UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

CORSO DI LAUREA IN BIOINGEGNERIA

Tesi di laurea Magistrale

Analisi ed applicazione della Normativa Europea sulla Protezione del Dato in ambito Sanitario:

Progettazione e realizzazione del Registro dei Trattamenti per il reparto di Radiologia

Relatore

Prof. Andrea Facchinetti

Laureanda: Dott.ssa Elena Crepaldi

Matricola: 2003040

ANNO ACCADEMICO 2021-2022

Data di laurea: 13 ottobre 2022

All'ingegner Tenan,
che ha la pessima abitudine
di dedicare agli altri più tempo
di quanto non ne abbia effettivamente
a disposizione.

È stato un privilegio
averne potuto approfittare.

Abstract

La complessità tecnologica dei sistemi ospedalieri è in costante crescita e l'utilizzo di nuove tecnologie, sempre più performanti ed interdipendenti, comporta un evidente e costante miglioramento della qualità delle prestazioni sanitarie offerte, una crescente personalizzazione ed attenzione per il paziente e la capacità di conservare agevolmente informazioni mediche utili a diagnosi e statistiche per progressi in campo medico. Tuttavia, uno dei problemi legati all'avanzamento tecnologico, all'aumento dei dispositivi biomedicali e dei dati da loro prodotti è la sicurezza dei dati stessi.

La sicurezza delle informazioni mediche è tutelata dalla Normativa Europea per la Protezione del Dato (GDPR) ha un impatto significativo sulle organizzazioni sanitarie ed introduce l'obbligo di tenere il Registro delle Attività di Trattamento, deputato a contenere tutte le informazioni relative ai trattamenti dei dati personali svolti presso un'azienda ospedaliera, nell'ottica di un ragionamento complessivo volto alla tutela della privacy del paziente. L'obiettivo di questa tesi magistrale è analizzare gli aspetti del nuovo Regolamento europeo più rilevanti sia per i fabbricanti di dispositivi medici sia, particolarmente, per gli operatori sanitari, e come conseguenza realizzare e mettere in atto un protocollo di Analisi e Valutazione dei Rischi, costruendo infine il Registro delle attività di Trattamento svolte nel Reparto di Radiologia, presso l'Azienda Ospedaliera Aulss5, nel Polo Ospedaliero di Rovigo.

Indice

Indice delle tabelle

Indice delle immagini

Introduzione

Il presente lavoro, svolto nel contesto di un tirocinio curricolare presso il Dipartimento di Ingegneria Clinica del Polo Ospedaliero di Rovigo (Azienda Ospedaliera ULSS 5), intende affrontare il tema relativo al trattamento dei dati in ambito sanitario, in particolar modo alla luce del Regolamento Europeo 2016/679, anche noto come GDPR. Il Regolamento Generale sulla Protezione del Dato è entrato in vigore a partire da maggio 2018 ed ha lo scopo di chiarire ed unificare, per ogni paese dell'Unione, le modalità di trattamento, raccolta, utilizzo, protezione e condivisione dei dati personali. L'ambito sanitario è uno dei settori maggiormente sensibili all'applicazione del suddetto regolamento, sia perché opera su dati personali relativi alla salute del singolo interessato, sia per l'elevato rischio in caso di diffusione dei dati stessi.

Il diritto alla salute pubblica e il diritto alla protezione dei dati relativi alla salute sono entrambe questioni fondamentali che, con il progressivo avanzamento tecnologico e la crescente integrazione di carattere informatico dei diversi reparti ospedalieri in una rete comune, si trovano ad essere fortemente correlate tra loro ed interdipendenti. Come verrà evidenziato con maggiore dettaglio nei Capitoli seguenti, se da un lato il diritto alla privacy è di fondamentale importanza per la tutela della persona fisica, quando si entra in un contesto sanitario diviene necessario bilanciare la tutela della privacy con il diritto alla salute, considerando il secondo di pari – se non di maggiore importanza - rispetto al primo.

Data la necessità di rafforzare, all'interno dell'Azienda Ospedaliera, delle opportune procedure che garantiscano l'adeguamento della stessa alla Normativa Europea, due saranno gli obiettivi principali sviluppati nel corso della seguente trattazione.

In primo luogo, si è procederà con la realizzazione di un protocollo di Analisi e Valutazione del Rischio: la cosiddetta DPIA (Data Protection Impact Assessment) costituisce infatti uno dei punti cardine del Regolamento Europeo, che definisce di fondamentale importanza la necessità, da parte dell'Azienda, di essere sempre al corrente delle possibili criticità inerenti i trattamenti effettuati, a maggior ragione se tali trattamenti riguardano dati particolarmente sensibili, quali i dati sanitari.

La procedura redatta permetterà, per ogni reparto, di trasformare informazioni di carattere tipicamente qualitativo - inerenti alle modalità di trattamento dei dati sanitari dei pazienti ed ai controlli effettuati sui dispositivi - in quantità numeriche ben definibili e calcolabili, col fine di determinare un valore specifico di Rischio Residuo per i trattamenti operati in Azienda. Tale valore costituisce un punto di partenza per l'effettuazione di procedure di miglioramento delle modalità di trattamento poste in essere.

Il secondo obiettivo, nonché scopo finale della Tesi, consisterà, sulla base dei risultati ottenuti dalle procedure di Analisi del Rischio, nella stesura del Registro dei Trattamenti. In via generale, tale documento raccoglie, per ogni reparto - e quindi, una volta completato, per tutta la struttura ospedaliera - informazioni riguardanti i trattamenti svolti in Azienda facendo riferimento alle modalità di trattamento effettuate da ciascun dispositivo, elettromedicale, monitor o device medico di altra natura.
Specificamente, in questa sede è stato da me redatto il primo Registro delle Attività di Trattamento per l'Azienda Ospedaliera ULSS5 Polesana.
Il reparto in cui si è scelto di svolgere l'analisi è la UOC (Unità Operativa Complessa) Radiologia; la Radiologia è, storicamente, il primo reparto ospedaliero che, per le particolari caratteristiche degli esami effettuati, ha richiesto lo sviluppo di software medici dedicati alla gestione di tutte le informazioni sanitarie raccolte, da associare poi alle numerose immagini che permettono ai medici di effettuare valutazioni precise sulle condizioni sanitarie dei pazienti. La presenza, dunque, di una rete informatica che collega densamente ogni dispositivo medico del suddetto reparto con il Sistema Informativo Ospedaliero, oltre a favorire la velocità e la correttezza degli esami svolti, comporta una serie di rischi nella gestione dei dati sensibili, che dovranno essere opportunamente valutati e monitorati.
Al termine del procedimento, ogni dispositivo presente nel reparto di Radiologia verrà catalogato ed opportunamente esaminato, e presenterà una valutazione del rischio che permetterà di effettuare delle considerazioni sul rischio complessivo riscontrabile nel reparto in esame.
La procedura redatta in questa sede non è fine a sé stessa, si tratta bensì di una serie di passaggi metodologici che permetteranno all'Azienda, nel prossimo futuro, di completare il lavoro da me iniziato e redigere in modo adeguato un Registro delle Attività di Trattamento comprensivo di ogni prestazione sanitaria erogata e, più nello specifico, di ogni dispositivo medico atto a tale scopo. Si tratta di un'attività indispensabile, nonché obbligatoria, dall'entrata in vigore del GDPR, a tutela sia dell'Azienda che, soprattutto, degli utenti che si avvalgono dei servizi forniti.

Nel primo capitolo verrà brevemente descritto il contesto aziendale in cui questo lavoro è stato realizzato, e successivamente saranno riportate e descritte le normative alle quali devono sottostare i dispositivi medici, con particolare riferimento al GDPR, punto focale dell'analisi, ed all'MDR, il Regolamento sui Dispositivi Medici, nell'indispensabilità di coniugare la necessità di una protezione sia per quanto riguarda la privacy dei dati elaborati, sia di poter contare su un dispositivo che garantisca un funzionamento ottimale.

Il secondo capitolo vedrà una descrizione delle modalità di individuazione ed analisi del rischio, con particolare attenzione ai concetti, introdotti dal GDPR, di privacy by design e privacy by default - ovvero la necessità che ciascun dispositivo in grado di elaborare o anche solo visionare e raccogliere dati possieda caratteristiche di tutela e protezione del dato fin dalla sua progettazione ed ideazione – procedendo successivamente, da un punto di vista generale, all'identificazione dell'architettura e delle funzionalità dei dispositivi che devono essere esaminati e che verranno impiegati in un contesto di gestione del dato, alle tipologie di eventi avversi che possono manifestarsi e alle diverse modalità di controllo da effettuare. Si entrerà quindi, più nello specifico, nell'esame del Sistema Informativo Ospedaliero, la rete di comunicazione che collega tutti i dispositivi e gli elettromedicali impiegati a livello di struttura sanitaria, valutandone il funzionamento e le principali criticità.
Infine, nel terzo capitolo verrà sia realizzata che eseguita la procedura di valutazione del rischio per i trattamenti operati in Azienda effettuando, in fase di applicazione della procedura, una differenziazione tra le workstation – i monitor di gestione dei dati sanitari e delle immagini raccolte mediante i device - e il resto dei dispositivi medici, ciascuno operante in modalità proprie.
In questa fase risulta importante sottolineare che il Regolamento Europeo non fornisce linee guida specifiche per effettuare la Valutazione del Rischio, ma solo informazioni generali a tutela del dato. Sarà dunque compito della seguente trattazione individuare, sulla base di ulteriori principi riscontrabili nelle normative ISO (International Organization for Standardization) e delle linee guida riportate dal gruppo dei Garanti Privacy UE WP29[1], dall' AgID[2] (Agenzia per l'Italia Digitale) e dall'ENISA[3] (Agenzia Europea per la Sicurezza Informatica), una metodologia di Analisi del Rischio e di Protezione del Dato che sia in grado di comprendere le indicazioni precedentemente riportate ed adeguarle ad un contesto sanitario.

Al termine del lavoro di tesi verrà riportato il Registro dei Trattamenti per il reparto di Radiologia, ottenuto nella sua interezza, contenente tutte le informazioni maggiormente rilevanti per la conoscenza dei rischi associati ai trattamenti ed alle modalità in cui ciascun dispositivo opera, i controlli a cui è sottoposto ed il valore di Rischio Residuo calcolato. Tale valore permetterà di comprendere appieno l'entità dei rischi relativi alla privacy associati alle

[1] WP248 rev.01: *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely result in high risk" for the purposes of Regulation 2016/679*
[2] *Linee Guida per la modellazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del Secure/Privacy by Design*, documento rilasciato il 7 maggio 2020
[3] *Regolamento (UE) 2019/881 sulla certificazione della cybersicurezza nelle tecnologie dell'informazione e della comunicazione (Cyber act)*, documento rilasciato il 17 aprile 2019

prestazioni erogate da tale reparto e, di conseguenza, di attuare tutta una serie di strategie a mitigazione degli stessi, se il valore di rischio riscontrato dovesse risultare sproporzionato al beneficio clinico offerto.

Capitolo 1.

Le direttive che disciplinano i Dispositivi Medici

1.1 Introduzione al contesto Aziendale di Tirocinio

Il mio percorso di tirocinio, della durata di sei mesi, si è svolto presso l'Unità Operativa Semplice (UOS) Ingegneria Clinica dell'Azienda Ospedaliera ULSS5 Polesana.

L'obiettivo finale del tirocinio consisteva nell'ideare, ed in seguito attuare - limitatamente ai reparti di Radiologia ed Emodinamica - una strategia per la valutazione dei rischi associati ai trattamenti svolti presso la struttura ospedaliera, nell'ambito della gestione e protezione dei dati sanitari raccolti dai pazienti, in adempimento a quanto stabilito dal Regolamento Europeo per la Protezione dei Dati, anche noto come GDPR. Il procedimento adottato, descritto con precisione nel capitolo successivo, comprende la realizzazione di un Registro dei Trattamenti, in cui le attività svolte presso i due reparti sono state riportate considerando nel dettaglio le tipologie di dati trattate, le modalità di gestione, il rischio associato ed eventuali indicazioni per la riduzione delle criticità riscontrate.

Di seguito viene proposta una breve panoramica del contesto aziendale e delle condizioni del Sistema Sanitario Regionale.

1.1.1 Il Sistema Socio-Sanitario della Regione Veneto

La nascita del Sistema sociosanitario della Regione (SSR) del Veneto risale all'approvazione del suo Statuto[4], nel 1971. Sin da subito, in Veneto, si è voluto seguire un approccio finalizzato all'integrazione tra l'area sanitaria e quella sociale, consolidatosi con l'istituzione appunto del Sistema sanitario nazionale.

La concreta applicazione, poi, dei principi di aziendalizzazione e regionalizzazione[5], ha condotto all'approvazione di due leggi[6] regionali fondamentali, per mezzo delle quali vengono definiti gli strumenti e le modalità della programmazione, i meccanismi e le fonti di

[4] Statuto della Regione Veneto, **Legge 22 maggio 1971, n. 340**, *Principi Fondamentali*, par.4: "A questi fini la Regione veneta esercita i propri poteri: per rendere effettivo l'esercizio del diritto allo studio, al lavoro e alla sicurezza sociale, e dei diritti della famiglia; [..] per garantire a tutti i cittadini i servizi sociali, con particolare riguardo all'abitazione, alla scuola, alla tutela della salute, ai trasporti, alle attrezzature sportive [..]; per svolgere una politica intesa a promuovere le attività culturali e la ricerca scientifica e tecnologica.

[5] D.lgs. 30 dicembre 1992, n. 502, *Riordino della disciplina in materia sanitaria* e il D.lgs. 17 dicembre 1993, n. 517, *Modificazioni al decreto legislativo 30 dicembre 1992, n. 502, recante riordino della disciplina in materia sanitaria.*

[6] Il riferimento è alla legge regionale 14 settembre 1994, n. 55: *Norme sull'assetto programmatorio, contabile, gestionale e di controllo delle Unità locali sociosanitarie e delle aziende*; e alla legge regionale 14 settembre 1994, n. 56: *Norme e principi per il riordino del servizio sanitario regionale*.

finanziamento delle Aziende sanitarie, il loro assetto contabile, gestionale e di controllo; inoltre, viene delineato l'impianto organizzativo del Sistema sanitario regionale.

Vanno evidenziati alcuni elementi costitutivi tipici del SSR del Veneto: innanzitutto, vi è una visione della salute quale stato di completo benessere fisico, mentale e sociale - e non semplicemente come assenza di malattia o infermità; in secondo luogo, si attua una modalità operativa che contempla il raggiungimento del maggior grado di salute possibile come un risultato sociale notevole, la cui realizzazione richiede la compartecipazione di diversi soggetti. Per questo motivo, il Veneto conosce una struttura organizzativa che si discosta dagli altri modelli regionali, tanto a livello di macrostruttura quanto nel più ristretto ambito aziendale. Infatti, al di là della denominazione delle Aziende sanitarie come AULSS (Azienda Unità Sanitaria Locale Socio Sanitaria), anziché come ASL (Azienda Sanitaria Locale), la Regione Veneto ha deciso di porre ai vertici istituzionali di ciascuna ULSS anche un Direttore dei servizi sociali e della funzione territoriale. Conseguentemente, si garantisce una costante interazione con gli Enti locali e con gli altri attori coinvolti nel sistema.

1.1.2 L'istituzione di Azienda Zero e il riassetto organizzativo delle ULSS

È di relativamente recente promulgazione la legge regionale[7] che ha portato all'istituzione di Azienda Zero quale ente di governance della sanità veneta ed al conseguente riordinamento dell'assetto organizzativo e funzionale delle Aziende Sanitarie.

La motivazione principale è stata quella di ricondurre in capo ad un solo soggetto le funzioni di supporto alla programmazione sanitaria e sociosanitaria, nonché al coordinamento del SSR, convogliando in esso le attività di gestione tecnico-amministrativa su scala regionale.

Tra i ruoli[8] di Azienda Zero troviamo, in particolare:

- Le funzioni e le responsabilità della Gestione Sanitaria Accentrata;
- Il finanziamento del fabbisogno sanitario e la redazione del bilancio preventivo e consuntivo;
- I servizi tecnici per la valutazione dell'Health Technology Assessment.

Per quanto concerne, invece, il riassetto organizzativo-funzionale delle ULSS, lo scopo della norma è stato quello di migliorare la qualità e l'efficienza nella gestione dei servizi resi, in un'ottica di razionalizzazione e riduzione dei costi, erogando le prestazioni in modo

[7] Legge Regionale 25 ottobre 2016, n. 19, *Istituzione dell'ente di governance della sanità regionale veneta denominato "Azienda per il governo della sanità della Regione del Veneto - Azienda Zero"*.

[8] Per tutte le azioni di competenza di Azienda Zero si rimanda alla lettura dell'atto aziendale, al par. 1.3*, La missione e la visione dell'Azienda* ed al par. 3.1, *Funzioni*. Questo è disponibile sul sito ufficiale di Azienda Zero https://www.azero.veneto.it/

appropriato e uniforme e promuovendo il coinvolgimento attivo dei cittadini. Inoltre, è contemplata una periodica revisione dell'offerta assistenziale ospedaliera, secondo una logica di rete coordinata, integrando cioè reti cliniche e enti del territorio ed individuando i fabbisogni del personale ospedaliero, medico e non.

Le nove ULSS, entrate in vigore dal 1° gennaio 2017, sono:

ULSS 1 – Dolomiti;
ULSS 2 – Marca Trevigiana;
ULSS 3 – Serenissima;
ULSS 4 – Veneto Orientale;
ULSS 5 – Polesana;
ULSS 6 – Euganea;
ULSS 7 – Pedemontana;
ULSS 8 – Berica;
ULSS 9 – Scaligera.

Di seguito si riportano alcune informazioni di carattere generale per quanto concerne l'Azienda Ospedaliera AULSS 5, con particolare riferimento all'Ospedale S. Maria della Misericordia di Rovigo ed al Dipartimento di Ingegneria Clinica in si è svolto il tirocinio.

1.1.2.1 Azienda Ospedaliera Aulss 5

L'ULSS 5 Polesana si è costituita dalla fusione fra le vecchie Ulss 18 di Rovigo e Ulss 9 di Adria; ha mantenuto la sede nel capoluogo e con i servizi forniti copre tutta la provincia.
In Figura 2 sono riportati i centri di erogazione dei servizi sociosanitari di competenza dell'ULSS 5.

Figura 1. Logo Azienda Ospedaliera ULSS5 Polesana

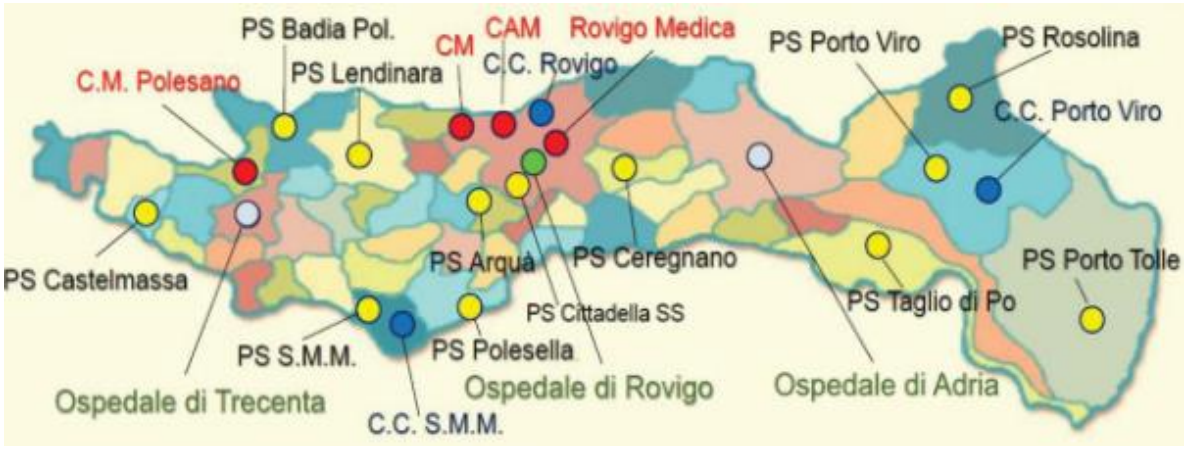


Figura 2. Mappa Provinciale dei punti di prenotazione ed erogazione dei servizi dell'Azienda AULSS 5. Immagine tratta dalla Relazione sulla Gestione Aziendale, 2020.

