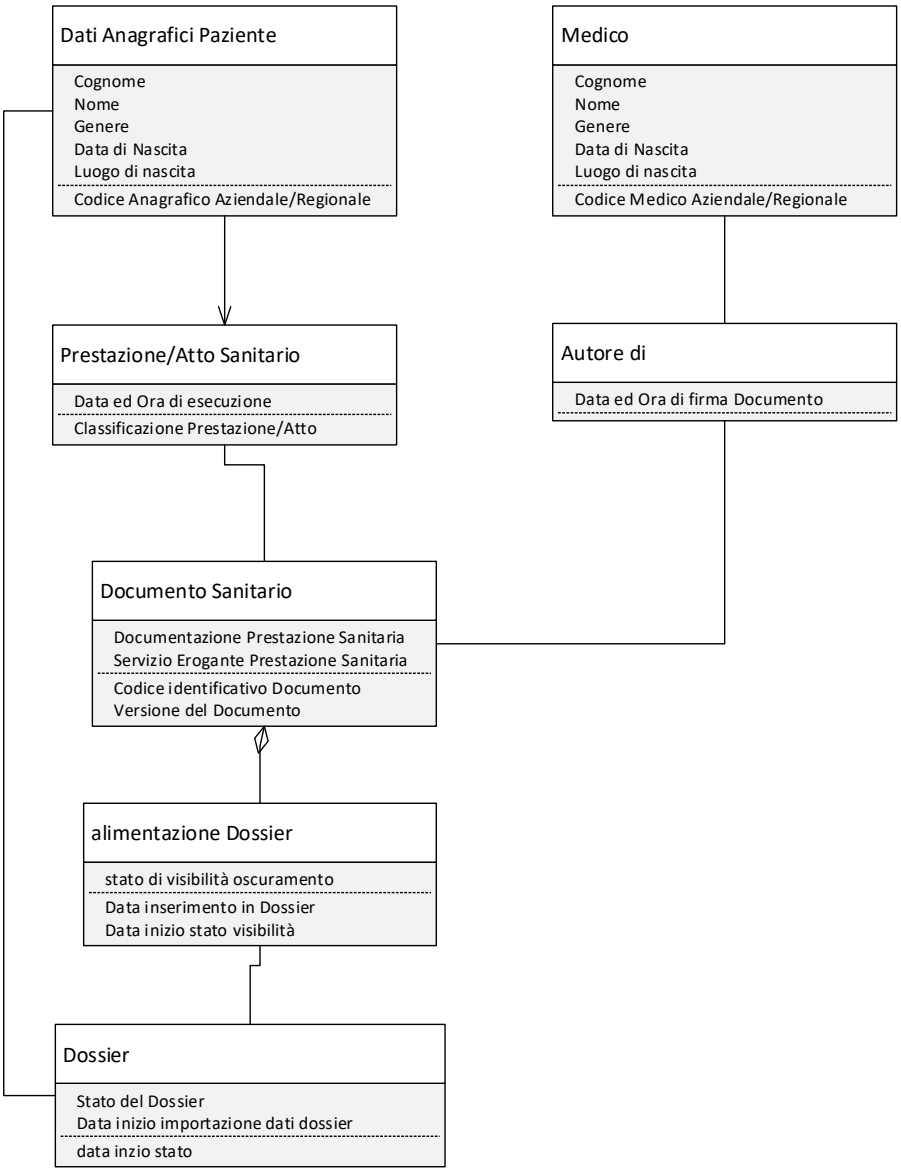


Figura 70. Information Model contenuto minimo “Gestione dati oscurati”

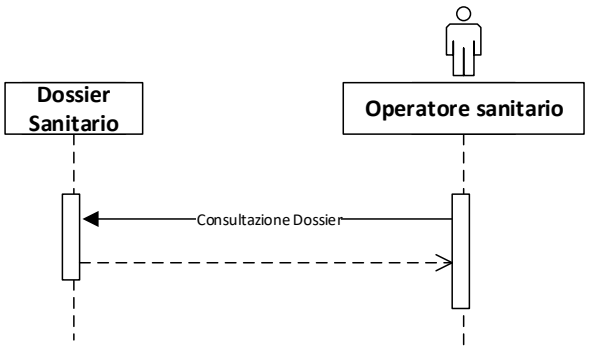


Figura 71. Interaction Model “Gestione dati oscurati”

4.3.16 SC16 – Richiesta de-oscuramento Dati

Descrizione del caso d'uso

Il presente caso d'uso – alla luce del *punto 5.1* delle Linee guida del Dossier sanitario – il paziente, o suo Genitore / Tutore, vuole de-oscurare i dati o i documenti sanitari rendendoli, pertanto, consultabili ai soggetti abilitati all'accesso al Dossier sanitario.

Attore Primario

Paziente.

Precondizioni

Al fine di poter impostare i criteri di visibilità l'Operatore sanitario dovrà:

- SC14, UCM D14 – Richiesta accesso e oscuramento dei dati.

Scenari

Il paziente chiede che vengano de-oscurati tutti i dati ovvero una parte di essi, che in precedenza aveva deciso di oscurare, rendendoli così visibili agli operatori che stanno seguendo il suo percorso di cura.

Post-condizione

Impostato – secondo la volontà del paziente – il sistema automaticamente permetterà la visualizzazione dei dati de-oscurati.

Use Case Model

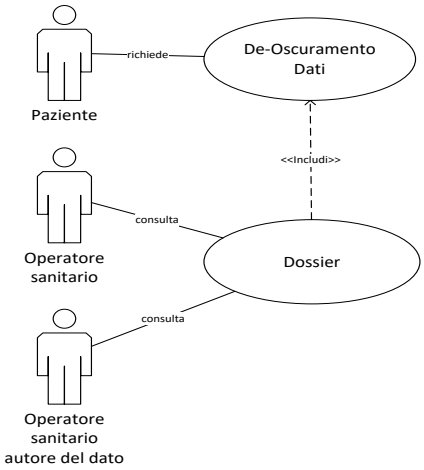


Figura 72. UCM D16 "Gestione de-oscuramento dati"

Information Model

Lista delle informazioni da trattare:

- Dati anagrafici del paziente
- Dati del consenso
- Dati del Medico operatore

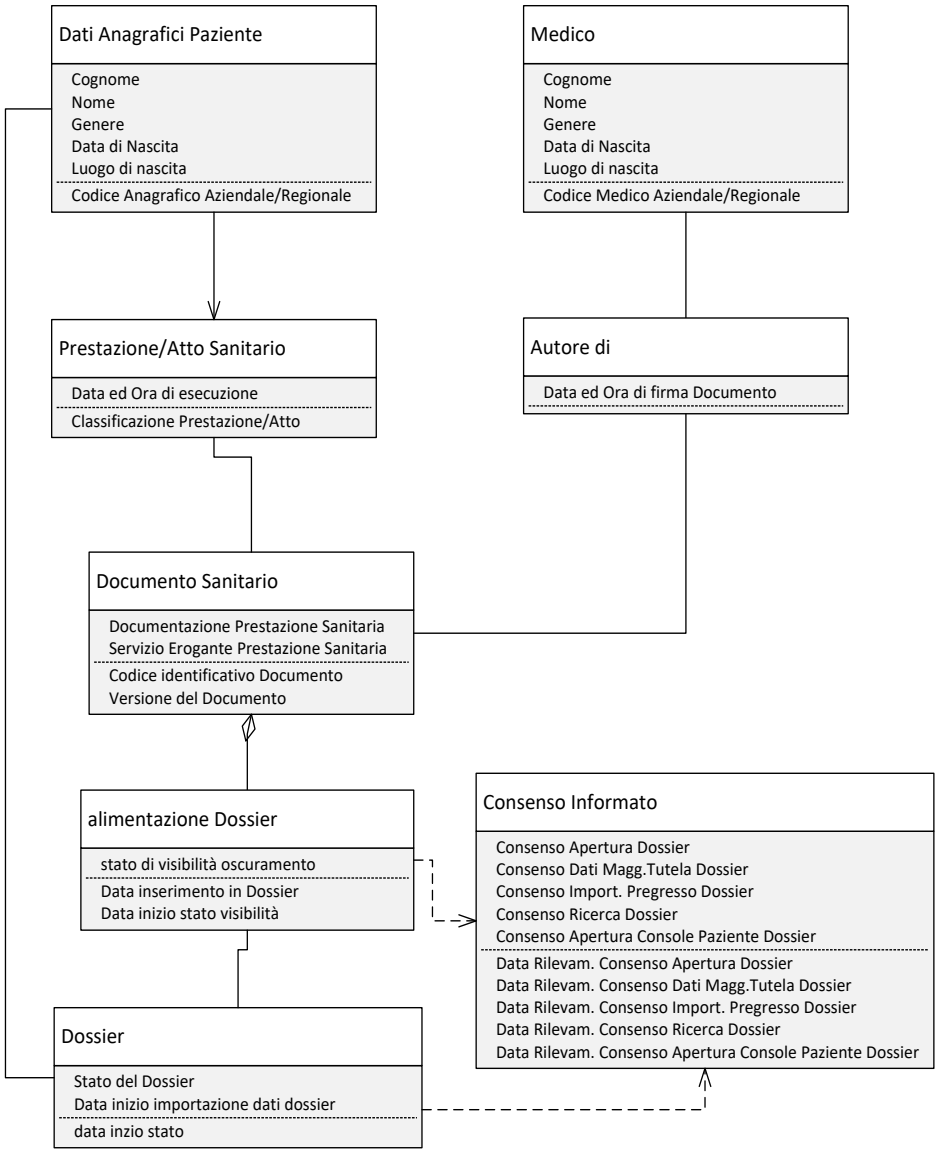


Figura 73. Information Model Generale “Gestione de-oscuramento dati”

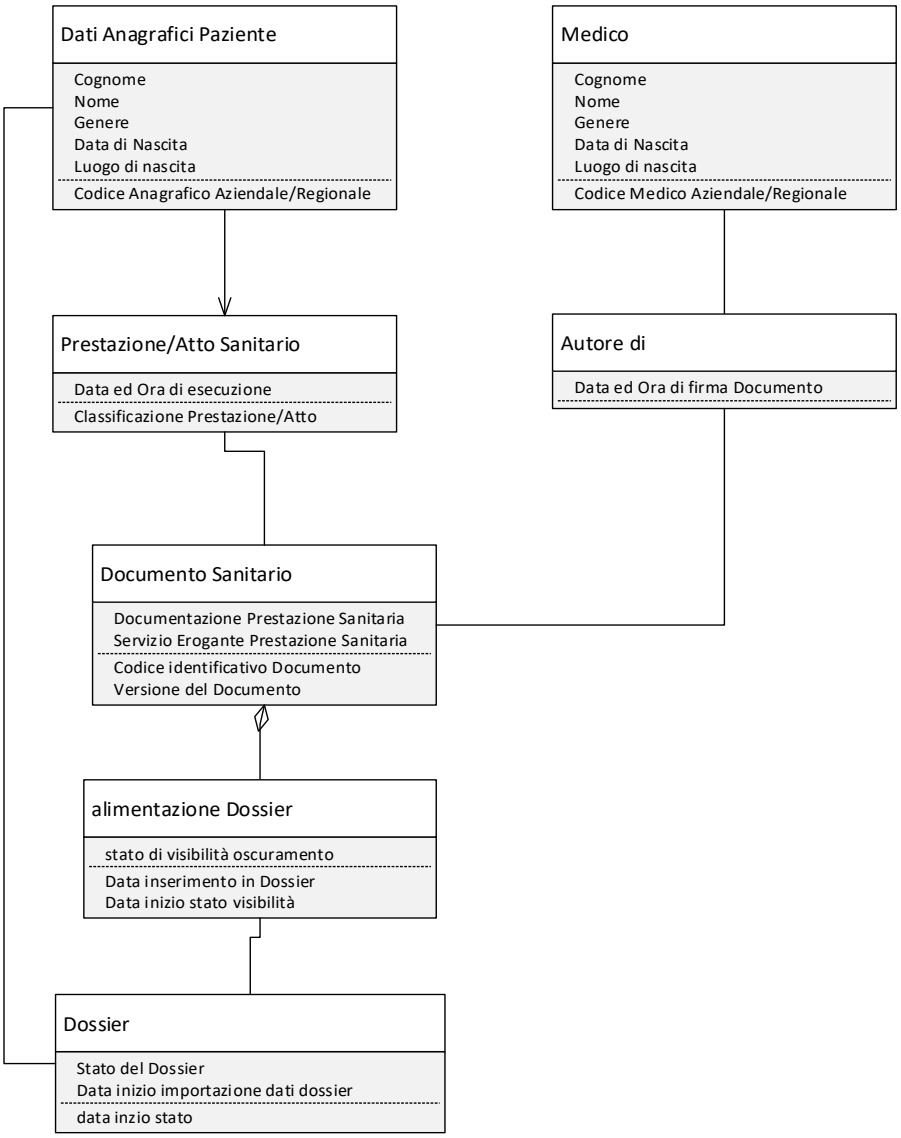


Figura 74. Information Model contenuto minimo “Gestione de-oscuramento dati”

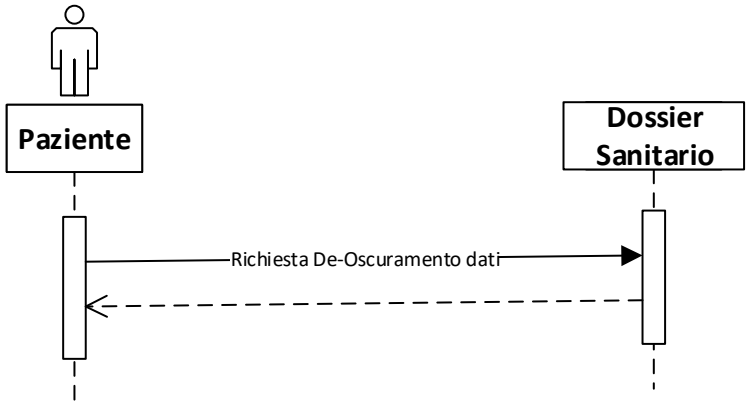


Figura 75. Interaction Model “Gestione de-oscuramento dati”

4.3.17 SC17 - Consenso paziente minore / sottoposto a tutela

Descrizione del caso d'uso

Il presente caso d'uso permette all'interessato Genitore o Tutore - secondo quanto previsto dal *punto 3* dalle Linee guida sul Dossier Sanitario - di gestire il consenso all'apertura e successiva consultazione dei dati e dei documenti sanitari contenuti nel sistema del Dossier Sanitario afferente ad un minore o a un soggetto sottoposto a tutela.

Attore Primario

Genitore o Tutore.

Precondizioni

Al fine di poter esprimere il consenso il Genitore o Tutore dovrà:

- essere il rappresentante legale di un minore o soggetto sottoposto a tutela,
- verificare che il minore sia iscritto all'anagrafe sanitaria,
- essere identificato con idonei meccanismi che ne garantiscano l'identità,
- SC01, UCM D01 Consultazione dell'Informativa.

Scenario

Il Genitore o il Tutore, spuntando il SI/NO nel modulo di consenso cartaceo e firmandolo *ovvero* rilasciandolo oralmente, fornisce alla struttura sanitaria il consenso per la costituzione del Dossier Sanitario del paziente tutorato.

Post-condizione

Il consenso acquisito viene riportato nei sistemi informatici di gestione del Dossier da parte del personale addetto. Il Genitore o il Tutore potrà d'ora in avanti effettuare le operazioni legate ai consensi rilasciati oppure revocarli.

Use Case Model

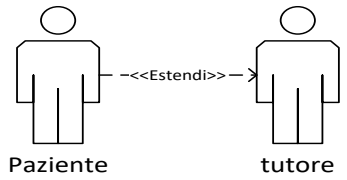


Figura 76. UCM D17 "Consenso paziente minore / sottoposto a tutela"

Information Model

Lista delle informazioni da trattare:

- Dati anagrafici del paziente,
- Dati anagrafici del tutore, relazione tutore/paziente.
- Dati del consenso

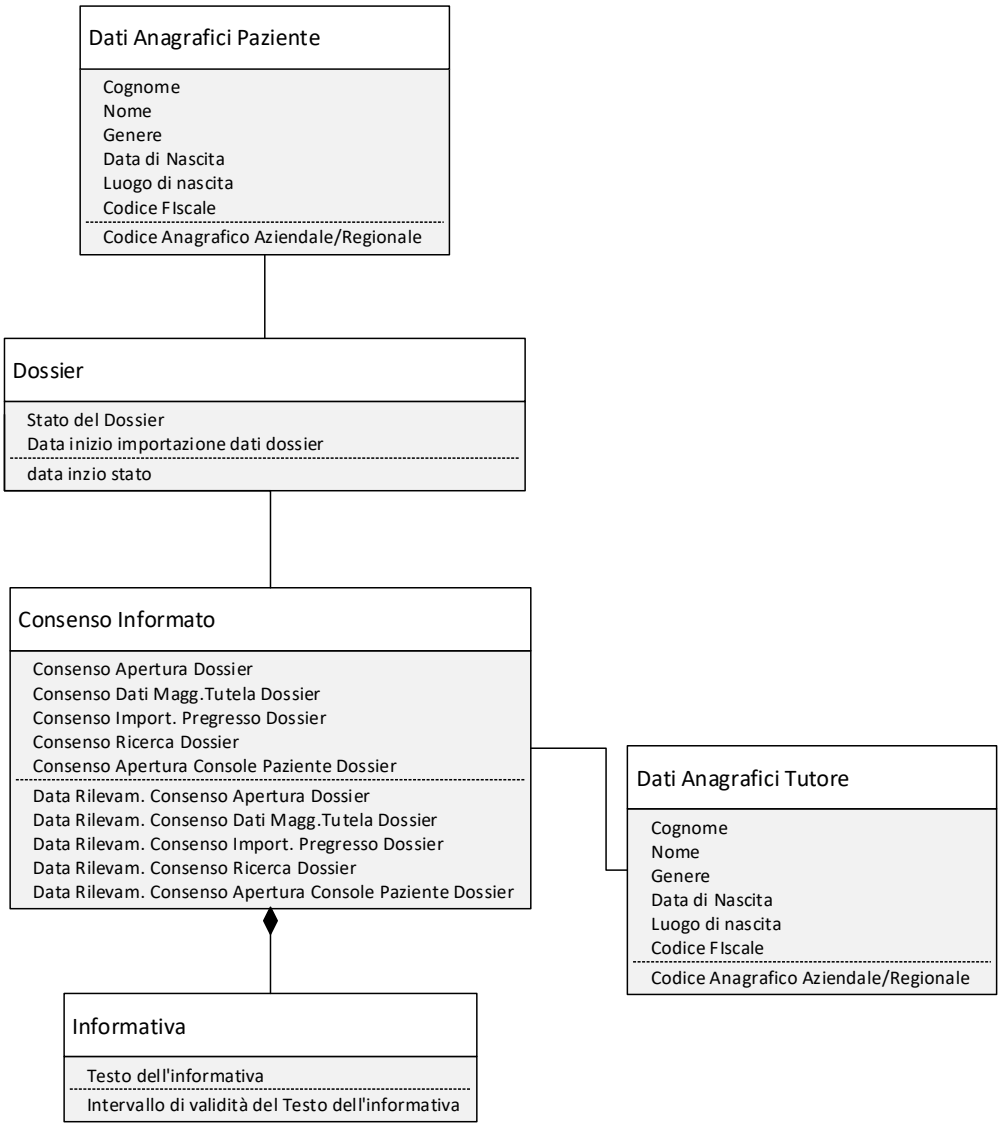


Figura 77. Information Model Generale “Consenso paziente minore / sottoposto a tutela”

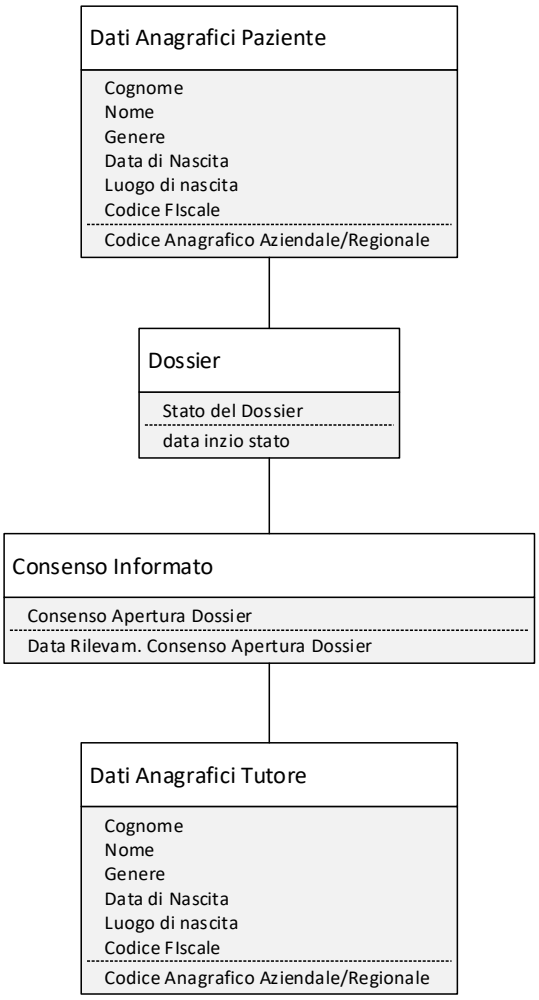


Figura 78. Information Model contenuto minimo "Consenso paziente minore / sottoposto a tutela"

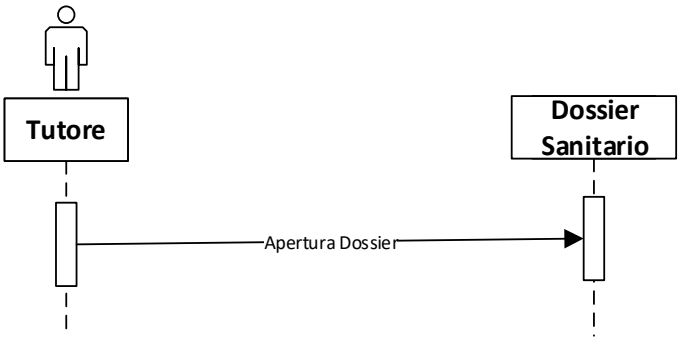


Figura 79. Interaction Model "Consenso paziente minore / sottoposto a tutela"

4.3.18 SC18 - Consenso Importazione dati e documenti pregressi paziente minore / sottoposto a tutela

Descrizione del caso d'uso

Il presente caso d'uso permette all'interessato Genitore o Tutore - secondo quanto previsto dal *punto 3* dalle Linee guida sul Dossier Sanitario - di gestire il consenso all'importazione dei dati e dei documenti sanitari pregressi nel sistema del Dossier Sanitario afferente ad un minore o a un soggetto sottoposto a tutela.

Attore Primario

Genitore o Tutore.

Precondizioni

Al fine di poter esprimere il consenso il Genitore o Tutore dovrà:

- essere il rappresentante legale di un minore o soggetto sottoposto a tutela,
- essere identificato con idonei meccanismi che ne garantiscano l'identità,
- SC02, UCM D02 Consenso Apertura Dossier sanitario.

Scenario

Il Genitore o il Tutore, spuntando il SI/NO nel modulo di consenso cartaceo e firmandolo *ovvero* rilasciandolo oralmente, fornisce alla struttura sanitaria il consenso per l'importazione dei dati e dei documenti sanitari pregressi nel Dossier Sanitario del paziente tutorato.

Post-condizione

Il consenso acquisito viene riportato nei sistemi informatici di gestione del Dossier da parte del personale addetto. Il Genitore o il Tutore potrà d'ora in avanti effettuare le operazioni legate ai consensi rilasciati oppure revocarli.

