

INDICE

1. LA DISCIPLINA PER IL TRATTAMENTO DEI DATI RELATIVI ALLA SALUTE IN AMBITO SANITARIO

di Maria Livia Rizzo

- 1.1. L'evoluzione normativa e il valore dei dati nella società della conoscenza pag. 1
- 1.2. L'accountability e l'applicazione dei principi del Reg. UE 679/2016 in sanità pag. 3
 - 1.2.1. Liceità, correttezza e trasparenza pag. 4
 - 1.2.1.1. Le basi giuridiche pag. 5
 - 1.2.1.2. Le condizioni di liceità per il trattamento dei dati relativi alla salute pag. 6
 - 1.2.1.3. L'informativa privacy in sanità pag. 10
 - 1.2.2. Limitazione della finalità e riutilizzo dei dati per la ricerca scientifica pag. 14
 - 1.2.3. Necessità e minimizzazione del trattamento dei dati pag. 15
 - 1.2.4. Esattezza pag. 16
 - 1.2.5. Integrità e riservatezza: le misure di sicurezza pag. 17
 - 1.2.6. Limitazione della conservazione: la policy di data retention pag. 19
- 1.3. La privacy by design e by default pag. 20
- 1.4. L'importanza di un Sistema di gestione dei dati personali e il suo monitoraggio pag. 22

2. LA GOVERNANCE IN AMBITO SANITARIO NELL'OTTICA DEL GDPR

di Silvia Stefanelli e Alessandra Di Nunzio

- 2.1. I "ruoli privacy": il titolare, i contitolari, il responsabile, i destinatari e gli autorizzati pag. 25
 - 2.1.1. Il titolare del trattamento pag. 25
 - 2.1.2. I contitolari pag. 29
 - 2.1.3. I responsabili del trattamento pag. 33
 - 2.1.4. I destinatari dei dati pag. 36

2.1.5. Gli autorizzati (o designati) al trattamento	pag. 38
2.2. Le problematiche collegate alla definizione dei ruoli nell'organizzazione del SSN: i medici e i pediatri convenzionati, le farmacie, le strutture sanitarie accreditate e contrattualizzate	pag. 39
2.2.1. I medici e i pediatri convenzionati	pag. 39
2.2.2. Le farmacie	pag. 44
2.2.3. Le strutture sanitarie accreditate e contrattualizzate	pag. 46
2.3. I ruoli privacy nella continuità clinica	pag. 48
3. IL RESPONSABILE DELLA PROTEZIONE DEI DATI O DATA PROTECTION OFFICER di Alessandra Delli Ponti	
3.1. Introduzione	pag. 51
3.2. Quando è obbligatoria la designazione del DPO	pag. 53
3.3. I Requisiti del DPO	pag. 58
3.3.1. Qualità Professionali	pag. 58
3.3.2. Autonomia e indipendenza	pag. 61
3.3.3. DPO interno o esterno?	pag. 64
3.4. Compiti del DPO	pag. 66
4. I PRINCIPALI ADEMPIMENTI di Fabio Marinello, Alessandra Delli Ponti e Vittoria Piretti	
4.1. Premesse	pag. 75
4.2. Il Registro delle attività di trattamento	pag. 75
4.2.1. Tipi e contenuti del Registro	pag. 77
4.2.1.1. Premesse	pag. 78
4.2.1.2. Elenco dei trattamenti	pag. 78
4.2.2. I modelli dei Garanti europei	pag. 80
4.3. Gestione fornitori	pag. 81
4.3.1. Scelta del fornitore	pag. 83
4.3.2. Forma dell'accordo o nomina come Responsabile	pag. 84
4.3.3. Oggetto della nomina	pag. 86
4.3.4. Contenuto	pag. 86
4.3.5. Patologie nel rapporto di fornitura	pag. 89
4.4. Gestione del personale interno	pag. 90
4.4.1. Istruzioni operative e norme comportamentali	pag. 91
4.4.2. Formazione del personale	pag. 93
4.5. Sicurezza dei sistemi informatici	pag. 94
4.5.1. Obiettivi della sicurezza informatica	pag. 94
4.5.2. L'adeguamento a partire dalla precedente normativa	pag. 96