Il LEA[9] "Assistenza Ospedaliera" nell'Azienda ULSS 5 Polesana è garantito da tre presidi ospedalieri pubblici e tre strutture private accreditate, di seguito elencati:

- Presidio Ospedaliero "S. Maria della Misericordia", Rovigo;
- Presidio Ospedaliero "S. Luca", Trecenta;
- Presidio Ospedaliero "S. Maria Regina degli Angeli", Adria;
- Casa di Cura "S. Maria Maddalena", Occhiobello;
- Casa di Cura "Città di Rovigo", Rovigo;
- Casa di Cura "Madonna della Salute", Porto Viro.

I posti letto al 31/12/2020 per gli ospedali direttamente gestiti consistono di 745 unità, mentre per quelli convenzionati di 297 unità[10].

Di seguito è riportata in modo dettagliato, per l'anno 2020, la dotazione di posti letto, suddivisi per reparto, dei presidi ospedalieri pubblici nominati in precedenza (Tabella 1).

Presidio ospedaliero "S. Maria della Misericordia", Rovigo - Dotazione di Posti Letto	
Reparti	*PL Totali*
Area Medica	
Cardiologia	20
Dermatologia	2
Gastroenterologia	6
Geriatria	43
Malattie infettive	6
Medicina Generale	40

[9] L'acronimo LEA identifica i Livelli Essenziali di Assistenza, ovvero, *le prestazioni e i servizi che il Servizio sanitario nazionale (SSN) è tenuto a fornire a tutti i cittadini, gratuitamente o dietro pagamento di una quota di partecipazione (ticket), con le risorse pubbliche raccolte attraverso la fiscalità generale (tasse),* Definizione e aggiornamento dei livelli essenziali di assistenza, di cui all'articolo 1, comma 7, del D. Lgs.del 30 dicembre 1992, n. 502.

[10] Le informazioni riportate sono ricavate dalla Relazione sulla Gestione Aziendale 2020, redatta in ottemperanza al D. Lgs. 118/2011 e contenente tutte le informazioni atte ad una rappresentazione esaustiva della gestione sanitaria ed economico-finanziaria dell'esercizio 2020.

Nefrologia	5	
Neurologia	20	
Oncologia	12	
Pneumologia	15	
Psichiatria	16	
Totale		*185*
Area Chirurgica		
Chirurgia Generale	30	
Neurochirurgia	10	
Oculistica	3	
Ortopedia e Traumatologia	30	
Otorinolaringoiatria	12	
Urologia	12	
Totale		*97*
Area Materno Infantile		
Ostetricia e Ginecologia (Ostetricia)	18	
Ostetricia e Ginecologia (Ginecologia)	14	
Patologia Neonatale	4	
Pediatria	8	
Totale		*44*
Area Terapia Intensiva		
Rianimazione - Terapia Intensiva	14	
Terapia Intensiva Coronarica UTIC	8	
Terapia Intensiva Neonatale	2	
Totale		*24*
Area Riabilitativa		
REF Cardiologia	2	
REF Neurologia	5	
Totale		*7*
TOTALE PRESIDIO OSPEDALIERO ROVIGO		**357**

Presidio ospedaliero "S. Maria degli Angeli", Adria - Dotazione di Posti Letto		
Reparti	*PL Totali*	
Area Medica		
Cardiologia	8	
Medicina Generale	8	
Psichiatria	62	
Totale		*78*
Area Chirurgica		
Chirurgia Generale	24	
Oculistica	2	
Ortopedia e Traumatologia	20	
Otorinolaringoiatria	4	
Urologia	7	
Totale		*57*
Area Materno Infantile		
Ostetricia e Ginecologia	18	
Pediatria	6	
Totale		*24*
Area Terapia Intensiva		
Rianimazione - Terapia Intensiva	4	
Terapia Intensiva Coronarica UTIC	1	
Totale		*5*
Area Riabilitativa		
Lungodegenza	17	
RRF (Recupero Riabilitazione Funzionale)	16	
Totale		*33*
TOTALE PRESIDIO OSPEDALIERO Adria		**197**

Presidio ospedaliero "S. Luca", Trecenta - Dotazione di Posti Letto		
Reparti		*PL Totali*
Area Medica		
Medicina Generale		61
Pneumologia COVID		104
	Totale	*165*
Area Chirurgica		
Chirurgia Generale		10
Day Surgery Multidisciplinare		12
	Totale	*22*
Area Materno Infantile		
Ostetricia e Ginecologia		18
Pediatria		6
	Totale	*24*
Area Terapia Intensiva		
Rianimazione - Terapia Intensiva		4
	Totale	*4*
TOTALE PRESIDIO OSPEDALIERO Trecenta		**191**

TOTALE POSTI LETTO PUBBLICI AZ. ULSS5	**745**

Tabella 1. Le tre tabelle riportano la dotazione di Posti Letto per i tre presidi ospedalieri (Rovigo, Trecenta e Adria) suddivisi per reparto. Immagine tratta dalla Relazione sulla Gestione Aziendale, 2020.

1.1.2.2 Unità Operativa Semplice di Ingegneria Clinica

La UOS Ingegneria Clinica (Figura 3) fa capo alla UOC Servizi Tecnici e Patrimoniali, colloquialmente chiamato Ufficio Tecnico. Sono numerose le attività che questo dipartimento svolge[11], tra le quali si elencano:

- Gestione dei contratti relativi alle apparecchiature elettromedicali, per quanto riguarda la corretta e periodica manutenzione, i collaudi, i rapporti con le Aziende fornitrici, la redazione dei contratti per i bandi di gara, etc.;
- Supporto all'intero Ufficio Tecnico nelle decisioni inerenti il parco elettromedicali, per acquisti, spostamenti e dismissioni e nella gestione di commissioni di gara;
- Predisposizione, in accordo con la parte sanitaria, di capitolati per l'acquisto o il noleggio di elettromedicali per la sostituzione di dispositivi datati o per l'allestimento di nuove sale;
- Coordinamento delle verifiche elettriche sulle apparecchiature;
- Coordinamento dei collaboratori dell'intero dipartimento;

[11] Le principali aree di responsabilità attribuite all'Ingegneria Clinica all'interno delle strutture sanitarie sono riportate dall'Associazione Italiana degli Ingegneri Clinici (AIIC) nel documento *Il ruolo dell'Ingegnere Clinico nel Servizio Sanitario Nazionale* (www.aiic.it)

1.2 I dispositivi medici

Si definisce[12] dispositivo medico un qualunque strumento, apparecchio, impianto, software, sostanza o altro prodotto utilizzato da solo o in combinazione con altri dispositivi o accessori e destinato dal fabbricante ad essere impiegato sull'uomo a fini di:

- diagnosi, prevenzione, monitoraggio, terapia o attenuazione di una malattia, di una ferita o di un handicap;
- studio, sostituzione o modifica dell'anatomia o di un processo fisiologico o patologico;
- fornire informazioni attraverso l'esame in vitro di campioni provenienti dal corpo umano, inclusi sangue e tessuti donati, e che non esercita nel o sul corpo umano l'azione principale cui è destinato mediante mezzi farmacologici, immunologici o metabolici, ma la cui funzione può essere coadiuvata da tali mezzi.

Si considerano dispositivi medici anche i seguenti prodotti:

- dispositivi per il controllo del concepimento o il supporto al concepimento;
- i prodotti specificamente destinati alla pulizia, disinfezione o sterilizzazione dei dispositivi[13].

Il Consiglio dell'Unione Europea ha emanato delle direttive, al fine di dare garanzia di sicurezza e di protezione ai pazienti quando si utilizzano dispositivi medici, nonché in termini di buon funzionamento del dispositivo stesso e di elevate prestazioni. Tali direttive hanno lo scopo di regolamentare, nei paesi dell'Unione Europea, il settore dei dispositivi medici in tutti i suoi aspetti: produzione, requisiti essenziali, indagini cliniche, valutazione e gestione dei rischi, ottenimento marcatura CE fondamentale per la commercializzazione del dispositivo nel mercato europeo, e sorveglianza post market.

Nel corso del seguente Capitolo verranno riportati i due Regolamenti Europei di maggiore impatto per l'ambiente Sanitario, nonché con maggiore riscontro per l'obiettivo del percorso di tirocinio: si introdurrà in breve Il Regolamento Europeo sui Dispositivi Medici, anche noto come MDR, per meglio inquadrare l'ambito tecnico operativo nel quale ci si trova ad agire se si gestiscono elettromedicali; si passerà quindi alla disamina del nuovo Regolamento Europeo sulla Protezione dei Dati, noto come GDPR, la cui applicazione per la protezione dei dati sanitari si configura nell'obiettivo finale di questo lavoro di tesi.

[12] Regolamento (UE) 2017/745 Del Parlamento Europeo E Del Consiglio Del 5 Aprile 2017, **art. 2**: *Definizioni*, D.Lgs. n. 46 del 24 febbraio 1997

[13] All'interno del Regolamento (UE) 2017/745 "i dispositivi medici, gli accessori per i dispositivi medici e i prodotti elencati [..] sono denominati «dispositivi»."

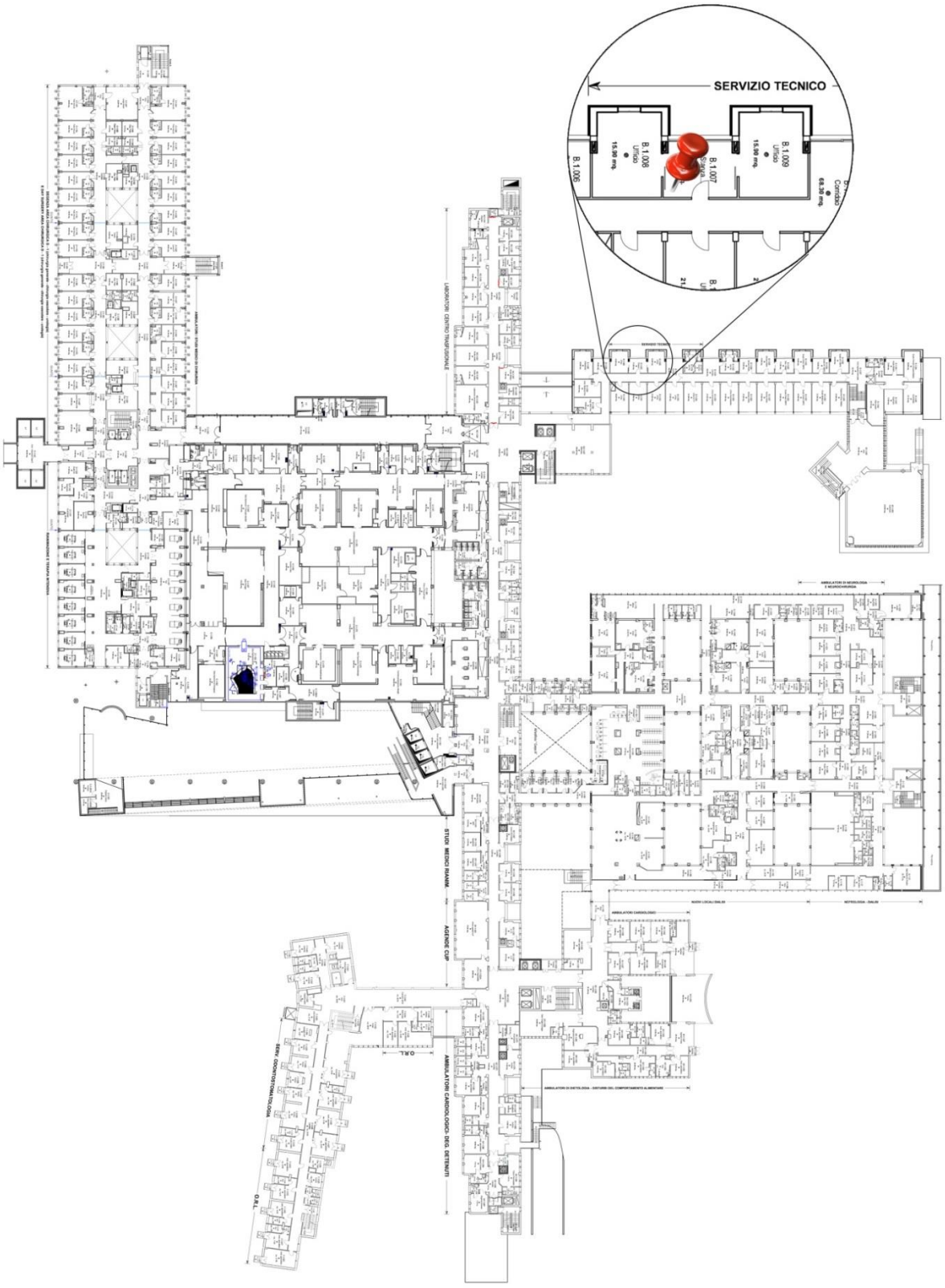


Figura 3. Planimetria del primo piano dell'Ospedale di Rovigo; nella sede di Ingegneria Clinica è evidenziato l'ufficio in cui ho svolto il tirocinio.

1.2.1 Il Regolamento Europeo sui Dispositivi Medici

Il Regolamento UE 2017/745 (Medical Device Regulation – MDR) disciplina le norme che si applicano ai dispositivi medici di diversa natura; è composto di 123 articoli, raggruppati in 10 capitoli; è divenuto pienamente efficace lo scorso 26 maggio 2021, con un anno di ritardo a causa dell'Emergenza Covid.

Detto Regolamento, rispetto alle disposizioni precedenti[14], alza il livello di attenzione non soltanto sulla sicurezza dei dispositivi, ma anche sulla loro efficacia, affidando ai produttori importanti oneri di controllo sui processi di fabbricazione, diffusione e commercializzazione del dispositivo; inoltre, abroga le precedenti direttive sui dispositivi medici e impiantabili attivi[15].

Tra gli obiettivi auspicati dall'introduzione dell'MDR è possibile trovare:

- Maggiore omogeneità tra le norme degli stati membri, compresa la struttura della documentazione tecnica;
- Rafforzamento del sistema di vigilanza e sorveglianza, soprattutto grazie al controllo degli Organismi Notificati[16] sulle Aziende;
- Aumentata sorveglianza post-commercializzazione;
- Tracciamento minuzioso dei dispositivi medici nei loro spostamenti con annesso processo di rintracciabilità tramite codice di identificazione univoco (UDI[17]);
- Aggiornamento tecnologico, con una particolare attenzione ai dispositivi di recente introduzione che non venivano trattati dai Regolamenti precedenti (software, nanomateriali, etc.);
- Migliore compatibilità con sistemi extra UE: allineamento dell'assetto di regolamentazione europeo a quello di altri paesi partner commerciali, come USA e Canada, in emulazione ad un medesimo processo in ambito di legislazione farmaceutica;

[14] Dir. 93/42/CEE (*Medical Devices Directive* - MDD) del 24/02/1997 e Dir. 98/79/CEE del 18/09/1998. Notare che L'MDR non emenda l'MDD, non lo sostituisce, si tratta di due certificazioni diverse, le due certificazioni possono coesistere sullo stesso dispositivo medico. Al contrario, l'MDR abroga interamente l'AIMDD, relativo ai dispositivi medici impiantabili attivi.

[15] Dir. 90/385/CEE (*Active Implantable Medical Devices Directive* - AIMDD) del 20/05/1990.

[16] Si tratta di organismi autorizzati dalle Autorità Designanti ad espletare le procedure di certificazione ai fini della marcatura CE dei dispositivi (https://www.salute.gov.it/portale/home.html).

[17] L'identificazione unica dei dispositivi (UDI) è un codice numerico o alfanumerico unico associato a un dispositivo medico, che permette di identificare in modo chiaro e inequivocabile dispositivi specifici immessi sul mercato facilitandone la tracciabilità. L'UDI si affiancherà agli attuali requisiti di etichettatura per i dispositivi medici, senza sostituirli. Attualmente si è ancora nella fase iniziale dell'adozione di tale codice, perciò è prevista la doppia registrazione operatoria a livello nazionale nella Banca Dati Italiana (istituita ai sensi dell'art.13 del d.lgs 46/97, dall'1 dicembre 2021 ha subito un adeguamento per consentire a fabbricanti e mandatari di adempiere agli obblighi di registrazione dei dispositivi medici marcati CE ai sensi dell'MDR), mentre la registrazione nel Sistema Europeo avviene su base volontaria, fino a quando la banca dati europea EUDAMED non sarà pienamente operativa.

- Estensione dei requisiti regolatori a tutta la filiera, con importanti obblighi per gli importatori e per i distributori di dispositivi medici.

Il proposito principale del seguente Regolamento è il miglioramento della sicurezza del paziente, attraverso la definizione di norme relative all'approvazione dei dispositivi medici per uso umano nell'Unione Europea. L'approccio alla sicurezza interessa tutta la vita utile del dispositivo, in tutte le diverse fasi, comprese quelle di distribuzione ed utilizzazione: sono coinvolti pertanto i fabbricanti (perno attorno al quale ruota tutta la normativa) ma anche i mandatari, gli importatori e i distributori, a maggior tutela dall'utilizzatore finale.
Le disposizioni regolamentano gli stati di controllo del device, nelle fasi di pre e di post marcatura, sia con un'estensione della procedura di valutazione della conformità per i prodotti nelle categorie a rischio più elevato (classi IIb e III), sia attraverso il rafforzamento del ruolo svolto dagli Organismi Notificati.
L'MDR stabilisce inoltre nuovi standard, più elevati rispetto a quanto previsto dalle disposizioni precedenti, per garantire la generazione di dati affidabili dalle indagini cliniche: non richiede più solo salute, ma salute e prestazione. La valutazione clinica viene svolta anche attraverso i dati raccolti dal dispositivo ed il follow-up clinico post-vendita può corroborare e perfezionare le previsioni dei benefici clinici nel tempo; gli effetti clinici indiretti, infatti, possono influenzare l'aderenza al trattamento e il benessere dei pazienti e possono emergere in una fase successiva alla commercializzazione. I dati clinici dell'ambito sanitario miglioreranno la comprensione del produttore dei vantaggi del proprio dispositivo, modificando potenzialmente le affermazioni sui benefici clinici previsti nelle successive valutazioni.

Infine, il recente Regolamento Europeo sui Dispositivi Medici impatta fortemente nell'ambito, in questo contesto, di elevato interesse, dei software di area medicale. Grazie a questa regolamentazione, infatti, nella definizione aggiornata di dispositivo medico è compreso il software destinato dal fabbricante ad essere impiegato specificamente con finalità diagnostiche o terapeutiche, necessario al corretto funzionamento del dispositivo stesso.
In altri termini, si identifica quale dispositivo medico qualsiasi prodotto progettato al fine di prevenire, diagnosticare, curare o controllare una malattia/ferita/handicap, il cui meccanismo d'azione è di norma fisico (es.: azione meccanica, conduzione di corrente elettrica, stimolazione, sostituzione, ausilio di organi) e non farmacologico/metabolico/immunologico, anche se nello svolgimento della propria funzione un dispositivo medico può essere coadiuvato con funzione accessoria da sostanze che agiscono con questi ultimi meccanismi

d'azione. Viene chiarito, dunque, tutti i software che hanno finalità di diagnosi e cura e altresì i software che supportano l'operatore sanitario ad assumere una decisione terapeutica oppure assistono, favoriscono o permettono l'erogazione della prestazione stessa devono farsi rientrare nella nozione di dispositivo medico[18].
I software medicali diventano dispositivi medici a tutti gli effetti, con tutti i controlli del caso.