Use Case Model

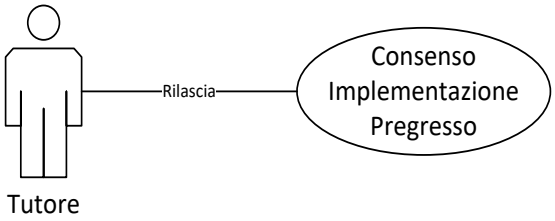


Figura 80. UCM D18 "Consenso Importazione dati e documenti pregressi paziente minore / sottoposto a tutela"

Information Model

Lista delle informazioni da trattare:

- Dati anagrafici del paziente
- Dati anagrafici del tutore, relazione tutore/paziente
- Dati del consenso

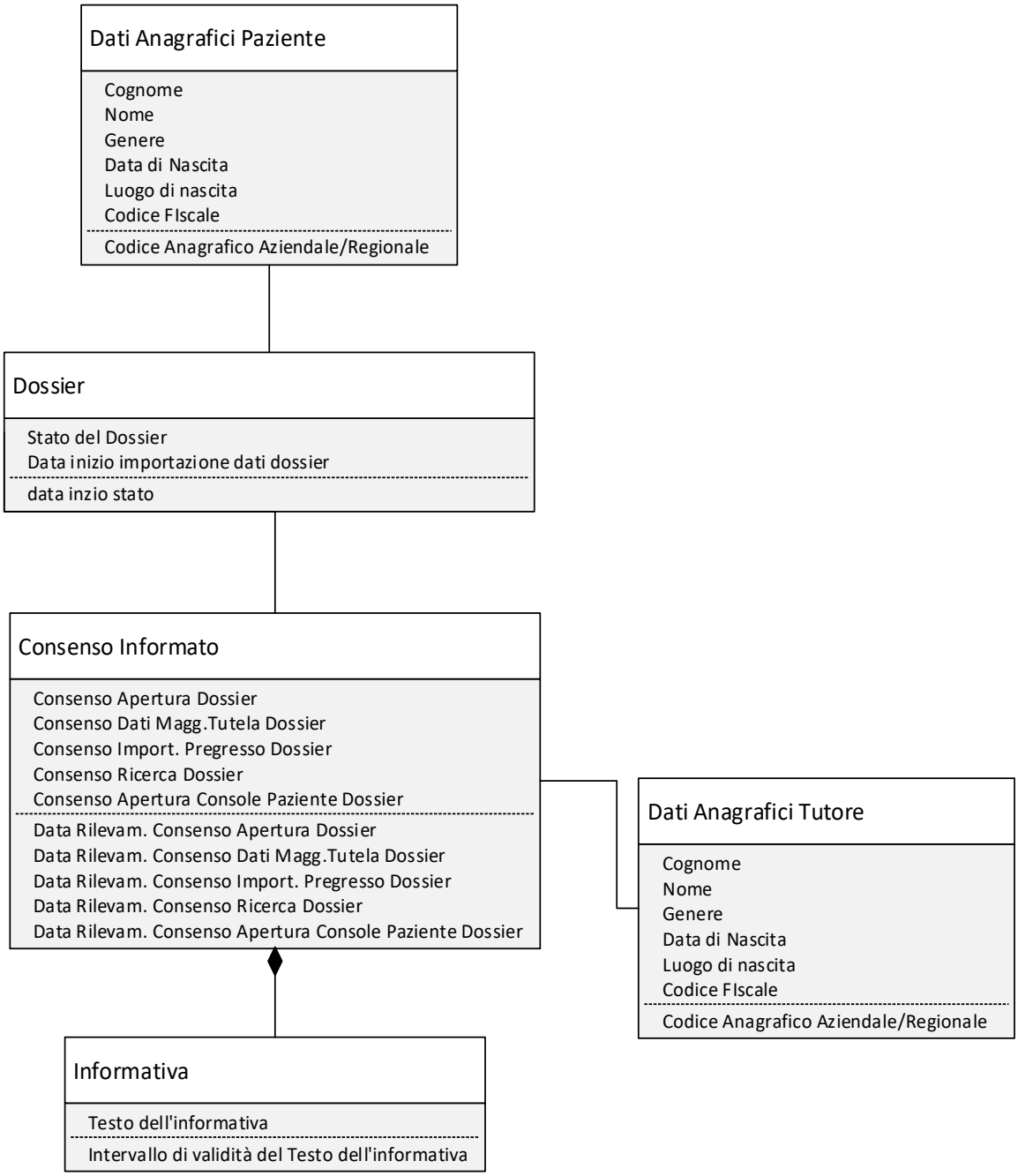


Figura 81. Information Model Generale "Consenso Importazione dati e documenti pregressi paziente minore / sottoposto a tutela"

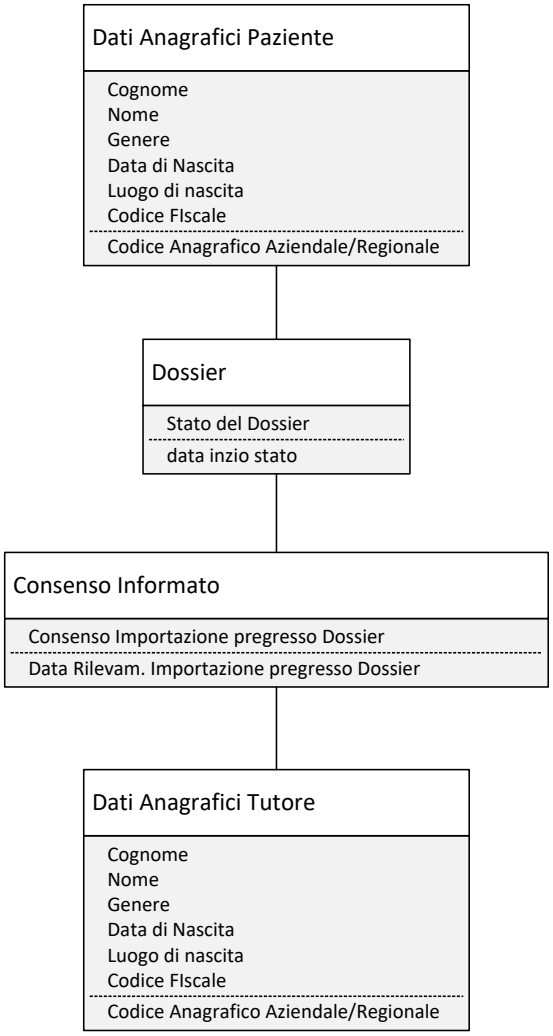


Figura 82. Information Model contenuto minimo "Consenso Importazione dati e documenti pregressi paziente minore / sottoposto a tutela"

Figura 83. Interaction Model "Consenso importazione dati e documenti pregressi"

4.3.19 SC19 – Consenso dati "a maggior tutela" paziente minore / sottoposto a tutela

Descrizione del caso d'uso

Il presente caso d'uso permette all'interessato Genitore o Tutore - secondo quanto previsto dal *punto 3.1* dalle Linee guida sul Dossier Sanitario - di concedere agli operatori sanitari di popolare il sistema del Dossier sanitario con i dati e documenti sanitari "a maggior tutela", afferenti ad un minore o a un soggetto sottoposto a tutela.

Attore Primario

Genitore o Tutore.

Precondizioni

Al fine di poter esprimere il consenso il Genitore o Tutore dovrà:

- essere il rappresentante legale di un minore o soggetto sottoposto a tutela,
- essere identificato con idonei meccanismi che ne garantiscano l'identità,
- SC02, UCM D02 Consenso Apertura Dossier sanitario.

Scenario

Il Genitore o il Tutore, spuntando il SI/NO nel modulo di consenso cartaceo e firmandolo *ovvero* rilasciandolo oralmente, fornisce alla struttura sanitaria il consenso per l'importazione dei dati e dei documenti sanitari pregressi nel Dossier Sanitario del paziente tutorato.

Post-condizione

Il consenso acquisito viene riportato nei sistemi informatici di gestione del Dossier da parte del personale addetto. Il Genitore o il Tutore potrà d'ora in avanti effettuare le operazioni legate ai consensi rilasciati oppure revocarli.

Use Case Model

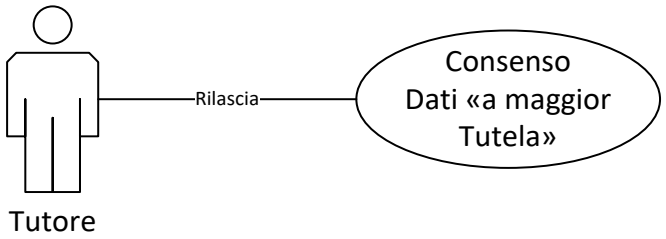


Figura 84. UCM D19 "Consenso per dati "a maggior tutela" paziente minore / sottoposto a tutela"

Information Model

Lista delle informazioni da trattare:

- Dati anagrafici del paziente
- Dati anagrafici del tutore, relazione tutore/paziente
- Dati del consenso

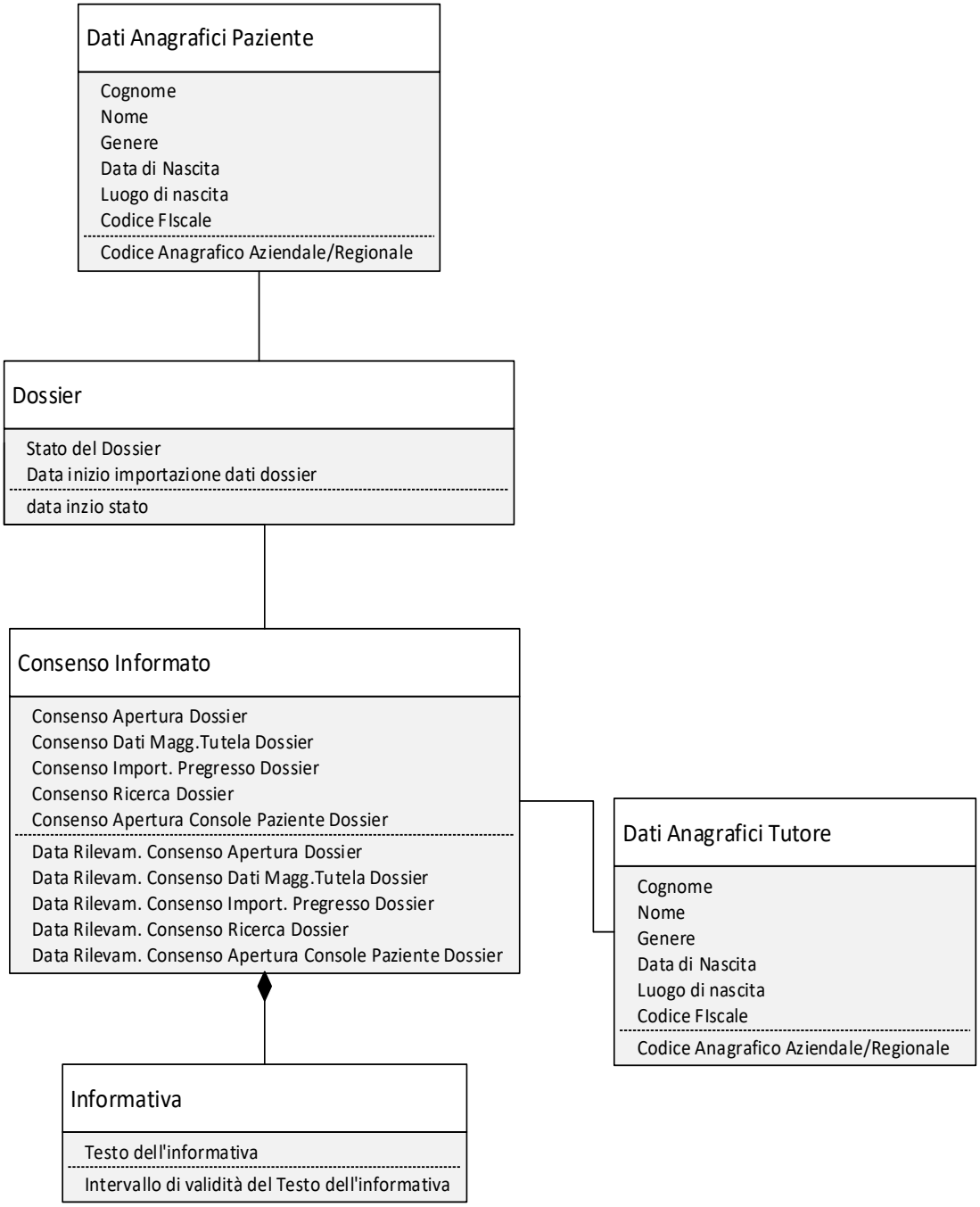


Figura 85. Information Model Generale "Consenso dati a maggior tutela paziente minore / sottoposto a tutela"

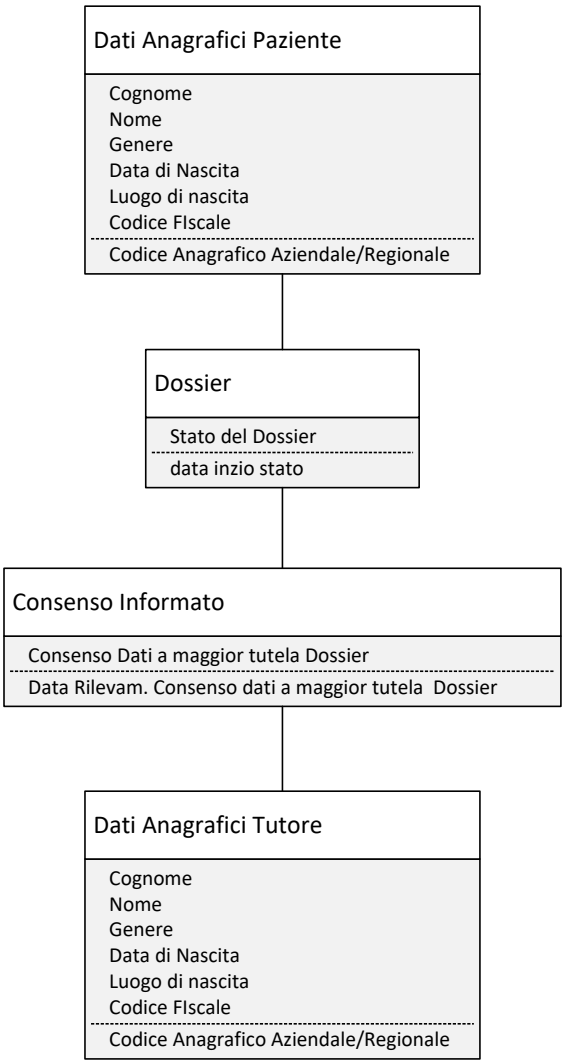


Figura 86. Information Model contenuto minimo "Consenso dati a maggior tutela paziente minore / sottoposto a tutela"

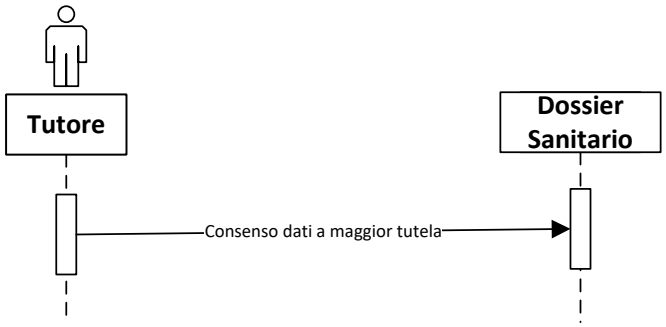


Figura 87. Interaction Model "Consenso dati a maggior tutela paziente minore / sottoposto a tutela"

4.3.20 SC20 - Consenso dati finalità di Ricerca paziente minore / sottoposto a tutela

Descrizione del caso d'uso

Il presente caso d'uso, successivamente all'apertura del Dossier, permette al Genitore o Tutore – secondo quanto previsto dal *punto 3* dalle Linee guida sul Dossier Sanitario – di esprimere il proprio consenso libero ed informato al fine di concedere agli Operatori di ricerca di utilizzare il sistema del Dossier Sanitario, contenente i dati e i documenti del paziente minore / sottoposto a tutela, per finalità di ricerca.

Attore Primario

Genitore o Tutore.

Precondizioni

Al fine di poter esprimere il consenso il Genitore o Tutore dovrà:

- essere il rappresentante legale di un minore o soggetto sottoposto a tutela,
- essere identificato con idonei meccanismi che ne garantiscano l'identità,
- SC02, UCM D02 Consenso Apertura Dossier sanitario.

Scenario

Il Genitore o il Tutore, spuntando il SI/NO nel modulo di consenso cartaceo e firmandolo *ovvero* rilasciandolo oralmente, fornisce alla struttura sanitaria il proprio consenso esplicito, libero ed informato per utilizzare i dati del Dossier Sanitario del paziente tutorato per finalità di ricerca.

Post-condizione

Il consenso all'utilizzo dei dati per finalità di ricerca viene registrato nei sistemi informatici di gestione del dossier da parte del personale addetto. Il Genitore o il Tutore potrà d'ora in avanti effettuare le operazioni legate ai consensi rilasciati oppure revocarli.

Use Case Model

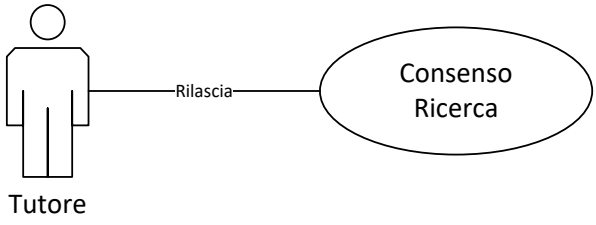


Figura 88. UCM D20 "Consenso dati finalità di Ricerca paziente minore / sottoposto a tutela"

Information Model

Lista delle informazioni da trattare:

- Dati anagrafici del paziente
- Dati anagrafici del tutore, relazione tutore/paziente
- Dati del consenso

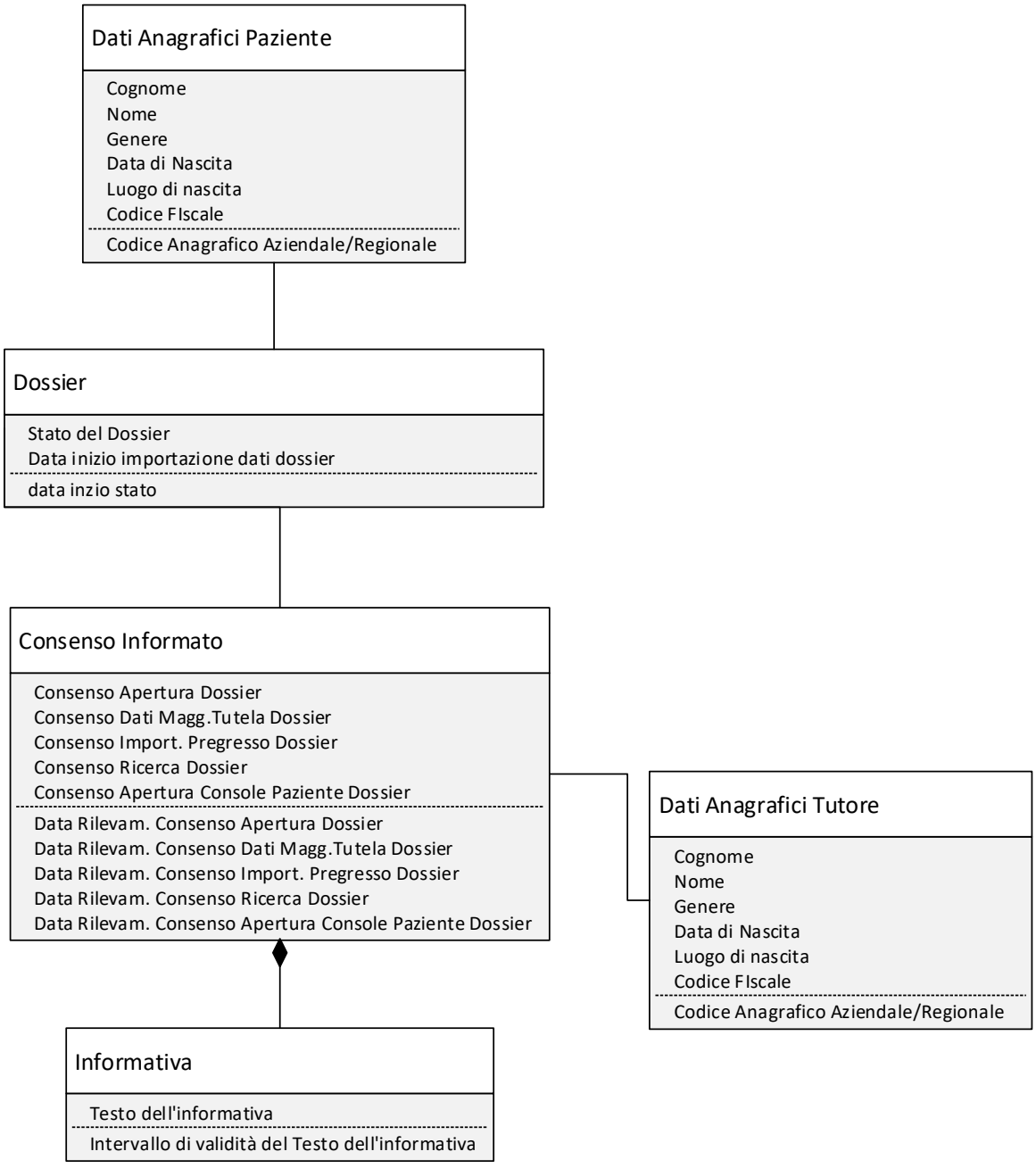


Figura 89. Information Model Generale "Consenso finalità di ricerca paziente minore / sottoposto a tutela"

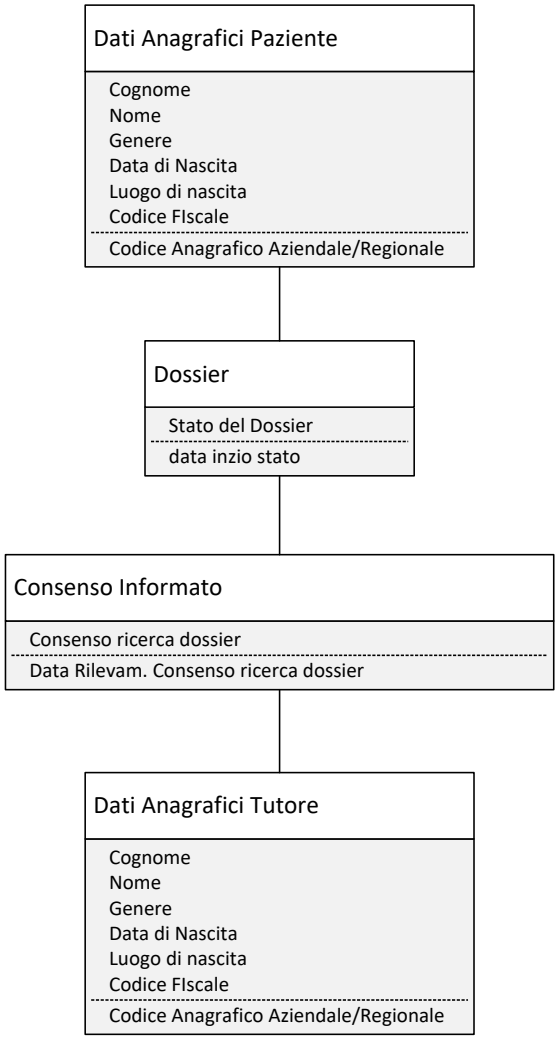


Figura 90. Information Model contenuto minimo “Consenso finalità di ricerca paziente minore / sottoposto a tutela”

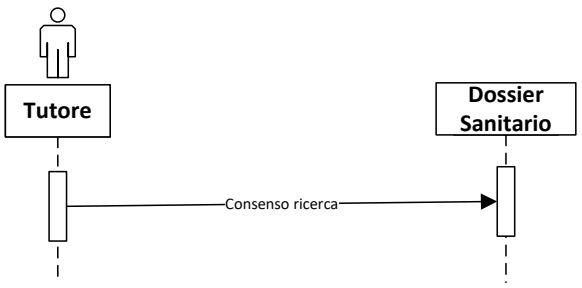


Figura 91. Interaction Model “Consenso finalità di ricerca paziente minore / sottoposto a tutela”

4.3.21 SC21 - Scadenza del dossier a seguito della maggiore età del paziente

Descrizione del caso d'uso

Il presente caso d'uso – secondo quanto previsto dal *punto 3* delle Linee guida del Dossier sanitario – prevede, al compimento del 18esimo anno di età del paziente Minore, il congelamento in automatico del Dossier.

Attore Primario

Sistema informatico di gestione del Dossier.

Precondizioni

Al fine di poter riattivare il Dossier Sanitario il paziente dovrà:

- essere divenuto maggiorenne,
- essere registrato presso l'anagrafe sanitaria,
- SC02, UCM D02 Consenso Apertura Dossier Sanitario, dato dal tutore.

Scenario

Il sistema informatico di gestione del Dossier blocca in automatico la consultazione e alimentazione da parte degli operatori sanitari.

Post-condizione

Il paziente dovrà rilasciare un nuovo consenso.

Use Case Model

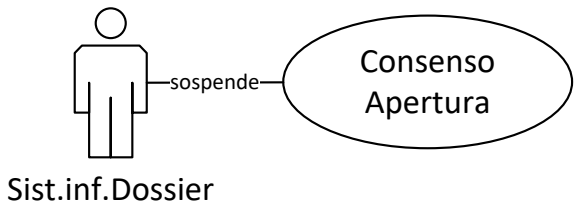


Figura 92. UCM D21 "Scadenza del dossier a seguito della maggiore età del paziente"

Information Model

Lista delle informazioni da trattare:

- Dati anagrafici del paziente
- Dati del dossier

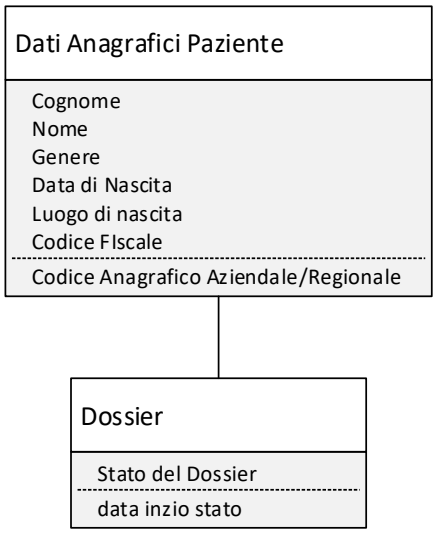


Figura 93. Information Model Generale "Scadenza del dossier a seguito della maggiore età del paziente"

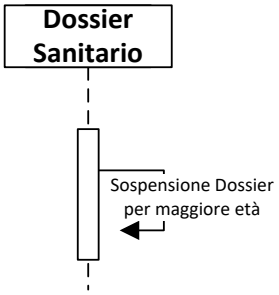


Figura 94 Interaction Model "Scadenza del dossier a seguito della maggiore età del paziente"

4.3.22 SC22 - Riattivazione del dossier a seguito della maggiore età del paziente

Descrizione del caso d'uso

Il presente caso d'uso – secondo quanto previsto dal *punto 3* delle Linee guida del Dossier sanitario – prevede, al compimento del 18esimo anno di età del paziente Minore, il congelamento in automatico del Dossier. Il paziente, divenuto maggiorenne, per poterlo utilizzare deve riattivarlo al primo contatto utile.

Attore Primario

Paziente.

Precondizioni

Al fine di poter riattivare il Dossier Sanitario il paziente dovrà:

- il paziente sarà identificato con idonei meccanismi che ne garantiscano l'identità,
- essere divenuto maggiorenne,
- essere registrato presso l'anagrafe sanitaria,
- SC01, UCM D01 Consultazione dell'Informativa, verso il paziente,
- SC02, UCM D02 Consenso Apertura Dossier Sanitario, dato dal tutore.

Scenario

Il Paziente fornisce alla struttura sanitaria il proprio consenso esplicito, libero ed informato per la riattivazione nel Dossier Sanitario, spuntando il SI nel modulo di consenso e firmandolo.

Post-condizione

Il consenso acquisito viene riportato nei sistemi informatici di gestione del Dossier da parte del personale addetto e il sistema viene riattivato.