4.5.3. Procedura di analisi dei rischi	pag. 98
4.5.3.1. Minacce	pag. 98
4.5.3.2. Valutazione dei criteri di rischio	pag. 100
4.5.4. Misure di sicurezza	pag. 102
4.6. La valutazione di impatto sul trattamento di dati personali	pag. 108
4.6.1. Casi di obbligo di valutazione	pag. 108
4.6.2. Strumenti per lo svolgimento della valutazione d'impatto	pag. 110
4.7. Data breach dalla teoria alla pratica	pag. 111
4.7.1. Le fasi della gestione di un Data breach	pag. 113
4.8. Esercizio dei diritti degli interessati	pag. 116
4.9. Procedura di gestione dei pazienti	pag. 123
4.10. Gestione della documentazione medica	pag. 126
4.10.1. Il sistema di refertazione on line	pag. 127
4.10.2. Cartella clinica	pag. 129
4.10.3. L'accesso alla Cartella clinica	pag. 132
4.10.4. Il Dossier sanitario elettronico (DSE)	pag. 135
5. LA RICERCA SCIENTIFICA	
di Silvia Stefanelli e Alessandra Di Nunzio	
5.1. Nozioni generali	pag. 141
5.1.1. La ricerca scientifica	pag. 141
5.1.2. La ricerca nel mondo dei Farmaci	pag. 142
5.1.3. La ricerca nel mondo dei Dispositivi Medici	pag. 144
5.2. La disciplina sul trattamento dei dati personali nella ricerca scientifica	pag. 144
5.2.1. Il GDPR, l'European Data Protection Board e l'European Data Protection Supervisor	pag. 144
5.2.2. La disciplina del Codice Privacy nell'ambito della ricerca scientifica	pag. 152
5.2.3. I provvedimenti del garante Privacy sulla ricerca scientifica	pag. 157
5.3. I ruoli privacy nella ricerca	pag. 158
5.4. La natura dei dati	pag. 160
5.4.1. Dato pseudonimizzato	pag. 161
5.4.2. Dato de-identificato	pag. 162
5.4.3. Dato anonimo	pag. 163

6. LA SANITÀ DIGITALE

di Giorgia Verlato, Maria Livia Rizzo, Alice Giannini, Giorgia Rosati
e Alessandra Delli Ponti

- 6.1. La telemedicina pag. 169
- 6.2. Internet Of Medical Things (IoMT) pag. 172
- 6.3. Stampa 3D pag. 173
- 6.4. Le mobile applications mediche pag. 176
 - 6.4.1. Introduzione pag. 176
 - 6.4.2. Le nuove disposizioni stabilite dalle Linee guida del Garante pag. 176
 - 6.4.3. Aspetti peculiari relativi al consenso del paziente espresso tramite app mobile pag. 178
- 6.5. Il trattamento dei Big Data in sanità e Intelligenza Artificiale pag. 180
 - 6.5.1. I problemi definatori relativi all'Intelligenza Artificiale pag. 180
 - 6.5.2. Big Data e IA pag. 181
 - 6.5.3. Il quadro normativo a livello europeo ed i profili privacy pag. 182
 - 6.5.4. Campi di applicazione dell'intelligenza artificiale in sanità pag. 185
- 6.6. I patient support program pag. 186
 - 6.6.1. I patient support program (PSP): un modello di cura patient-oriented pag. 186
 - 6.6.2. Gli impatti della normativa privacy sulla gestione dei PSP pag. 188
- 6.7. Localizzazione dei pazienti e nuovi sistemi di tracciamento pag. 190