Per conoscenza, si aggiunge che l'MDR disciplina anche:

- dispositivi medici per uso umano e relativi accessori[19];
- dispositivi non immessi sul mercato ma utilizzati nell'ambito di un'attività commerciale per fornire un servizio diagnostico o terapeutico mediante i servizi della società dell'informazione o con altri mezzi di comunicazione[20];
- gruppi di prodotti che non hanno una destinazione d'uso medica[21];

1.2.1.1 Classificazione dei dispositivi medici

La classificazione dei dispositivi medici - fatta esclusione per i dispositivi impiantabili attivi e i dispositivi diagnostici in vitro - dipende dalla loro particolare destinazione d'uso, indicata dal fabbricante ed attribuita consultando le regole di classificazione[22].
La classificazione si basa su profili di sicurezza e complessità e prevede la distinzione dei dispositivi medici in quattro diverse classi, in ordine crescente di rischio comportato dalla loro natura: classe I, IIa, IIb e III.
La complessità ed il profilo di sicurezza dei device (e dunque la loro appartenenza a una classe tra quelle riportate) sono determinati da tre elementi: il livello di invasività, l'eventuale dipendenza da una fonte di energia e la durata del tempo di contatto con il corpo del paziente.

Per quanto riguarda il criterio di invasività:

- I dispositivi non invasivi non penetrano in alcuna parte del corpo, né attraverso un orifizio né attraverso la cute;

[18] Regolamento UE/2017/745, **art. 2**: *Definizioni*
[19] Regolamento UE/2017/745, **art. 1**: *Oggetto e campo di applicazione*
[20] Regolamento UE/2017/745, **art. 6:** *Vendite a distanza*
[21] Questi sono elencati nell'Allegato XVI del MDR e sono, in breve: lenti a contatto; prodotti destinati a essere introdotti totalmente o parzialmente nel corpo umano (esclusi piercing); sostanze, associazioni di sostanze o elementi utilizzati per filling cutanei o per le mucose attraverso iniezione (eccetto quelli per i tatuaggi); apparecchiature per liposuzione, lipolisi o lipoplastica; apparecchiature che emettono radiazioni elettromagnetiche ad alta intensità; attrezzature destinate alla stimolazione cerebrale che applicano correnti elettriche o campi magnetici o elettromagnetici .
[22] Queste sono riportate nell'Allegato IX del D.Lgs. 24 febbraio 1997, n. 46, "Attuazione della direttiva 93/42/CEE concernente i dispositivi medici".

- I dispositivi invasivi sono invece destinati a penetrare anche solo parzialmente nel corpo, tramite un orifizio o una superficie corporea.
  Questi si dividono in:
    - dispositivi invasivi, che penetrano attraverso gli orifizi del corpo;
    - dispositivi invasivi di tipo chirurgico, che penetrano attraverso la superficie corporea sia nel contesto di un intervento chirurgico che al di fuori di esso;
    - dispositivi impiantabili, destinati a essere impiantati totalmente nel corpo umano mediante un intervento chirurgico e a rimanere in tale sede dopo l'intervento (un esempio sono i pacemaker).

È considerato dispositivo impiantabile anche quello introdotto parzialmente nel corpo umano mediante intervento chirurgico e destinato a rimanere in sede dopo l'intervento per un periodo di almeno trenta giorni.

Per quanto riguarda, invece, la durata del tempo di contatto, distinguiamo i dispositivi destinati a:

- utilizzo temporaneo, in questo caso la durata continua prevista è inferiore a 60 minuti;
- utilizzo a breve termine: la durata continua prevista non è superiore a 30 giorni;
- utilizzo a lungo termine: se la durata continua è superiore a 30 giorni.

In base alla potenziale pericolosità, più il dispositivo medico è a contatto con una parte sensibile, più variano le regole necessarie da seguire in fase di progettazione o messa sul mercato.

Infine, l'ultima caratteristica distintiva si basa sulla dipendenza o non dipendenza da una fonte di energia, suddividendo quindi i dispositivi in attivi e non attivi:

- I dispositivi attivi sono quelli il cui funzionamento è legato necessariamente a una fonte di energia - diversa da quella generata dal corpo umano o dalla forza di gravità - e che agiscono convertendo tale energia;
- I dispositivi non attivi sono quelli il cui funzionamento non dipende dal collegamento ad una fonte di energia.

In base a questi tre elementi distintivi, passiamo a descrivere le tipologie di dispositivi che rientrano in ciascuna classe.

- Classe I: dispositivi a rischio medio/basso;

Appartengono alla Classe I le apparecchiature generiche non attive che non penetrano nel corpo o apparecchiature chirurgicamente non-invasive per uso transitorio. I dispositivi che ricadono in questa classe possono essere prodotti per l'aiuto esterno del paziente, come stampelle o sedie a rotelle, ma anche prodotti come stetoscopi; dispositivi di classe I non richiedono, tranne taluni casi, l'intervento di un Organismo Notificato ma devono comunque essere registrati presso le autorità locali di competenza.

Si dividono, a loro volta, in tre sottoclassi:

- Classe I_R: Dispositivi riusabili
- Classe Im: Dispositivi di misura
- Classe Is: Dispositivi sterili

I dispositivi sterili e di misura, pur appartenendo alla Classe I, richiedono l'intervento di un Organismo notificato.

- Classe IIa: dispositivi a rischio medio.

Fanno parte di questa classe alcuni dispositivi non attivi (invasivi e non) e dispositivi attivi che interagiscono con il corpo in maniera non pericolosa. Un esempio sono le lenti a contatto e i tubi endotracheali.

- Classe IIb: dispositivi a rischio medio/alto

Appartengono alla suddetta classe alcuni dispositivi non attivi (solitamente invasivi) e dispositivi attivi che interagiscono con il corpo in maniera pericolosa. Nella Classe IIb possiamo trovare gli stent uretrali e le apparecchiature a raggi X.

- Classe III: dispositivi ad alto rischio, che richiedono un monitoraggio permanente durante tutta la loro vita utile. Come esempio di device appartenenti a questa classe troviamo le protesi al seno, le valvole cardiache prostetiche e le reti chirurgiche.

La distinzione in classi di rischio permette di distinguere le procedure di valutazione della conformità da attuare per ciascuna categoria.

1.2.2 Il Regolamento Generale Europeo sulla Protezione dei Dati

Il Regolamento Generale Europeo sulla Protezione dei Dati - Regolamento (UE) 2016/679, noto anche come GDPR (General Data Protection Regulation) è entrato in attuazione in Italia e nel resto dell'Unione Europea lo scorso 25 maggio 2018, è costituito di 88 pagine e include 99 articoli che spaziano nei più diversi campi di applicazione. Introdotto per adattarsi al

contesto digitale, normativo e tecnologico contemporaneo, supera le leggi in materia di protezione dei dati dei singoli Stati Membri e costituisce una sostituzione del contenuto della precedente Direttiva[23].

Il GDPR si applica a tutte le organizzazioni con sede nell'Unione Europea, siano esse pubbliche o private, che raccolgono, memorizzano o trattano dati personali di residenti nell'UE; ulteriormente, anche le organizzazioni extra-UE che monitorano o offrono beni e servizi a residenti UE in modo continuativo o occasionale dovranno attenersi alle norme previste dal GDPR ed assicurare un livello uguale di protezione dei dati personali.

Possiamo identificare due scopi principali alla sua istituzione:

1. Migliorare la fiducia dei consumatori di tutta l'Unione nelle organizzazioni e/o aziende che custodiscono e trattano i loro dati personali, ponendo una maggiore attenzione ai diritti di riservatezza e sicurezza, al diritto di verifica e al diritto alla cancellazione dei dati;
2. Semplificare il libero flusso di dati personali nell'UE mediante una normativa coerente e solida, comune a tutti gli Stati membri.

Fondamentalmente, il nuovo Regolamento non cambia alcuna delle regole base della precedente Direttiva sulla Protezione dei Dati (DPD), ma ne amplia notevolmente le disposizioni introducendo un insieme di nuovi obblighi a sostegno.

1.2.2.1 Il dato personale nel settore sanitario

Obiettivo del Regolamento Generale Europeo sulla Protezione dei dati non è solo quello di ottenere un consolidamento normativo e una maggiore chiarezza nell'ambito della gestione della privacy, ma ha come scopo principale e fondativo l'estensione del range di protezione dei dati. Questo viene a sua volta ottenuto ampliando la definizione di dato personale.

Il GDPR in questo senso si differenzia dalle norme precedentemente applicate: non viene più attuata la differenziazione tra i due concetti di "dati sensibili" e "dati comuni"; il dato viene considerato in quanto tale, e per questo motivo tutelato.

Il Regolamento stabilisce[24] che per dato personale si fa riferimento ad una "qualsiasi informazione relativa ad una persona fisica identificata o identificabile; una persona fisica identificabile è una persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un identificatore, che può essere un nome, un numero identificativo, dati relativi all'ubicazione, un identificatore online o uno o più fattori specifici

[23] Direttiva sulla protezione dei dati 95/46/CE, nota anche come DPD, e D.Lgs. n. 196/2003 (*Codice in materia di protezione dei dati personali*) agli artt. da 75 a 94

[24] Regolamento UE/2016/679, **art. 4**: *Definizioni*, par.1

dell'aspetto fisico, fisiologico, identità genetica, psichica, economica, culturale o sociale dei quella persona fisica".

All'interno della definizione di dato è stata operata nel Regolamento una differenziazione, che tiene in considerazione l'esistenza di dati particolari, tra cui rientrano tre tipologie di dati personali particolarmente rilevanti nel settore sanitario[25]; questi sono:

1. dati relativi alla salute;
2. dati genetici;
3. dati biometrici.

I *dati relativi alla salute* sono definiti dal GDPR come "dati personali relativi alla salute fisica o mentale di una persona fisica"; in questa definizione viene inclusa la tipologia di prestazione sanitaria ricevuta, la quale consente di dedurre informazioni sullo stato di salute del paziente.

I *dati genetici* sono definiti dal GDPR come "i dati personali relativi a caratteristiche genetiche ereditarie o acquisite di una persona fisica"; questi sono tali se forniscono informazioni uniche sulla fisiologia o sulla salute di tale persona fisica e risultano, in particolare, dall'analisi di un campione biologico della persona fisica in questione.

Per *dati biometrici* si intendono "i dati personali risultanti da specifici trattamenti tecnici relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, che consentono o confermano l'identificazione univoca di tale persona fisica"; questi includono immagini facciali, dati dattiloscopici, tratti dell'andatura etc. perché si possa parlare di dati biometrici, occorre che la verifica dell'identità sia automatizzata, tramite l'ausilio di appositi strumenti hardware o software.

In ragione della loro natura, i dati sanitari sono qualificati dal Regolamento Generale Europeo sulla Protezione dei Dati come dati sensibili e meritevoli, quindi, di una specifica protezione sotto il profilo dei diritti e delle libertà fondamentali. A differenza della Direttiva 95/46/CE di precedente applicazione, il GDPR ricomprende nella definizione dei dati sensibili anche i dati genetici e quelli biometrici, il cui trattamento, come quello dei dati sanitari, può esser soggetto a condizioni e/o limitazioni ulteriori, liberamente mantenute o introdotte dai singoli Stati membri.

Con particolare riferimento a quanto ribadito dalla Corte Suprema di Cassazione[26], ogniqualvolta si faccia riferimento a dati riguardanti la salute e/o il sesso degli interessati, detti dati sono da considerarsi come dati estremamente sensibili, in quanto sono involgenti la

[25] Regolamento UE/2016/679), **art. 4**: *Definizioni*, parr. 13-15

[26] Cass. civ., sez. VI, sent. del 11/01/2016, n. 222; sez. I, sent. del 7 ottobre 2014, n. 21107; sez. I, sent. 1/082013, n. 18443; sent. 8/07/2005, n. 14390.

parte più intima della persona nella sua corporeità e nelle sue convinzioni psicologiche più riservate. Pertanto, essi beneficiano di una protezione rafforzata.

Le organizzazioni sanitarie che si trovano a dover gestire i dati sanitari degli utenti hanno dunque l' onere aggiuntivo di mantenere i dati relativi alla salute, i dati genetici e i dati biometrici ad uno standard di protezione più elevato rispetto ai dati personali, intesi nella loro accezione più generale. Di questo si occupa il Titolare del Trattamento.

1.2.2.2 Il trattamento dei dati sanitari

Il GDPR vieta il trattamento delle forme di dati sanitari precedentemente citate, a meno di alcune condizioni previste[27], che possiamo così riassumere:

1. Per finalità di cura: il trattamento è necessario ai fini della medicina preventiva o del lavoro, per la valutazione della capacità lavorativa del dipendente, per la diagnosi medica, per l'erogazione di cure o per la gestione di sistemi e servizi sanitari o di assistenza sociale; si configura, in breve, nel caso tipico di paziente che si reca volontariamente dal proprio medico o in una Struttura Sanitaria e garantisce l'esecuzione di un contratto di cui l'interessato è parte.

[27] Regolamento UE/2016/679, art.9: *Trattamento di categorie particolari di dati personali*, par. 2: Il divieto di trattamento dei dati personali non si applica quando: "a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1; b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato; c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato; e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali; g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato."

2. Il trattamento è necessario per lo svolgimento di un compito svolto nel pubblico interesse, sulla base della legge nazionale o di leggi dell'Unione Europea – nel settore della Sanità Pubblica o in casi di Emergenza Sanitaria, come la protezione contro gravi minacce per la salute a carattere transfrontaliero o la garanzia di standard elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali o dispositivi medici.
3. Ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Risulta particolarmente notevole l'innovazione introdotta in questo ambito dal Regolamento Generale Europeo sul Trattamento dei Dati, ovvero la base giuridica di legittimità: la giustificazione legale, giuridica, che rende legittimo un determinato trattamento. Il Regolamento UE 2016/679 è più flessibile ed amplia, rispetto alla Direttiva precedente, il novero di ipotesi che legittimano il trattamento dei dati sanitari.
Finché era in vigore il DPD, infatti, il trattamento dei dati sanitari - quindi di tutti i dati che riguardano lo stato di salute, necessari per effettuare l'anamnesi, valutare la storia clinica del paziente e per fornire una diagnosi – poteva effettuarsi esclusivamente previo consenso al trattamento fornito dal paziente. Il consenso deve necessariamente possedere delle caratteristiche specifiche, una delle quali è che deve essere libero: l'interessato, cioè la persona fisica di cui vengono trattati i dati, deve poter dare il proprio consenso senza temere che il non darlo provochi un pregiudizio (nella fattispecie, la non erogazione del servizio sanitario nel caso di mancata autorizzazione al trattamento dei dati sanitari). Appare evidente, dunque, che l'assenza del consenso deve essere controbilanciata dalla presenza di un professionista sanitario, soggetto a segreto professionale, vincolato a degli obblighi di gestione della privacy ben precisi.
Con l'entrata in vigore del GDPR, il consenso costituisce soltanto una delle basi giuridiche possibili; viene trovata una base giuridica diversa: nella maggior parte dei casi questa si configura nel dare esecuzione al contratto di richiesta di cura, assunto come implicito nel momento in cui ci si reca in una struttura sanitaria per ricevere un determinato trattamento o anche solo un parere medico. In questo modo aumenta il numero di condizioni che autorizza al trattamento del dato sanitario.

Di conseguenza, è possibile affermare che tutti i trattamenti che sono essenziali per il raggiungimento di una o più finalità determinate ed esplicitamente connesse alla cura della salute e che sono effettuai da – o sotto la responsabilità di – un professionista sanitario

soggetto a segreto professionale o da altra persona fisica, anch'essa soggetta ad obbligo di segretezza, sono legittimamente svolti.
È invece richiesto espressamente il consenso (libero e informato) dell'interessato per effettuare trattamenti ulteriori, che esulano dalla mera prestazione sanitaria: ad esempio, consultazione online del fascicolo sanitario elettronico, per la consegna dei referti online, per l'utilizzo di applicazioni mediche con finalità di telemedicina, per finalità di marketing o fidelizzazione.

1.3 Obblighi e adempimenti per gli Operatori Sanitari

I soggetti che possono trattare i dati sanitari sono gli esercenti una professione sanitaria – medici, farmacisti, infermieri, etc. – e gli organismi sanitari pubblici più generalmente intesi. All'interno di questi, troviamo alcune figure di spicco introdotte dal Regolamento Generale Europeo e che saranno responsabili, all'interno dell'Azienda Sanitaria, delle modalità di raccolta e gestione dei dati dei pazienti.
Questi soggetti sono vincolati da un segreto professionale e sono dunque legittimati a trattare i dati sanitari, nelle modalità e nei limiti imposti dalla nuova regolamentazione.

1.3.1 Termini e definizioni

Di seguito sono riportati alcuni termini chiave e le relative definizioni fornite dal Regolamento. Sono prese in considerazione, in particolare, espressioni che fanno riferimento alla persona fisica o all'ente che ha un qualche coinvolgimento nella gestione del dato[28]. Questi concetti verranno ripresi spesso nel corso della seguente disamina ed è quindi utile fornire una panoramica descrittiva generale, alla luce del contenuto legislativo associato.

> Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi di trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Il Titolare del trattamento ha la responsabilità, dunque, di stabilire le finalità e le modalità del trattamento dei dati personali. Di seguito, quando si utilizzerà il termine "Titolare del Trattamento", si intenderà l'Azienda Sanitaria, nella figura del Direttore Generale, a cui spetta

[28] Regolamento UE 2016/679, **art. 4**: *Definizioni,* par.2,7,8

la responsabilità decisionale e di gestione dei dati raccolti durante tutte le procedure e i trattamenti effettuati.

Lo stesso Titolare del trattamento, per l'esercizio del suo ruolo, deve attenersi a quanto previsto nel Regolamento Europeo[29]; in breve: i dati personali devono essere trattati in modo lecito, corretto e trasparente; i dati personali devono essere raccolti per finalità determinate, esplicite e legittime e devono essere adeguati e necessari rispetto alle finalità per le quali sono raccolti. Inoltre, i dati personali devono essere accurati, aggiornati e conservati per un periodo non superiore a quello necessario; infine, devono essere trattati in modo da garantire un'adeguata sicurezza.

Il Titolare del trattamento deve inoltre essere in grado di dimostrare la conformità di quanto effettuato alle norme previste dal Regolamento.

L'articolo 35 del GDPR richiede che i titolari del trattamento dei dati effettuino una valutazione d'impatto (DPIA) per il "trattamento ad alto rischio" ed implementino misure per mitigare un rischio. A loro volta, i responsabili del trattamento sono tenuti a informare i titolari del trattamento di qualsiasi violazione dei dati, che deve essere segnalata all'ufficio del Garante per la protezione dei dati (DPC) entro 72 ore ove sussista un rischio per i diritti dell'interessato.

Ad affiancare la figura del Titolare troviamo il Responsabile del trattamento, la cui gestione dei dati personali raccolti in Azienda è svolta per diretta delega del Titolare; solitamente si tratta di un ente o soggetto esterno all'Azienda.

> Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

[29] Regolamento UE 2016/679, **art.5**: *Principi applicabili al trattamento di dati personali: "*1. I dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»); b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»); c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici [..] («limitazione della conservazione»); f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Il Regolamento Generale Europeo sulla Protezione dei Dati ha introdotto una ulteriore figura, il Data Protection Officer (DPO), anche noto con il nome di Responsabile della Protezione dei dati.