Use Case Model

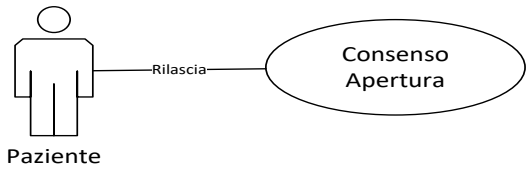


Figura 95. UCM D22 "Riattivazione del dossier a seguito della maggiore età del paziente"

Information Model

Lista delle informazioni da trattare:

- Dati anagrafici del paziente
- Dati del consenso
- Dati del dossier

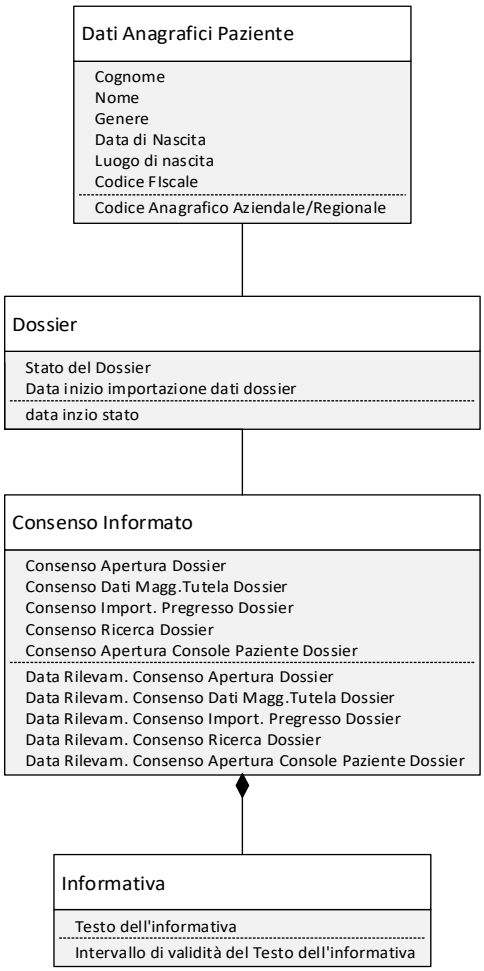


Figura 96. Information Model Generale "Riattivazione del dossier a seguito della maggiore età del paziente"

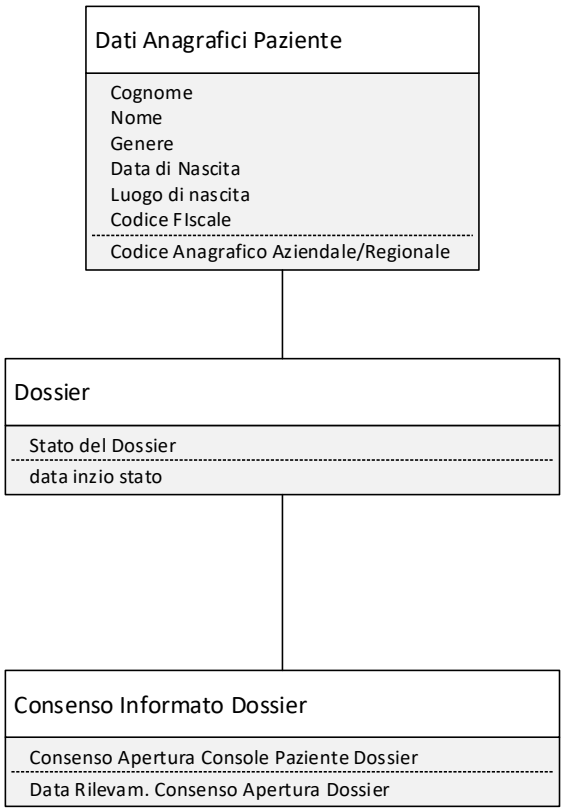


Figura 97. Information Model contenuto minimo "Riattivazione del dossier a seguito della maggiore età del paziente"

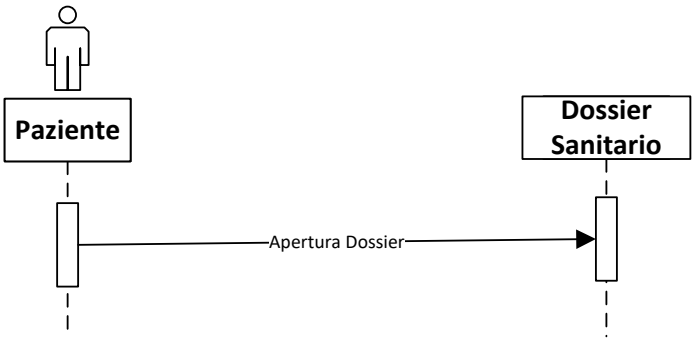


Figura 98 Interaction Model "Riattivazione del dossier a seguito della maggiore età del paziente"

4.3.23 SC23 – Gestione Dati a maggior tutela

Descrizione del caso d'uso

Il presente caso d'uso – alla luce del *punto 3.1* delle Linee guida del Dossier sanitario – permette all'Operatore sanitario in merito ai dati "a maggior tutela dell'anonimato" d'inserirli nel Dossier e renderli consultabili a fronte di una specifica e libera manifestazione di volontà del paziente, o dal Genitore / Tutore.

Attore Primario

Operatore sanitario.

Precondizioni

Al fine di poter impostare i criteri di visibilità l'Operatore sanitario dovrà:

- SC04, UCM D04 Consenso Dati a maggior tutela.

Scenari

Scenario 1:

Impostato – secondo la volontà del paziente - il criterio di visibilità dei dati sul SI, il sistema automaticamente autorizzerà l'Operatore sanitario di consultare i dati e i documenti a maggior tutela che ha richiesto in visualizzazione.

Scenario 2:

Impostato – secondo la volontà del paziente - il criterio di visibilità dei dati sul NO, il sistema automaticamente negherà all'Operatore sanitario di consultare i dati e i documenti a maggior tutela che ha richiesto in visualizzazione.

Scenario 3:

Impostato – secondo la volontà del paziente - il criterio di visibilità dei dati sul NO, il sistema automaticamente permetterà la visualizzazione al solo Operatore sanitario che ha elaborato, ovvero prodotto o partecipato alla catena di produzione per trattamenti non anonimizzati, i dati e i documenti a maggior tutela.

Post-condizione

Secondo la volontà del paziente verranno impostati i criteri di visibilità dei dati o documenti soggetti a maggior tutela.

Use Case Model

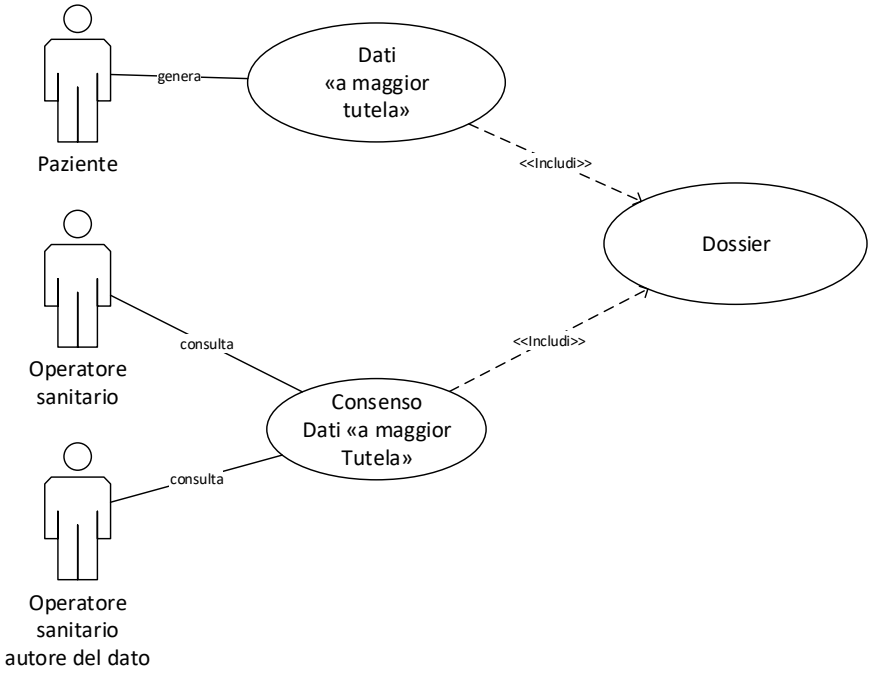


Figura 99. UCM D23 “Gestione Dati a maggior tutela”

Information Model

Lista delle informazioni da trattare:

- Dati anagrafici del paziente
- Dati del consenso
- Dati del Medico operatore
- Dati dell’esame consultato

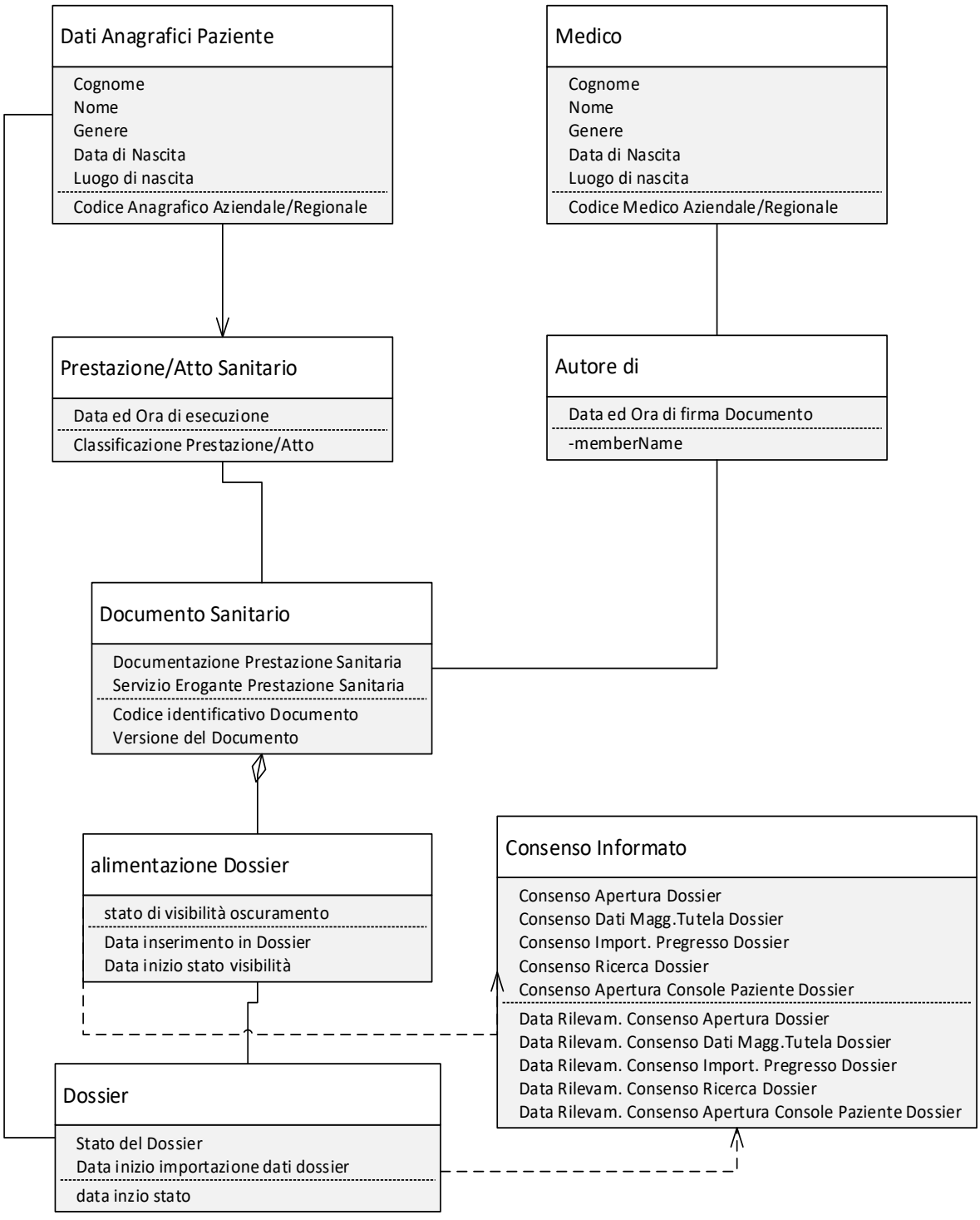


Figura 100. Information Model Generale “Gestione Dati a maggior tutela”

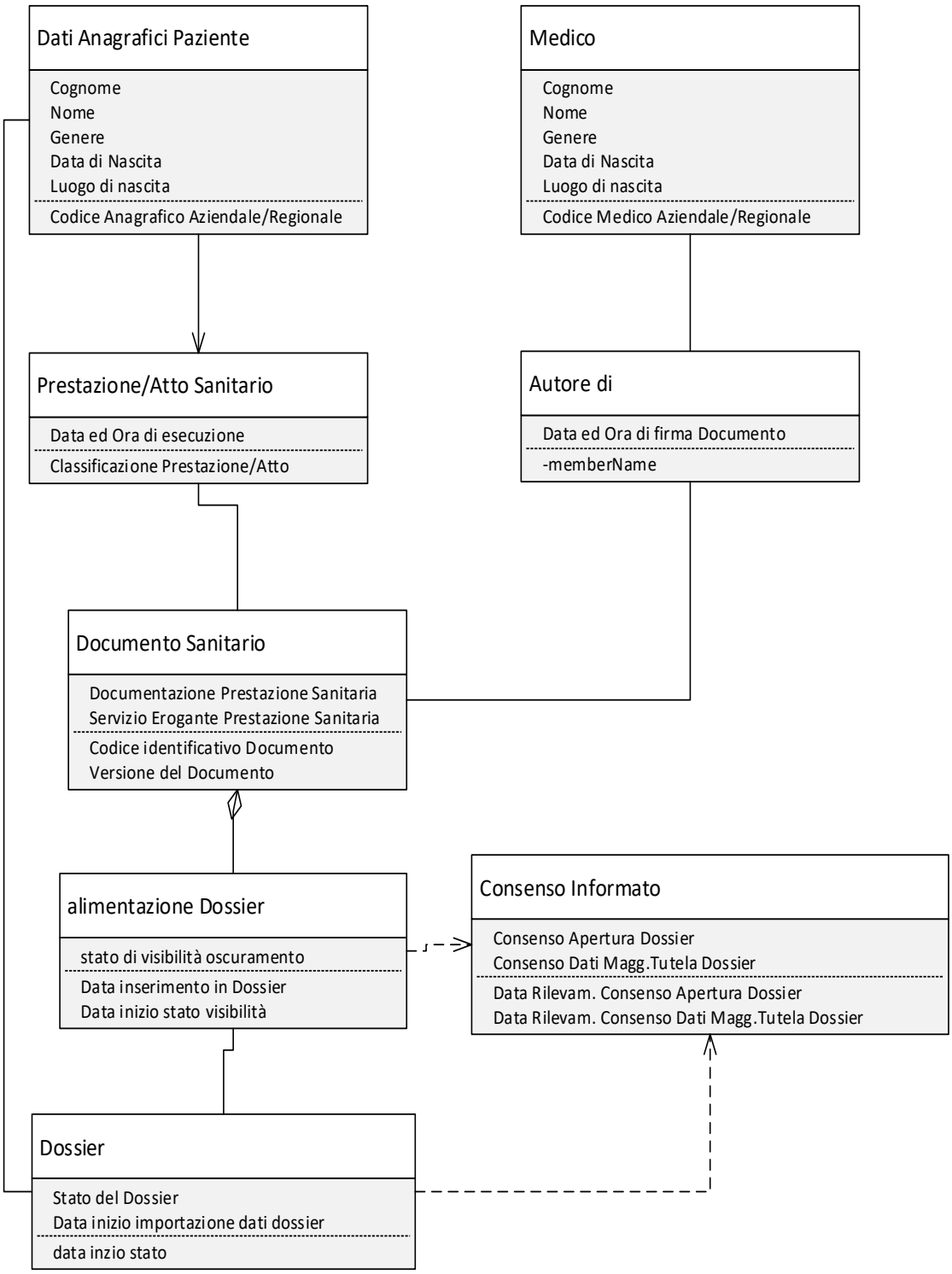


Figura 101. Information Model contenuto minimo “Gestione Dati a maggior tutela”

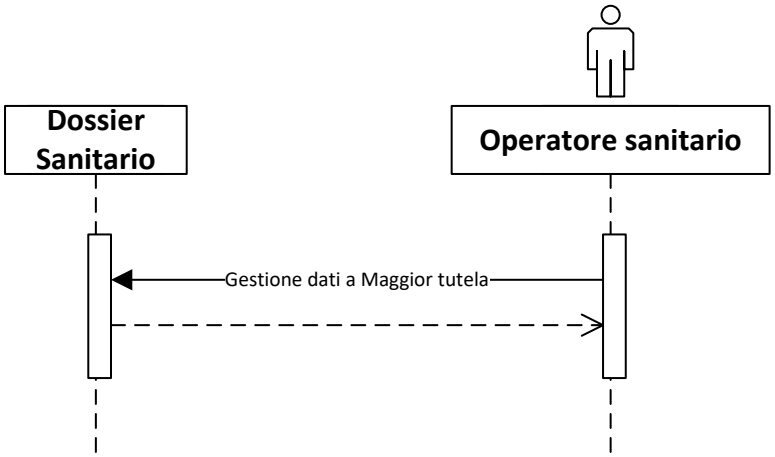


Figura 102. Interaction Model contenuto minimo “Gestione Dati a maggior tutela”

4.3.24 SC24 - Gestione Finalità di ricerca anonima

Descrizione del caso d'uso

Il presente caso d'uso permette all'incaricato dello svolgimento di ricerche e studi, acquisito il consenso libero ed informato dell'interessato/paziente, di trattare i dati e i documenti sanitari contenuti nel Dossier sanitario per finalità di studio e ricerca scientifica anonima.

Attore Primario

Operatore di ricerca.

Precondizioni

Lo studio di ricerca deve essere preventivamente definito ed approvato dai comitati etici e deontologici di riferimento del titolare del Dossier.

L'Operatore di ricerca dovrà essere specificamente incaricato al trattamento dati relativi allo studio. Per trattare i dati per finalità di studio e ricerca dovrà:

- SC5, UCM D5 Consenso dati finalità di Ricerca,
- usare i dati in forma aggregata oppure in forma anonima.

Il dossier consente l'estrazione di dati anonimizzati.

Scenario

L'operatore di ricerca usando gli strumenti messi a disposizione del sistema informatico di supporto al dossier invoca una estrazione (es.: report delle glicemie dei pazienti secondo i parametri di selezione popolazione pazienti definiti dallo studio, come: pazienti oltre 65 anni, maschi, con 3 ricoveri negli ultimi 12 mesi e diagnosi di dimissione di scompenso cardiaco.

Le glicemie sono associate ad un identificativo completamente anonimo del paziente ed all'istante di rilevamento della glicemia).

Post-condizione

Al termine dello studio l' Operatore di ricerca elimina i dati estratti dal Dossier.

Use Case Model

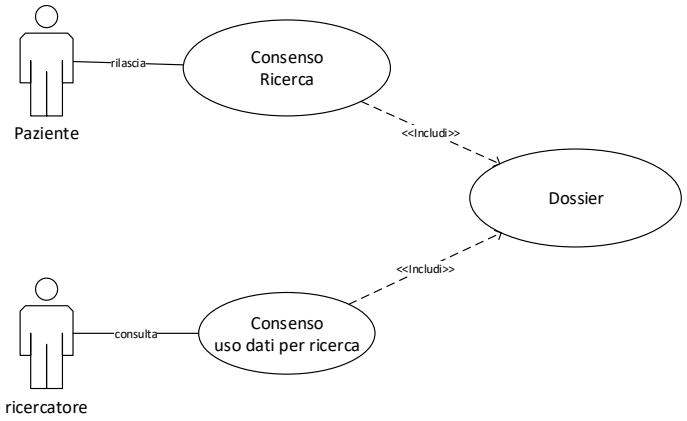


Figura 103. UCM D24 “Gestione Finalità di ricerca anonima”

Information Model

Lista delle informazioni da trattare:

- Dati clinici del paziente
- Dati del consenso

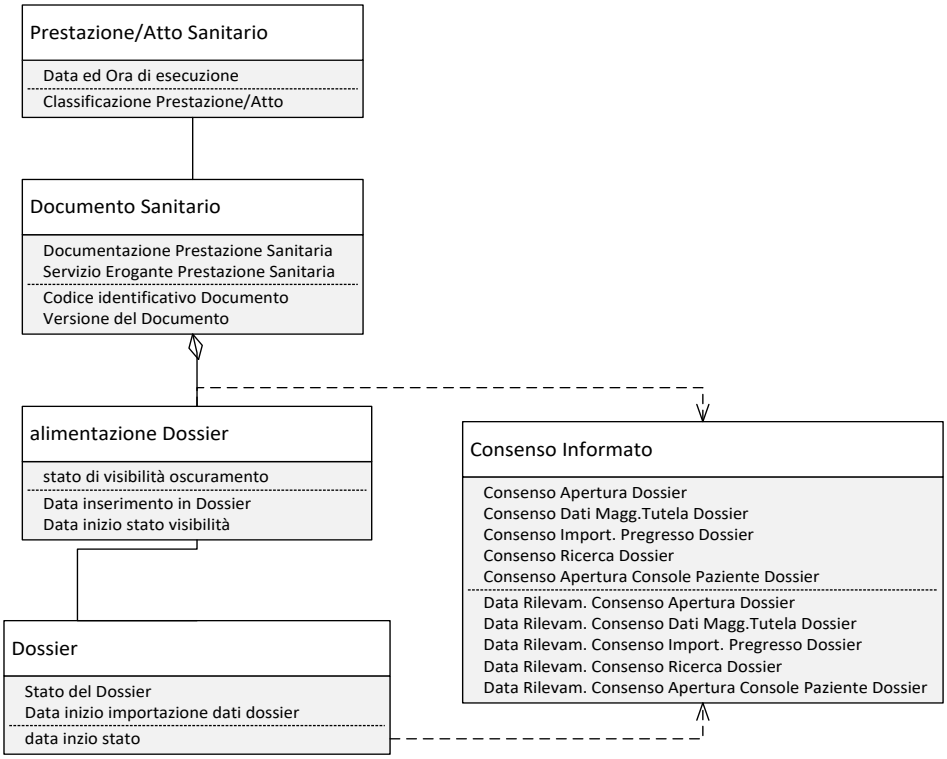


Figura 104. Information Model Generale “gestione finalità di ricerca anonima”

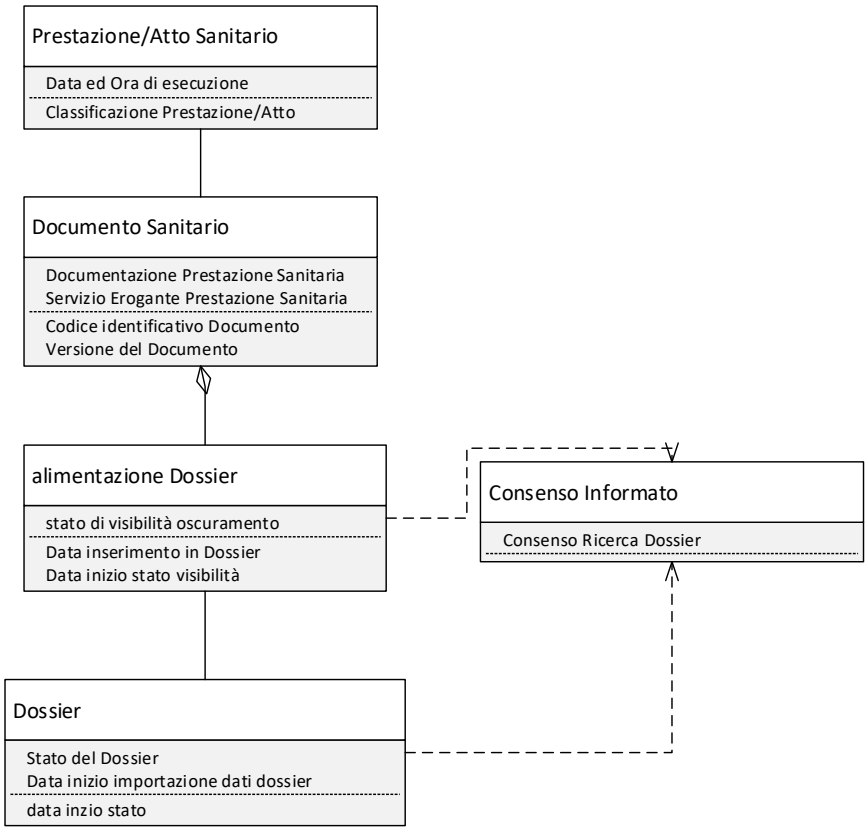


Figura 105 Information Model contenuto minimo "gestione finalità di ricerca anonima"

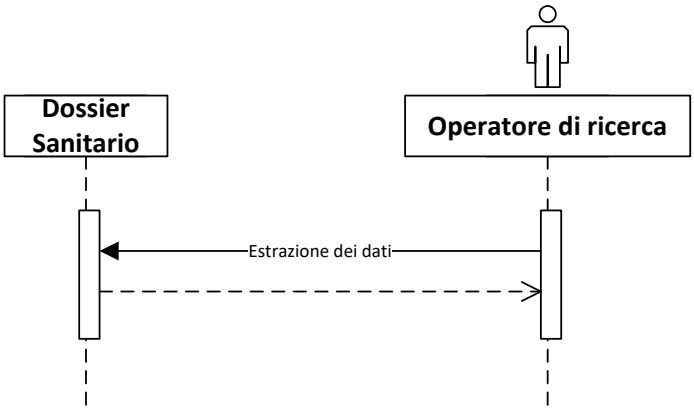


Figura 106. Interaction Model contenuto minimo "Gestione Finalità di ricerca anonima"

4.3.25 SC25 - Gestione Finalità di ricerca aggregata

Descrizione del caso d'uso

Il presente caso d'uso permette all'incaricato dello svolgimento di ricerche e studi, acquisito il consenso libero ed informato dell'interessato/paziente, di trattare i dati e i documenti sanitari contenuti nel Dossier sanitario per finalità di studio e ricerca scientifica aggregata.

Attore Primario

Operatore di ricerca.

Precondizioni

Lo studio di ricerca deve essere preventivamente definito ed approvato dai comitati etici e deontologici di riferimento del titolare del Dossier.

L'Operatore di ricerca dovrà essere specificamente incaricato al trattamento dati relativi allo studio.

Per trattare i dati per finalità di studio e ricerca dovrà:

- SC05, UCM D05 Consenso dati finalità di Ricerca,
- usare i dati in forma aggregata.

Il Dossier contiene dati documentali non anonimizzabili.

Scenario

L'operatore di ricerca usando gli strumenti messi a disposizione del sistema informatico di supporto al dossier invoca una estrazione (es.: report del numero di pazienti secondo i parametri di selezione popolazione pazienti definiti dallo studio, come: pazienti oltre 65 anni, maschi, con 3 ricoveri negli ultimi 12 mesi e diagnosi di dimissione di scompenso cardiaco.

Il sistema di gestione del dossier gli ritorna indietro un numero di pazienti che soddisfano il criterio di ricerca).

Post-condizione

Nessuna

Use Case Model

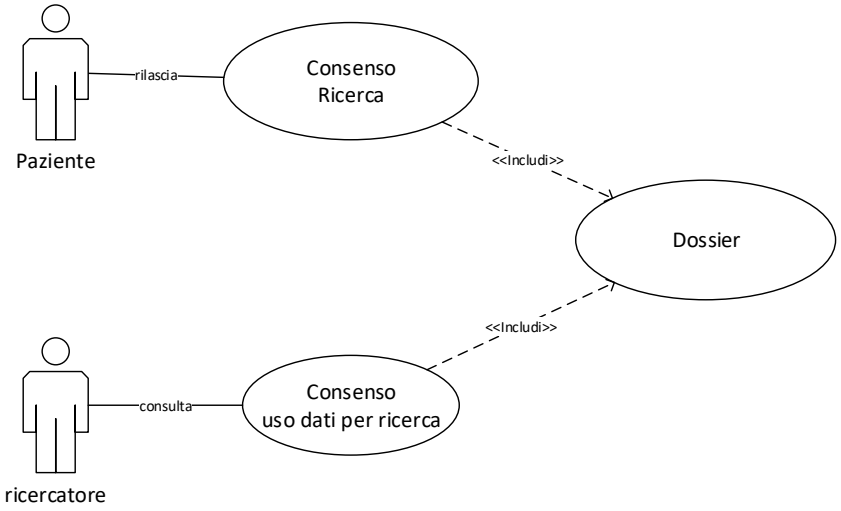


Figura 107. UCM D25 “Gestione Finalità di ricerca aggregata”

Information Model

Lista delle informazioni da trattare:

- Dati clinici del paziente
- Dati del consenso

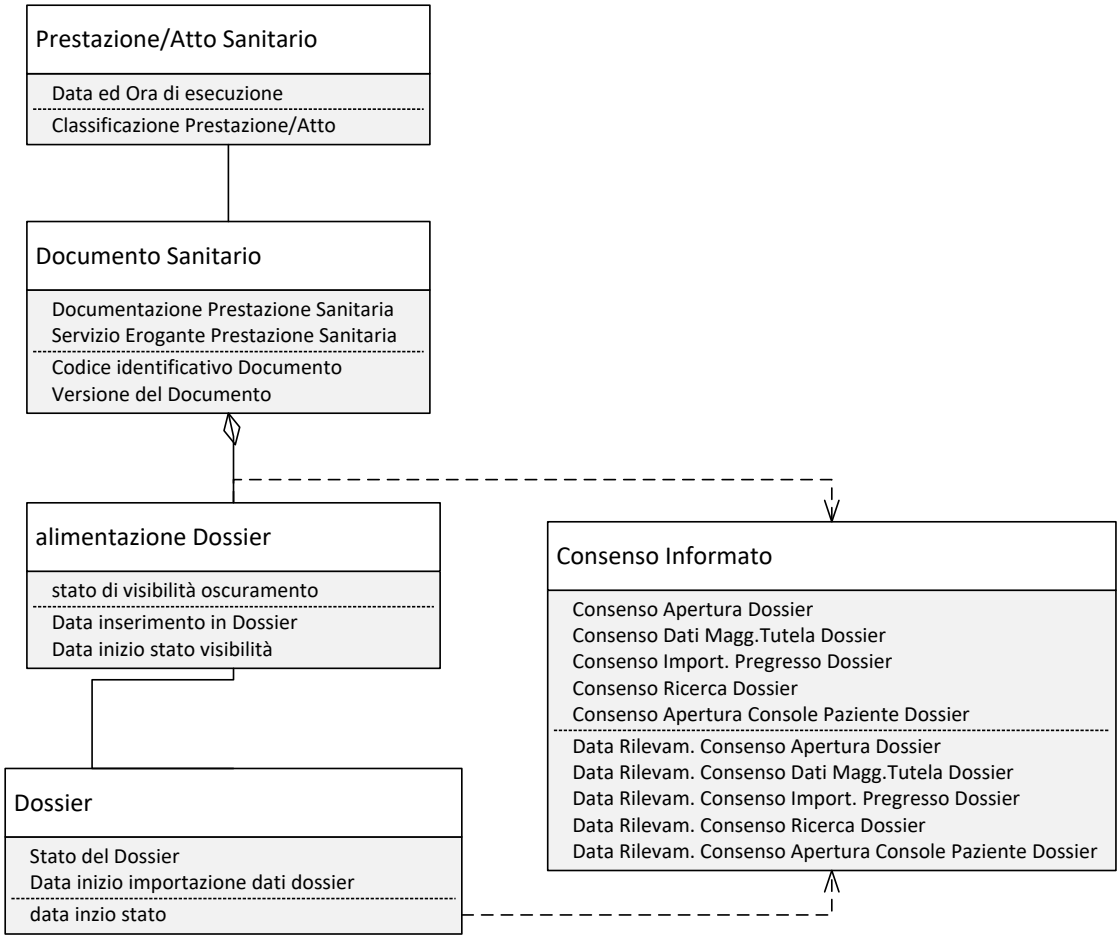


Figura 108. Information Model Generale “Gestione Finalità di ricerca aggregata”

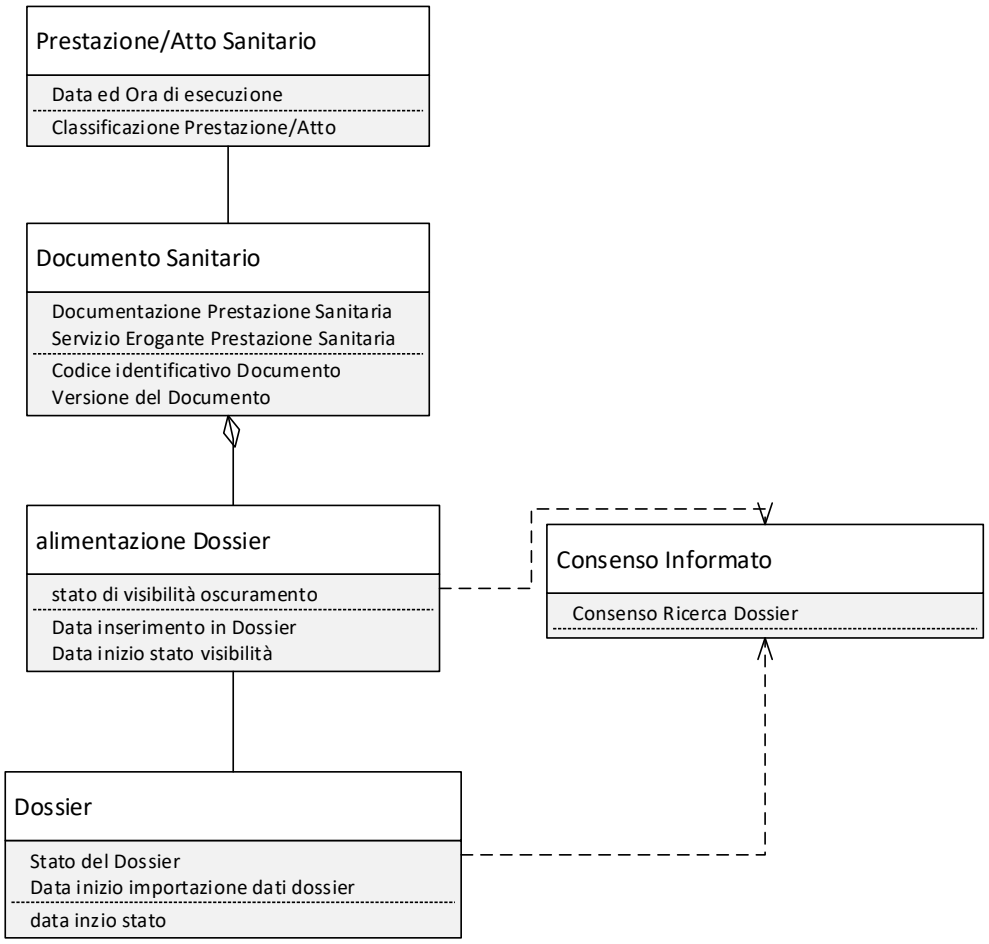


Figura 109. Information Model contenuto minimo "Gestione Finalità di ricerca aggregata"

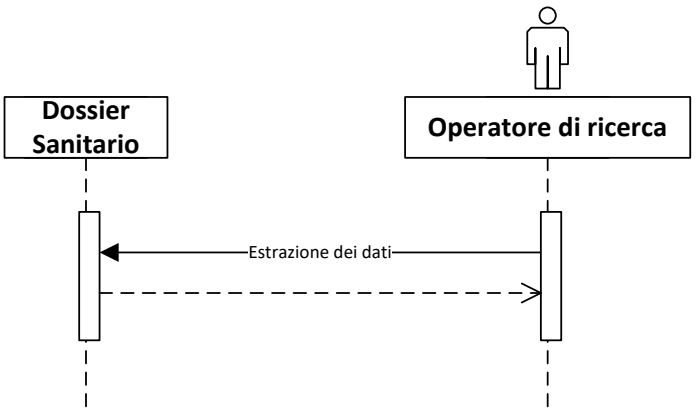


Figura 110. Interaction Model contenuto minimo "Gestione Finalità di ricerca aggregata"

4.3.26 SC26 – Rilascio delega per accesso dossier

Descrizione del caso d'uso

Il presente caso d'uso permette ad un paziente di rilasciare una delega in favore di un altro soggetto al fine poterlo far accedere al dossier per poter visionare i suoi dati e i documenti sanitari contenuti nel Dossier sanitario.

Attore Primario

Paziente.

Precondizioni

Al fine di poter rilasciare una delega il paziente dovrà:

- essere identificato con idonei meccanismi che ne garantiscano l'identità,
- essere maggiorenne,
- essere registrato presso l'anagrafe sanitaria,
- SC2, UCM D2 Consenso apertura.

Il delegato dovrà:

- essere identificato con idonei meccanismi che ne garantiscano l'identità,
- essere maggiorenne.

Scenario

Il paziente rilascia apposita delega ad un soggetto terzo da lui prescelto al fine di permettergli di visualizzare, nei limiti di durata della delega, i dati e le informazioni contenute nel proprio dossier sanitario.

Post-condizione

Nessuna.

Use Case Model

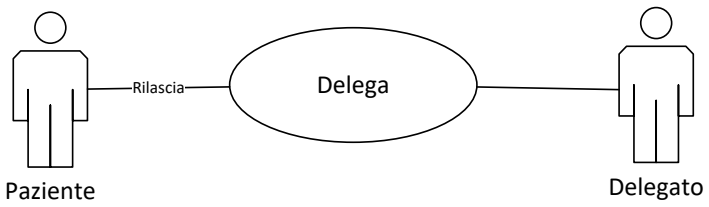


Figura 111. UCM D26 "Rilascio delega accesso Dossier"

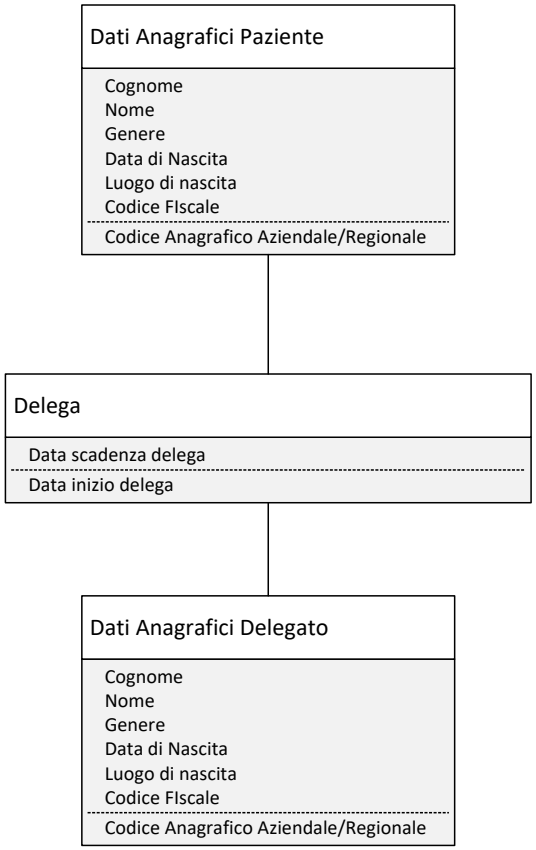


Figura 112. Information Model “Rilascio delega accesso Dossier”

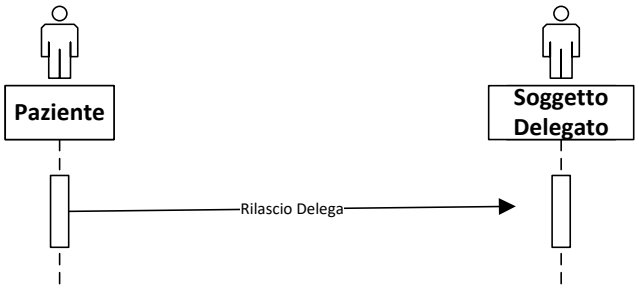


Figura 113. Interaction Model “Rilascio delega accesso Dossier”

4.3.27 SC27 - Gestione visualizzazione dossier con delega

Descrizione del caso d'uso

Il presente caso d'uso permette ad un soggetto delegato dall'incaricato di poter accedere al dossier al fine di poter visionare e gestire i dati e i documenti sanitari contenuti nel Dossier sanitario.

Attore Primario

Delegato.

Precondizioni

Al fine di poter consultare i dati e i documenti il soggetto delegato deve:

- SC26, UCM D26 Rilascio delega per accesso dossier.

Scenario

Il soggetto delegato in caso di necessità d'accesso, dopo essersi autenticato con proprie credenziali, potrà visionare i documenti contenuti nel dossier del soggetto delegante.

Post-condizione

Nessuna.

Use Case Model

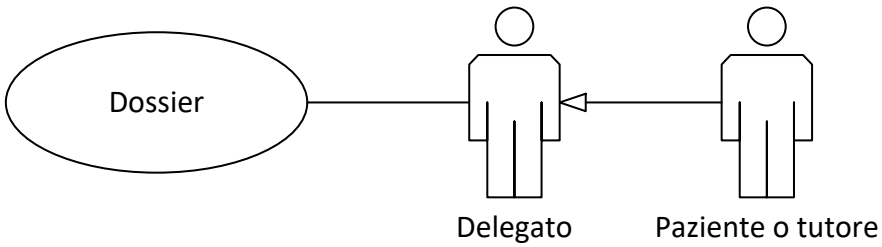


Figura 114. UCM D27 "Gestione visualizzazione dossier con delega"

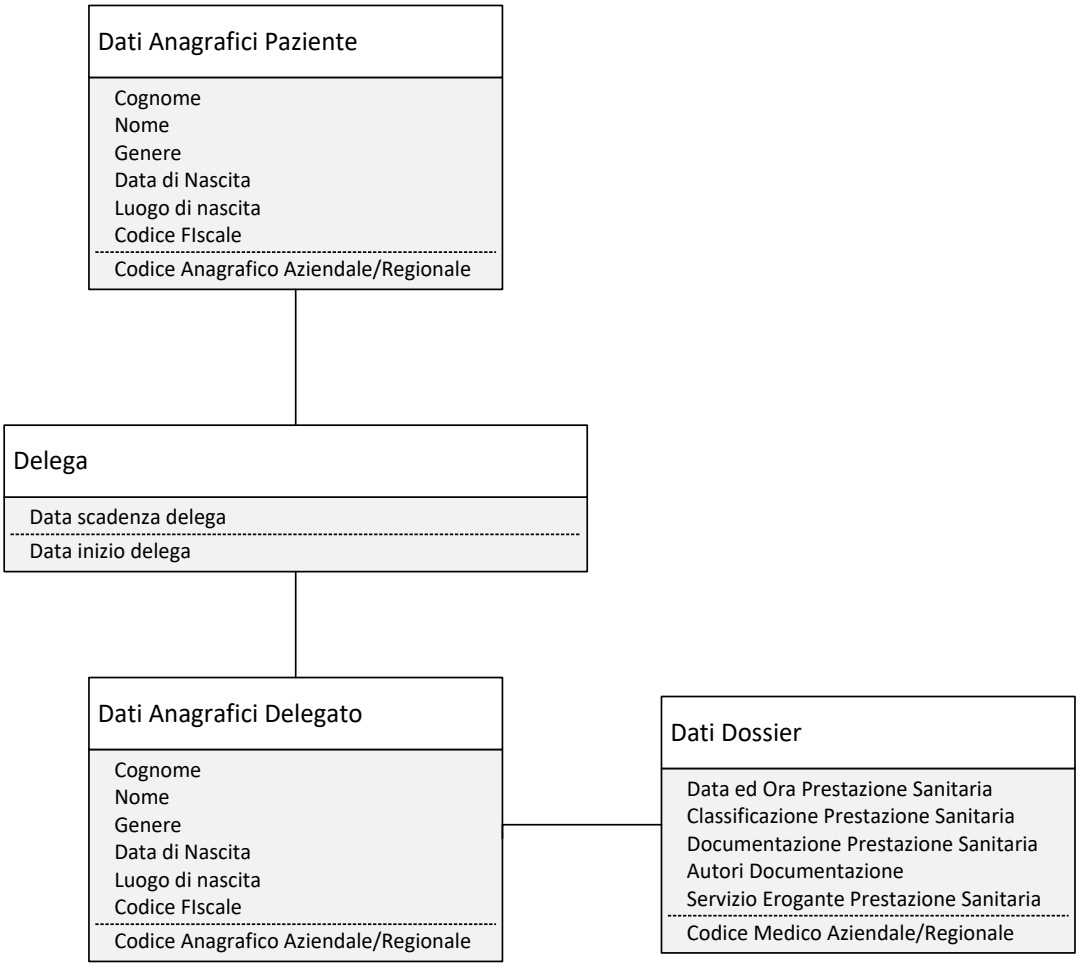


Figura 115. Information Model "Gestione visualizzazione dossier con delega"

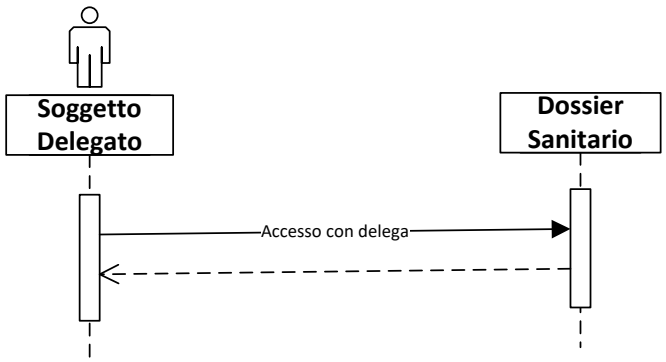


Figura 116. Interaction Model "Gestione visualizzazione dossier con delega"

4.4 Applicazioni degli Use Case in strumenti di gestione del dossier

4.4.1 Strumenti per i pazienti

Il sistema sviluppato presso la Fondazione G. Monastero prevede per il paziente due diverse tipologie di accesso al dossier.

Attraverso l'uso di un dispositivi *mobile (Utilizzando l'App)*

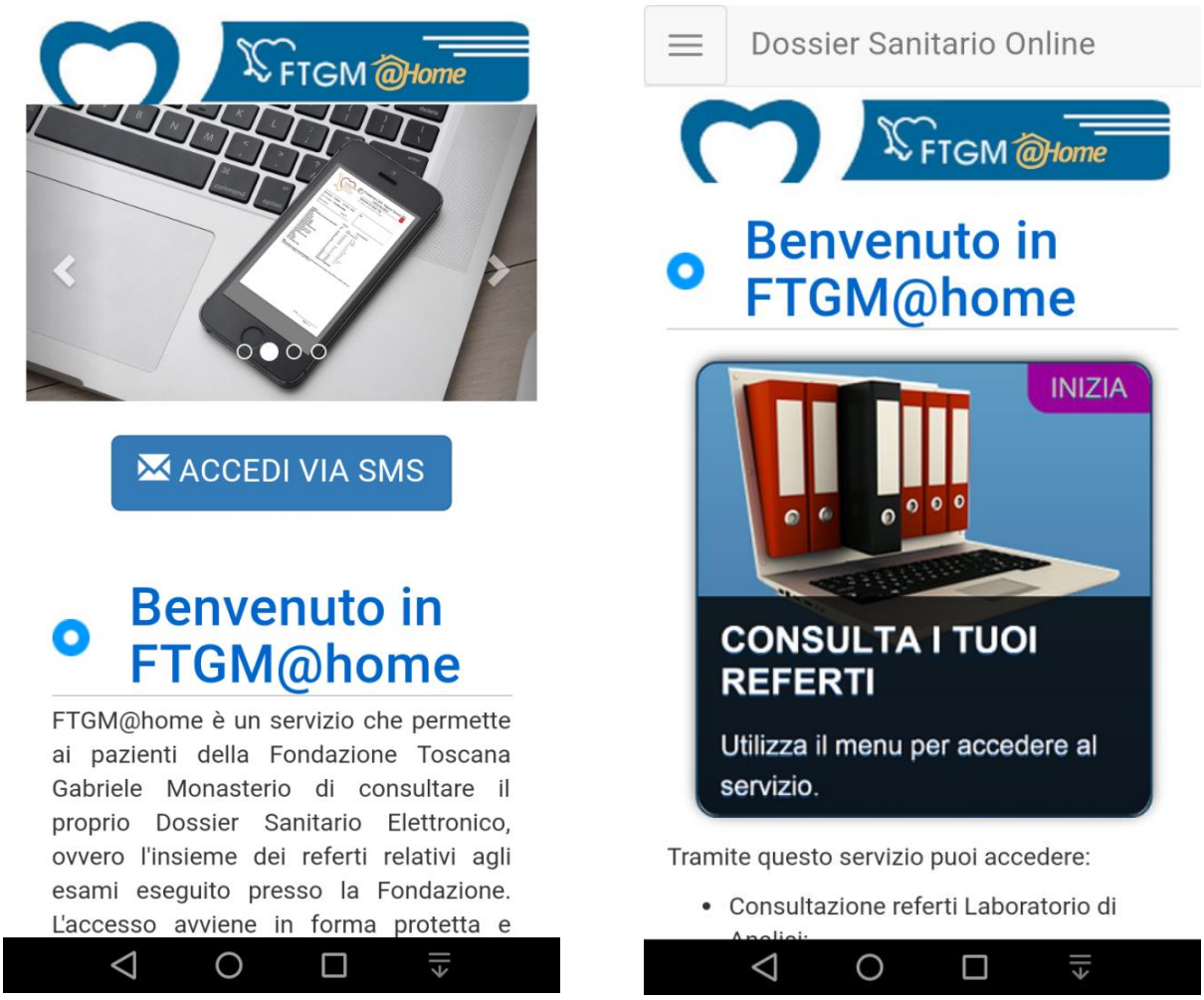
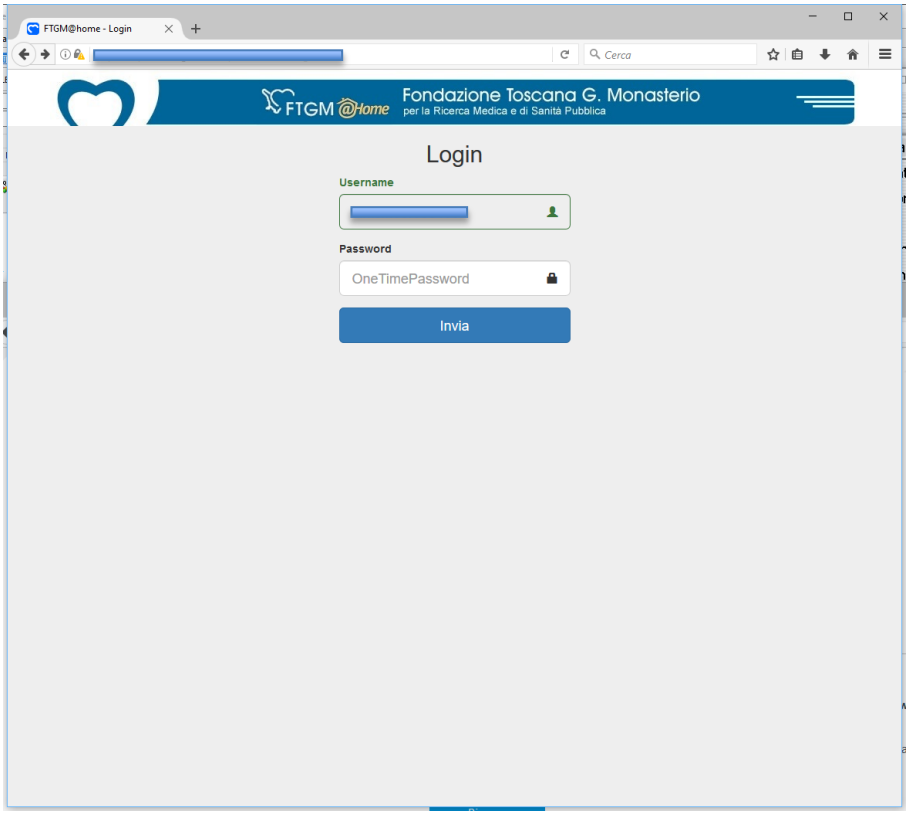


Figura 117. Interfaccia di accesso e di consultazione del Dossier attraverso *APP*