> Responsabile della Protezione dei dati (RPD): la persona fisica o giuridica nominata ai sensi dell'art. 37 del Regolamento[30], che svolge la propria attività ai sensi degli articoli 37, 38 e 39 del Regolamento medesimo[31] o di altre disposizioni ivi contenute.

Il DPO è una figura peculiare, interdisciplinare, con conoscenze in campo tecnologico, informatico e legale; è una sorta di organismo di vigilanza che affianca il Titolare per la corretta applicazione delle norme contenute nel GDPR all'interno dell'Azienda, lo supporta nei rapporti con gli Interessati nel caso di problemi nell'elaborazione dei loro dati personali raccolti e fornisce consulenza sulle modalità per garantire la piena conformità al quadro

[30] Regolamento UE 2016/679, **art. 37**, *Designazione del responsabile della protezione dei dati*, par.1:" Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta: a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

[31] Regolamento UE 2016/679, **art. 38**: *Posizione del responsabile della protezione dei dati*; parr. 1-6: "1. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. 2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica. 3. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento. 4 Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento. 5. Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri. 6. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi". Regolamento UE 2016/679, **art. 39**: *Compiti del responsabile della protezione dei dati*; parr. 1,2:"
1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti: a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento [..]; d) cooperare con l'autorità di controllo; e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione. 2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo."

normativo vigente; inoltre, funge da tramite tra il l'Azienda e il Garante della Privacy in caso di necessità.

La nomina del Responsabile della Protezione dei dati – si utilizzerà in questa trattazione sempre l'acronimo DPO - da parte dell'Azienda è obbligatoria nei casi in cui:

- Si operi all'interno di Enti pubblici o Pubbliche Amministrazioni; questi sono tenuti per legge a nominare un DPO;
- Il Titolare del trattamento svolga un monitoraggio sistematico e su larga scala[32] di categorie di dati.
- Il Titolare del trattamento svolga un monitoraggio su larga scala di dati particolari o giudiziari.

Le strutture sanitarie rientrano certamente all'interno degli organismi che richiedono tale figura[33].

Una ulteriore figura a cui far riferimento, da un punto di vista legislativo, per le tematiche trattate, è il Garante Privacy.

> Il Garante per la protezione dei dati personali (Garante Privacy) è l'autorità di controllo nazionale italiana, un'autorità amministrativa indipendente istituita dalla legge sulla privacy[34].

Ogni stato membro dell'Unione Europea ha la sua Autorità di Controllo preposta, la quale ha competenze per la gestione dei reclami o per eventuali violazioni del Regolamento Europeo e delle norme nazionali in materia di protezione dei dati.

Il Garante si occupa di:

- verificare la conformità alla legge dei trattamenti e prescrivere ai Titolari le misure da adottare;
- esaminare i reclami;
- limitare, sospendere o vietare i trattamenti in violazione delle norme;
- adottare le autorizzazioni generali;
- promuovere codici di deontologia e condotta;

[32] *Cons. 91* e *Linee Guida sui Responsabili della Protezione dei dati*: il termine *larga scala* si fa riferimento ad una grande quantità di dati sia di tipo numerico sia come estensione geografica, in rapporto all'area di gestione in cui l'ente si trova ad operare.

[33] Provvedimento n.55 del 7 marzo 2019 del Garante per La protezione dei Dati Personali; ai sensi del Decreto Commissariale di Azienda Zero n. 157/2018 risulta nominato un unico DPO per le Aziende SSR del Veneto.

[34] D.lg. 31 dicembre 1996 n. 675, *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali,* in attuazione della direttiva comunitaria 95/46/CE. Oggi è disciplinata dal Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003 n. 196)

- partecipare alle attività comunitarie e internazionali (anche quale componente dell'EDPB[35]);
- irrogare sanzioni correttive.

Con il nuovo regolamento europeo l'Autorità di controllo interviene principalmente ex post, cioè la sua valutazione si colloca successivamente alle valutazioni del Titolare del trattamento, con abolizione delle notifiche preventive dei trattamenti e sostituzione con obblighi di tenuta di un Registro dei trattamenti e da valutazioni di impatto autonome da parte del titolare del trattamento.

Ulteriori figure previste, tutelate e normate dal GDPR sono l'Interessato ed il Destinatario:

Interessato: la persona fisica identificata o identificabile a cui si riferisce il dato personale oggetto di trattamento.

Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.

1.3.2 Informativa

Il GDPR prevede che, in base alle finalità del trattamento, il Titolare debba fornire agli interessati le informazioni richieste dal nuovo Regolamento Europeo[36]. Ciò avviene tramite l'informativa.

---

[35] European Data Protection Board, o Comitato europeo per la Protezione dei Dati (EDPB) è un organismo europeo indipendente il cui scopo è garantire un'applicazione coerente del Regolamento generale sulla Protezione dei Dati (RGPD) e promuovere la cooperazione tra le autorità di protezione dei dati dell'UE. Dal 25 maggio 2018 sostituisce il Gruppo di lavoro Articolo 29.

[36] Regolamento UE 2016/679, **art.13**:*Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato*; par. 1: "In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni: a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante; b) i dati di contatto del responsabile della protezione dei dati, ove applicabile; c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; d) [..]i legittimi interessi perseguiti dal titolare del trattamento o da terzi; e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale [..]"; in aggiunta a queste troviamo al par.2: " a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; [..] a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; d) il diritto di proporre reclamo a un'autorità di controllo; e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati; f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione [..] nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. Regolamento UE 2016/679, **art.14:** *Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato*, par.1:"Qualora i dati non siano stati ottenuti presso l'interessato, il

L'informativa è un presidio di trasparenza, una comunicazione chiara ed intellegibile rivolta all'interessato che ha lo scopo di informare il cittadino, anche prima che diventi interessato (cioè prima che inizi il trattamento), sulle finalità e le modalità dei trattamenti operati dal Titolare del trattamento. Il fascicolo informativo dovrebbe essere progettato utilizzando un linguaggio semplice di facile comprensione per il pubblico previsto e la categoria di età.
Esso è condizione, non tanto del rispetto del diritto individuale ad essere informato, quanto del dovere del Titolare del trattamento di assicurare la trasparenza e correttezza dei trattamenti fin dalla fase di progettazione dei trattamenti stessi, e di essere in grado di comprovarlo in qualunque momento (principio di *accountability*).

Nell'informativa vanno inseriti:

- L'identità e i dati di contatto, per individuare facilmente il Titolare del trattamento (Azienda Sanitaria o il professionista sanitario), i dati di contatto dei Responsabili del trattamento, adeguatamente nominati, e i dati di contatto del DPO, se nominato.
- La tipologia di dati trattati (dati comuni e dati particolari attinenti al quadro clinico del paziente, già ottenuti o ancora da prelevare) e per quale finalità;
- Le basi giuridiche, ovvero le condizioni di liceità del trattamento del dato; in ambito sanitario si tratterà solitamente di finalità clinico-assistenziali.
- Informazioni sul trasferimento dei dati fuori dall'Unione Europea; si fa riferimento in questo caso al dato elettronico localizzato su strutture cloud con server localizzati fuori dal territorio Europeo: è necessario verificare che i partner esteri con i quali si collabora siano affidabili (ossia che rispondano a standard di mercato elevati, che consentano il trasferimento del dato col rispetto dei canoni previsti dal GDPR).
- I destinatari.

Oltre a questo, una ulteriore importante informazione per l'interessato, facente parte dei suoi diritti, riguarda il periodo di conservazione del dato personale: il dato non può essere conservato per un tempo indefinito, ha una scadenza ben determinata e una volta esaurita la finalità per la quale lo abbiamo raccolto siamo tenuti ad eliminarlo.

---

titolare del trattamento fornisce all'interessato le seguenti informazioni: a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante; b) i dati di contatto del responsabile della protezione dei dati, ove applicabile; c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; d) le categorie di dati personali in questione; e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale [..]".

Devono essere riportati all'interno dell'informativa anche i diritti riconosciuti all'interessato, previsti dal regolamento[37] e l'eventuale esistenza di un processo decisionale automatizzato, soggetto a monitoraggio sistematico o costante dei valori clinici del paziente che portano ad una decisione finale in ambito terapeutico o a livello assistenziale, come il ricovero.

L'informativa, che non richiede la raccolta di un consenso espresso, deve essere messa a disposizione dell'interessato prima della raccolta dei dati di interesse; può essere fornita anche oralmente, dal momento che non necessita di essere sottoscritta. Tuttavia, dato il principio di accountability, per essere certi di aver consegnato o inviato per altri mezzi l'informativa, in modo corretto e conforme alla normativa vigente, è possibile consegnare un modulo cartaceo e farlo firmare per presa visione.

1.3.3 Il Registro dei Trattamenti

Per l'adeguamento dell'Azienda al Regolamento Europeo per la Protezione dei Dati è necessario redigere il Registro dei Trattamenti[38], un documento fondamentale in un'ottica di responsabilizzazione della gestione del dato e del rischio associato, nonché unico strumento idoneo a fornire un quadro aggiornato dei trattamenti svolti in Azienda; di conseguenza, tutti i Titolari del trattamento ed i Responsabili sono tenuti a possederne uno, ed in generale tutti gli Operatori che trattano dati sanitari devono avervi accesso[39]. Delle modalità di redazione di

---

[37] Regolamento UE 2016/679, **art.15,** *Diritto di accesso dell'Interessato;* **art. 16:** *Diritto di Rettifica***; art. 17:** *Diritto alla Cancellazione ("Diritto all'oblio")***; art.18:** *Diritto di Limitazione al Trattamento;* **art. 20:** *Diritto alla portabilità dei Dati;* **art.21:** *Diritto di Opposizione.*

[38] Regolamento UE 2016/679, **art.30:** *Registri delle attività di trattamento*, par. 1: "Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni: a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati; b) le finalità del trattamento; c) una descrizione delle categorie di interessati e delle categorie di dati personali; d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali; e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate; f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati; g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative [..] ; par.5:"Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti [..]

[39] Provvedimento n. 55 del 7 marzo 2019 del il Garante per la protezione dei dati personali, intitolato "*Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*", par. 4: Il Garante ricorda le proprie raccomandazioni sulla tenuta del registro delle attività di trattamento, inteso quale elemento essenziale per il governo dei trattamenti e per l'efficace individuazione di quelli a maggior rischio, non operando per l'ambito sanitario le deroghe previste dal par. 5 dell'art. 30 del GDPR (trattamento che presenta un rischio per i diritti e le libertà per l'interessato, trattamento non occasionale, trattamento che includa categorie particolari di dati di cui all'art. 9 o dati relativi a condanne penali e a reati). Il Garante ritiene dunque che non ricadano nelle ipotesi di esenzione i singoli professionisti sanitari che agiscano in libera professione, ospedali privati, le case di cura, le RSA **e le aziende sanitarie appartenenti al SSN** [..]. Tutti tali soggetti dovranno quindi tenere e mantenere aggiornato il registro dei trattamenti, sia lato titolare, sia lato responsabile ossia nei casi in cui essi agiscano per conto del titolare.

questo Registro si parlerà nei capitoli successivi e sarà tra gli obiettivi principali del seguente lavoro di tesi.

Si tratta, in breve, di una mappa di tutte le attività di trattamento svolte, che descrive in modo chiaro e schematico di come i dati vengono trattati all'interno dell'Azienda Sanitaria, nella totalità delle attività lavorative dell'Azienda stessa.
Il registro può essere tenuto con modalità sia cartacee che telematiche, vige in questo caso la libertà di forma, a discrezione dell'Azienda; tuttavia, deve contenere alcune informazioni essenziali:

- Le generalità del Titolare;
- Le tipologie di dati trattati (anagrafici, sanitari, comuni, etc.);
- Le tipologie di interessati (clienti, fornitori, dipendenti, nel caso di Aziende Sanitarie naturalmente si tratterà di pazienti);
- Le tipologie di trattamento effettuato e le finalità dello stesso;
- Le operazioni di trattamento effettuate (raccolta, registrazione, suddivisione in categorie, modifica, estrazione, consultazione, uso, diffusione o comunicazione a soggetti terzi, cancellazione);
- Eventuali categorie di terzi a cui i dati vengono comunicati;
- La base giuridica utilizzata;
- L'eventuale trasferimento verso paesi terzi e le misure di garanzia adottate;
- Le misure di sicurezza a protezione dei dati;
- Le politiche di conservazione, ovvero le tempistiche previste per la gestione e la successiva eliminazione del dato.

I tempi di conservazione dei dati, se non espressi da direttive precise, vengono decisi dal Titolare in base alle finalità del trattamento e devono essere indicati anche nell'informativa.

Un esempio di quanto appena riportato è visibile in Tabella 1.

Dati di contatto del titolare del trattamento	Finalità di trattamento e basi giuridiche	Categoria interessati	Categoria di dati	Categorie di destinatari	Conservazione	Misure di sicurezza
Ragione sociale, P. IVA, sede legale, indirizzo PEC, dati del legale rappresentante [..]	Trattamento dei dati dei pazienti per l'erogazione delle prestazioni sanitarie	Pazienti	Dati anagrafici, dati sanitari, dati biometrici, dati genetici [..]	Istituto esterno per la fornitura di consulenze specialistiche e di vario genere [..]	In base alla normativa vigente, esistono differenti tempistiche per le diverse tipologie di dati raccolti	Capacità di ripristinare la disponibilità all'accesso dei dati personali in caso di incidenti, malfunzionamenti, blackout [..]

Tabella 2. Rappresentazione concettuale di un modello semplificato di Registro di Trattamenti.

Il Registro potrà successivamente essere ampliato secondo le necessità del Titolare, inserendo ad esempio le Valutazioni di impatto effettuate (DPIA, *Paragrafo 3.2*), i luoghi di conservazione del dato, l'adesione a codici di condotta, l'elenco degli autorizzati alla gestione del dato e via dicendo. Più il Registro sarà dettagliato nelle descrizioni, più sarà conforme ai principi di liceità, correttezza e trasparenza alla base del Regolamento Generale Europeo sulla Protezione dei Dati.

1.4 MDR e GDPR, analisi del connubio tra i due Regolamenti

Il nuovo Regolamento Europeo impatta in maniera importante sull'intero settore degli elettromedicali e dei dispositivi elettrici diagnostici e, per alcuni suoi aspetti, si lega fortemente alla normativa europea sulla protezione dei dati personali, il GDPR. Si analizzano di seguito le due criticità principali riscontrate.

In primo luogo, come già stato analizzato, il Regolamento sui Dispositivi Medici richiede espressamente la riduzione dei rischi, intesi come possibili effetti avversi sviluppabili durante l'impiego di un device. Questa richiesta risulta naturalmente analoga a quanto stabilito dal Regolamento Generale sulla Protezione dei Dati per quanto riguarda l'applicazione di requisiti di accuratezza e robustezza dei sistemi medicali, per garantire una sicurezza dei dati trattati costante nel tempo. In questo modo, dalla combinazione delle due Normative, si rende necessaria la progettazione di un parco macchine tale da garantire riproducibilità, affidabilità e prestazioni in linea con la destinazione d'uso.

In questo contesto, per quanto riguarda la sicurezza tecnica, che passa anche dalla protezione del dato sanitario e quindi dall'analisi dei rischi derivanti da problemi legati alla gestione del dato stesso, si devono includere strategie per l'analisi del rischio che sono applicabili a

entrambi i Regolamenti. Le tipologie di analisi a cui si fa riferimento, analizzate nella pratica nel Capitolo 2, non si devono fermare solamente al dato direttamente immesso nel sistema né unicamente al dato di output, ma anche a tutti i dati accessori che possono essere ottenuti dall'utilizzo dei dispositivi, come ad esempio gli accessi e il numero di interazioni; è proprio in questo punto che si manifesta una criticità non irrilevante.

In seguito a diversi confronti con i tecnici dei dipartimenti di Radiologia ed Emodinamica dell'Ospedale in cui è stato svolto il tirocinio, è emerso che anche ditte esterne, in special modo le ditte che hanno in carico la gestione di elettromedicali collegati con consolle per il monitoraggio e la raccolta dati, hanno la possibilità di accedere, con piena autorizzazione e visuale completa, ai dati che i sistemi elaborano. Il motivo di tale autorizzazione è da individuarsi nella necessità, in caso di guasti o semplicemente di malfunzionamenti transitori di sistema, di poter avere a disposizione dei tecnici informatici che non solo effettuino le dovute riparazioni ma anche che possano accedere e recuperare, per conto dell'operatore sanitario, i dati necessari al completamento della procedura clinica. L'MDR richiede il monitoraggio di qualità e funzionalità costante di qualunque dispositivo durante tutto il corso della sua vita utile, ma per ottenere tutto ciò si rende necessario, per taluni dispositivi - ma sono sempre di più i device collegati ad una postazione telematica di lavoro - la possibilità di accesso a tali postazioni a tecnici nelle cui competenze non rientra però la gestione dei dati sanitari. Sappiamo inoltre che, allargando la cerchia del personale autorizzato alla visione del dato, la tutela dello stesso diviene più critica, entrando di fatto in conflitto con quanto richiesto dal GDPR, ovvero che siano ben identificate e opportunamente ridotte le persone fisiche che possono accedere ai dati sensibili.

Il secondo punto di conflitto tra MDR e GDPR riguarda la Valutazione Clinica che i fabbricanti di dispositivi medici sono tenuti a redigere per dimostrare che i device che vengono messi in circolazione rispettano i requisiti essenziali di sicurezza e prestazione richiesti dal Regolamento; tale dimostrazione deve essere redatta basandosi su *dati clinici*[40], ovvero tutte quelle informazioni acquisite dopo l'immissione in commercio del dispositivo medico già marcato CE.

[40] L'art. 2 lett. 48 dell'MDR stabilisce che per **dati clinici** si intendono le "informazioni sulla sicurezza o sulle prestazioni ricavate dall'impiego di un dispositivo e che provengono: a) dalle indagini cliniche relative al dispositivo in questione; b) dalle indagini cliniche o da altri studi pubblicati nella letteratura scientifica relativi a un dispositivo di cui è dimostrabile l'equivalenza al dispositivo in questione; c) da relazioni pubblicate nella letteratura scientifica sottoposta a valutazione inter pares su altre esperienze cliniche relative al dispositivo in questione o a un dispositivo di cui è dimostrabile l'equivalenza al dispositivo in questione; d) da informazioni clinicamente rilevanti risultanti dalla sorveglianza post-commercializzazione, in particolare il follow-up clinico post-commercializzazione."
Si evidenzia che al punto a) sulle "indagini cliniche" e al punto d) sulle "informazioni clinicamente rilevanti" si rientra nel campo dei dati relativi alla salute da trattarsi ai sensi del GDPR.

La definizione di dato clinico secondo l'MDR non coincide esattamente con il "dato personale" o "dato relativo alla salute" riportato all'interno del GDPR, tuttavia all'interno della più ampia nozione di dato clinico possono essere comprese diverse tipologie di trattamento di dati personali o relativi alla salute.
La sorveglianza post commercializzazione è uno strumento introdotto dall'MDR per valutare le performance tecniche e cliniche del dispositivo medico, raccogliendo principalmente dati sui rischi effettivi, con l'obiettivo di valutare e/o confermare il beneficio clinico, punto fondamentale della definizione di un dispositivo che garantisca piena funzionalità e vantaggi per il paziente. Sono queste attività che comportano l'implementazione, da parte del fabbricante, di processi che, oltre a essere analizzati ai fini di una corretta valutazione clinica, dovranno anche essere esaminati sotto il profilo del corretto trattamento di dati personali che coinvolgono la valutazione stessa. Ne deriva che il fabbricante dovrà esaminare tutti gli aspetti di trattamento dei dati di tali processi, valutando inoltre a corredo tutti i profili di privacy by design e by default richiesti dal GDPR.
In breve, i fabbricanti hanno la necessità di poter esaminare i dati clinici raccolti dai dispositivi che hanno prodotto, per poter ottenere un Certificato CE conforme a quanto richiesto dall'MDR, e allo stesso tempo necessitano di poter implementare in maniera corretta i nuovi processi di raccolta dati per rafforzare i fascicoli tecnici dei prodotti senza venir meno ai principi fondamentali di tutela della privacy previsti dal GDPR.