Attraverso l’utilizzo di un personal computer accedendo da sito web

Figura 118. Interfaccia di accesso attraverso sito web



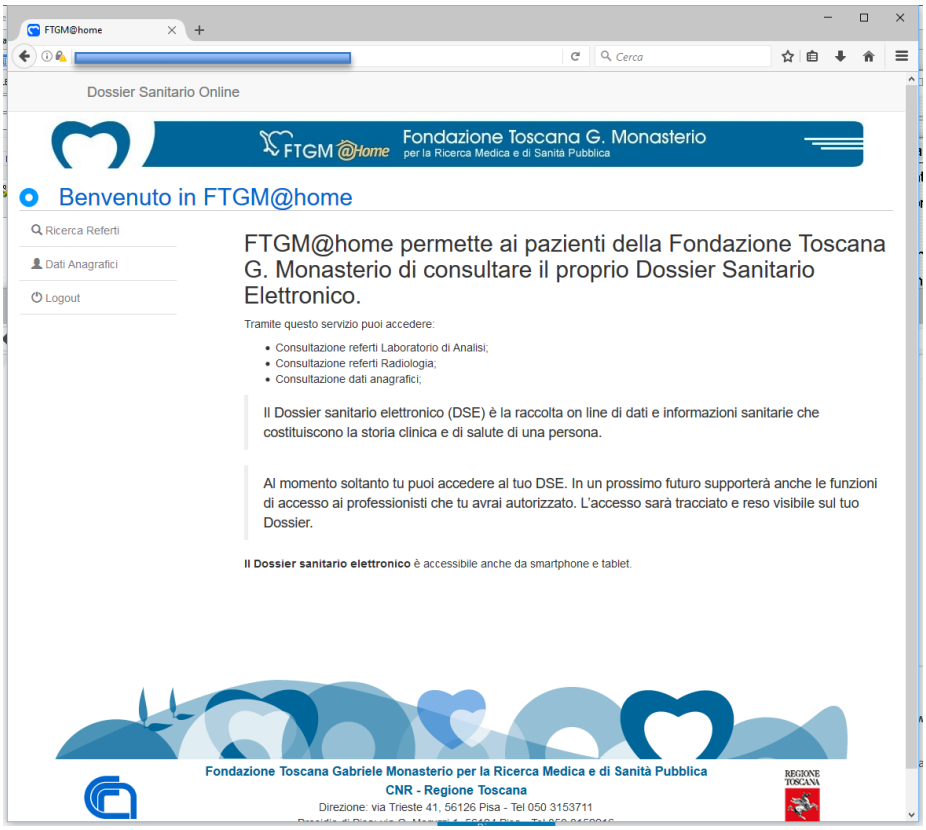
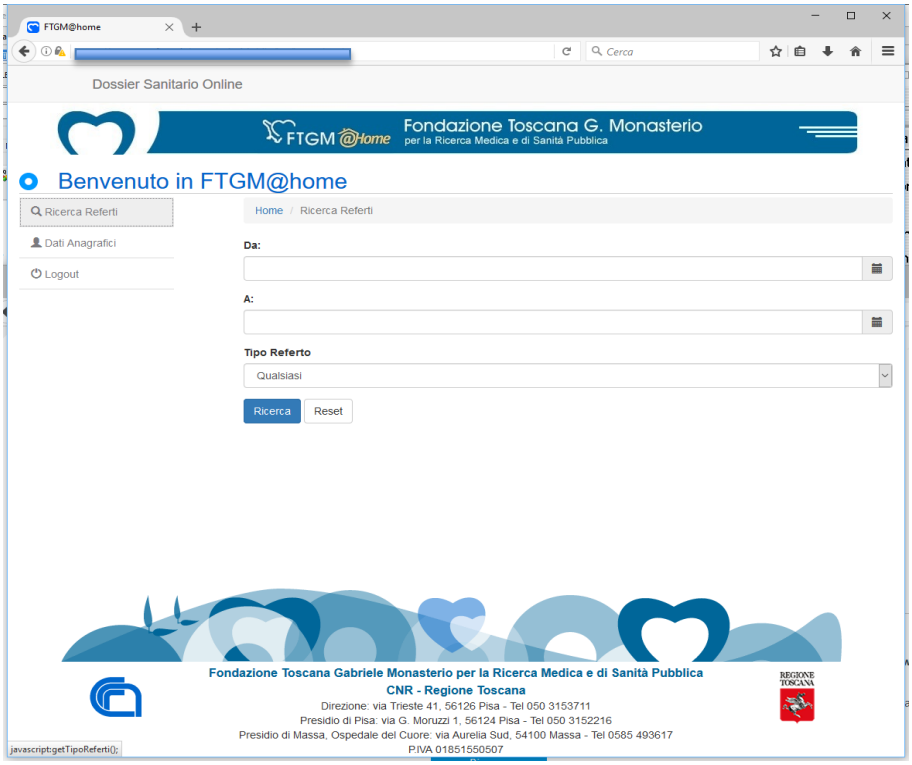


Figura 119. Interfaccia Login e Benvenuto via sito web

A)



B)

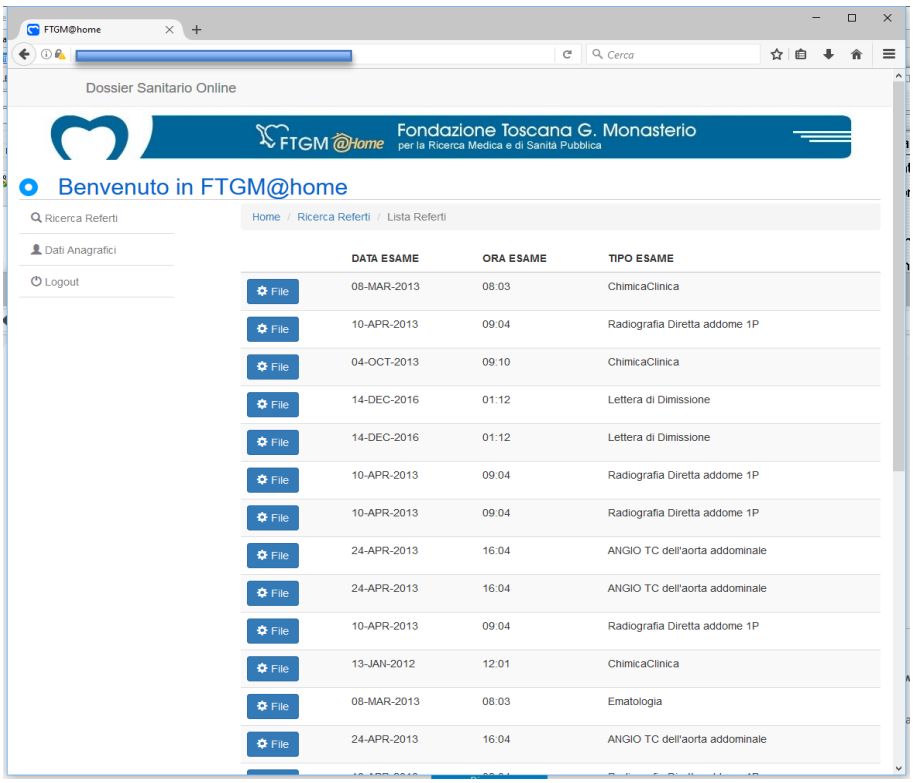
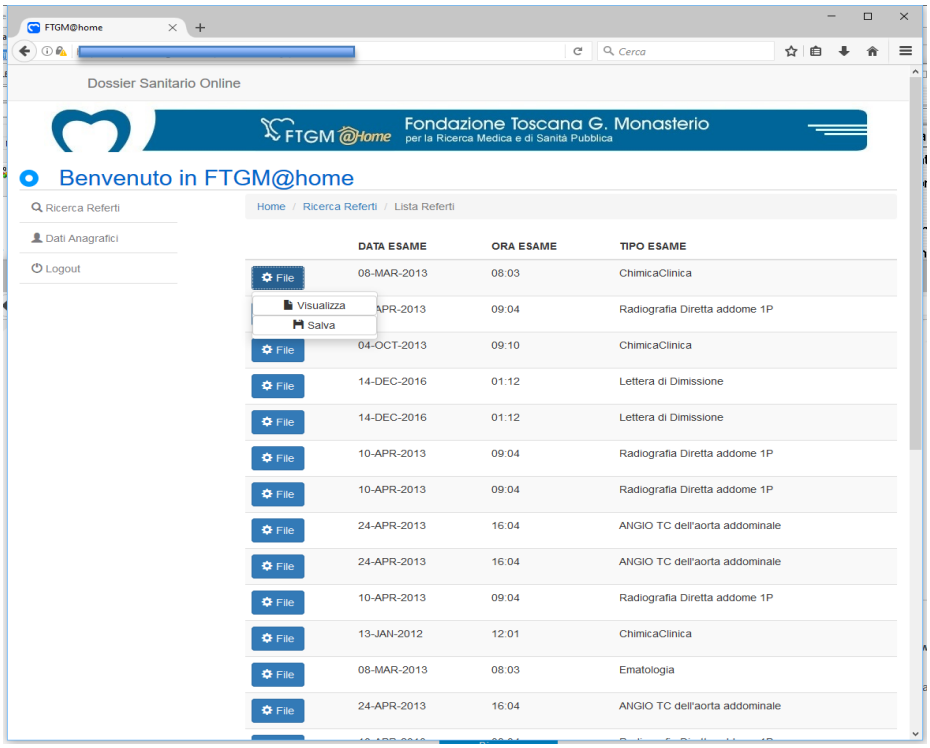


Figura 120. Interfaccia di Ricerca (A) e di consultazione (B) della lista referti

A)



B)

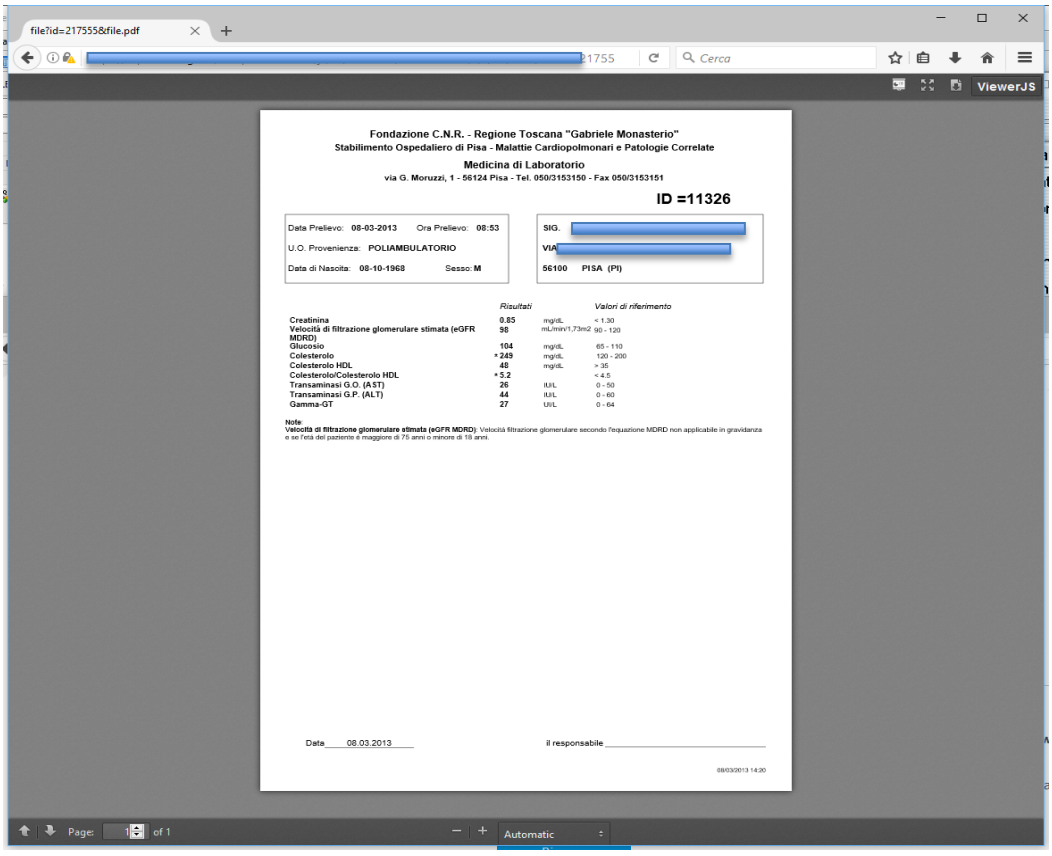


Figura 121. Interfaccia di consultazione (A) e di visualizzazione (B) dei referti

4.4.2 Strumenti per gli operatori sanitari

Di seguito si riportano a titolo esemplificativo e non esaustivo alcune schede del sistema che gli operatori sanitari trovano accedendo in *back office* con le proprie credenziali.

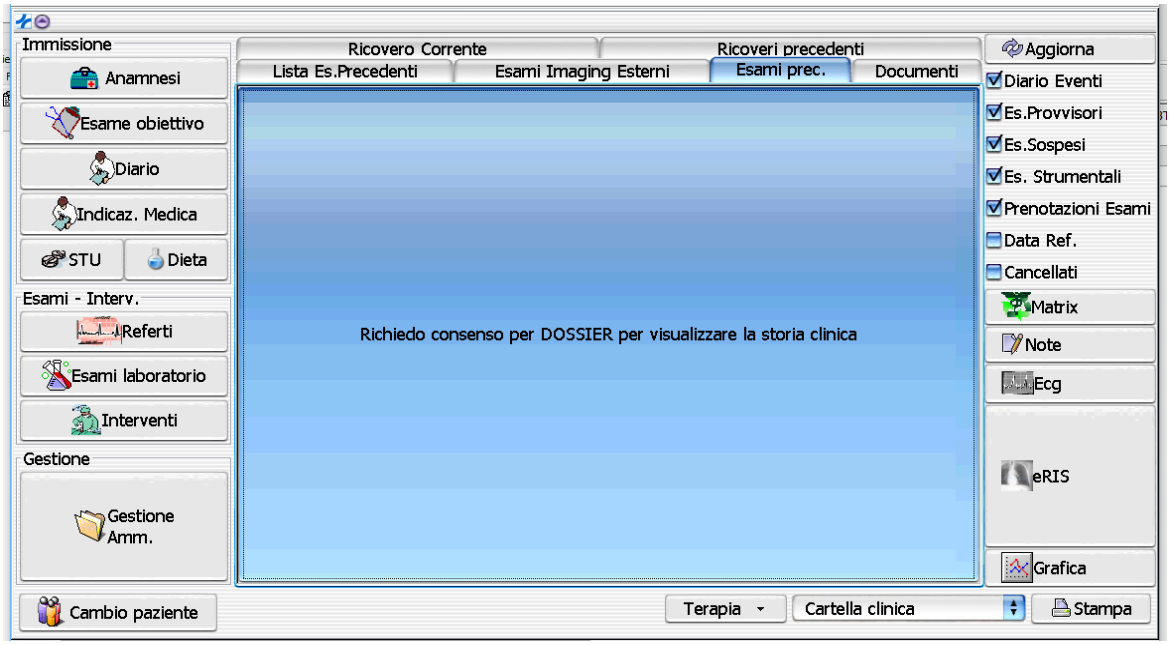


Figura 122. Accesso ai sistemi senza consenso al Dossier

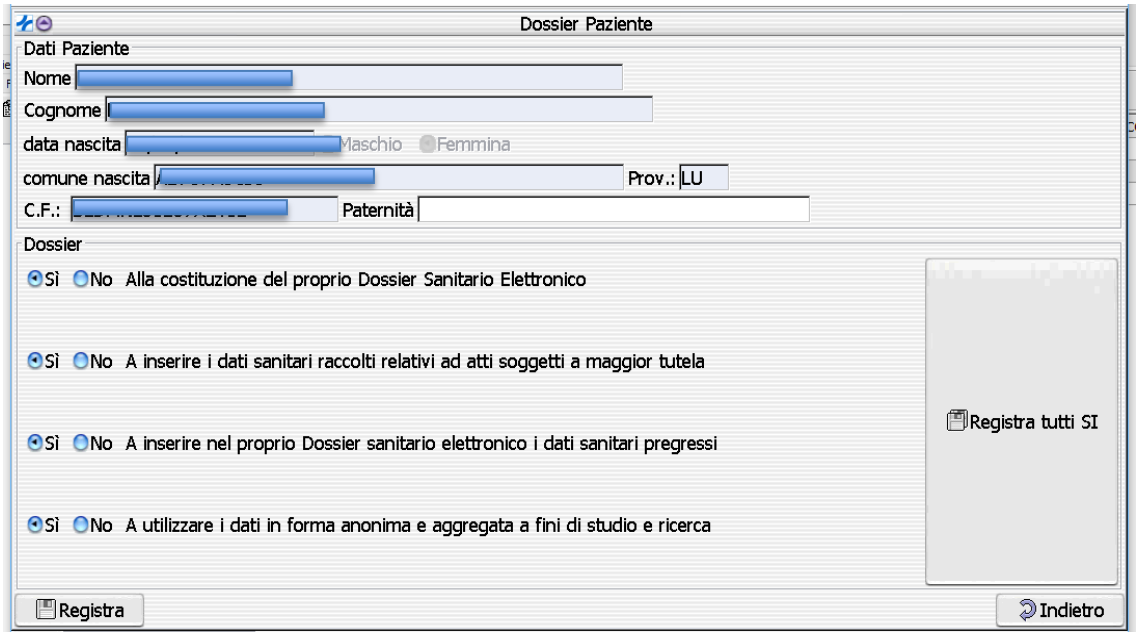


Figura 123. Esempio di acquisizione del consenso alla apertura.

Il documento cartaceo di consenso[187], firmato dal paziente, viene riportato come scelte nei sistemi informatici.

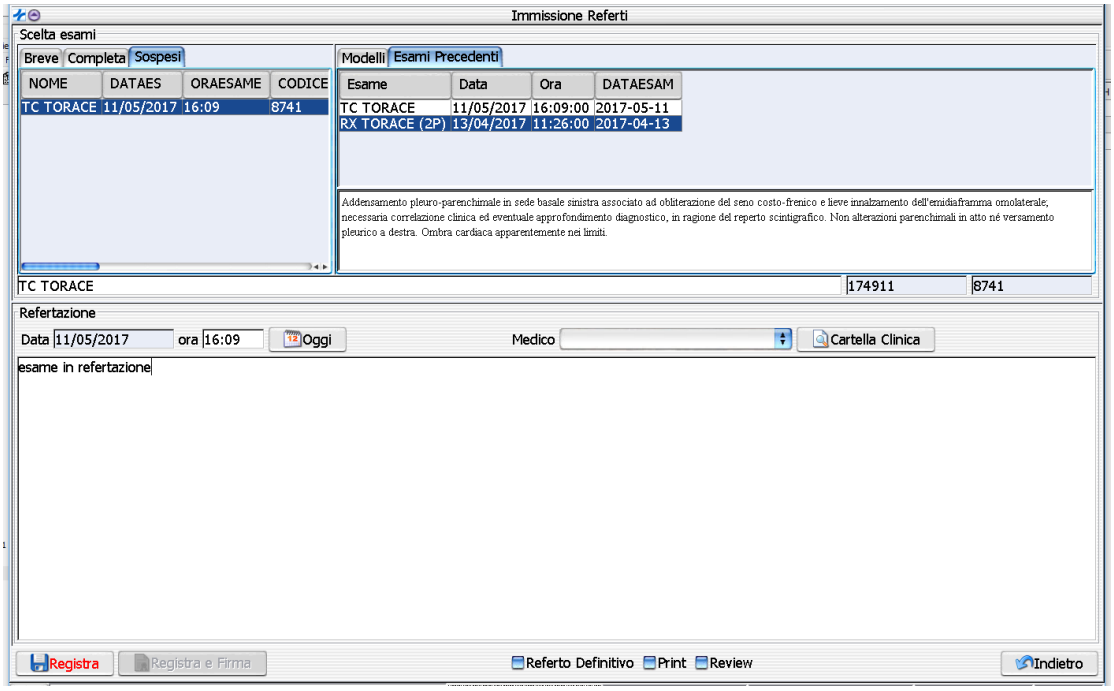


Figura 124. Esempio di uso del dossier da parte di un medico radiologo nella refertazione di una indagine TAC.

[187] *Cfr. Modulo consenso trattamento dati con DS*, in Appendice, p.246-248.

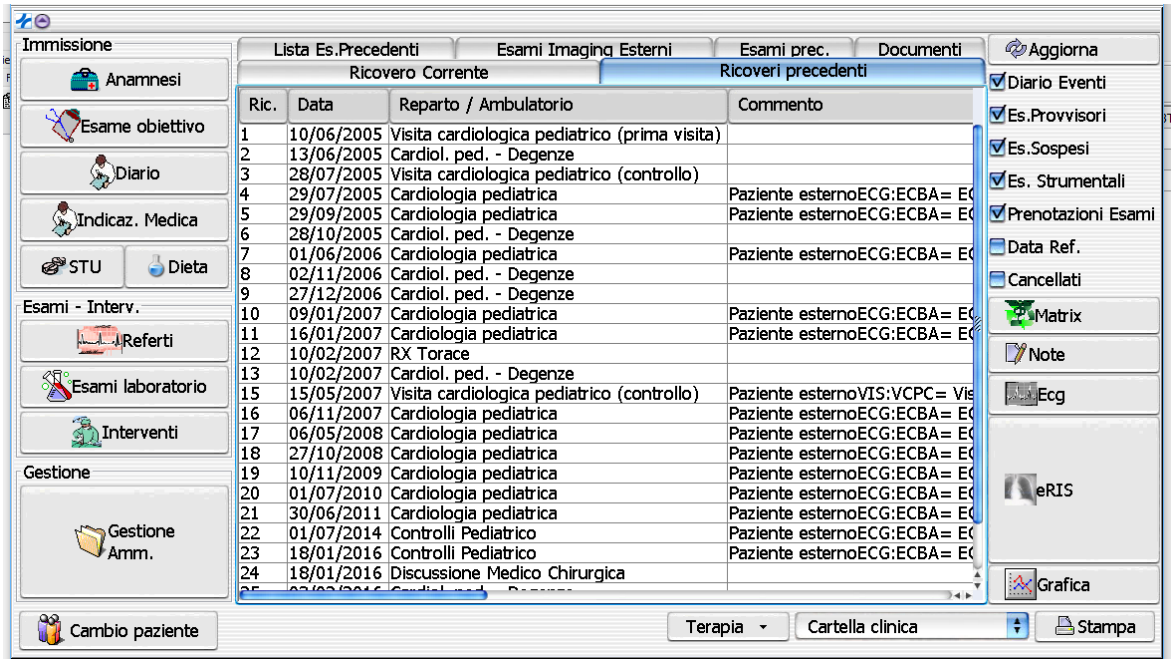


Figura 125. Esempio di visualizzazione sintetica Dossier per la consultazione integrata in una cartella clinica di ricovero.

Interessante è notare dalla figura sopra riportata (Figura 125) che nella linguetta *"Ricoveri precedenti"* compare la lista, eventualmente filtrata dagli oscuramenti, dei precedenti accessi alla struttura sanitaria.

CONCLUSIONI

L'approfondimento svolto nel presente lavoro di ricerca ha reso ben evidente la grandissima utilità che strumenti informativi quali il Dossier Sanitario, la Cartella Clinica Elettronica, il Fascicolo Sanitario Elettronico, i sistemi di *Personal Health Record* possono offrire allo sviluppo e all'efficienza dei sistemi sanitari e al potenziamento dei trattamenti diagnostici e di cura.

L'introduzione di siffatti strumenti in un percorso diagnostico-terapeutico determina, infatti, vantaggi assai rilevanti in capo alle strutture e ai diversi operatori sanitari; a meno di non voler immaginare, laddove possibile, l'esistenza di un equivalente cartaceo di tali supporti, con analoghe capacità di completezza informativa e di facilità di accesso.

E, d'altra parte, non si possono ritenere meno rilevanti i vantaggi sotto il profilo delle efficienze di spesa conseguibili attraverso l'implementazione dell'*eHealth* nell'ambito del Sistema Sanitario Nazionale, attraverso cui è possibile, pur a fronte degli elevati costi della sanità pubblica, un'allocazione delle risorse[188] che riduca al minimo gli sprechi e i trattamenti impropri e/o inefficaci.

IT, innovazione di processo, centralità della persona e privacy sono indubbiamente i quattro principali *driver* che stanno indirizzando e cambiando i servizi sanitari nel sistema di sanità "2.0", o di nuova generazione che dir si voglia, con esiti tangibili di miglioramento della gestione del paziente e della prevenzione del rischio clinico.

Come emerso nei primi due capitoli, nuovi saperi, uniti a tecnologie sempre più intelligenti, interattive e personalizzate, stanno ponendo sempre più al centro dell'attenzione la persona, che costituisce il fulcro di tutti i programmi internazionali legati alla crescita e allo sviluppo strategico della popolazione: soltanto favorendo un miglioramento delle condizioni e della qualità della vita, *in primis* preservandone

---

[188] Sotto questo profilo, la recente ricerca dell'Osservatorio Innovazione Digitale in Sanità della School of Management del Politecnico di Milano, presentata il 4 maggio 2016 a Milano durante il convegno *"Sanità digitale: non più miraggio, non ancora realtà",* afferma che: *"La Sanità digitale in Italia non è più un miraggio, ma un piano perseguibile che dà frutti concreti, anche se la velocità di attuazione è ancora modesta e disomogenea. E il principale ambito su cui hanno investito le strutture sanitarie è la Cartella Clinica Elettronica (CCE), con una spesa di 64 milioni di euro (+10% rispetto al 2014), valore che nel 2016 dovrebbe aumentare per il 43% delle aziende del campione. Seguono i sistemi di front-end (61 milioni di euro budget), il Disaster Recovery e continuità operativa (48 milioni), la gestione amministrativa delle risorse umane (39 milioni), la gestione informatizzata dei farmaci (26 milioni). Rilevante è anche l'ambito dei sistemi di gestione documentale e di conservazione a norma, per il quale il 58% dei CIO prospetta aumenti nel 2016, a fronte di una spesa attuale di 24 milioni di euro. Il 40% dei CIO prevede incrementi di spesa nei servizi digitali al cittadino (oggi 19 milioni di euro)".*

l'integrità e le condizioni di salute, le persone possono immaginare e costruire il proprio futuro, e contribuire al comune progresso.

Se davvero così potenzialmente forieri di benefici per le persone e per la collettività, perché gli strumenti digitali dell'*e-health* sono ancora percepiti come portatori di rischi perlomeno in egual misura rispetto ai vantaggi che essi possono arrecare?

Perché dei nodi critici sussistono, e questi vanno anche al di là dei più dibattuti temi dell'accesso ai dati contenuti in questi supporti.

Sul piano della pratica medica, innanzitutto, vi è da rilevare che il disporre di maggiori e più precise informazioni sui trascorsi sanitari di un paziente è arma a doppio taglio: se ciò può indurre il medico ad intervenire con minori esitazioni e con la probabilità di minori margini di errore su casi per i quali dispone di un quadro informativo adeguato e che non presentino particolari problemi secondo l'*id quod plerumque accidit*, è altrettanto vero che l'evenienza di ritrovarsi a trattare casi per i quali FSE o Dossier risultino avari di dati o, al contrario, ne presentino più che a sufficienza per delineare un spiccato quadro di rischio del paziente, potrebbe indurre i medici più cauti o con trascorsi di *malpractice* medica accertata a rifugiarsi nella "medicina difensiva"[189], anche al costo di non intraprendere, con tutte le eventuali conseguenze del caso, eventuali misure terapeutiche probabilmente più efficaci ma anche più rischiose, pur di non incorrere in situazioni da cui possa scaturire la propria responsabilità civile e penale. Così che, se da un lato il continuo progresso tecnologico ha accresciuto il grado di adeguatezza e di originalità dell'intervento sanitario, dall'altro ha condotto verso la diretta conseguenza dell'assoggettamento della pratica medica e di tutte le attività connesse ad un'esigenza di controllo giuridico. In quest'ottica, non sembra azzardato asserire che medicina e diritto possono essere intese come due facce di una stessa medaglia: da prospettive diverse, entrambi mirano ad assicurare la salute dell'individuo, ma con risvolti applicativi non di rado confliggenti[190]. È nel solco di

---

[189] Tale pratica si verifica quando i medici prescrivono test, procedure diagnostiche o visite, oppure evitano pazienti o trattamenti ad alto rischio, principalmente (ma non esclusivamente) per ridurre la possibilità del realizzarsi di conseguenza dannose che possono sfociare in un successivo giudizio di responsabilità in capo al medico. La medicina difensiva, pertanto, determina conseguenze fortemente negative poiché riduce in favore degli assistiti, le loro aspettative di guarigione e la fruizione di servizi rispondenti alle loro richieste. Sul punto *Cfr.* G. Guerra, *La 'medicina difensiva': fenomeno moderno dalle radici antiche,* in Salute e Diritto, Ottobre-Dicembre 2013, Vol. 14, N. 4; E. Balboni, M. Campagna, *Osservazioni sul governo clinico anche come origine alla medicina difensiva*, in De Vincenti, Finocchi Ghersi, Tardiola (a cura di), *La sanità in Italia. Organizzazione, governo, regolazione, mercato*, Collana 'Quaderni di Astrid, 2011, Bologna, Il Mulino.