Emerge dunque un quadro operativo molto complesso, e solo nel recente periodo tutte le disposizioni riportate nel presente Capitolo sono state prese seriamente in esame da tutte le Aziende coinvolte, che si trovano a dover gestire diversi ambiti di indagini e di intervento; tuttavia, i due Regolamenti sono fondamentali per l'introduzione di una procedura comune a tutti i Paesi dell'Unione Europea ed istituiscono degli adeguamenti tecnici e normativi indispensabili per il corretto allineamento delle tecnologie di nuova generazione dei presìdi già esistenti, in un'ottica di continua innovazione e tutele sempre crescenti, in linea con la trasformazione tecnologica nella quale siamo tutti coinvolti.

Capitolo 2.
Progettazione e valutazione dei rischi per i sistemi medicali

2.1 Privacy by Design e Privacy by Default

Gli ambienti sanitari sono sempre più oggetto di una trasformazione digitale che riguarda tutto il percorso di cura del paziente, dalla diagnosi alla terapia. Diventa quindi vitale l'utilizzo di adeguate misure di sicurezza che tengano conto di tutti gli aspetti inerenti all'intero ciclo di vita del dato trattato, partendo dalla raccolta, passando per conservazione e gestione, fino ad arrivare alla sua eliminazione.

Tra le novità più importanti introdotte dal Regolamento Generale Europeo sulla Protezione dei Dati si affermano i due principi fondamentali di Privacy by Design e Privacy by Default. Quando parliamo di trattamento dei dati personali, il Titolare deve adottare tutte le misure di sicurezza necessarie per gestire i suddetti in maniera corretta per tutta la durata del trattamento.

L'espressione *misure di sicurezza* è da intendersi come l'insieme delle prescrizioni di carattere tecnologico, procedurale ed organizzativo finalizzate all'implementazione di un adeguato livello di sicurezza nel trattamento dei dati, al fine di garantirne la riservatezza, l'integrità e la disponibilità, nonché la resilienza dei sistemi informativi (analogici e digitali) utilizzati per la gestione dei dati stessi.

Tali misure tecnico-organizzative sono volte a ridurre al minimo i rischi di:

- distruzione o perdita, anche accidentale, dei dati;
- accesso ai dati da parte di personale non autorizzato;
- trattamento non consentito o non conforme alle finalità della raccolta;
- modifica dei dati in conseguenza di interventi non autorizzati o non conformi alle regole.

Un'importante considerazione preventiva da fare è la seguente: l'attività di valutazione e gestione del rischio associato al trattamento non potrà mai comportare, in alcun modo, la completa eliminazione del rischio stesso, ma esclusivamente una sua minimizzazione, tale per cui le criticità possano essere considerate accettabili rispetto ai benefici ottenuti dall'interessato grazie al trattamento.

Di seguito si riportano le due diverse definizioni[41]:

> Privacy by Design (o privacy fin dalla progettazione): prevede l'integrazione delle attività volte alla protezione dei dati personali in tutte le fasi del ciclo di vita dei sistemi e delle applicazioni di Information Technology (IT), dalla fase di progettazione, messa in esercizio, utilizzo e dismissione finale; l'intera gestione del trattamento deve dunque essere costruita per rispettare i diritti e le libertà fondamentali degli interessati.
>
> Privacy by Default (o privacy dei dati per impostazione predefinita): prevede, nelle imposizioni dei servizi e dei prodotti che trattano dati personali, il rispetto dei principi generali della protezione delle informazioni, quindi la minimizzazione dei dati (in termini sia di quantità e che di tempi di utilizzo) e la limitazione delle finalità.

Risulta dunque di particolare interesse, anche per l'ambito di trattazione del seguente elaborato, la comprensione di come il GDPR condiziona le modalità di verifica, configurazione, modifica, sviluppo e progettazione di software di dispositivi elettromedicali di diagnosi e cura.

2.1.1 Considerazioni del Regolamento UE (2016/679)

Come già riportato nel precedente Paragrafo, per soddisfare il principio di privacy by default, una opportuna azione da intraprendere consiste nella minimizzazione del dato accessibile: si tratterà dunque di ridurre al minimo il numero di dati, forniti al e gestiti dal programma, per ogni operazione. Sarà necessario comprovare che i dati personali raccolti sono sufficienti, pertinenti e non eccessivi e che non rivelino, direttamente o indirettamente, informazioni sensibili, quali origine etnica, opinioni politiche, filosofiche o religiose, l'appartenenza sindacale, le informazioni sulla salute o sulla vita sessuale di un individuo, ad enti, organizzazioni o soggetti terzi non autorizzati.

Questa accortezza, seppur apparentemente molto semplice, è alla base della gestione in sicurezza del dato personale; basti pensare che minore è la quantità di informazioni disponibili ed in circolazione tra diversi sistemi operativi, minore sarà anche la probabilità che i dati possano andare perduti o essere trafugati.

[41] Regolamento UE/2016/679, **art. 25**: *Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita*

Anche la diminuzione del tempo di permanenza dei dati in memoria fa capo al principio di minimizzazione, tuttavia in questo caso si esplica un'ulteriore necessità progettuale: sarà infatti necessario implementare, in fase di realizzazione, delle strategie di eliminazione dei dati al termine della loro vita utile, quando dunque non saranno più necessari ai fini del trattamento. In particolare, sarà necessario associare una scadenza ai diversi dati trattati, di modo che il software avvisi quando è possibile procedere alla loro eliminazione.
La riduzione del periodo di conservazione[42] dei dati personali comporta una riduzione dell'impatto dei rischi: minore è il tempo di sosta del dato all'interno della memoria del software, minore sarà anche in questo caso il rischio di diffusione di informazioni di carattere personale.

2.1.2 Data Protection Impact Assessment

Il GDPR è un regolamento che non fornisce indicazioni pratiche riguardanti gli aspetti tecnici o metodologici alla base della fabbricazione o della modifica dei software che conservano ed elaborano i dati personali; dal Regolamento sono però deducibili delle linee guida teoriche, che approfondiscono le caratteristiche che deve possedere il programma per essere ritenuto conforme alla normativa vigente.
La valutazione di impatto della protezione dei dati (Data Protection Impact Assessment, DPIA) è un processo già previsto all'interno del GDPR[43] e indica tutte le attività coordinate per gestire un'organizzazione con riferimento ai rischi. Ne include pertanto l'identificazione, la valutazione, il trattamento e il suo monitoraggio e miglioramento.
La gestione del rischio clinico in Sanità ha per suo campo specifico il paziente e i rischi nei quali esso incorre quando sottoposto a pratiche di tipo clinico-assistenziale all'interno delle strutture sanitarie; rappresenta l'insieme delle azioni messe in campo per migliorare la qualità delle prestazioni sanitarie e garantire la sicurezza dei pazienti.

In generale, è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati quando il tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche derivanti dall'utilizzo di dati personali, in ragione, ad esempio, della natura del trattamento, del contesto in cui ci si trova ad operare ed anche della particolare tecnologia

[42] Regolamento UE/2016/679, **cons. 39**: "[..] I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. È opportuno adottare tutte le misure ragionevoli affinché i dati personali inesatti siano rettificati o cancellati. I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento."
[43] Regolamento UE/2016/679, a**rtt. 24 e 35**

utilizzata, nella probabilità più o meno evidente che i dati in gestione possano essere cancellati, intercettati, manomessi o modificati.

Secondo il Regolamento, la DPIA è richiesta nei tre casi seguenti[44]:

- Valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- Trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati;
- Sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

È possibile sia svolgere una valutazione specifica per ogni trattamento, sia scegliere di raggruppare trattamenti tra loro similari e con analoghi rischi ed esaminarli assieme tramite un'unica procedura.

A completezza di quanto già riportato si evidenzia che, a norma di legge[45], all'interno di ogni struttura sanitaria sia pubblica che privata devono essere istituite delle funzioni di gestione del rischio clinico; ulteriormente, per ogni Regione deve essere creato il Centro Regionale per la Gestione del Rischio Clinico. Questo perché è determinante che sia attuato un coordinamento di queste funzioni e che vengano attivati dei percorsi con formulazione di metodologie della gestione del rischio finalizzate allo studio di tutti i processi interni nelle possibili criticità più frequenti.
Gli enti citati si occupano di qualunque tipologia di rischio associato all'ambiente ospedaliero e purtroppo, nel recente passato, è stato spesso tralasciata l'importanza di una accorta gestione del rischio relativo alla gestione dei dati, a favore invece di indagini in ambiti diversi

[44] Regolamento UE/2016/679, **art. 35**, *Valutazione d'impatto sulla protezione dei dati*; par. 1:"Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi."; par.4:" L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68."; Provvedimento n. 9058979 del Garante per la Privacy dell'11 ottobre 2018: *Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679*

[45] La legge dell'8 marzo 2017, n. 24 *Disposizioni in materia di sicurezza delle cure e della persona assistita, nonché in materia di responsabilità professionale degli esercenti le professioni sanitarie* riporta al comma 539 che per la realizzazione di attività di prevenzione e gestione del rischio è richiesta "l'attivazione dei percorsi di audit o altre metodologie finalizzati allo studio dei processi interni e delle criticità più frequenti, con segnalazione anonima del quasi-errore e analisi delle possibili attività finalizzate alla messa in sicurezza dei percorsi sanitari."

(anch'esse essenziali), quali ad esempio la diminuzione del rischio alla salute del paziente nelle prestazioni sanitarie, rischi relativi a modalità di contagio, alla tutela degli operatori etc. Tutte queste attenzioni, che giustamente ricoprono ed hanno sempre ricoperto enorme importanza, non devono però lasciar passare l'idea che quella della gestione dei dati non sia un problema, oltre che fortemente attuale, anche altamente rischioso sia per la struttura sanitaria che per i soggetti sottoposti a trattamento, che affidano una quantità rilevante di dati personali particolari all'Azienda Sanitaria e confidano che questi siano tutelati a dovere.

2.1.3 Requisiti

Una guida metodologica per lo svolgimento del Risk Assessment è stata fornita dal gruppo dei Garanti Privacy UE WP29[46] attraverso un primo provvedimento, WP248 rev.01: *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely result in high risk" for the purposes of Regulation 2016/679*.

Fondamento di questo provvedimento è che, vista la particolare utilità e rilevanza che può avere una valutazione del rischio associato al trattamento di dati sensibili, si suggerisce la necessità di formulare un'analisi preventiva dei rischi per qualunque tipologia di trattamento, non solo nei casi (già elencati) in cui questa è richiesta formalmente.

Questo procedimento è in carico al Titolare del trattamento, con eventuale supporto del Responsabile e in stretta collaborazione con il DPO[47], che deve sempre essere coinvolto nelle valutazioni dei rischi associati; la decisione sull'entità delle criticità deve essere presa prima che il trattamento sia posto in essere, con particolare attenzione alle linee guida presenti nel GDPR.

Al netto di queste considerazioni, va sottolineato che il DPIA deve essere, nel suo complesso, considerato come un processo valutativo ungoing: non si configurerà dunque in una unica valutazione del rischio svolto in una fase di pre-processing, una volta individuata una criticità all'interno delle modalità di trattamento, ma al contrario si tratterà di un'attività ripetuta, in cui un determinato programma o dispositivo potrà essere sottoponibile a riesame nella misura in cui determinate circostanze interne o esterne al progetto possano portare alla necessità di rivalutare anche solo una parte del processo.

[46] Article 29 Working Party o Gruppo di Lavoro Articolo 29 per la protezione dei dati; è il gruppo di lavoro comune delle autorità nazionali di vigilanza e protezione dei dati. Dal 25 maggio 2018 è stato sostituito dal Comitato Europeo per la Protezione dei Dati (EDPB), che ne mantiene i propositi.

[47] Regolamento UE/2016/679, **art. 35**: *Valutazione d'impatto sulla protezione dei dati*; par. 2: "Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno."

Nonostante non siano state stipulate, all'interno del Regolamento Generale Europeo sulla Protezione dei Dati, linee guida concrete sull'adeguamento dei dispositivi elettromedicali, sono comunque presenti dei requisiti minimi obbligatori perché sia verificabile la conformità della valutazione dei rischi a quanto previsto dal GDPR stesso. La valutazione deve possedere almeno quattro contenuti fondamentali[48]:

1. Una descrizione del trattamento, delle sue finalità e del legittimo interesse alla base del trattamento stesso;
2. Una valutazione rispetto alla necessità del trattamento e alla sua proporzionalità rispetto alle finalità previste;
3. Una valutazione del rischio rilevato per i diritti e le libertà degli individui;
4. Una descrizione delle misure e degli accorgimenti che il Titolare ritiene opportuno adottare al fine di mitigare il rischio riscontrato.

Per procedere alla stesura della DPIA diverse sono le modalità possibili; una di queste consiste nell'estendere il già presente Registro dei Trattamenti, collocando l'analisi dei rischi e le valutazioni di impatto fra le caratteristiche dei trattamenti di cui occorre tener conto per mettere in atto tutte le misure tecniche e organizzative adeguate. In questo modo è possibile ottenere in un unico documento una valutazione generale su ciò che comportano i singoli processi o gruppi di processi tra loro similari.

È possibile osservare che il provvedimento WP248 rev.01 rappresenta una linea coerente con l'intero contesto di collocazione del Regolamento Generale Europeo e ribadisce a sua volta la centralità del Titolare del Trattamento per quanto riguarda la valutazione dei rischi associati ai trattamenti in essere nell'Azienda a cui afferisce.
Riemerge il principio dell'accountability, ovvero della responsabilizzazione, già introdotto in questa trattazione e alla base del GDPR, e che si concretizza in questo ambito nella necessità, da parte del Titolare del trattamento, di utilizzare la procedura di DPIA per valutare e poi dimostrare la conformità delle modalità di gestione dei dati alla normativa vigente.
Si prevede inoltre un ruolo molto rilevante delle Autorità di controllo. Esse, infatti possono redigere e rendere pubblico un elenco delle tipologie di trattamenti per i quali è richiesta la

[48] Regolamento UE/2016/679, **art. 35**: *Valutazione d'impatto sulla protezione dei dati*, par. 7: "La valutazione contiene almeno: a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, 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 di cui al paragrafo 1; e 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 presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione."

valutazione di impatto; così come possono, se lo ritengono opportuno, redigere un elenco delle tipologie di trattamenti per i quali essa non è necessaria. In entrambi i casi gli elenchi eventualmente adottati devono essere comunicati al Comitato europeo dei garanti[49] (EDPB). Si stabilisce inoltre la consultazione preventiva obbligatoria[50] dell'Autorità di controllo quando il Titolare ritiene che i trattamenti richiedano misure specifiche per attenuarne i rischi. La valutazione è preventiva al trattamento dei dati e deve essere prevista una procedura di aggiornamento periodico per tenere conto delle eventuali variazioni nelle modalità di trattamento o nelle tecnologie impiegate.

2.2 Misure tecniche e organizzative per la protezione del dato

Per questo aspetto della progettazione si prenderanno in considerazione documenti di diversa entità, che esaminano nella pratica le modalità di realizzazione di nuovi programmi e di valutazione e correzione di quelli attualmente in uso, per far fronte alle richieste del Regolamento Europeo in merito alla gestione del dato sanitario. In particolar modo, si farà riferimento ai seguenti documenti:

- *Linee Guida per la modellazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del Secure/Privacy by Design*, documento rilasciato il 7 maggio 2020 da AgID (Agenzia per l'Italia Digitale), organo della Presidenza del Consiglio dei Ministri;
- *Regolamento (UE) 2019/881 sulla certificazione della cybersicurezza nelle tecnologie dell'informazione e della comunicazione (Cyber act)*, rilasciato dall'ENISA (Agenzia Europea per la Sicurezza Informatica) il 17 aprile 2019.

Va ricordato che le linee guida, fondamentali per una buona pratica di progettazione, ai fini della conformità con le norme contenute nel Regolamento Generale Europeo sulla Protezione

[49] Regolamento UE/2016/679, **art. 65**: *Composizione delle controversie da parte del comitato*, par. 1: "Al fine di assicurare l'applicazione corretta e coerente del presente regolamento nei singoli casi, il comitato adotta una decisione vincolante nei seguenti casi: a) se[..] un'autorità di controllo interessata ha sollevato un'obiezione pertinente e motivata a un progetto di decisione dell'autorità di controllo capofila e l'autorità capofila di controllo non abbia dato seguito all'obiezione o abbia rigettato tale obiezione in quanto non pertinente o non motivata; b) se vi sono opinioni contrastanti in merito alla competenza delle autorità di controllo interessate per lo stabilimento principale; c) se un'autorità di controllo competente non richiede il parere del comitato [..]

[50] Regolamento UE/2016/679, **art. 36:** *Consultazione preventiva,* par 1: "Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio."; par 3:" Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo: a) ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale; b) le finalità e i mezzi del trattamento previsto; c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento; d) ove applicabile, i dati di contatto del responsabile della protezione dei dati; e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35; e f) ogni altra informazione richiesta dall'autorità di controllo."

dei Dati, vanno però sempre applicate dopo che è stata svolta una valutazione dei rischi, preliminare a qualsiasi trattamento.

2.2.1 Scenari per l'identificazione e l'analisi del rischio

Nel lavoro di progettazione, la considerazione degli scenari d'uso è il punto di partenza per la mappatura della tecnologia: questi permettono di comprendere le modalità di impiego del programma e/o dell'applicazione, consentono di identificare i flussi di dati e le attività legate a creazione, aggiornamento, lettura e cancellazione dei dati. Mediante un'analisi più approfondita, inoltre, sarà possibile individuare le falle nel sistema, e quindi in che modo lo stesso programma potrebbe essere utilizzato in modo improprio.

Esistono diverse tipologie di eventi avversi che possono manifestarsi nel corso di un processo di trattamento dei dati. Con particolare riferimento alla valutazione di probabilità di accadimento di una minaccia e al livello di gravità (impatto) che un dato evento può determinare sui diritti e le libertà degli interessati, l'ENISA definisce i tre concetti di: minaccia, vulnerabilità e rischio.

> Minaccia: una qualsiasi circostanza o evento che potenzialmente può determinare un impatto negativo (un male o un danno) ad una cosa o persona.

Le minacce tendono ad essere specifiche relativamente a determinati ambienti. La scelta del tipo di minaccia da prendere in considerazione al loro potenziale di rischio dovrà ricadere, ovviamente, su quelle che si presentano caratterizzanti[51] per l'organizzazione in relazione ai tipi di trattamento svolto e al contesto in cui detti trattamenti si svolgono.

> Vulnerabilità: modalità d'uso di un oggetto che potrebbe essere sfruttata da una minaccia esistente per creare effetti negativi.

> Rischio: possibilità misurabile (probabilità) che un processo sviluppi un evento avverso inatteso durante il suo svolgimento; perché si presenti l'eventualità di un rischio è necessario avere sia un fattore di minaccia che un fattore di vulnerabilità.