[190] U. Izzo, *Medicina e diritto nell'era digitale: i problemi giuridici della cybermedicina*, Danno e Responsabilità, 8; 9/2000, p. 807.

queste potenziali conflittualità tra pratica medica e diritto che, negli ultimi anni, oltre alle varie norme succedutesi nel tempo nell'ambito della responsabilità medica[191], si è sempre più sviluppata l'*Informatica Forense Sanitaria,* branca dell'Informatica forense[192] che costituirà un necessario supporto nelle operazioni di corretto trattamento ed acquisizione dei dati, a fini di indagine[193], per la tutela dei diritti lesi a causa o in occasione dell'espletamento di attività sanitaria e/o per la difesa delle parti coinvolte, a vario titolo[194].

Vi sono poi le criticità sul piano tecnico. Basti pensare alla mancanza di interoperabilità tra i sistemi informativi, che rendono le informazioni accessibili solo a livello locale e spesso hanno caratteristiche comprensibili solo a chi le ha elaborate, oppure al più volte citato diritto di oscuramento, che se da un lato assicura un pieno diritto di autodeterminazione del paziente, dall'altro determina *gap* informativi in capo agli operatori sanitari. In questo scenario influiscono anche i cambiamenti evolutivi dell'ICT, talvolta così repentini da mettere in difficoltà i pazienti appartenenti alle fasce meno giovani della popolazione o con maggiori difficoltà di accessibilità e fruibilità,

---

[191] Da ultimo lo scorso 28 febbraio 2017 è stato approvato il disegno di legge C-259, proposto dall'onorevole Federico Gelli da cui ha preso il nome (c.d. Legge Gelli), che reca "*disposizioni in materia di sicurezza delle cure e della persona assistita, nonché in materia di responsabilità professionale degli esercenti le professioni sanitarie*". E' stato così abrogato l'art. 3, comma 1, D.L. 158 del 13 settembre 2012 (c.d. Decreto Balduzzi) che disponeva che *"L'esercente la professione sanitaria che nello svolgimento della propria attività si attiene a linee guida e buone pratiche accreditate dalla comunità scientifica non risponde penalmente per colpa lieve. In tali casi resta comunque fermo l'obbligo di cui all'art. 2043 del codice civile. Il giudice, anche nella determinazione del risarcimento del danno, tiene debitamente conto della condotta di cui al primo periodo"*.

In particolare, la Legge Gelli affronta e disciplina i temi della sicurezza delle cure e del rischio sanitario, della responsabilità dell'esercente la professione sanitaria e della struttura sanitaria pubblica o privata, delle modalità e caratteristiche dei procedimenti giudiziari aventi ad oggetto la responsabilità sanitaria, nonché degli obblighi di assicurazione e dell'istituzione del Fondo di garanzia per i soggetti danneggiati da responsabilità sanitaria. Sul punto un primo commento v. L. Roccatagliata, *Il Ddl Gelli è legge. Ecco tutte le novità in tema di responsabilità medica,* in Giurisprudenza Penale Web, 2017, 3. http://www.giurisprudenzapenale.com/2017/03/01/ddl-gelli-legge-tutte-le-novita (ultimo accesso giugno 2017).

[192] L'informatica forense si occupa dell'acquisizione, conservazione e analisi di tutti dati e le informazioni contenute in dispositivi digitali, con lo scopo di evidenziare l'esistenza di prove utili allo svolgimento di attività investigative. Per approfondire l'argomento v. C. Maioli, *Dar voce alle prove: elementi di Informatica Forense*, in P. Pozzi (a cura di), *Crimine virtuale, minaccia reale*, Franco Angeli, 2004.

[193] Sulle investigazioni in ambito informatico v. L. Luparia - G. Ziccardi, *Investigazione penale e tecnologia informatica*, Giuffrè, 2007.

[194] D. Caccavella; A. Gammarota, *Informatica Forense Sanitaria per l'eHealth,* in C. Faralli, R. Brighi, M. Martoni (a cura di) *Strumenti, diritti, regole e nuove relazioni di cura: il paziente europeo protagonista nell' eHealth*, Giappichelli, 2015, p. 213; D. Caccavella, M. Ferrazzano, F. Banorri, *L'implementazione dei processi organizzativi finalizzati alla gestione del rischio nell'ambito di strutture sanitarie*, in C. Faralli, R. Brighi, M. Martoni (a cura di), Strumenti, diritti, regole e nuove relazioni di Cura. Il Paziente europeo protagonista nell'eHealth, Giappichelli, 2015, pp. 221-230.

aumentando il c.d. *digital divide*[195], e depotenziando o persino annullando l'efficacia dell'intero scopo funzionale dei sistemi elettronici (es. il Dossier sanitario), pensati per assicurare al fruitore anche una prevenzione proattiva. Non di rado queste difficoltà sono causate da un rifiuto culturale, ma spesso è legato anche alla condizione economica o semplicemente le persone non hanno l'abitudine ad usare le tecnologie digitali.

Al fine di contenere i *gap* informativi in questione e di garantire su più ampia scala (pensiamo, in prima battuta, alla sola UE) la continuità assistenziale, il trattamento sanitario dei cittadini dell'Unione su basi informative adeguate e la capacità di essere soggetti attivi e consapevoli, anche al di fuori del territorio nazionale, si rendono evidentemente necessari tanto sistemi informativi sanitari standardizzati e interoperabili, quanto la definizione di un quadro normativo comune ai 27 Paesi dell'Unione europea nel quale questi siano armonicamente regolati. Quindi, le leve dell'armonizzazione tra standard e dell'armonizzazione normativa debbono procedere di pari passo.

Quest'ultima non è, però, soltanto una prospettiva auspicata, ma è ciò verso cui il contesto unionale si sta ormai concretamente indirizzando, sia con il Regolamento (UE) eiDAS, n. 910/2014[196], sia con il Regolamento europeo sulla privacy. La messa a punto di tali fondamentali atti normativi è maturata in un'ottica di rafforzamento, da parte del Legislatore europeo, della fiducia di cittadini, autorità pubbliche, professionisti e imprese verso lo sviluppo di servizi IT innovativi e sicuri, semplificando gli adempimenti amministrativi e burocratici e rendendo il mercato dei servizi di autenticazione più trasparenti e in generale più rispettosi della privacy dei cittadini.

Alla luce di tutto ciò, in un futuro recente, si potrebbe ipotizzare di integrare i dati ed i documenti strutturati e certificati, contenuti nel Dossier sanitario, con altri, magari raccolti in maniera più occasionale ma rigorosamente certificabili e ritenuti attendibili grazie all'identificazione e tracciamento del soggetto cui si riferiscono, ed utili agli operatori sanitari per farsi un'idea attendibile sullo stile di vita e quindi dello stato di salute del paziente.

Infatti, bisogna iniziare a pensare ad una digitalizzazione della sanità non solo come una semplice "dematerializzazione" dei vari servizi, ma anche come *fattore chiave* per consentire, in maniera completa ed in tempo reale, anche grazie all'architettura *cloud* ed alle tecnologie *mobile*, una gestione oggettiva e professionale

---

[195] *Cfr.* P. Norris, *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide,* Cambridge University Press, Oxford, 2001, 3 ss.

[196] Regolamento (UE) n. 910/2014 del parlamento europeo e del consiglio del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

del singolo caso.

Insomma, le *wearable technologies*[197] (ad es. *Google Glass*, *Smart watch),* applicate al monitoraggio quotidiano dei parametri biomedici e all'utilizzo di *apps* medicali potrebbero fornire un ottimo contributo per arricchire il Dossier sanitario, consentendo un migliore monitoraggio dello stato di salute della persona ed accrescendo ancor più l'efficacia dei percorsi di cura e degli esiti delle strategie di prevenzione.

L'obiettivo principale in sanità dovrebbe essere quindi quello di puntare ad individuare e razionalizzare, a livello nazionale, le basi di dati delle singole strutture sanitarie (pubbliche e private) e darvi accesso al paziente e ai soggetti legittimati, tramite il Sistema Pubblico di Identità Digitale[198] (Spid) e la connessione alla Anagrafe Unica della Popolazione Residente (ANPR)[199].

La maturità delle architetture tecnologiche e dei sistemi informativi, insieme alle recenti norme e ai principi cardini che le compongono, come ad esempio la *"Privacy by design",* permettono infatti di immaginare costruttivamente l'impatto positivo che questi, nell'attuale società "a cambiamento velocissimo"[200], potranno avere sulla qualità della vita delle persone, nella gestione della sanità pubblica e privata, nella cura della salute e del benessere e nella prevenzione e nella predizione delle patologie, anche se, per far sì che ciò accada, occorre intraprendere azioni come: creare canali specifici e affidabili che siano in grado di coinvolgere i cittadini-pazienti nella gestione della propria salute (prevenzione attiva); diffondere gli ausili tecnologici della sanità digitale attraverso buone pratiche comunicative; strutturare linee guida giuridiche e operative per l'utilizzo degli strumenti in parola; potenziare la volontà e la capacità degli operatori sanitari di individuare e condividere sistematicamente le informazioni che ritengono maggiormente interessanti, ma avendo sempre ben presente la doverosità di espletare la

---

[197] I *wearable technologies (c.d.* dispositivi indossabili) sono dispositivi elettronici che come caratteristica primaria hanno quella di essere portabili e modellati attorno al corpo delle persone (possono anche essere integrati negli indumenti) e grazie alla rilevazione ed il monitoraggio di segnali del corpo permettono a queste tecnologie di diventare un valido assistente per i bisogni dell'utente. Un esempio di questo tipo di tecnologia è il progetto Glass di Google.

[198] Spid è la soluzione che permettere di accedere a tutti i servizi della pubblica amministrazione con un'unica Identità Digitale. Per maggiori informazioni sul progetto visitare il sito www.spig.gov.it (ultimo accesso giugno 2017).

[199] Attraverso l'ANPR si realizza un'unica banca dati con tutte le informazioni anagrafiche della popolazione a cui faranno riferimento non solo i comuni, ma l'intera Pubblica amministrazione e a tutti coloro che sono interessati ai dati anagrafici, in particolare i gestori di pubblici servizi. Per maggiori informazioni sul progetto visitare il sito www.anpr.interno.it (ultimo accesso giugno 2017).

[200] v. Discorso del Garante per la protezione dei dati personali, Prof. Francesco Pizzetti, al Parlamento, in occasione della presentazione della Relazione dell'attività del Garante nel 2005, pubblicato in www.garanteprivacy.it. Sull'evoluzione delle tecnologie della «società dell'informazione» cfr. A. Di Martino, *La protezione dei dati personali,* in S.P. Panunzio (a cura di), *I diritti fondamentali e le Corti in Europa,* Napoli, Esi, 2005.

pratica clinica nel rispetto delle normative.

La diffusione e l'applicazione scrupolosa di buone prassi e linee guida giuridiche con riferimento alle tecnologie "inanimate"[201] è quanto mai necessaria in un "ecosistema" digitale contraddistinto dal costante interfacciarsi tra oggetti e sistemi informativi che, seppur formidabile volano di innovazioni di prodotto e di processo, pone rilevanti problematiche, anzitutto sotto il profilo della sicurezza degli strumenti stessi, alla luce della loro connessione permanente in rete.

Ne è la prova il fatto che, negli ultimi mesi, non sono mancati su scala internazionale attacchi informatici in ambito sanitario capaci di bloccare la regolare attività medica, provocando, con la sospensione della funzionalità dei sistemi informatici, un grave rischio per la vita dei pazienti.

Ciò conduce alla necessità di rafforzare il concetto di sicurezza, che quando tocca l'ambito sanitario deve più che mai racchiudere e riassumere in sé i significati dei due vocaboli inglesi che in esso trovano unitaria traduzione, ossia "Safety" e "Security", come ben osserva Giustozzi[202] in un suo recente intervento. Dove per *safety*, nel caso di specie, s'intende l'assenza per il paziente di danni accidentali[203] (in altri termini, gli strumenti con cui entrerà in contatto non dovranno arrecargli nocumento, preservando così l'incolumità delle persone; per garantire questo risultato vi è necessità di procedure e di processi dei servizi sanitari che riducano la possibilità di errori e/o massimizzino la capacità di intercettarli prima che essi accadano).

Con il termine *security* si richiama invece la sicurezza dei sistemi informatici e delle reti internet e mira ad evitare che soggetti non autorizzati possano interferire nel funzionamento degli stessi.

In questo quadro, ruolo primario è quello di chi progetta il sistema, che dovrà essere capace di applicare gli standard operativi di settore, ma non meno importante è il comportamento corretto e la piena contezza, da parte dell'utente, delle interazioni da lui compiute col sistema.

Le riflessioni svolte in queste pagine conclusive inducono a ritenere che la ricerca condotta, attraverso un approccio traslazionale[204] tra discipline, risorse e competenze,

---

[201] R. Moro Visconti, *Internet delle cose, networks e plusvalore della connettività*, Il Diritto industriale, 2016, fasc. 6 pag. 536-544.

[202] Intervento pubblico tenuto al TED^{x} CNR l'8 ottobre 2016.

[203] Un esempio a riguardo è un caso del 2013 in cui un pacemaker non è entrato in funzione, fallendo il colpo, procurando il coma vegetativo alla paziente. http://milano.corriere.it/notizie/cronaca/15_marzo_11/pacemaker-non-funziono-milione-paziente-finita-coma fd4c3e16-c7cc-11e4-a75d-5ec6ab11448e.shtml, (ultimo accesso giugno 2017).

[204] Il presente studio è stato infatti condotto, nella fase della ricerca applicata, sull'assunto del passaggio dalla teoria alla pratica e poi nuovamente alla teoria, così che da implementare e verificare costantemente le evidenze ipotizzate.

focalizzata sullo stato dell'arte in materia di definizione giuridica e tecnologica degli attuali strumenti di gestione delle informazioni del paziente, pur autosufficiente, può altresì essere intesa come primo *step*[205] di un percorso di approfondimento più ampio, suscettibile di estendersi agli ulteriori sviluppi tecnologici e normativi con cui sicuramente dovremo confrontarci da qui a breve, quali IoT[206], intelligenza artificiale[207] e robotica, e ai flussi di informazioni e alle modalità di interazione tra i soggetti della prestazione sanitaria che da questi deriveranno, con un salto di qualità nella percezione sociale di ciò che rappresenta la sanità digitale.

[205] Non da ultimo, all'atto di redazione delle presenti conclusioni, è stata pubblicata dal Garante privacy la *"Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali"* del 28 aprile 2017, http://www.garanteprivacy.it/fondamenti-di-liceita-del-trattamento (ultimo accesso giugno 2017).

[206] Sul tema *cfr*. recentemente Gruppo articolo 29 Parere n8/2014 "sui recenti sviluppi nel campo dell'Internet degli oggetti", 16 settembre 2014.

[207] A riguardo si ha notizia di un sistema cognitivo, denominato Watson e sviluppato da IBM, che è stato utilizzato recentemente in ambito sanitario per analizzare il genoma dei pazienti affetti da cancro al cervello, al fine di accelerare e aiutare i medici a personalizzare i trattamenti di cura

APPENDICE

Normativa Nazionale in tema di *"Sanità elettronica"*

Dossier Sanitario

Garante:

Linee guida in materia di Dossier sanitario - 4 giugno 2015

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4084632

Fascicolo Sanitario elettronico

Ministero:

29/09/2015 DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI n. 178

Regolamento in materia di fascicolo sanitario elettronico.

21/06/2013 DECRETO-LEGGE n. 69

Disposizioni urgenti per il rilancio dell'economia. (v. art. 17)

17/12/2012 LEGGE n. 221

Conversione in legge, con modificazioni, del decreto-legge 18 ottobre 2012, n. 179, recante ulteriori misure urgenti per la crescita del Paese.

18/10/2012 DECRETO-LEGGE n. 179

Ulteriori misure urgenti per la crescita del Paese. (v. art. 12)

04/04/2012 INTESA della Conferenza permanente per i rapporti tra lo stato le regioni e le province autonome di Trento e Bolzano

Intesa ai sensi dell'articolo 8,comma 6 della legge 5 giugno 2003 n. 131 tra il governo le regioni e le province autonome di Trento e Bolzano sul documento recante "Linee guida per la dematerializzazione della documentazione clinica in diagnostica per immagini - Normativa e prassi". (rep. atti n. 81)

10/02/2011 INTESA della Conferenza permanente per i rapporti tra lo stato le regioni e le province autonome di Trento e Bolzano

Intesa, ai sensi dell'articolo 8 comma 6, della legge 5 giugno 2003, n. 131, tra il Governo, le Regioni e le Province autonome di Trento e Bolzano sul documento recante: Il fascicolo sanitario elettronico - Linee guida nazionali. (Rep. Atti n. 19/CSR del 10 febbraio 2011).

Garante:

Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario - 16 luglio 2009

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1634116

Referti on-line

Garante:

Linee guida in tema di referti on-line – 19 novembre 2009

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1679033

Ricette digitali e TS

Ministero:

02/07/2012 DECRETO del Ministero dell'economia e delle finanze

Avvio a regime delle procedure per la trasmissione telematica dei dati delle ricette a carico del Servizio sanitario nazionale da parte dei medici prescrittori regionali e ricetta elettronica presso le regioni Veneto, Friuli-Venezia Giulia, Umbria, Marche, Lazio e Sicilia

02/11/2011 DECRETO del Ministero dell'economia e delle finanze

De-materializzazione della ricetta medica cartacea, di cui all'articolo 11, comma 16, del decreto-legge n. 78 del 2010 (Progetto Tessera Sanitaria).

21/07/2011 DECRETO del Ministero dell'economia e delle finanze

Trasmissione telematica delle ricette del servizio sanitario nazionale da parte dei medici prescrittori e la ricetta elettronica (Progetto Tessera Sanitaria). Avvio a regime del Sistema presso le Regioni Toscana, Puglia, Sardegna e la provincia autonoma di Trento.

21/02/2011 DECRETO del Ministero dell'economia e delle finanze

Avvio a regime del sistema di trasmissione telematica dei dati delle ricette del SSN da parte dei medici prescrittori, presso le regioni Valle d'Aosta, Emilia Romagna, Abruzzo, Campania, Molise, Piemonte, Calabria, Liguria, Basilicata e la provincia Autonoma di Bolzano.

14/07/2010 DECRETO del Ministero dell'economia e delle finanze

Comunicazione dell'avvio a regime del sistema regionale della regione Lombardia, per la trasmissione telematica dei dati delle ricette a carico del Servizio sanitario nazionale da parte dei medici prescrittori regionali.

29/04/2010 INTESA della Conferenza permanente per i rapporti tra lo stato le regioni e le province autonome di Trento e Bolzano

Intesa, ai sensi dell'articolo 8, comma 6, della legge 5 giugno 2003, n .131, tra il Governo, le Regioni e le Province autonome di Trento e Bolzano concernente il documento recante "Sistema CUP - Linee guida nazionali" .

26/02/2010 DECRETO del Ministero della Salute

Definizione delle modalità tecniche per la predisposizione e l'invio telematico dei dati delle certificazioni di malattia al SAC.

25/02/2010 DECRETO del Ministero dell'economia e delle finanze

Aggiornamento del decreto 11 marzo 2004 e successive modificazioni, attuativo del comma 1 dell'articolo 50 della legge n. 326/2003 (Progetto tessera sanitaria).

25/02/2010 DECRETO del Ministero dell'economia e delle finanze

Aggiornamento del decreto 11 marzo 2004 e successive modificazioni, attuativo del comma 1 dell'articolo 50 della legge n. 326/2003 (Progetto tessera sanitaria).

26/03/2008 DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

Attuazione dell'articolo 1, comma 810, lettera c), della legge 27 dicembre 2006, n. 296, in materia di regole tecniche e trasmissione dati di natura sanitaria, nell'ambito del Sistema pubblico di connettività.

23/10/2007 DECISIONE del Parlamento Europeo - Consiglio dell'Unione Europea n. 1350

Decisione n. 1350/2007 del Parlamento europeo e Consiglio, del 23 ottobre 2007,che istituisce un secondo programma d'azione comunitaria in materia di salute (2008-2013) - Pubblicata nel n. L 301 del 20 novembre 2007.

11/03/2004 DECRETO del Ministero dell'economia e delle finanze

Applicazione delle disposizioni di cui al comma 1 dell'art. 50 del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326, concernente la definizione delle caratteristiche tecniche della Tessera sanitaria (TS).

24/11/2003 LEGGE n. 326

Conversione in legge, con modificazioni, del decreto-legge 30 settembre 2003, n. 269, ha introdotto l'obbligo di trasmissione telematica dei dati delle ricette ai fini del controllo della spesa, ed il DL 78/2010 (art 11, comma 16) ha dato valore legale alla trasmissione telematica dei dati delle ricette (scompare "ricetta rossa" cartacea).

Struttura del Codice Privacy (D. Lgs. 196/2003)

I Disposizioni Generali

- Principi generali (artt. 1-6);
- Diritti dell'interessato (artt. 7-10);
- Regole generali per il trattamento dei dati:
  - Regole per tutti i trattamenti (artt. 11-17);
  - Regole ulteriori per i soggetti pubblici (artt. 18-22);
  - Regole ulteriori per privati ed enti pubblici economici (artt. 23-27);
- I soggetti che effettuano il trattamento (artt. 28-30);
- La sicurezza dei dati e dei sistemi:
  - Misure di sicurezza (artt. 31-32);
  - Misure minime di sicurezza (artt. 33-36);
- Gli adempimenti (artt. 37-41);
- Trasferimento dei dati all'estero (artt. 42-45).

II Disposizioni relative a specifici settori

- Trattamenti in ambito giudiziario:
  - Profili generali (artt. 46-49);
  - Minori (art. 50);
  - Informatica giuridica (artt. 51-52);
- Trattamenti da parte di forze di polizia:
  - Profili generali (artt. 53-57);
- Difesa e sicurezza dello Stato:
  - Profili generali (art. 58);

- Trattamenti in ambito pubblico:
  - Accesso a documenti amministrativi (artt. 59-60);
  - Registri pubblici e albi professionali (art. 61);
  - Stato civile, anagrafi e liste elettorali (artt. 62-63);
  - Finalità di rilevante interesse pubblico (artt. 64-74);

- Trattamento di dati personali in ambito sanitario:
  - Principi generali (artt. 75-76);
  - Modalità semplificate per informative e consenso (artt. 77- 84);
  - Finalità di rilevante interesse pubblico (artt. 85-86);
  - Prescrizioni mediche (artt. 87-89);
  - Dati genetici (art. 90);
  - Disposizioni varie (artt. 91-94);

- Istruzione:
  - Profili generali (artt. 95-96);

- Trattamento per scopi storici, statistici e scientifici:
  - Profili generali (artt. 97-100);
  - Trattamento per scopi storici: (artt. 101-103);
  - Trattamento per scopi statistici o scientifici (artt. 104-110);

- Lavoro e previdenza sociale:
  - Profili generali (artt. 111-112);
  - Annunci di lavoro e dati riguardanti prestatori di lavoro (art. 113);
  - Divieto di controllo a distanza e telelavoro (artt. 114-115);
  - Istituti di patronato e di assistenza sociale (art. 116);

- Sistema bancario, finanziario ed assicurativo;
  - Sistemi informativi (artt. 117-120);

- Comunicazioni elettroniche:
  - Servizi di comunicazione elettronica (artt. 121-132-bis);
  - Internet e reti telematiche (art. 133);
  - Videosorveglianza (art. 134);

- Libere professioni e investigazione privata:
  - Profili generali (art. 135);

- Giornalismo ed espressione letteraria ed artistica:
  - Profili generali (artt. 136-138);
  - Codice di deontologia (art. 139);

- Marketing diretto:
  - Profili generali (art. 140).

III Tutela dell'interessato e sanzioni

- Tutela amministrativa e giurisdizionale:
  - Principi generali (art. 141);
  -Tutela amministrativa (artt. 142-144);
  - Tutela alternativa a quella giurisdizionale (artt. 145- 151).
  - Tutela giurisdizionale (art. 152);

- L'Autorità:
  - Il Garante per la protezione dei dati personali (artt. 153- 154);
  - L'Ufficio del Garante (artt. 155-156);
  - Accertamenti e controlli (artt. 157-160);

- Sanzioni:
  - Violazioni amministrative (artt. 161-166);
  - Illeciti penali (artt. 167-172);

- Disposizioni modificative, abrogative, transitorie e finali:
  - Disposizioni di modifica (artt. 173-179);
  - Disposizioni transitorie (artt. 180-182);
  - Abrogazioni (art. 183);
  - Norme finali (artt. 184-186).

Gli allegati al Codice della Privacy

- Allegato A.1. - Codice di deontologia - Trattamento dei dati personali nell'esercizio dell'attività giornalistica.

- Allegato A.2. - Codice di deontologia - Trattamento dei dati personali per scopi storici.

- Allegato A.3. - Codice di deontologia - Trattamento dei dati personali a scopi statistici.

- Allegato A.4. - Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici.

- Allegato A.5. - Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti.

- Allegato A.6. - Codice di deontologia e di buona condotta per i trattamenti di dati personali effettuati per svolgere investigazioni difensive;

- Allegato B. - Disciplinare tecnico in materia di misure minime di sicurezza.

- Allegato C. - Trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia.

Modello "Informativa Dossier sanitario"

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI
EFFETTUATO MEDIANTE DOSSIER SANITARIO (DS)

ex art. 13 Codice in materia di protezione dei dati personali (D. Lgs. 196/2003)

Gentile Paziente,
con la presente informativa, rilasciata ai sensi dell'articolo 13 del decreto legislativo n. 196/2003, l'Azienda Sanitaria _____ intende informarla su che cos'è il Dossier sanitario (DS) e i motivi per i quali Le viene richiesto il consenso, libero e informato, sui dati personali e sensibili trattati attraverso questo strumento, in uso presso la nostra struttura, volto a migliorare l'efficienza del servizio sanitario e a semplificare l'esercizio del suo diritto alla salute in ogni momento del percorso socio-sanitario.

1. Cos'è il Dossier sanitario

Il Dossier raccoglie, in formato digitale, l'insieme dei dati personali e sensibili generati da eventi clinici presenti e trascorsi relativi alle prestazioni sanitarie erogate a ciascun paziente e potrà essere consultato, da parte dei professionisti sanitari che prenderanno in cura l'assistito all'interno dell'Azienda sanitaria, al fine di migliorare e personalizzare le procedure di cura per garantire il diritto alla salute. Il Dossier è uno strumento che differisce in contenuto e gestione dalla compilazione e tenuta della cartella clinica, intesa come lo strumento informativo finalizzato a rilevare tutte le informazioni anagrafiche e cliniche significative relative ad un paziente e ad un singolo episodio terapeutico.

La costituzione del Dossier sanitario, predisposta a seguito delle misure previste dalle Linee guida in tema di Dossier sanitario del 04.06.20015, pubblicate in Gazzetta Ufficiale del 17 luglio 2015, n. 164, è facoltativa e libera.

2. Finalità del Dossier sanitario (DS)

Il Dossier è istituito presso la nostra struttura ospedaliera per finalità di:

- Cura
- Prevenzione
- Diagnosi
- Riabilitazione
- Ricerca

3. Consenso alla costituzione e consultazione del Dossier sanitario (DS)

Il consenso alla creazione del dossier è libero e facoltativo.

Pertanto, sebbene Lei abbia già espresso il consenso generale al trattamento dei dati sanitari, qualora ritenesse opportuno attivare il suo Dossier Sanitario, si informa che per la creazione del Dossier e la consultazione delle informazioni in esso contenuto è necessario che rilasci un ulteriore e specifico consenso, che naturalmente potrà revocare in qualsiasi momento.

Tuttavia, con la costituzione e la consultazione del Dossier il personale sanitario aziendale può contare su un quadro clinico il più completo possibile e di disporre delle informazioni relative alla sua salute al fine di poterLe offrire un'assistenza sempre più adeguata ed ottimizzando il processo di cura.

Il consenso alla costituzione del Dossier è raccolto dal personale sanitario in forma scritta attraverso la compilazione e firma dell'apposito modulo *ovvero* espresso in forma orale, con contestuale annotazione informatica della dichiarazione espressa dal paziente, al momento della Sua presa in carico.

Con riguardo all'integrazione e consultazione dei dati clinici pregressi, o comunque formati precedentemente alla costituzione del Dossier, deve rilasciare un apposito consenso. Con tale consenso viene data la possibilità al personale sanitario aziendale di consultare i dati pregressi creati e conservati presso i singoli sistemi dipartimentali di cui è Titolare l'azienda. Ma doveroso è sottolineare che non vi è possibilità di garantire per questa tipologia di dati garanzia della loro completezza.

4. Modifica, Revoca o Mancato Consenso al trattamento mediante Dossier sanitario (DS)

Il consenso alla costituzione e al trattamento dei dati per mezzo del Dossier può essere modificato o revocato in qualsiasi momento. Altresì, l'eventuale rifiuto a costituire il Dossier non avrà conseguenze negative; infatti, il personale sanitario aziendale avrà a disposizione solo le informazioni da Lei rese in quel momento o in precedenti prestazioni fornite allo stesso professionista.

In caso di revoca, il sistema automaticamente non sarà più alimentabile, con nuove e successive prestazioni sanitarie, e consultabile da parte del personale aziendale precedentemente autorizzati, fino ad eventuale nuova dichiarazione di consenso.
Tuttavia, il Dossier potrà essere alimentato - da eventuali correzioni dei dati e dei documenti che lo hanno composto fino alla revoca del consenso – e consultato solamente da parte del personale sanitario che ha generato tali dati e documenti e che mantengono la titolarità su di essi.

5. Diritto di Oscuramento e De-oscuramento dei dati nel Dossier Sanitario (DS)

L'oscuramento è il diritto del paziente di non rendere visibili e consultabili alcuni dati inseriti nel Dossier e relativi ai singoli episodi di cura. Si evidenzia come l'oscuramento non viene in alcun modo evidenziato, per cui nessuno può venire a conoscenza del fatto che Lei abbia esercitato tale diritto (c.d. Oscuramento dell'oscuramento).

Si ritiene opportuno informare del rilevante impatto di tale diritto sui dati trattati attraverso il Dossier. Infatti l'oscuramento dei dati potrebbe non consentire una prestazione sanitaria calibrata alle esigenze di cura, dal momento che le informazioni potrebbero essere approssimate e lacunose.

Tale diritto può essere esercitato:

- Immediatamente cominciandolo al personale sanitario aziendale refertante la prestazione di cura,
- Successivamente, rivolgendosi all'Ufficio Privacy, compilando l'apposito modulo.

Tale facoltà può essere revocata in qualunque momento (c.d. De-oscuramento).

6. Consenso dati "a maggior tutela" dell'anonimato

Al fine di garantire la riservatezza e la dignità del paziente, determinate categorie di dati e documenti nascono per legge oscurate e rese visibili nel DS solo previo consenso espresso e specifico.

In particolare sono i dati I dati e documenti sanitari e socio sanitari che riguardano: le persone siero-positive, le donne che si sottopongono a interruzione volontaria di gravidanza, le vittime di atti di Violenza sessuale o pedofilia, le persone che fanno uso di sostanze stupefacenti,

psicotrope e di alcool, le donne che decidono di partorire in anonimato, nonché i dati e i documenti riferiti ai servizi offerti dai consultori familiari.

7. Modalità di trattamento

I dati sono trattati informaticamente con strumenti elettronici.

I dati identificativi quali nome ad esempio il nome, il cognome e quelli riguardanti lo stato di salute sono trattati conformemente ai principi di pertinenza, correttezza, liceità e osservando le misure minime di sicurezza previste dall'Allegato B – Disciplinare Tecnico.

8. Accesso al Dossier Sanitario (DS)

L'Azienda sanitaria garantisce che l'accesso ai dati clinici, reso possibile dal Dossier, è consentito solo agli operatori sanitari medici, infermieri, tecnici e amministrativi che saranno impegnati nel percorso di cura ovvero nel caso di urgenza/emergenza per cui verrà rilasciata anche un'apposita dichiarazione attestante la necessità dell'accesso.

Lei potrà, altresì, sapere in qualsiasi momento, attraverso appositi sistemi di controlli e autorizzazioni, predisposti dal Titolare del trattamento, identificare e tracciare l'identità del personale sanitario aziendale che ha avuto accesso alle informazioni contenute nel Dossier.

9. Titolare del Trattamento

Il Titolare del trattamento è l'Azienda Sanitaria _____

10. Esercizio dei diritti del paziente

Qualora ritenesse necessario ottenere maggiori informazioni sul trattamento dei Suoi dati attraverso il Dossier, revocare il consenso precedentemente espresso, esercitare le facoltà di oscurare e di de-oscurare, consultare gli elenchi dei Responsabili del trattamento, Incaricati del trattamento e Amministratori di Sistema, nonché esercitare i Suoi diritti di accesso cosi come previsti dall'articolo 7 del d.lgs. n. 196/03 (vedere di seguito dettagliato), Lei può rivolgersi presso _____

Art. 7. Diritto di accesso ai dati personali ed altri diritti
1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
a) dell'origine dei dati personali;
b) delle finalità e modalità del trattamento;
c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi, in tutto o in parte:
a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Modello “Consenso trattamento dati con DS”

Mod. A

CONSENSO AL TRATTAMENTO DEI DATI PERSONALI E SENSIBILI CON DOSSIER SANITARIO

Io sottoscritto (nome e cognome)
_____
nato a _____il ____ / ____ / ____
codice fiscale _____
residente a (Comune, Provincia,
Stato)_____
in via (indirizzo)
_____

ACCONSENTO ALLA COSTITUZIONE DEL DOSSIER SANITARIO E ALL’ALIMENTAZIONE DELLO STESSO CON DATI PRODOTTI DA ORA IN POI
□ Si □ No

ACCONSENTO ALL’ALIMENTAZIONE DEL DOSSIER SANITARIO CON DATI PREGRESSI
□ Si □ No

ACCONSENTO ALL’ALIMENTAZIONE DEL DOSSIER SANITARIO CON DATI “A MAGGIOR TUTELA”
□ Si □ No

ACCONSENTO ALL’UTILIZZO DEI DATI PER FINI DI RICERCA
□ Si □ No

Alla consegna presentarsi con documento di identità valido

Con la firma seguente dichiaro esplicitamente di aver compreso l’informativa di cui all’art. 13 del decreto legislativo n. 196/2003 sulle modalità di trattamento dei dati personali e sensibili informatizzati poste in essere dall’Azienda Sanitaria _____ e di esprimere liberamente il mio consenso al trattamento.

_____ _____
luogo e data firma (estesa e leggibile)

Mod. A/2

CONSENSO AL TRATTAMENTO DEI DATI PERSONALI E SENSIBILI CON DOSSIER SANITARIO

(modulo per soggetto sottoposto a tutela)

Io sottoscritto (nome e cognome)
_____
nato a _____il ____ / ____ / ____
codice fiscale _____
residente a (Comune, Provincia,
Stato)_____
in via (indirizzo)
_____
per sé o in qualità di (produrre documentazione comprovante la qualità):
□ Tutore □ Legale rappresentante □ Amministratore di sostegno
□ Esercente la responsabilità genitoriale
di (nome e cognome)_____
nato a _____ il ____ / ____ / ____
codice fiscale □□□ □□□ □□□□□ □□□□□
residente a (Comune, Provincia, Stato)
_____
in via (indirizzo)
_____

ACCONSENTO ALLA COSTITUZIONE DEL DOSSIER SANITARIO E ALL'ALIMENTAZIONE DELLO STESSO CON DATI PRODOTTI DA ORA IN POI
□ Si □ No

ACCONSENTO ALL'ALIMENTAZIONE DEL DOSSIER SANITARIO CON DATI PREGRESSI
□ Si □ No

ACCONSENTO ALL'ALIMENTAZIONE DEL DOSSIER SANITARIO CON DATI "A MAGGIOR TUTELA"
□ Si □ SI, SOLAMENTE NEL REPARTO/AMBULATORIO DI CURA □ No

ACCONSENTO ALL'UTILIZZO DEI DATI PER FINI DI RICERCA
□ Si □ No

Alla consegna presentarsi con documento di identità valido

Con la firma seguente dichiaro esplicitamente di aver compreso l'informativa di cui all'art. 13 del decreto legislativo n. 196/2003 sulle modalità di trattamento dei dati personali e sensibili informatizzati poste in essere dall'Azienda Sanitaria _____ e di esprimere liberamente il mio consenso al trattamento.

_____ _____
luogo e data firma (estesa e leggibile)

Modello “Oscuramento / Deoscuramento dei dati”

Mod. B

RICHIESTA DI OSCURAMENTO/DEOSCURAMENTO

Io sottoscritto (nome e cognome)
_____
nato a _____il ____ / ____ / ____
codice fiscale _____
residente a (Comune, Provincia,
Stato)_____
in via (indirizzo)
_____

CHIEDO L’OSCURAMENTO DEI SEGUENTI EVENTI/EPISODI:
1)_____

2)_____

3)_____

4)_____

CHIEDO IL DEOSCURAMENTO DEI SEGUENTI EVENTI/EPISODI:
1)_____

2)_____

3)_____

4)_____

Alla consegna presentarsi con documento di identità valido

Con la firma seguente dichiaro esplicitamente di aver compreso l’informativa di cui all’art. 13 del decreto legislativo n. 196/2003 sulle modalità di trattamento dei dati personali e sensibili informatizzati poste in essere dall’Azienda Sanitaria _____ (pubblicata anche sul sito _____) e di esprimere liberamente il mio consenso al loro trattamento.

_____ _____
luogo e data firma (estesa e leggibile)

Mod. B/2

RICHIESTA DI OSCURAMENTO/DEOSCURAMENTO
(modulo per soggetto sottoposto a tutela)

Io sottoscritto (nome e cognome)
_____
nato a _____il ____ / ____ / ____
codice fiscale _____
residente a (Comune, Provincia,
Stato)_____
in via (indirizzo)
_____
per sé o in qualità di (produrre documentazione comprovante la qualità):
□ Tutore □ Legale rappresentante □ Amministratore di sostegno
□ Esercente la responsabilità genitoriale
di (nome e cognome)_____
nato a _____ il ____ / ____ / ____
codice fiscale □□□ □□□ □□□□□ □□□□□
residente a (Comune, Provincia, Stato)
_____
in via (indirizzo)
_____

CHIEDO L'OSCURAMENTO DEI SEGUENTI EVENTI/EPISODI:
1)_____

2)_____

3)_____

CHIEDO IL DEOSCURAMENTO DEI SEGUENTI EVENTI/EPISODI:
1)_____

2)_____

3)_____

Alla consegna presentarsi con documento di identità valido

Con la firma seguente dichiaro esplicitamente di aver compreso l'informativa di cui all'art. 13 del decreto legislativo n. 196/2003 sulle modalità di trattamento dei dati personali e sensibili informatizzati poste in essere dall'Azienda Sanitaria _____ (pubblicata anche sul sito _____) e di esprimere liberamente il mio consenso al loro trattamento.

_____ _____
luogo e data firma (estesa e leggibile)

Modello “Revoca Alimentazione e consultazione DS”

Mod. C

RICHIESTA DI RICHIESTA DI REVOCA ALIMENTAZIONE E CONSULTAZIONE DOSSIER

Io sottoscritto (nome e cognome)
_____
nato a _____il ____ / ____ / ____
codice fiscale _____
residente a (Comune, Provincia,
Stato)_____
in via (indirizzo)
_____

CHIEDO LA REVOCA

- all’alimentazione del Dossier sanitario con nuove e successive prestazioni sanitarie;
- alla consultazione del Dossier sanitario da parte degli Operatori sanitari precedentemente autorizzati

Alla consegna presentarsi con documento di identità valido

Con la firma seguente dichiaro esplicitamente di aver compreso l’informativa di cui all’art. 13 del decreto legislativo n. 196/2003 sulle modalità di trattamento dei dati personali e sensibili informatizzati poste in essere dall’Azienda Sanitaria _____ (pubblicata anche sul sito _____) e di esprimere liberamente il mio consenso al loro trattamento.

_____ _____
luogo e data firma (estesa e leggibile)

Mod. C/2

RICHIESTA DI REVOCA ALIMENTAZIONE E CONSULTAZIONE DOSSIER

(modulo per soggetto sottoposto a tutela)

Io sottoscritto (nome e cognome)
_____
nato a _____il ____ / ____ / ____
codice fiscale _____
residente a (Comune, Provincia,
Stato)_____
in via (indirizzo)
_____
per sé o in qualità di (produrre documentazione comprovante la qualità):
□ Tutore □ Legale rappresentante □ Amministratore di sostegno
□ Esercente la responsabilità genitoriale
di (nome e cognome)_____
nato a _____ il ____ / ____ / ____
codice fiscale □□□ □□□ □□□□□ □□□□□
residente a (Comune, Provincia, Stato)
_____
in via (indirizzo)
_____

CHIEDO LA REVOCA

- all'alimentazione del Dossier sanitario con nuove e successive prestazioni sanitarie;
- alla consultazione del Dossier sanitario da parte degli Operatori sanitari precedentemente autorizzati

Alla consegna presentarsi con documento di identità valido

Con la firma seguente dichiaro esplicitamente di aver compreso l'informativa di cui all'art. 13 del decreto legislativo n. 196/2003 sulle modalità di trattamento dei dati personali e sensibili informatizzati poste in essere dall'Azienda Sanitaria _____ (pubblicata anche sul sito _____) e di esprimere liberamente il mio consenso al loro trattamento.

_____ _____

luogo e data firma (estesa e leggibile)

Modello Valutazione del rischio e Check-List delle misure di sicurezza nel DS[208]

Tipologia Rischio	Valutazione del Rischio		
	Alto	Medio	Basso
Accesso Abusivo			
Furto o smarrimento parziale o integrale dei supporti di memorizzazione			
Furto o smarrimento parziale o integrale dei sistemi di elaborazione portatili o fissi			
Comunicazione a soggetti non legittimati			

Tabella Chek-List			
A	**Sistemi di autenticazione e di autorizzazione**	**SI**	**NO**
1	Il Titolare ha adottato idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle concrete esigenze di accesso ai *dossier*?		
2	Il sistema adottato consente un accesso selettivo al dossier solo al personale sanitario coinvolto nel processo di cura e a quello amministrativo per le sole finalità strettamente correlate alla cura?		
3	L'accesso al *dossier* da parte del personale amministrativo consente a questi di accedere ai soli dati strettamente necessari allo svolgimento dei loro compiti?		
4	Il Titolare ha individuato procedure (audit) per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati?		
B	**Tracciabilità degli accessi e delle operazioni effettuate**		
5	Il Titolare ha rispettato l'applicazione della disciplina sui controlli a distanza (art. 4 legge n. 300/1970)?		
6	Il Titolare ha adottato procedure che prevedano la registrazione automatica in appositi file di log degli accessi e delle operazioni compiute?		
7	Il file di log registra la data e l'ora di accesso?		
8	Il file di log registra il codice della postazione di lavoro utilizzata dall'incaricato?		
9	Il file di log registra l'identificativo del paziente il cui *dossier* è interessato dall'operazione di accesso?		
10	Il file di log registra la tipologia dell'operazione compiuta sui dati?		
11	Il sistema traccia anche le operazioni di semplice consultazione (*inquiry*)?		
12	La congruità del tempo di conservazione dei log è stata valutata tenendo conto da un lato dell'esigenza degli interessati di venire a conoscenza dell'avvenuto accesso ai propri dati personali e dall'altro delle esigenze medico-legali della struttura sanitaria ?		
13	I log delle operazioni sono comunque conservati per un periodo non inferiore a 24 mesi dalla data di registrazione dell'operazione?		
C	Sistemi di audit log		
14	Il titolare del trattamento ha predisposto e configurato specifici alert che individuino comportamenti anomali?		
15	Il titolare ha predisposto una periodica attività di controllo interno che consenta di verificare l'adeguatezza delle misure di sicurezza, sia di tipo organizzativo, sia di tipo tecnico?		
16	L'attività di controllo è demandata a personale diverso rispetto a quello cui è affidato il trattamento dei dati sanitari dei pazienti?		
17	L'attività di controllo viene svolta solo in seguito al verificarsi di allarmi ?		
18	L'attività di controllo viene svolta anche a campione ?		
19	L'attività di controllo è documentata?		
20	I risultati dell'attività di controllo sono comunicati al management o comunque a coloro che sono legittimati a prendere decisioni ?		
D	**Separazione e cifratura dei dati**		
21	Il titolare ha individuato criteri per separare i dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati sessuali (artt. 22, commi 6 e 7, del D.Lgs. n. 196/2003)?		
22	Il titolare ha individuato criteri per la cifratura dei dati sensibili?		

[208] Schede riprese da Soffientini, (a cura di), *Privacy, Protezione e trattamento dati*, cit., p.127.

BIBLIOGRAFIA

R. ACCIAI, *Le nuove norme in materia di privacy, decreto legislativo 28 dicembre 2001 n. 467, autorizzazioni generali al trattamento dei dati sensibili, codici deontologici, regole per i flussi di dati fuori dall'Unione europea*, Maggioli, Rimini 2003.

R. ACCIAI, (a cura di), *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice*, Maggioli, Rimini 2004.

N. AGABUTI, M. DAVOLI, D. FUSCO, M. STAFOGGIA, C. A. PERUCCI, *Valutazione di esito degli interventi sanitari*, Epidemiologia & Prevenzione2011; 35(2) Suppl 1: 1-80, Cap. 3.8 (Sistemi Informativi Sanitari).

G. ALPA, *La normativa sui dati personali. Modelli di lettura e problemi esegetici*, in V. Cuffaro, V. Ricciuto, V. Zeno-Zencovich (a cura di), Trattamento dei dati e tutela della persona, Giuffrè, Milano 1998, pp. 26 ss.

G. ALPA, *La disciplina dei dati personali, note esegetiche sulla legge 31 dicembre 1996 n. 675 e successive modifiche*, Seam, Roma 1998.

G. ARNO', *La tutela della privacy nella rete internet*, Giappichelli, Torino 2002.

N. ARCHER et al, *Personal health records: a scoping review*, J Am Med Inform Assoc 2011.

P. ATZENI, S. CERI, S. PARABOSCHI, R. TORLONE. *Basi di Dati: modelli e linguaggi di interrogazione* - Quarta Edizione. McGraw-Hill Italia, 2013.

E. BALBONI, M. CAMPAGNA, *Osservazioni sul governo clinico anche come origine alla medicina difensiva*, in De Vincenti, Finocchi Ghersi, Tardiola (a cura di), *La sanità in Italia. Organizzazione, governo, regolazione, mercato*, Collana 'Quaderni di Astrid, Bologna 2011, Il Mulino.

BALDASSARRE, *Diritto della persona e valori costituzionali*, Giappichelli, Torino 1997.

R. BALDUZZI, voce *Salute* (diritto alla), in Diz. Dir. Pubbl., diretto da S. Cassese, vol. VI, Milano, 2006.

A. BARBERA, *Sub art. 2*, in G. Branca (a cura di) *Commentario della Costituzione*, Bologna, Zanichelli editore, Roma, 1975.

V. BARSOTTI, *Privacy e orientamento sessuale. Una storia americana*, Torino, Giappichelli, 2005.

C. M. BIANCA, *Tutela della privacy. Note introduttive*, in Nuove leggi civili commentate, fascicoli 2-3, 1999.

M. BIN, *Privacy e trattamento dei dati personali: entriamo in Europa in Contratto e impresa Europa*, 1997, pp. 459 ss.

M. BIROLI, *Process Analysis o Process Management*, Milano, Sistemi & Impresa, n° 9, 1992.

L. BOLOGNINI, E. PELINO, C. BISTOLFI, *ll Regolamento Privacy Europeo*, Giuffrè, 2016.

L. BRANDEIS, S. WARREN, *The right to privacy*, in Harward Law Review, 4, 1890.

F. BRAVO, *Le condizioni di liceità del trattamento dei dati*, in J. Monducci - G. Sartor (a cura di), Il Codice in materia di protezione dei dati personali, Cedam, Padova 2004.

R. BRIGHI, *Il ruolo dei dati informatici nella costruzione della realtà. Tra vulnerabilità e esigenze di trasparenza*, Aracne editrice, Roma 2016.

R. BRIGHI; M.G. VIRONE, *Una tutela "by design" del diritto alla salute. Prospettive di armonizzazione giuridica e tecnologica*, in: *A Matter of Design: Making Society trough Science and Technology*, Milano, Open Access Digital Publication by STS Italia Publishing, 2014, p. 1218.

O. BUCCI, La cartella clinica. Profili strumentali, gestionali, giuridici ed archivistici, Santarcangelo di Romagna, 1999.

L. BUCCOLIERO, *E-HEALTH 2.0 - Tecnologie per il patient empowerment*, Mondo digitale n. 4. 2010.

L. BUCCOLIERO, C. CACCIA, G. NASI, e-*He@lt : percorsi di implementazione dei sistemi informativi in sanità*, McGraw-Hill, Milano 2005.

G. BUSIA, voce Riservatezza (diritto alla), in Digesto delle discipline pubblicistiche, quarta edizione, agg. 2000, pp. 476 ss.

G. BUTTARELLI, *Banche dati e tutela della riservatezza*, Giuffrè, Milano 1997.

G. BUTTARELLI, *Il dibattito sulla privacy è sempre aperto, 2002, http://www.interlex.it/675/buttarelli2.htm.*

D. CACCAVELLA; A. GAMMAROTA, *Informatica Forense Sanitaria per l'eHealth,* in C. Faralli, R. Brighi, M. Martoni (a cura di) *Strumenti, diritti, regole e nuove relazioni di cura: il paziente europeo protagonista nell' eHealth*, Giappichelli, 2015, p. 213.

D. CACCAVELLA, M. FERRAZZANO, F. BANORRI, *L'implementazione dei processi organizzativi finalizzati alla gestione del rischio nell'ambito di strutture sanitarie*, in C. Faralli, R. Brighi, M. Martoni (a cura di), Strumenti, diritti, regole e nuove relazioni di Cura. Il Paziente europeo protagonista nell'eHealth, Giappichelli, 2015, pp. 221-230.

C. CACCIA, *Management dei sistemi informativi in sanità*, McGraw-Hill, Milano, 2008.

C. CACCIA, G. NASI, *Il sistema informativo automatizzato nelle aziende sanitarie*, McGraw-Hill, Milano 2002.

L. CALIFANO, *Privacy e Sicurezza*, Democrazia & Sicurezza, 2013.

L. CALIFANO, *Fascicolo sanitario elettronico (Fse) e dossier sanitario: il contributo del Garante privacy al bilanciamento tra diritto alla salute e diritto alla protezione dei dati personali*, in Sanità pubblica e privata, 2015, fasc. 3, p. 7-22.

CAMMEO-VITTA, *Sanità Pubblica, in Trattato di diritto amministrativo italiano,* a cura di V.E. Orlando, IV, 2° parte, Milano 1905, p. 213.

D. CAMPILONGO, *Privacy informatica: il regime degli esoneri e delle semplificazioni introdotte dal D. Lgs. N. 255 del 1997 di attuazione della L. delega n. 676/1996 sulla protezione dei dati personali*, in Fisco, 1997, pp. 11015 ss..

P. CAPPELLETTI, *La Medicina Personalizzata fra ricerca e pratica clinica: il ruolo della Medicina di Laboratorio,* RIMeL / IJLaM 2009; 5(Suppl.):26-32.

A..CARRIERO, M. CENTONZE, T. SCARABIN, Management in radiologia, Springer, 2010, pag. 191-201.

C. CASALEGNO, G.P. ZANETTA, *La tutela della privacy nella sanità: il trattamento dei dati personali e sensibili.* Milano: Il Sole 24 Ore.

G. CASATI, la gestione dei processi in sanità, QA vol. 13 n. 1, 2002.

G. CASCIARO, *Il consenso informato*, Giuffrè, 2012.

C..CASONATO, *Diritto alla riservatezza e trattamenti sanitari obbligatori: un'indagine comparata*, Trento, Università degli studi, 1995.

CATAUDELLA, Riservatezza (diritto alla), I) Diritto civile, in Enciclopedia giuridica, XXVII, Roma 1991.

A..CAVOUKIAN (presentation by), *Privacy by Design: Building Trust into Technology*, 1st Annual Privacy and Security Workshop. Centre for Applied Cryptographic Research, Toronto 2000.

A..CAVOUKIAN, *Moving Forward From PETs to PETs Plus: The Time for Change is Now*, Toronto 2009, p. 4.

A..CAVOUKIAN, *Privacy by Design: Take the Challenge*, Toronto 2009, pp. 361 ss.

A..CAVOUKIAN, K. EL EMAM, *A Positive-Sum Paradigm in Action in the Health Sector*, Toronto 2010, pp. 6 ss.

A. CAVOUKIAN, *Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices*, Toronto 2010, pp. 12 ss.

A..CAVOUKIAN, R. C. ALVAREZ, *Embedding Privacy into the Design of EHRs to Enable Multiple Functionalities - Win/Win*, Toronto 2012, pp. 19 ss.

A..CAVOUKIAN, M. CHANLIAU, *Privacy and Security by Design: A Convergence of Paradigms*, Toronto 2013, pp. 19 ss.