[51] Le tipologie di rischi associati ai diversi ambienti operativi sono disponibili sui seguenti documenti: *Normativa ISO/IEC 29134:2018* e *Report Enisa Threat Landscape, Report 2018 – 15 Top Cyberthreats and Trends (ETL2018)*

2.2.2 Progettazione dell'architettura

In primo luogo, per procedere con le analisi di sicurezza e vulnerabilità dei software si opterà per una suddivisione del programma nelle sue componenti fondamentali, considerandone dunque l'architettura:

- Topologia di rete dei componenti, ossia dove si cala l'applicazione (Intranet, Extranet, Internet);
- Livelli logici, nel caso di architetture multilivello (Business logic layer, Data Access layer, interfaccia utente);
- Componenti chiave, i componenti più importanti all'interno di ogni livello logico;
- Processi chiave (i servizi principali che l'applicazione implementa)
- Porte di rete e protocolli di comunicazione per i flussi di dati tra i componenti;
- Identità e profili utente rilevanti utilizzati all'interno dell'applicazione;
- Dipendenze (applicazioni ulteriori) rivolte verso sistemi esterni;

Questi elementi possono essere identificati come i componenti principali di un'apparecchiatura; considerarne le criticità è il primo passo per una buona pratica di progettazione.

2.2.3 Identificazione dei ruoli e delle tecnologie

È importante identificare i ruoli all'interno dell'applicazione - ovvero chi la sta utilizzando; questi servono per determinare in maniera esplicita ed univoca come dovrebbero essere utilizzate le risorse, tra le quali figurano anche i dati personali. Da queste informazioni si arriva a conoscere, per deduzione, anche le modalità errate o non consentite di gestione.
L'assegnazione dei ruoli deve essere centralizzata, con la presenza un profilo autorizzativo all'interno dell'Azienda che assegni i ruoli, regolamenti i comandi, le transazioni e gli accessi ai dati.

Si rende necessario fare un richiamo ai principi di privacy per impostazione predefinita (la già menzionata *privacy by default*): per ridurre la superficie di attacco è necessario stabilire quali devono essere i privilegi minimi per ogni componente dell'applicazione, ovvero l'assegnazione, l'accesso alla risorsa in utilizzo, deve essere limitata il più possibile, nel migliore dei casi ridotta al minimo indispensabile. Inoltre, è importante riconoscere tutte le tecnologie utilizzate e le loro caratteristiche. L'identificazione delle tecnologie fornisce allo sviluppatore un maggiore controllo sulle minacce che possono emergere, legate alle specifiche tecnologie in uso, ed aiuta a determinare le eventuali tecniche di mitigazione del

rischio. Le singole tecnologie hanno ciascuna le proprie vulnerabilità e i propri vantaggi; andranno considerati nel loro complesso: sistemi operativi, web server, server di database, le tecnologie utilizzate per implementare la presentazione dei dati a livello utente e nel business layer (ossia gestione delle regole applicative, le tecnologie alla base dell'accesso ai dati raccolti ed infine il linguaggio di sviluppo utilizzato).

Le vulnerabilità specifiche delle diverse tecnologie, e le conseguenti azioni mitigatrici da mettere in atto per ogni singola tecnologia, possono essere definite anche mediante l'utilizzo della letteratura associata.

2.2.4 Meccanismi applicativi di sicurezza

Qualunque sia l'applicazione in fase di ideazione e/o valutazione, una buona pratica di progettazione consiste nell'identificare i meccanismi di sicurezza applicativa: nella pratica, il programma viene diviso in dieci domini di riferimento, per ciascuno dei quali saranno identificate le minacce e le vulnerabilità riscontrate.

1. Autenticazione, conferma dell'identità di un utente collegato ad un sistema;
2. Autorizzazione, definizione dei privilegi, ruoli e permessi di un utente per l'accesso ad un sistema;
3. Modalità di validazione input e dati inseriti dall'utilizzatore esterno per le elaborazioni del sistema;
4. Gestione della configurazione dell'applicazione e dei suoi componenti associati;
5. Dati sensibili (se presenti), quali etnia, religione, opinioni filosofiche, politiche, sindacali, condizioni di salute, orientamento e vita sessuale dell'interessato;
6. Gestione della sessione;
7. Crittografia;
8. Manipolazione dei parametri che vengono trasmessi fra i componenti delle applicazioni perché questi collaborino tra loro;
9. Gestione delle eccezioni;
10. Audit[52] e gestione dei log: si tratta di verifiche di conformità, permettono di tenere traccia di eventi importanti avvenuti nel corso delle sessioni di lavoro, assieme ad autori, data e ora.

[52] Per audit clinico si intende un processo in cui "medici, infermieri e altri professionisti sanitari, effettuano una revisione regolare e sistematica della propria pratica clinica e, dove necessario, la modificano" (*Primary Health Care Clinical Audit Working Group*, 1995). È dunque una valutazione del processo e del livello assistenziale che riguarda i trattamenti clinici in essere all'interno dell'Azienda, solitamente da un punto di vista più medico che tecnologico. Per questo motivo l'inserimento, nel team di analisi, anche di figure esperte nell'ambito della gestione degli elettromedicali, quali ovviamente l'Ingegnere Clino e l'Ingegnere Biomedico, consentiranno una migliore valutazione dei processi che involvono i pazienti ed una pratica di gestione del rischio a tutto tondo.

Per ciascuno di questi ambiti è possibile riscontrare delle particolari vulnerabilità associate, di seguito elencate:

1. Furto di identità, accesso non autorizzato all'archivio delle cartelle cliniche con possibile reimpostazione o modifica delle stesse, o diffusione nel Dark Web;
2. Influenza sui controlli di autorizzazione per accedere ad operazioni privilegiate o per elevare i privilegi;
3. Invio di comandi non autorizzati o input non validi per influenzare la logica di protezione adottata dal server o per bloccare l'applicazione;
4. Accesso a funzioni di amministratore o a dati di configurazione dell'applicazione;
5. Visualizzazione, manipolazione e diffusione di dati sensibili contenuti in un database non crittografato o con chiave di traduzione accessibile (Data Breach), con lo scopo di diffusione su piattaforme illegali o di furto di dati provenienti da attività di ricerca innovative;
6. Controllo della sessione mentre altri utenti sono collegati;
7. Algoritmi di crittografia facilmente bypassabili;
8. Manipolazione dei parametri e dei dati sensibili presenti negli stessi;
9. Accesso a funzioni non concesse nel momento di blocco dell'applicazione;
10. Manipolazione dei dati raccolti con lo scopo di nascondere azioni illecite.

2.2.5 Anonimizzazione e Pseudonimizzazione del dato

Una volta che i dati sono stati inseriti all'interno del software di elaborazione prescelto, è possibile implementare diverse strategie per garantire una maggiore sicurezza, in particolar modo nascondendo ad enti non autorizzati i dati trattati. Tra le strategie di occultamento possiamo trovare:

- Pseudonimizzazione[53] o partizione del dato, ovvero separare i nominativi personali di riferimento dai dati ai quali sono associati; questi ultimi verranno gestiti utilizzando un riferimento a degli pseudonimi che non saranno direttamente

[53] Regolamento UE/2016/679, **cons.26:** È auspicabile applicare i principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile. I dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile. Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato.

collegati al nominativo di partenza. Questo è possibile, ad esempio, attraverso la gestione separata di dati e nomi in database diversi.

- Cifratura[54]: attraverso la crittografia si sceglie di rendere incomprensibili determinate informazioni a chiunque acceda senza autorizzazione. Si parla di crittografia in diversi contesti; è possibile crittografare il contenuto dei dischi rigidi, determinati file particolarmente sensibili, l'intera raccolta di dati o anche gli stessi canali di comunicazione. Sarà necessario scegliere il tipo di crittografia da implementare e la conseguente chiave di decodifica, adottando sistemi crittografici riconosciuti e verificati.

Va ricordato che, all'occorrenza e su richiesta del soggetto interessato proprietario dei dati elaborati, questi dovranno essere resi disponibili integralmente in modo chiaro e comprensibile.

- Anonimizzazione[55], procedimento attuato nel caso in cui non sia di interesse, per lo scopo di elaborazione, ricondurre i dati trattati a persone fisiche (è il caso, ad esempio, dei dati impiegati in un contesto di ricerca); in questo particolare caso non si lede alla libertà dei singoli individui, non è possibile risalire ai proprietari dei dati trattati nemmeno tramite deduzione.

2.3 Il Sistema Integrato delle apparecchiature elettromedicali

Nel corso del precedente Capitolo si è già discusso di cosa costituisce o meno un dispositivo medico, tenendo in considerazione che il Regolamento Europeo sui Dispositivi Medici ha ampliato notevolmente la definizione originale, chiarendo – e questo è particolarmente rilevante ai fini della trattazione – che anche i software destinati all'uso in un contesto biomedicale devono essere considerati dispositivi medici (Figura 4). Riassumendo quanto riportato nelle linee guida MEDDEV, un software può avere scopo medico quando:

i. Controlla direttamente un dispositivo medico;
ii. Fornisce informazioni decisionali mediche immediate;
iii. Fornisce supporto agli operatori sanitari.

[54] Regolamento UE/2016/679, **art. 32:** *Sicurezza del trattamento*, par.1:" Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; [..] d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

[55] La definizione di "Anonimizzazione" maggiormente completa è quella resa dallo standard in materia di Health Informatics ISO/TS 25237:20: "*L'anonimizzazione è un processo mediante il quale i dati personali vengono modificati in modo irreversibile così che il titolare del trattamento, da solo o in collaborazione con altre parti, non possa più identificare direttamente o indirettamente l'interessato"*

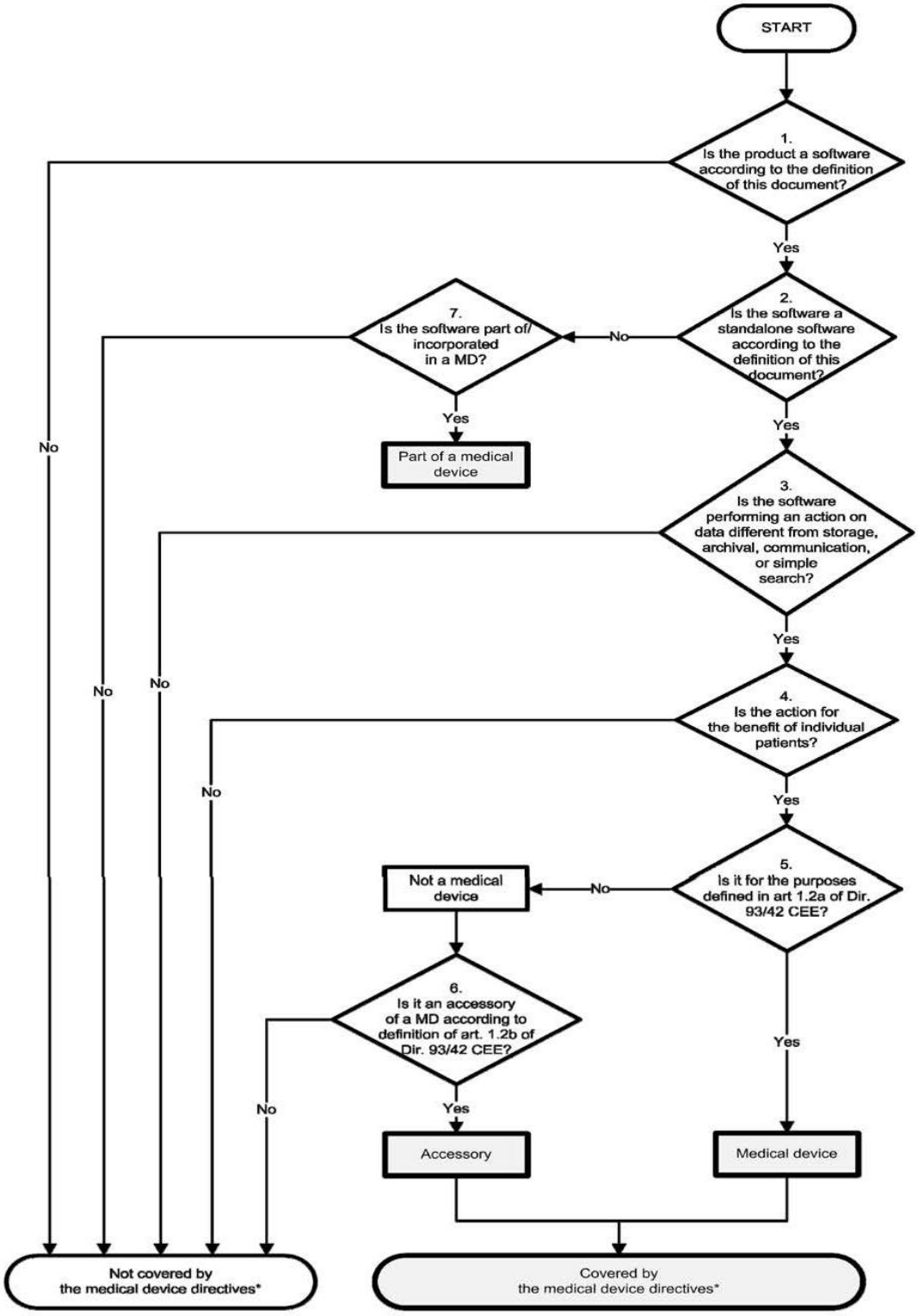


Figura 4. Diagramma decisionale per assegnare ad un software la designazione di dispositivo medico, estrapolato dalle linee guida MEDDEV 2.1/6, *Guidelines On The Qualification And Classification Of Stand Alone Software Used In Healthcare Within The Regulatory Framework Of Medical Devices.*

Oltre a prevedere l'istituzione di una banca dati europea sui dispositivi medici (EUDAMED) ed un sistema di trasparenza e tracciabilità dei dispositivi (UDI), il GDPR prevede, oltre che una valutazione fondata sulla sicurezza, anche una valutazione clinica circa la destinazione d'uso del dispositivo, conforme alle tipologie di dati personali raccolti e trattati.
L'individuazione delle caratteristiche applicative e dei rischi inerenti diventa particolarmente complessa quando si va ad analizzare un software biomedicale; questa complessità è dovuta in parte all'innovazione degli stessi programmi forniti ed utilizzati, perché una maggiore capacità di gestione ed elaborazione comporta necessariamente la presenza di una rete di collegamenti più difficile da identificare e districare. In secondo luogo, la crescente implementazione dei software all'interno degli elettromedicali[56], fino ad arrivare ad un device unico con prestazioni avanzate, rende complesso identificare e discernere le criticità dell'uno e dell'altro, che seppur note per le due singolarità, tenderanno a modificarsi e ad accrescere se i due dispositivi verranno impiegati, e quindi valutati, assieme. Il software può di fatto avere un fattore di rischio elevato, se inserito in un sistema di dispositivi interconnessi, mentre potrebbe essere praticamente innocuo quando isolato.

Per questo motivo è importante procedere con l'identificazione dei software ad uso medico, ciò permetterà una migliore conoscenza dei processi operativi e di conseguenza renderà più agevole intervenire per la risoluzione dei problemi riscontrati durante la valutazione dei rischi associati ai trattamenti per i quali sono impiegati tali dispositivi.

Gli elettromedicali, i dispositivi di diagnosi e i sistemi informatici che operano all'interno delle Aziende Sanitarie possono essere classificati[57] in funzione della loro criticità, in base alle attività svolte:

[56] Si noti la differenza tra **dispositivo medico** ed **elettromedicale**: un dispositivo medico è *qualsiasi strumento, apparecchio, impianto, sostanza o altro prodotto, utilizzato da solo o in combinazione (compreso il software informatico impiegato per il corretto funzionamento) e destinato dal fabbricante ad essere impiegato nell'uomo a scopo di diagnosi, prevenzione, controllo, terapia o attenuazione di una malattia; di diagnosi, controllo, terapia, attenuazione o compensazione di una ferita o di un handicap; di studio, sostituzione o modifica dell'anatomia o di un processo fisiologico; di intervento sul concepimento, il quale prodotto non eserciti l'azione principale, nel o sul corpo umano, cui è destinato, con mezzi farmacologici o immunologici né mediante processo metabolico ma la cui funzione possa essere coadiuvata da tali mezzi* (MDR 745/2017); invece, un elettromedicale è *un apparecchio elettrico dotato di una parte applicata che trasferisce energia verso il o dal paziente, o rileva tale trasferimento di energia verso il o dal paziente* (norma CEI 62.5). In breve, tutti gli elettromedicali sono dispositivi medici, ma non tutti i dispositivi medici (ad esempio i software) sono elettromedicali.
[57] La classificazione presentata è fornita dalle linee guida MEDDEV 2.1/6, *Guidelines On The Qualification And Classification Of Stand Alone Software Used In Healthcare Within The Regulatory Framework Of Medical Devices*; e dalla guida tecnica CEI 62-237, *Guida alla gestione del software e delle reti IT-medicali nel contesto sanitario*.

- Business Critical: applicativi per la gestione delle attività in ambito amministrativo, economico o logistico;
- Operational Critical: applicativi per la gestione delle attività in ambito medico o clinico indispensabili per il funzionamento dell'organizzazione sanitaria;
- Mission Critical: applicativi o sistemi per la gestione delle attività e dei processi in ambito diagnostico, terapeutico, interventistico. Sono quelli di cui ci si occuperà più nel dettaglio.
- Life Critical: dispositivi o sistemi o applicativi vitali per la salute del paziente e la qualità del trattamento somministrato.

Dal momento che le apparecchiature elettromedicali di nuova o recente progettazione hanno iniziato ad usare degli applicativi informatici come loro parte integrante, si rende necessaria una classificazione dei sistemi medicali; questa può essere data o in base alle caratteristiche informatiche del sistema o in base alle caratteristiche telematiche possedute.

Per quanto riguarda le caratteristiche informatiche, troviamo:

- Embedded: software incorporato nel dispositivo medico (ad es. pompe ad infusione, ECG);
- On-board: software installato sul dispositivo medico, che in questo caso è un PC dedicato (ad es. ecografi);
- Accoppiato: software installato su PC collegato direttamente al dispositivo medico per il controllo del dispositivo e/o per l'elaborazione e l'archiviazione dei dati (ad es. microscopio);
- Console: workstation di refertazione, essa stessa dispositivo medico di un sistema Software Dispositivo Medico.
- Terminale: software installato su PC fisso, che è connesso via rete ad un sistema medicale per refertazione o elaborazione dei dati;
- Remoto: software installato su PC portatile, il quale è connesso alla rete aziendale e ad un sistema medicale per refertazione o elaborazione dei dati attraverso una VPN (rete virtuale protetta);
- Mobile: software installato su tablet o smartphone, che è connesso attraverso un portale aziendale per la visualizzazione dei dati medicali.

Per quanto riguarda, invece, le caratteristiche telematiche, distinguiamo i sistemi in:

- Stand-alone: tecnologia medicale che utilizza un software non connesso alla rete aziendale;
- Isolati: sistemi con postazioni connesse tra loro tramite una rete isolata;
- Intranet: sistemi connessi tramite rete aziendale;
- Private Cloud: sistemi connessi ad un server aziendale ma al di fuori della rete aziendale;
- Internet: sistemi connessi ad un server esterno alla rete aziendale via internet;
- Wireless: software dispositivi medici connessi alla rete aziendale con una connessione wireless.

Un aspetto che è importante riportare è che, a motivo della differenza esistente tra software integrato in un dispositivo medico (rientrano in questa definizione i software Embedded e gli on-board), software "accessorio[58]" (accoppiato, remoto, mobile, terminale e console possono essere inquadrati come software di tipo accessorio) e software stand-alone, sarà differente anche la catalogazione assegnata. Questo perché, in quanto dispositivi medici a tutti gli effetti, anche questi necessitano di essere ricondotti ad una propria classificazione.

Nel caso di un dispositivo Embedded, essendo il software integrato nel device medico, deve anche essere classificato nella stessa classe di quest'ultimo, se è necessario al suo funzionamento e/o se ne influenza l'uso (cosa che avviene nella maggior parte dei casi).