A..CAVOUKIAN, *Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era*, in Yee G.O.M., Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards, IGI Global, Hershey, 2012, pp. 170-208.

G. CORASANITI, *La sicurezza dei dati personali*, in Cardarelli, Sica, Zeno-Zencovich (a cura di), "Il codice dei dati personali. Temi e problemi", Giuffrè, Milano 2004, pp. 112-163.

A. CERRI, *Riservatezza (diritto alla), II) Diritto comparato e straniero*, in *Enc. giur*., Roma, 1991, vol. XXVII.

A. CERRI, *Riservatezza (diritto alla), III) Diritto costituzionale*, in *Enc. giur*., XXVII (aggiornamento), Roma, 1995.

F. CICILIANO, *La disciplina giuridica del consenso informato*, Arnus University Books, Pisa, 2013;

L. CIFALDI, V. FELICETTI, G. CRISTINA, *La richiesta di un secondo parere in oncologia: sfiducia o bisogno?* Med 2010, 101: 299-302.

L. CIMMINO, *Dalla formazione del diritto alla privacy, alla libertà informatica, in Rivista di diritto pubblico e scienze politiche*, 1997, pp. 463 ss.

G.P. CIRILLO, *Il codice sulla protezione dei dati personali*, Giuffrè, Milano, 2004.

G. COMANDÈ, *Banche di dati giuridici e privacy*, in F. Di Ciompo (a cura di), Atti del Convegno Il diritto del cittadino all'informazione giuridica", CED della Corte di Cassazione, Roma, 25 settembre 2000.

G. COMANDÈ, *La funzione "giurisprudenziale" del Garante per la protezione dei dati personali: a proposito di una recente decisione su informativa e consenso al trattamento, in Diritto dell'Informazione e Informatica*, 6, 1997, pp. 975 ss..

G. COMANDÈ, G. PASCUCCI, *Diritto e informatica*, Giuffrè, Milano, 2002.

V. CUFFARO, V. RICCIUTO, V. ZENO-ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, Giuffrè, Milano, 1998, pp. 26 ss.

V. CUFFARO, V. RICCIUTO (a cura di), *La disciplina del trattamento dei dati personali*, Giappichelli, Torino, 1997.

S. DALMIANI, A. TADDEI, M. GLAUBER, M. EMDIN, *An Informative System For Structured Data Management To Build A Cardiological Multidimensional Database*, Computers in Cardiology 2002; 29:369−372, IEEE Computer Society Press.

S. DALMIANI, A. TADDEI, M. GLAUBERS, S. BEVILACQUA, M. EMDIN, *Matrix a generic scheme for clinical registry data management for multidisciplinary environment*, MEDICON 2004 - IFMBE Proceedings; 6: 276.

S. DALMIANI, P. MARCHESCHI, A. MAZZARISI, *HL7 clinical document architecture to share structured data in wide hospital information systems*, EUROPACS-MIR 2004; 311-314.

S. DALMIANI, *Patient File: La Sanità Elettronica in Italia* - Pag 26-29, Cardiologia negli Ospedali n. 157 anno 2007 – Rivista ANMCO (Associazione Nazionale Medici Cardiologi Ospedalieri).

A..DEL NINNO, *La tutela dei dati personali. Guida pratica al Codice della privacy (d.lgs. 30.6.2003. n. 196)*, Cedam, 2006.

A. DE CUPIS, Riservatezza e segreto (diritto a), in Novissimo Digesto Italiano XVI, Torino, 1969, pp.115 ss.

C. DE GIACOMO, *Diritto, libertà e privacy nel mondo della comunicazione globale. Il contributo della teoria generale del diritto allo studio della normativa sulla tutela dei dati personali*, Giuffrè, Milano, 1999.

A..DE MAURO, M. GRECO e M. GRIMALDI, *A Formal definition of Big Data based on its essential Features*, in *Library Review*, vol. 65, nº 3, 2016, pp. 122-135.

L. DE PANFILIS, S. ZULLO, *Aspetti etici delle applicazioni eHealth,* in C. Faralli, R. Brighi, M. Martoni (a cura di) Strumenti, diritti, regole e nuove relazioni di cura: il paziente europeo protagonista nell' eHealth, Giappichelli, 2015, pp. 55 ss..

U. DE SIERVO, *La nuova legislazione sulla tutela della riservatezza,* in Orientamenti sociali, 1997, pp. 93 ss.

U. DE SIERVO, *La privacy*, in Panunzio, *I diritti fondamentali e le Corti in Europa*, cit., p. 356; D. Caldirola, *Il diritto alla riservatezza*, Padova, Cedam, 2006, pp. 59 ss.

A. DI MARTINO, *La protezione dei dati personali*, in S.P. Panunzio (a cura di), *I diritti fondamentali e le Corti in Europa*, Napoli, Esi 2005.

G. DI PIETRO, *I dati sensibili e la privacy nel rapporto di lavoro*, in Diritto del lavoro, I, 1998, pp. 449 ss.

R. DUCATO, P. GUARDA, *Profili giuridici dei "personal health records": l'autogestione dei dati sanitari da parte del paziente tra "privacy" e tutela della salute*, in Rivista critica del diritto privato, 2014, fasc. 3, pp. 389-419.

G. EYSENBACH, *What is e-health?, J Med Internet Res 2001*.

R. A. ELMASRI, S.B. NAVATHE. *Sistemi di basi di dati Fondamenti* - Prima edizione italiana, Addison Wesley, 2004.

C..FARALLI, Introduzione, in Id. (a cura di), *Consenso informato in medicina. Aspetti etici e giuridici*, Franco Angeli, 2012.

C. FARALLI, R. BRGHI, M. MARTONI, *Strumenti, diritti, regole e nuove relazioni di cura. Il Paziente europeo protagonista nell'e-Health,* Giappichelli, 2015.

A. L. FAZZARI, *Sistemi di gestione per la qualità,* Giappichelli, Torino 2012.

G. FERRANDO, Diritto alla salute e autodeterminazione, tra diritto europeo e costituzione, in Politica del diritto, XLIII, 1, 2012.

R. FERRARA, *L'ordinamento della sanità*, in Sistema del diritto amministrativo italiano, diretto da F. G. Scoca, F. A. Roversi Monaco, G. Morbidelli, Torino 2007, pp. 111 ss.

R. FERRARA, *Il diritto alla salute: principi costituzionali*, in Salute e sanità, a cura di R. Ferrara, in Trattato di biodiritto, diretto da S. Rodotà, P. Zatti, Milano 2010, pp. 3 ss.

G. FINOCCHIARO, *Una prima lettura della legge 31 dicembre 1996, n. 675 "tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali"*, in Contratto e Impresa,1, 1997, pp. 299 ss.

G. FINOCCHIARO, *Il trattamento dei dati sanitari: alcune riflessioni critiche a dieci anni dall'entrata in vigore del Codice in materia di protezione dei dati personali*, Sanità pubblica e privata, 2: 10-18.

G. FINOCCHIARO, *Identità personale su Internet: il diritto alla contestualizzazione dell'informazione*, Diritto dell'informazione e dell'informatica, 3: 383-394.

G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, Diritto dell'informazione e dell'informatica, 4-5: 591-604.

G. FINOCCHIARO, *Privacy e protezione dei dati personali*, Zanichelli, 2012.

V. FROSINI, *Banche dati, telematica e diritti della persona*, Cedam, Padova 1981.

I. GENITSARIDIA et al., Evaluation of personal health record systems through the lenses of EC research projects, Computers in Biology and Medicine, 2013.

G. GIACOBBE, *Il diritto alla riservatezza: da diritto di elaborazione giurisprudenziale a diritto codificato*, in Iustitia, 2, 1999, pp.93 ss.

G. GIACOBBE, Riservatezza (diritto alla), in Enciclopedia del diritto, XL, Milano 1989, pp. 1245 ss.

E. GIANNANTONIO, G. LOSANO, V. ZENO-ZENCOVICH, (a cura di), *La tutela dei dati personali. Commentario alla legge n. 675/96*, seconda edizione, Cedam, Padova 1999.

P. GUARDA, *Fascicolo sanitario elettronico e protezione dei dati personali*, Trento 2011.

G. GUERRA, *La 'medicina difensiva': fenomeno moderno dalle radici antiche,* in Salute e Diritto, Ottobre-Dicembre 2013, Vol. 14, N. 4.

L. HOOD, *Systems Biology and P4 Medicine: Past, Present, and Future,* in Rambam Maimonides Med J. 2013 Apr 30;4(2):e0012. doi: 10.5041/RMMJ.10112.

R. e R. IMPERIALI, *Codice della privacy. Commento alla normativa sulla protezione dei dati personali*, Il sole 24 ore, Milano 2004.

U. IZZO, *Medicina e diritto nell'era digitale: i problemi giuridici della cibermedicina*, in Danno e resp., 2000, p. 807.

U. IZZO, P. GUARDA, *Sanità elettronica, tutela dei dati personali e digital divide generazionale. Ruolo e criticità giuridica della delega alla gestione dei servizi di sanità elettronica da parte dell'interessato*, Trento Law and Technology Research Group, Research Paper Series n. 3, 2010.

L. JINGQUAN, Privacy policies for health social networking sites, J Am Med Inform Assoc., 2013.

K. JONES, R.C. JORDAN, *Patterns of second-opinion diagnosis in oral and maxillofacial pathology*, Oral Surg Oral Med Oral Pathol Oral Radiol Endod 2010, 109: 865-9.

J.S. KAHN al., What It Takes: Characteristics Of The Ideal Personal Health Record, Health Affairs, 28, no.2 (2009).

D. KARLA, *Electronic Health Records Standards*, IMIA Year Book of Medical Informatics, 2006, pp. 136-144.

M. KEITH - M. KATINA, *Big Data New Opportunities and new Challenges*, IEEE Computer Society, 2013.

H. KELSEN, *Allgemeine Staatslehre*, Berlin 1925.

R.D. KUSH et al. *Electronic Health Records, Medical Research, and the Tower of Babel*, N Engl J Med 2008 358: 1738-1740.

R. LATTANZI, *Dati sensibili: una categoria problematica nell'orizzonte europeo*, in Europa e diritto privato, 1998, pp. 724 ss.

K. LAUDON, *Management dei sistemi informativi*, Pearson, Milano 2006, pp. 17-19.

L. LUPARIA , G. ZICCARDI, *Investigazione penale e tecnologia informatica*, Giuffrè, 2007.

C..MAIOLI, E. SANCHEZ JORDAN, *Big Data e capacità informativa per l'autodeterminazione del paziente,* in C. Faralli, R. Brighi, M. Martoni (a cura di) Strumenti, diritti, regole e nuove relazioni di cura: il paziente europeo protagonista nell' eHealth, Giappichelli, 2015, pp. 155 ss.

C. MAIOLI, *Dar voce alle prove: elementi di Informatica Forense*, in P. Pozzi (a cura di), *Crimine virtuale, minaccia reale*, Franco Angeli, 2004.

M. MANCARELLA, *eHealth e diritti. L'apporto dell'Informatica giuridica*, Carocci, Roma, 2014.

D. MARTIN, A. SERJANTOV (edited by), *Privacy Enhancing Technologies, Proceeding of 4° international workshop, PET 2004*, Toronto 2004.

M. MARTONI, *Profili giuridici in tema di misure di sicurezza, par. 3, Cap. 6, 117-123; Il Garante per la protezione dei dati personali ed il ruolo dell'amministratore di sistema dal profilo giuridico*, par. 4, Cap.6, pp. 124-128, in AA.VV., *Informatica giuridica per le relazioni aziendali*, Giappichelli Editore, Torino 2012.

M. MARTONI, *Sanità digitale*, in AA.VV., *La Nuova Pubblica Amministrazione, Quaderni di Diritto ed Economia delle comunicazioni e dei media*, pp. 141-158, Aracne editrice, Roma 2014.

M..MARTONI, *Social "Sanitary" Network per l'eHealth: fra condivisione della conoscenza e protezione dei dati personali*, in C. Faralli, R. Brighi, M. Martoni (a cura di) Strumenti, diritti, regole e nuove relazioni di cura: il paziente europeo protagonista nell' eHealth, Giappichelli, 2015, pp. 85 ss.

S. MELCHIONNA, *La nuova privacy: semplificazioni senza rinunciare a regole e garanzie (D. lgs. 467/2001)*, in www.privacy.it, sezione saggi, Roma, 23 gennaio 2002.

F. MERUSI, *Servizi pubblici instabili*, Bologna, 1990.

A. MESSINA, N. BERNARDI, *Privacy e Regolamento Europeo*, IPSOA, 2015.

D. MESSINETTI, voce Personalità (diritti della), in Enciclopedia del Diritto, XXXIII, Milano, 1983, pp. 37 ss.

F. MODAFFERI, *Lezioni di diritto alla protezione dei dati personali, alla riservatezza e all'identità personale*, Lulu, 2015.

F. MODUGNO, *I nuovi diritti nella giurisprudenza costituzionale*, Torino, Giappichelli, 1995, pp. 21 ss.

J. MONDUCCI, *Diritti della persona e trattamento dei dati particolari*, Giuffrè, Milano, 2003.

L. MONTUSCHI, in Commentario della Costituzione a cura di G. BRANCA, *Rapporti etico-sociali (Art. 29-34)*, Bologna Roma, 1975, sub art. 32, 146 ss.

R. MORO VISCONTI, *Internet delle cose, networks e plusvalore della connettività,* Il Diritto industriale, 2016, fasc. 6 pag. 536-544.

M. MORUZZI, *La sanità dematerializzata e il fascicolo sanitario elettronico: il nuovo welfare a bassa burocrazia.* Roma: Il pensiero scientifico.

M. MORUZZI, *Il Fascicolo Sanitario Elettronico in Italia. La sanità ad alta comunicazione*, Milano: Il Sole 24 Ore.

M. MORUZZI, *Alta Comunicazione. Aziende, Fascicoli Elettronici, Emozioni e de-Materializzazioni*, Franco Angeli, Milano 2012.

C. MUCIO, *Il diritto alla riservatezza nella pubblica amministrazione: dati sensibili, dati personali e diritto di accesso*, Ipsoa, Milano 2003.

T. B. MURDOCH, A.S. DETSKY, *The inevitable application of big data to health care* JAMA 2013; 309: 1351-1352.

S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, Cedam, 2006, pp. 62 ss.

P. NORRIS, *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*, Cambridge University Press, Oxford 2001, 3 ss.

J. OVRETVEIT, *Valutazione degli interventi in sanità*, Centro Scientifico Editore, Torino 1998.

U. PAGALLO, *On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law*, in S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?*, Springer Science+Business Media B.V, 2012, pp. 331-346.

U. PAGALLO, *Privacy e Design*, in M. Pietrangelo (a cura di), *Diritti di libertà nel mondo virtuale della rete*, Fascicolo monografico di *Informatica e diritto*, 2009, 1, pp. 123-134.

U. PAGALLO, *Designing Data Protection Safeguards Ethically*, in Information, 2011, 2, pp. 247-265.

U. PAGALLO, E. BASSI, *The Future of EU Working Parties' "The Future of Privacy" and the Principle of Privacy by Design*, in M. Bottis (eds.), An Information Law for the 21st Century, Atene, Nomiki Bibliothiki, 2011, pp. 286-305.

C. PAGLIARI et al., *Potential of electronic personal health records*, British Medical Journal 2007; 335: 333.

G. PASCUZZI, *Il diritto dell'era digitale*, il Mulino, Bologna 2010, pp.14-8.

P. PERRI, *Introduzione alla sicurezza informatica e giuridica*, in Pattaro E. (a cura di), "Manuale di diritto dell'informatica e delle nuove tecnologie", Clueb s.c.a.r.l., Bologna, 2002, pp. 306 e ss.

P. PERRI, *Le misure di sicurezza*, in Monducci J., Sartor G., "Il codice in materia di protezione dei dati personali", CEDAM, Padova, 2004, pp. 137 e ss.

P. PERRI, *Privacy, diritto e sicurezza informatica*, Giuffrè, Milano, 2007, pp. 195 ss.

F. PIZZETTI, *La disciplina giuridica delle malattie rare tra diritto alla salute e tutela della riservatezza*, in S. PANUNZIO, G. RECCHIA, *Malattie rare. La ricerca tra etica e diritto*, Atti del Convegno di Studi, Roma, 14/2/2006, Giuffrè, Milano 2007; pp. 23 ss.

F. PIZZETTI, *Come garantire la tutela dei dati personali nella società dell'informazione,* in F. Di Resta (a cura di) in *"La tutela dei dati personali nella società dell'informazione",* Giappichelli, Torino 2008.

F. PIZZETTI, (a cura di), *Il caso di Diritto all'oblio*, Giappichelli, 2013.

F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento Europeo*, vol. I Giappichelli, Torino 2016.

F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento Europeo 2016/679, vol. II*, Giappichelli, Torino 2016.

B. PRIMICERIO, La cartella clinica e la documentazione sanitaria ad essa collegata: evoluzione, utilizzazione e responsabilità, in Il Diritto sanitario moderno, 2004, p. 207.

T. K. PRASAD, *Big Data and Smart Healthcare*, slides Symposium "Visions of the Future", marzo 2014.

C. RABBITO, *Sanità elettronica e diritto. Problemi e prospettive*, Società Editrice Universo, 2010.

R. RAMAKRISHNAN. *Database Management Systems*, McGraw-Hill, 2004.

RESTA, *Il diritto alla protezione dei dati personali*, in F. Cardarelli, S. Sica e V. Zeno Zencovich (a cura di), *Il codice dei dati personali*, Milano, Giuffrè, 2004, p. 28.

P. RESCIGNO, *Conclusioni*, in *Il diritto all'identità personale*, a cura di G. Alpa, M. Bessone e L. Boneschi, Padova, Cedam, 1981, pp. 183-194.

G..ROCCHIETTI, La documentazione clinica. Compilazione, conservazione, archiviazione, gestione e suo rilascio da parte della direzione sanitaria. Trattamento dei dati sanitari e privacy, in Minerva medicolegale, 2001, fasc. 1, p. 15.

S. RODOTA', *Privacy e costruzione della sfera privata. Ipotesi e prospettive*, in Politica del diritto, XXII, 1991, pp. 525 ss..

S. RODOTA', *Tecnologie e diritti*, Il Mulino, Bologna, 1995, pp. 106 ss..

S. RODOTA', *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in Rivista critica del diritto privato, 4, 1997, pp. 583 ss..

S. RODOTA', Affari e finanza, suppl. Repubblica, 10 dicembre 2002.

S. RODOTA', *Libera Circolazione e protezione dei dati personali*, a cura di Rocco Panetta, Tomo I, Milano 2006.

S. RODOTA', *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, Roma-Bari 2014.

L. RUFO, *Profili giuridici del Personal Health Record: tra diritto all'autodeterminazione e tutela della privacy*, in C. Faralli, R. Brighi, M. Martoni (a cura di) *Strumenti, diritti, regole e nuove relazioni di cura: il paziente europeo protagonista nell' eHealth*, Giappichelli, 2015.

G. M. SALERNO, *La protezione della riservatezza e l'inviolabilità della corrispondenza*, in P. Ridola, R. Nania (a cura di), *I diritti costituzionali*, Giappichelli, Torino, 2006, vol. II, pp. 617 ss.

E. SANTORO, *web 2.0 e medicina*, Pensiero, Roma, 2009.

G. SARTOR, J. MONDUCCI, Il Codice in materia di protezione dei dati personali. Commentario sistematico al D. lgs. 30 giugno 2003 n. 196, Cedam, Padova 2004.

K. SIKORA, *Second opinions for patients with cancer*, BMJ 1995, 311: 1179-80.

S. SIMI, *Dalla medicina basata sulle prove alla medicina basata sul paziente*, in AA.VV. *Quale salute per chi. Sulla dimensione sociale della salute*, Franco Angeli, 2010, p. 107.

M. SOFFIENTINI, (a cura di), *Privacy, Protezione e trattamento dati*, Wolters Kluwer, 2016.

P.C. TANG, Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption, J Am Med Inform Assoc. 2006 Mar-Apr; 13(2): 121–126 doi: 10.1197/jamia.M2025.

A. TETI, G. FESTA, *Sistemi informativi per la sanità*, APOGEO, Milano 2009.

Q. TIAN, *et al. Systems cancer medicine: towards realization of predictive, preventive, personalized and participatory (P4) medicine,* J. Intern. Med., 271 (2012), pp. 111-121.

E. TOSI, Il codice della privacy. Tutela e sicurezza dei dati personali: normativa nazionale e comunitaria, La Tribuna, Piacenza 2004. (Aggiornato con la L. 45/2004 in materia di data retention).

V. VACCARO, La cartella clinica (Nota a TAR VE sez. III 7 marzo 2003, n. 1674), in Trib. am. reg., 2003, 180.

P. VINCENTI AMATO, *Art. 32*, in Commentario alla Costituzione, a cura di G. Branca, Bologna, 1975.

M. G. VIRONE, *Il Fascicolo Sanitario Elettronico. Sfide e bilanciamenti fra Semantic Web e diritto alla protezione dei dati personali*, Aracne, 2015.

A.D. WESTON, L. HOOD, *Systems biology, proteomics, and the future of health care: toward predictive, preventative, and personalized medicine,* J. Proteome Res., 3 (2004), pp. 179-196.

D. WIJERS, L. WIESKE, M.D. VERGOUWEN, E. RICHARD, J. STAM, EM. SMETS, *Patient satisfaction in neurological second opinions and tertiary referrals*, J Neurol 2010, 257: 1869-74.

WORLD HEALTH ORGANISATION. *Telemedicine: Opportunities and developments in Member States. Based on the findings of the second global survey on eHealth*, Global observatory for eHealth series - Vol 2, Geneva, WHO Press, 2010.

E. ZAN, D.M. YOUSEM, M. CARONE, J.S. LEWIN, *Second-opinion consultations in neuroradiology*, Radiology 2010, 255: 135-41.

V. ZENO ZENCOVICH, I diritti della personalità dopo la legge sulla tutela dei dati personali, in Studium Iuris, 1997, pp. 467 ss.

V. ZENO ZENCOVICH, Privacy e informazioni a contenuto economico nel decreto legislativo n. 196 del 2003, in Studium Iuris, 2004, fasc. 4, pp. 452 ss.

V. ZENO ZENCOVICH, Personalità (diritti della), in Digesto delle Discipline Privatistiche - Sez. civile, vol. XIII, Utet, Torino, 1995, pp. 431 ss.

G. ZICCARDI, Internet, controllo e libertà, Raffaello Cortina Editore, Milano, 2015.

G. ZICCARDI, *La protezione informatica dei dati in ambito professionale,* Ciberspazio e Diritto, 2016, fasc. 3, pp. 469-496.

PROVVEDIMENTI LEGISLATIVI ITALIANI CITATI

L. 31 dicembre 1996 n. 675, *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*, pubblicata in G.U. n. 5 del 8.1.1997.

D. Lgs. 30 giugno 2003 n. 196, *Codice in materia di protezione dei dati personali*, pubblicato in G.U. n. 174 del 29.07.2003 e successive modifiche.

D. Lgs. 28 febbraio 2005 n. 42, *Istituzione del sistema pubblico di connettività e della rete internazionale della pubblica amministrazione, a norma dell'articolo 10, della legge 29 luglio 2003*, n. 229, pubblicato in G.U. n. 73 del 30.3.2005.

D. Lgs. 7 marzo 2005 n. 82, *Codice dell'amministrazione digitale*, pubblicato in G.U. n.112 del 16.05.2005 e successive modifiche.

D.L. 18 ottobre 2012 n. 179, *Ulteriori misure urgenti per la crescita del Paese*, pubblicato in G.U. n. 245 del 19.10.2012

D.L. 22 giugno 2012 n. 83, *Decreto Sviluppo*, pubblicato in G.U. n. 147 del 26.6.2012, convertito, con modificazioni, dalla legge 7 agosto 2012 n. 134, pubblicata in G.U. n. 187 del 11.8.2012

Decreto del Presidente del Consiglio dei Ministri, Regolamento in materia di fascicolo sanitario elettronico, n. 178 del 29 settembre 2015.

PROVVEDIMENTI AUTORITA' GARANTE PRIVACY CITATI

Linee guida in materia di Dossier sanitario - 4 giugno 2015.

Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario - 16 luglio 2009.

Provvedimento del Garante del 10 gennaio 2013 nei confronti dell'Azienda ospedaliero-universitaria Ospedali Riuniti di Trieste e delle altre aziende sanitarie della regione Friuli Venezia Giulia [doc. web n. 2284708].

Provvedimento del Garante del 3 luglio 2014 nei confronti dell'Azienda sanitaria dell'Alto Adige [doc. web n. 3325808].

Provvedimento del Garante del 23 ottobre 2014 nei confronti dell'Azienda ospedaliero-universitaria S. Orsola Malpighi di Bologna [doc. web n. 3570631].

Provvedimento del Garante del 18 dicembre 2014 nei confronti dell'Azienda Policlinico Umberto I di Roma [doc. web n. 3725976].

Provvedimento del Garante del 22 ottobre 2015 nei confronti dell'Azienda dall'Azienda USL 11 di Empoli [doc. web n. 4449114].

Provvedimento del Garante del 22 giugno 2016 nei confronti dell'Azienda Ospedaliera Sant'Andrea di Roma [doc. web. 5410033].

Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (cd. data breach), 4 aprile 2013, [doc. web 2388260].

Misure di sicurezza e modalità di scambio dei dati personali tra Amministrazioni pubbliche, 2 luglio 2015, , [doc. web n. 4129029].

PROVVEDIMENTI COMUNITARI CITATI

DIRETTIVA 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati.

Raccomandazione della Commissione del 2 luglio 2008 sull'interoperabilità transfrontaliera dei sistemi di cartelle cliniche elettroniche, (2008/594/CE) in http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32008H0594 (ultimo accesso 16/01/2016).

Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni, del 30 aprile 2004.

REGOLAMENTO (UE) N. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

REGOLAMENTO (UE) N. 679/2016 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 (regolamento generale sulla protezione dei dati).

GIURISPRUDENZA

Corte Costituzionale, sentenza n. 438 del 2008.

Corte di Cassazione, sentenza n. 22694 del 2005.

Consiglio di Stato, n. 146 del 18 settembre 2000.

Corte di Cassazione, sentenza n. 5658 del 1998.

Corte Costituzionale, sentenza n. 258 del 1994.

Corte Costituzionale, sentenza n. 132 del 1992.

Corte di Cassazione, sentenza n. 7958 del 1992.

Corte Costituzionale, sentenza n. 307 del 1990.

Corte Costituzionale, n.88 del 12 luglio 1979.

Corte di Cassazione, sentenza n. 2129 del 1975.

Corte di Cassazione, sentenza n. 4487 del 1956.