Nel caso, invece, di software "accessorio", questo avrà una classificazione a parte, indipendente da quella del dispositivo medico a cui è associato, assegnata seguendo i medesimi criteri riportati nel Paragrafo 1.2.2.2.

Infine, il software indipendente Stand-alone viene considerato, in base alla Direttiva vigente, come dispositivo medico attivo. Questa tipologia di software è relativamente poco diffusa ed è sempre meno richiesta dalle Aziende Sanitarie, a favore invece di dispositivi in grado di comunicare tra loro e condividere informazioni utili attraverso la rete aziendale, cosa che però aumenta notevolmente i problemi di gestione del rischio associato alla privacy dei dati sanitari.

2.3.1 I Sistemi Informativi

Nel settore sanitario è aumentata sempre più negli ultimi anni l'esigenza di gestire il rischio clinico e la prevenzione del rischio clinico. La necessità di tenere sotto controllo tale

[58] Dalla Direttiva 93/42/CEE: "accessorio: prodotto che pur non essendo un dispositivo, sia destinato in modo specifico dal fabbricante ad essere utilizzato con un dispositivo per consentirne l'utilizzazione prevista dal fabbricante stesso"

fenomeno ha portato all'adozione, da parte di molte strutture sanitarie, di strategie volte ad eliminare o limitare il più possibile il rischio di insorgere di problematiche ed errori nel processo di assistenza al paziente.
Recentemente, la tecnologia sta offrendo il proprio contributo in tal senso, attraverso l'introduzione di applicativi di nuova tecnologia web based, orientati al paziente, integrabili tra loro secondo standard definiti, caratterizzati da dizionari di base comuni (stessa base anagrafica, dizionari nazionali/regionali, utilizzo di codifiche).

In particolare, l'azienda ULSS5 ha tre poli ospedalieri, diverse strutture decentrate e qualche centinaio di ambulatori medici territoriali. Lo scambio di informazioni e di immagini tra i tre ospedali, e tra questi e il territorio, presuppone l'uso di un linguaggio unificato attraverso l'impiego complementare di diversi Sistemi Informativi. L'adozione di tali Sistemi consolidano i meccanismi di esatto riconoscimento del paziente, rafforzando i livelli di sicurezza nella fase di ingresso.
I sistemi informativi hanno alcune funzioni generali, tra cui la coordinazione della raccolta dei dati, lo loro gestione e presentazione e lo scambio di informazioni tra diversi centri. All'interno di un'Azienda Ospedaliera, e più precisamente per ogni reparto, il sistema informativo ha il fine specifico di consentire la gestione delle informazioni utili sia per il corretto svolgimento delle attività sanitarie, sia per mantenere monitorato lo stato di funzionamento dell'Azienda stessa.

Sono attualmente in uso tre sistemi informativi per l'ambito sanitario:

- Il *Radiology Information System* (Sistema Informativo Radiologico - *RIS*);
- Il *Picture Archiving and Communication System* (Sistema per l'Archiviazione e la Comunicazione delle Immagini - *PACS*);
- L'*Hospital Information System* (Sistema Informativo Ospedaliero - *HIS*), all'interno del quale i sistemi RIS e PACS sono integrati.
- Il sistema informatico è la componente automatizzata del sistema informativo.

All'interno dell'Azienda Ospedaliera, il sistema HIS gestisce tre principali tipologie di informazioni:

1. Informazioni relative al paziente: anagrafica, storia amministrativa e clinica, etc.;
2. Informazioni relative alle attività ed ai servizi erogati dalle diverse strutture;
3. Informazioni relative alle risorse (personale, attrezzature, risorse finanziarie).

In breve, questo Sistema si occupa di gestire le informazioni necessarie per i vari aspetti della vita di un'Azienda Ospedaliera.
Generalmente gli HIS installati sono sistemi prevalentemente orientati a finalità di tipo amministrativo e finanziario e rivestono poca importanza sul piano sanitario. Le informazioni sanitarie, i dati del paziente, gli esiti degli esami effettuati e le conseguenti refertazioni vengono gestite in prevalenza dai due sistemi informativi integrati, ovvero RIS e PACS.

2.3.1.1 Il Sistema Informativo Radiologico

Il RIS ha il compito di gestire specificamente le informazioni da erogare al o generate nel reparto di Radiologia. In particolare, il Sistema Informativo Radiologico si fa carico di fornire alla Radiologia le informazioni riguardanti prenotazione e accettazione dei pazienti, di aspetti logistici e amministrativi (occupazione di sale, personale in servizio, elettromedicali impiegati), della refertazione con assegnazione della firma digitale e dell'archiviazione dei referti.
Al RIS, oltre alle richieste esterne, possono pervenire richieste anche da altri reparti dell'ospedale; questa funzionalità è utile per orientare i medici, affinché possano facilmente effettuare ordini per esami radiologici attraverso il RIS stesso.

Il Sistema informativo Radiologico dell'Azienda Ospedaliera Aulss5 è configurato come un insieme di reti locali (Virtual Local Area Network, VLAN[59]); è naturalmente interfacciato con l'HIS o altri sistemi informatici dipartimentali (per esempio farmacia, banca del sangue).
Gli ordini possono anche essere passati ad una cartella clinica elettronica (EMR/EHR).

2.3.1.2 Il Sistema per l'Archiviazione e la Comunicazione delle Immagini

Se il RIS riguarda principalmente gli aspetti amministrativi inerenti alla gestione del paziente, il PACS è una tecnologia di imaging medico che viene utilizzata allo scopo di archiviare, recuperare, gestire, distribuire e presentare in modo sicuro immagini prodotte da varie modalità hardware mediche, come tomografia computerizzata (TAC), risonanza magnetica (MRI), raggi X e macchine ad ultrasuoni.
La Radiologia è, nel campo della medicina, il produttore tradizionalmente più prolifico di immagini, ed è quindi da questo specifico reparto che è iniziato lo sviluppo del sistema PACS, finalizzato alla completa gestione digitale dell'immagine, con conseguente eliminazione delle pellicole radiografiche. Tuttavia, con sempre maggiore frequenza le

[59] Rete fittizia di dispositivi che appartengono a una o più reti LAN (Local Area Network); in breve, ha lo scopo di suddividere i computer collegati alla rete in base a determinate caratteristiche e collegare computer separati.

tecnologie PACS sono state incorporate anche in numerosi altri reparti; il sistema RIS/PACS non è più limitato dunque alla sola Radiologia ma integra diagnostiche di vario tipo, che condividono lo standard DICOM. Tale approccio cambia in maniera radicale il modo in cui si utilizzano le informazioni cliniche, permettendo la distribuzione in tempo reale delle stesse, e il loro utilizzo da diversi reparti (Medicina Nucleare, Cardiologia, Oncologia, Dermatologia).

Il sistema è costituito da tre componenti fondamentali:

1. L'Archivio, con diversi livelli gerarchici di archiviazione:
    a. Archivio corrente, finalizzato a mantenere immediatamente disponibili indagini relative ad un periodo di una settimana;
    b. Archivio a lungo termine, che prevede la possibilità di mantenere in memoria i dati relativi alle indagini effettuate per un periodo di 7 anni.
    c. Archivio di back-up, per un'ulteriore garanzia di sicurezza del sistema, al fine di preservare tutti i dati prodotti e assicurare le funzioni di disaster recovery.

2. Le Workstation periferiche. Queste costituiscono l'elemento operativo di primo impatto del sistema, quello attraverso il quale operano i medici (Workstation di Refertazione) ed i tecnici di Radiologia (Workstation di Consultazione).

3. Il Network o Rete di Trasmissione Dati, attraverso la quale tutti i dati devono transitare; la gestione delle immagini radiologiche con tecnologia Web prevede che le stesse, dopo essere state prodotte in formato elettronico, vengano memorizzate su server residenti fisicamente all'interno del servizio di radiologia.

L'architettura dei sistemi PACS consente la manipolazione delle immagini e l'uso di stazioni di visualizzazione, inoltre promuove la trasmissione di immagini digitali a qualsiasi parte della rete ospedaliera grazie ad una connessione capillare tra tutte Workstation, le apparecchiature di acquisizione delle immagini e quindi con l'archivio digitale attraverso l'Intranet Aziendale; infine, permette a medici diversi l'accesso diretto e simultaneo alle immagini memorizzate.

I Sistemi RIS e PACS, pur svolgendo funzioni distinte, sono profondamente collegati e condividono un obiettivo comune: per questa ragione negli ultimi anni diversi centri radiologici ed industrie biomedicali hanno profuso un notevole impegno per rendere possibile una sempre più efficace integrazione tra RIS e PACS, che aiuti la struttura sanitaria a gestire

in modo completamente informatizzato tutte le attività legate alla radiologia e alla diagnostica per immagini**,** semplificando la consultazione sia per i pazienti, che per i medici.
Tale integrazione ha come obbiettivo quello di permettere la condivisione di informazioni anagrafiche/diagnostiche/cliniche in modo automatico e sicuro, evitando il diffondersi di errori. Con i Sistemi descritti, dunque, la documentazione medica e le immagini possono essere conservate in modo sicuro in server opportunamente realizzati e rese accessibili ai medici ed agli operatori attraverso le workstation di diagnosi e refertazione, che sono collegate al sistema integrato RIS/PACS.

Sono infine presenti due ulteriori sistemi informatici, CUP e ADT, distinti ma tra loro molto simili, dei quali non si è ancora parlato. Il CUP (Centro Unico di Prenotazione) raccoglie ed inoltra ai reparti le liste degli appuntamenti di utenti esterni (note come "liste di lavoro": l'ADT (Accettazione Dismissione Trasferimento) svolge le medesime azioni, ma con i degenti, ovvero pazienti interni all'Ospedale o presenti in strutture ospedaliere esterne.
Tali sistemi non rivestono particolare importanza all'interno delle considerazioni di carattere informatico; verranno ripresi nel capitolo successivo durante la spiegazione nel dettaglio dei percorsi dei dati all'interno del reparto di Radiologia.

2.3.2 Standard di comunicazione

La condivisione attiva di informazioni da e verso Workstation ed elettromedicali, e naturalmente da e verso il sistema integrato RIS/PACS è resa possibile grazie all'adozione di standard comuni di comunicazione. Il sistema utilizza dunque il modello centralizzato, in cui tutte le informazioni passano attraverso un unico punto a cui tutti fanno riferimento, in cui poi le informazioni sono decentrate.
Questi standard permettono di definire il formato dei messaggi con i dati personali dei pazienti, incluse le informazioni relative alla salute e agli esami necessari, le modalità di comunicazione e trasmissione dei messaggi; inoltre, garantiscono una efficace centralizzazione di tutte le informazioni cliniche, attraverso la trasmissione dei dati clinici tra i Sistemi e device medici spesso provenienti da differenti case costruttrici.
Sono due gli standard maggiormente utilizzati nell'ambito clinico, e che sono integrati nei sistemi di comunicazione dell'Azienda Ospedaliera ULSS5:

- HL7 (*Health Level Seven*), standard di archiviazione e scambio di dati clinici;
- DICOM (*Digital Imaging ad Communications in Medicine*) standard di archiviazione e scambio delle immagini medicali.

2.3.2.1 HL7

Lo standard HL7 garantisce lo scambio elettronico, la gestione e l'integrazione di informazioni mediche ed amministrative tra i diversi sistemi presenti in un'azienda sanitaria, in modo indipendente dagli applicativi che li implementano. Non si tratta di un software, ma di una specificazione che definisce i messaggi come stringhe di testo in formato ASCII[60] delimitate da separatori. I messaggi sono sempre bidirezionali (mettono in comunicazione due attori, un emittente e un ricevente) e le informazioni, in questo modo, vengono crittografate (ad eccezione del nome del paziente) durante lo scambio, e reinterpretate nel software applicativo utilizzato in Radiologia.

Questo standard nasce alla fine degli anni '80 e da allora è in continuo e costante aggiornamento, con l'obiettivo principale di semplificare le interfacce fra applicazioni di produttori diversi ed uniformare il formato e il protocollo utilizzati nello scambio di alcuni insiemi critici di dati. HL7 ambisce a diventare il linguaggio utilizzato per costruire le cartelle cliniche digitali e mettere in relazione diretta le applicazioni e i servizi che assicurano la presa in carico e la gestione, anche amministrativa, dei pazienti e più in generale di tutti i soggetti del sistema sanitario informatizzato.

2.3.2.2 DICOM

DICOM[61] è un protocollo standard che definisce i criteri per la comunicazione, la visualizzazione, l'archiviazione e la stampa di informazioni di tipo biomedico (prime tra tutte, le immagini radiologiche).

A differenza di HL7, non è costituito da una serie di dati in forma di messaggio, e non costituisce nemmeno un nuovo formato per le immagini. Si tratta invece di una Struttura Dati Object Oriented, si potrà perciò identificare un file DICOM come un "oggetto", costituito da un corpo dati che contiene una o più immagini e da un'intestazione (Header) contenente informazioni che indicano l'intero procedimento operativo per l'acquisizione dell'immagine stessa - informazioni generali sul paziente, come nome, ID, data di nascita, sesso; metodiche di analisi, come data, ora, medico referente; caratteristiche delle immagini, come numero della serie, tipo di modalità, dimensione della matrice, profondità del pixel, etc.

[60] *American Standard Code for Information Interchange*, sistema di codifica dei caratteri a 8 bit comunemente utilizzato nei calcolatori.

[61] Lo standard DICOM è gestito dalla Medical Imaging & Technology Alliance , una divisione della National Electrical Manufacturers Association. È uno standard pubblico e la sua documentazione è accessibile tramite il portale dedicato www.medical.nema.org

2.4 Considerazioni finali

Nel corso del seguente capitolo è emerso che il software applicativo in ambito biomedicale deve conformarsi, a seconda dei rischi e delle vulnerabilità riscontrate tramite analisi preliminare, ai principi del privacy by design e by default indicati dal GDPR come buone pratiche di progettazione. Se il detto software è già realizzato ed in funzione, va stabilito il livello di rischio associato e decisa una modalità di intervento per rendere tale rischio minimo e accettabile, in relazione allo scopo del trattamento dei dati, e soprattutto conforme alle norme introdotte dal Regolamento Generale Europeo sulla Protezione dei Dati. Per fare questo, una valida strategia consiste nel tener presente i dieci meccanismi di sicurezza applicativa e sviluppare per ciascuno delle strategie di mitigazione delle vulnerabilità.

È opportuno istituire dei processi di gestione della configurazione e di gestione delle modifiche apportate alla configurazione stessa, per tenere sotto controllo lo stato di conformità al GDPR del software. Questi processi andranno rivisti regolarmente, possibilmente con cadenza annuale (secondo quanto stabilito dal provvedimento WP248 rev.01), per verificare che i software applicativi impiegati siano ancora conformi al Regolamento Europeo, e dovranno essere necessariamente documentati all'interno del Registro dei Trattamenti, assieme ai loro risultati periodici.

Entrando maggiormente nel contesto del caso di studio che verrà analizzato nel successivo Capitolo, è stata introdotta la rete di trasmissione dei dati ospedaliera. Questa, in breve, si basa sull'impiego di due Sistemi informativi Integrati (RIS e PACS) che comunicano con tutti i reparti dell'Ospedale e permettono l'efficiente scambio delle informazioni sanitarie tra dispositivi e sistema centrale, dunque una corretta archiviazione dei dati sanitari ed il loro utilizzo per l'agevolazione di pratiche mediche, esami, prestazioni ed altro.

Questo tipo di comunicazione, permesso dai due standard maggiormente diffusi in ambito ospedaliero (HL7 e DICOM), è stato descritto perché propedeutico alla comprensione delle modalità di gestione del dato presso il reparto di Radiologia. L'evoluzione tecnologica ha consentito, e consentirà sempre di più nel prossimo futuro, di sviluppare sistemi automatici e digitali di movimentazione e raccolta dei dati all'interno delle aziende sanitarie, grazie alla convergenza di competenze informatiche, cliniche e ingegneristiche fin dalle prime fasi di progettazione.

La modalità di gestione integrata dei flussi di informazioni e le connessioni presenti tra elettromedicali, device medici per diagnosi, software installati ed il sistema informatico ospedaliero, oltre alle notevoli agevolazioni - una gestione programmabile delle informazioni e dei dati in uso dai dispositivi permette di supportare l'utilizzo dei dati anagrafici a livello

aziendale e di modalità di identificazione del paziente e permette inoltre di ottimizzare le informazioni richieste dal sistema informatico centrale - comporta però la necessità di un monitoraggio costante, sia dal punto di vista fisico che tecnologico, atto a garantire la sicurezza delle informazioni raccolte.

Sarà dunque necessario istituire una serie di controlli, legati alle modalità di raccolta e conservazione dei dati sanitari dei pazienti nel reparto di Radiologia, che concorreranno a limitare i rischi associati ai trattamenti effettuati ed alle prestazioni sanitarie erogate. I valori di rischio ottenuti dall'analisi, una volta inseriti all'interno del Registro dei Trattamenti, permetteranno di avere sempre ben chiaro all'interno dell'azienda quali sono gli standard da rispettare per mantenere una conformità con il Regolamento Europeo sulla Protezione dei Dati e, allo stesso tempo, verificare e correggere tutte le procedure, ad opera degli operatori o degli stessi dispositivi medici, che dimostrano di possedere un rapporto costi-benefici non congruente.

Capitolo 3.

Risk Assessment e Data Protection Impact Assessment per il Reparto di Radiologia

3.1 Introduzione

Il seguente Capitolo si occuperà, come prima questione, di descrivere le modalità con cui i dati sanitari vengono ottenuti, raccolti ed elaborati dal reparto di Radiologia, con particolare attenzione sia alle differenti tipologie di dato trattato, sia alla presenza di criticità nei percorsi in cui gli stessi dati viaggiano o vengono condivisi, nonché ai dispositivi che si occupano di questo aspetto. Una volta ottenute queste informazioni, si passerà alla stesura di un primo Registro dei Trattamenti, puramente indicativo e riassuntivo delle informazioni riportate, che servirà come punto di partenza per la realizzazione di una procedura di valutazione del rischio per i trattamenti operati in Azienda. Tale procedura verrà quindi applicata ai diversi dispositivi (dispositivi medici, monitor, elettromedicali impiegati per l'effettuazione dell'esame) del reparto di Radiologia, saranno studiati i rischi associati ai diversi device e tratte le opportune considerazioni sul livello di rischio residuo attribuibile.

A completamento di tale procedura si otterrà un Registro dei Trattamenti completo, conforme a quanto richiesto da Azienda Zero e da quanto previsto dal Regolamento Europeo sulla Protezione del Dato, che avrà riportato, per ogni dispositivo, il suo grado di rischio e le misure di sicurezza che vengono adottate per la protezione dei dati che lo stesso dispositivo tratta/conserva/elabora.

3.2 Unità Operativa Complessa di Radiologia

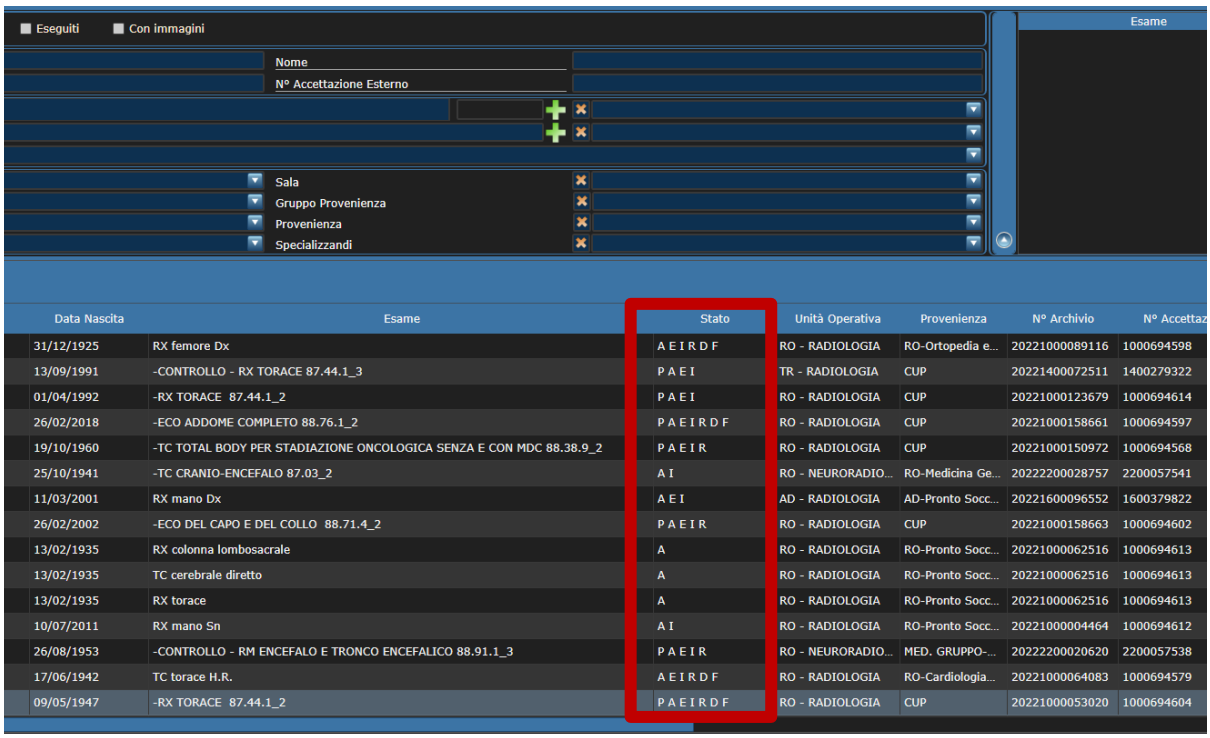
La Radiologia è una branca della medicina che si occupa della produzione e dell'interpretazione a fine diagnostico e terapeutico di immagini ottenute con l'ausilio di radiazioni ionizzanti (raggi X) o non ionizzanti (radiofrequenze ed ultrasuoni) applicate al corpo umano. Due sono le branche principali: la Radiologia diagnostica e la Radiologia interventistica. La Radiologia diagnostica è quell'insieme di metodiche radiologiche (radiografia tradizionale, ecografia, tomografia computerizzata, risonanza magnetica) a disposizione dello specialista radiologo e utilizzate con fine diagnostico. La Radiologia Interventistica è l'insieme delle procedure invasive diagnostiche e terapeutiche effettuate mediante guida radiologica (ecografica, fluoroscopia e TC).

La UOC Radiologia dell'Ospedale di Rovigo eroga le seguenti tipologie di prestazioni sanitarie:

- Ecografia;
- Esami di sala Operatoria;
- Densitometria;
- Mammografia;
- Radiografia;
- Risonanza Magnetica;
- Tomografia Computerizzata (TAC);
- Ortopantomografia.

Il software impiegato per la gestione degli esami, dalla raccolta delle anagrafiche fino alla redazione del referto, non solo in Radiologia ma anche in quasi tutti gli altri reparti dell'ospedale, è suitEstensa®, fornito dalla ditta Esaote. Questo software è perfettamente integrato nei sistemi informativi ospedalieri ed implementa sia lo standard DICOM per l'elaborazione delle immagini radiologiche acquisite, sia lo standard HL7 per l'interpretazione dei dati dei pazienti forniti dal sistema RIS/PACS.
Per lo svolgimento di ciascun esame vengono utilizzati elettromedicali di diversa natura, specifici per l'esame in questione. Ognuno di questi elettromedicali è collegato ad una workstation che permette al tecnico di Radiologia di gestire l'esame in tutte le sue differenti fasi. Per ogni elettromedicale viene creato un collegamento con una dedicata workstation di lavoro (o workstation di Consultazione, in seguito indicata anche come Consolle) tramite l'assegnazione di un codice identificativo, l'iTitle. Questo codice viene fornito dalla stessa ditta che provvede al software di gestione dati, e la specifica assegnazione consolle-elettromedicale consente di avere, all'interno delle diverse aree del reparto, una postazione specifica per ogni esame.

Per procedere con le analisi dei rischi associati alla circolazione dei dati sanitari, si ritiene utile fornire una breve descrizione di come si articola il flusso di lavoro all'interno del reparto di Radiologia. Il processo che subiscono i dati dei pazienti si articola in sette fasi, che il software suitEstensa®, collegato con il sistema RIS/PACS e utilizzato per la gestione dell'intero processo di raccolta e gestione dati, rende note aggiornando lo stato, assegnando una lettera di riferimento a ciascuna fase (Figura 5).



Data Nascita	Esame	Stato	Unità Operativa	Provenienza	N° Archivio	N° Accettaz
31/12/1925	RX femore Dx	A E I R D F	RO - RADIOLOGIA	RO-Ortopedia e...	20221000089116	1000694598
13/09/1991	-CONTROLLO - RX TORACE 87.44.1_3	P A E I	TR - RADIOLOGIA	CUP	20221400072511	1400279322
01/04/1992	-RX TORACE 87.44.1_2	P A E I	RO - RADIOLOGIA	CUP	20221000123679	1000694614
26/02/2018	-ECO ADDOME COMPLETO 88.76.1_2	P A E I R D F	RO - RADIOLOGIA	CUP	20221000158661	1000694597
19/10/1960	-TC TOTAL BODY PER STADIAZIONE ONCOLOGICA SENZA E CON MDC 88.38.9_2	P A E I R	RO - RADIOLOGIA	CUP	20221000150972	1000694568
25/10/1941	-TC CRANIO-ENCEFALO 87.03_2	A I	RO - NEURORADIO...	RO-Medicina Ge...	20222200028757	2200057541
11/03/2001	RX mano Dx	A E I	AD - RADIOLOGIA	AD-Pronto Socc...	20221600096552	1600379822
26/02/2002	-ECO DEL CAPO E DEL COLLO 88.71.4_2	P A E I R	RO - RADIOLOGIA	CUP	20221000158663	1000694602
13/02/1935	RX colonna lombosacrale	A	RO - RADIOLOGIA	RO-Pronto Socc...	20221000062516	1000694613
13/02/1935	TC cerebrale diretto	A	RO - RADIOLOGIA	RO-Pronto Socc...	20221000062516	1000694613
13/02/1935	RX torace	A	RO - RADIOLOGIA	RO-Pronto Socc...	20221000062516	1000694613
10/07/2011	RX mano Sn	A I	RO - RADIOLOGIA	RO-Pronto Socc...	20221000004464	1000694612
26/08/1953	-CONTROLLO - RM ENCEFALO E TRONCO ENCEFALICO 88.91.1_3	P A E I R	RO - NEURORADIO...	MED. GRUPPO-...	20222200020620	2200057538
17/06/1942	TC torace H.R.	A E I R D F	RO - RADIOLOGIA	RO-Cardiologia...	20221000064083	1000694579
09/05/1947	-RX TORACE 87.44.1_2	P A E I R D F	RO - RADIOLOGIA	CUP	20221000053020	1000694604

Figura 5. Dettaglio di una generica schermata di lavoro del software suitEstensa®. È possibile osservare nella terza colonna "Stato" (riquadro rosso) una serie di lettere che identificano in successione le operazioni che sono state svolte con i dati raccolti da ciascun paziente (P=Prenotazione; A=Accettazione; E=Esecuzione; I=Immagini; R=Refertazione; D=Definitivo; F=Firmato). Nella stessa schermata viene riportata in "Esame" la tipologia di prestazione che il device medico deve svolgere e in "Provenienza" il punto da cui arrivano le informazioni necessarie al suo svolgimento: le informazioni passano sempre attraverso il Sistema RIS, ma possono pervenire o dal CUP, nel caso di prestazioni eseguite in seguito a prenotazione, o dal Pronto Soccorso della struttura stessa.
Le prime due colonne, contenenti i nominativi dei pazienti, sono state escluse dalla visualizzazione per motivi di privacy.

1. Prenotazione

Il paziente che necessita di sottoporsi ad esame radiologico effettua la prenotazione attraverso il CUP (Centro Unico Prenotazioni), che conserva le informazioni che, una volta fornite al RIS, contribuiranno alla generazione della lista di lavoro univoca per il singolo paziente.

La worklist contiene:

- Dati anagrafici del paziente;
- Tipologia di esame da svolgere;
- Tempistiche associate all'esame stesso;
- Motivazione dell'esame (eventuale).

La prenotazione al CUP coincide anche con la creazione (se si tratta della prima prenotazione) del profilo associato al paziente, con assegnazione di un codice identificativo. Il paziente sarà inoltre chiamato a fornire il proprio consenso informato ai trattamenti ai quali verrà

sottoposto, tramite firma dell'informativa; come ribadito in precedenza, per la tipologia di esami svolti presso il reparto di Radiologia il consenso viene sempre richiesto[62].
È possibile che, nell'assegnazione dello stato all'interno del software, manchi per alcune categorie di pazienti la P di *Prenotazione* prima della A di *Accettazione*: questo accade quando vengono presi in carico pazienti già interni all'ospedale, degenti di diversi reparti che necessitano di svolgere esami specifici o pazienti provenienti dal Pronto Soccorso.

2. Accettazione

Il giorno previsto per l'esame il paziente si presenta in Ospedale e la lista di lavoro viene generata e quindi inviata dal RIS alla consolle associata all'elettromedicale per mezzo del quale si svolgerà l'esame. Il paziente viene identificato tramite un codice ID associato al paziente stesso, creato nel passaggio dal CUP al Sistema RIS/PACS in concomitanza della prenotazione.
L'immissione dei dati del paziente avviene dunque automaticamente, senza la necessità di un inserimento manuale da parte del tecnico che esegue l'esame, e la digitalizzazione di questo processo ha permesso di limitare notevolmente errori di attribuzione ed inserimento.

3. e 4. Esecuzione ed Immagini

L'Esecuzione coincide con la produzione delle immagini radiologiche e la raccolta dei dati ad esse associate; l'inizio dell'esame, e quindi la detta fase di Esecuzione, ha inizio solo a seguito della firma digitale da parte del tecnico che si occupa della prestazione. È possibile per i tecnici conoscere lo storico del paziente, il suo quadro clinico, richiamando dal Sistema gli esami precedentemente svolti e le immagini radiologiche ad essi associate; per questa operazione è sufficiente inserire nel sistema il nome e il cognome del paziente e, in caso di possibile omonimia, anche della data di nascita.

Si permetta in questo contesto una nota sulla sicurezza: il paziente è individuato in modo univoco a livello di Sistema tramite un identificativo, che viene creato automaticamente nel momento in cui la prenotazione effettuata presso il CUP viene inserita nel RIS/PACS. Il fatto di non utilizzare questo identificativo, ma – per una questione di velocità di esecuzione e di maggiore automatismo – le informazioni anagrafiche del paziente, crea un potenziale rischio nel momento in cui si ha accesso ad una serie di esami tutti collegati ad una persona fisica riconoscibile. In questo contesto, si fa affidamento alla scrupolosità ed alla attenzione dei tecnici coinvolti.

[62] Regolamento (UE) 2017/745, **art. 7**: *Condizioni per il consenso*

Il formato DICOM permette di raccogliere, oltre alle informazioni direttamente collegate al paziente, anche le modalità di acquisizione dell'immagine stessa (luminosità, opacità, numero e spaziatura dei pixel, numero di immagini acquisite, etc.).
In seguito all'introduzione del D. Lgs. 101/2020 è inoltre necessario tenere traccia, e comunicare poi al paziente in referto, la quantità di dose erogata durante lo svolgimento dell'esame. Anche questi dati vengono forniti dal Sistema RIS/PACS, assieme alle altre informazioni utili per procedere con l'esame, alla Workstation collegata all'elettromedicale che verrà utilizzato, e sono automaticamente memorizzati ed inseriti nel referto.

La fase di Immagini corrisponde invece all'invio delle stesse, al termine della loro acquisizione, al Sistema RIS/PACS. L'Azienda Ospedaliera Aulss5 può vantare tre Sistemi di questo tipo, uno centrale presso la Cittadella Socio-Sanitaria di Rovigo e due PACS "stelliti", anche chiamati PACS Cache, rispettivamente situati presso i Poli Ospedalieri di Adria e Trecenta. I due Sistemi satelliti sono stati creati per garantire una maggiore velocità di invio, una riduzione del tempo di elaborazione delle immagini e, di conseguenza, di visualizzazione da parte del medico. Per una maggiore sicurezza nella conservazione delle informazioni mediche, il punto di riferimento è il PACS centrale di Rovigo:

- Se le immagini provengono dal P.O. Rovigo, vengono inviate direttamente al PACS centrale;
- Se le immagini provengono dai P.O. Adria e Trecenta, sono inviate automaticamente sia al PACS satellite dedicato, sia al PACS centrale. Sono presenti in doppia copia circa sette giorni, per favorire un rapido accesso agli operatori che hanno eseguito l'esame, dopodiché vengono cancellate dal sistema satellite e permangono solo in quello centrale, dal quale possono comunque essere richiamate al bisogno.

L'eliminazione delle informazioni ripetute fa parte di una strategia di sicurezza ribadita anche all'interno del Regolamento Europeo sulla Protezione dei Dati, ovvero la necessità di limitare il più possibile il numero di siti in cui i dati sono conservati e da cui potrebbero essere trafugati.

Tramite la consolle legata alla macchina c'è la possibilità di avere una visualizzazione web del software utilizzato, compresa nell'Intranet aziendale, più leggera rispetto al programma completo.
Per avere accesso al software i tecnici e tutto il personale che ha necessità di operare con il sistema (operatori sanitari, medici, amministrativi, medici di altri reparti) deve possedere un

profilo di accesso, e ciascun profilo avrà delle possibilità di visualizzazione ed operatività diverse, in funzione del proprio ruolo all'interno dell'Azienda.

A titolo di esempio, in Figura 6 è riportato il profilo di visualizzazione software di un Tecnico Radiologo.

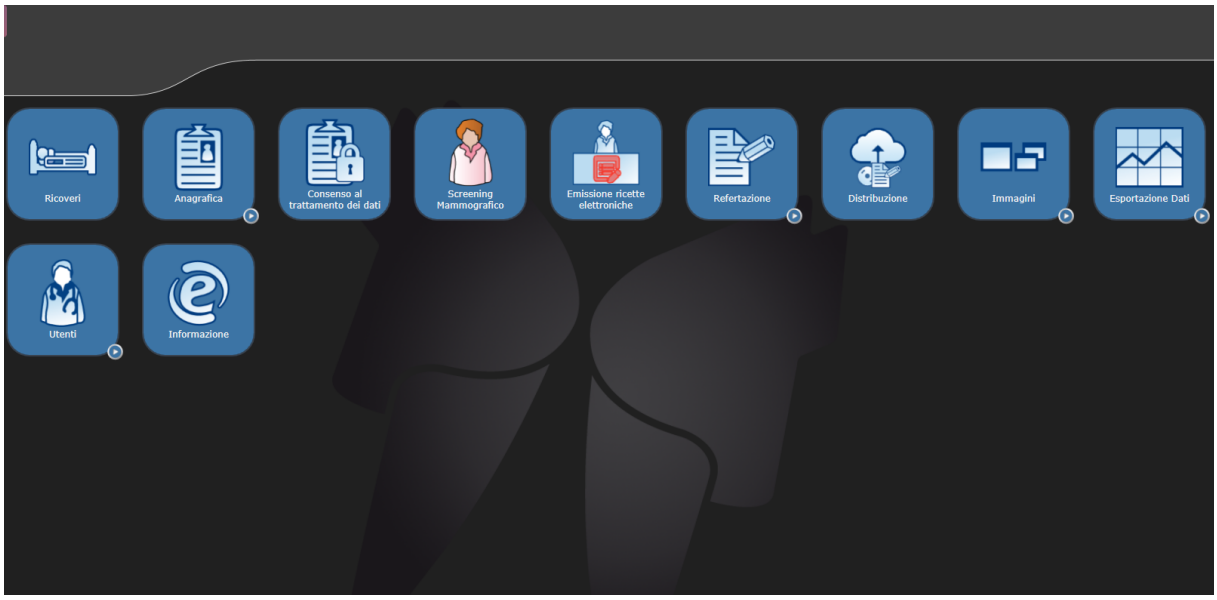


Figura 6. Schermata principale del software operativo suitEstensa®, con visualizzazione per i tecnici radiologi. Le diverse caselle permettono l'accesso a diversi ambiti di lavoro e, di conseguenza, ad un numero diverso di dati, in base al ruolo ricoperto in Azienda.

5. *Refertazione*

La fase di refertazione consiste nell'interpretazione, da parte di uno o più medici Radiologi, delle immagini mediche raccolte. Questa fase viene svolta su un dispositivo diverso, direttamente collegato con il Sistema RIS/PACS dal quale le immagini vengono ottenute. I monitor utilizzati per la refertazione garantiscono una visualizzazione delle immagini ad elevatissima risoluzione[63], ciò permette al medico di esaminare accuratamente quanto ricostruito dagli elettromedicali.

[63] In breve, i monitor delle workstation per le applicazioni radiologiche devono avere caratteristiche di luminanza tali che Lmax sia il più elevato possibile, per migliorare la sensibilità di contrasto, e che Lmin sia il più basso possibile, in modo che l'intervallo dei livelli di luminanza presenti in una immagine sia tale per cui Lmax/Lmin > 240. Di seguito sono elencate le normative di riferimento: **IEC 61223-2-5,** *Evaluation and routine testing in medical imaging departments* – Part 2-5: constancy tests – image display devices, 1994; **DIN V 6868-57** *Image quality assurance in X-Ray diagnosis* – Part 57: Acceptance testing for image display devices, 2001; **NEMA**, *Digital Imaging and Communications in Medicine (DICOM)* – Part 14: Grayscale Standard Display Function, PS 3.14, 2004-2008; **AAPM TG18** *Assessment of display performance for medical imaging systems,* (Assessment of display performance for medical imaging systems: executive summary of AAPM TG18 report. Med Phys. 2005 Apr;32(4):1205-25); **2001 Euref**, *European guidelines for quality assurance in breast cancer screening and diagnosis- forth edition,* 2006; **DIN V 6868-157**, *Image quality assurance in X-Ray diagnosis* – Part 57: Acceptance testing for image display devices 2011; **IEC 62563-1** *Medical electrical equipment / Medical image display systems* – Part 1: Evaluation methods, 2009.

Il documento di refertazione, in prima battuta, deve contenere:

- Descrizione dell'esame effettuato (informazione prodotta automaticamente dal Sistema RIS/PACS e contenuta anche all'interno del file DICOM);
- Codice dell'esame;
- Descrizione dei segni radiologici rilevati sull'immagine;
- Ipotesi diagnostica e diagnosi differenziale;
- Codifica diagnostica;
- Quantità di dose erogata.

Le Workstation di Refertazione non hanno accesso alla visualizzazione web di suiteEstensa®, al contrario delle consolle di lavoro utilizzate dai tecnici e dal resto del personale abilitato: i medici refertatori utilizzano il sistema completo, il quale ha incluse anche tutte le informazioni presenti sulla modalità web. Questa particolare premura è naturalmente volta alla protezione delle informazioni strettamente personali e particolarmente sensibili che vengono elaborate e fornite dal medico che referta l'esito dell'esame. Inoltre, il medico utilizza una particolare modalità di lavoro che prevede l'accesso al software presente sulle Workstation di Refertazione esclusivamente in seguito ad un passaggio riconoscitivo aggiuntivo.

In pratica, l'accesso segue due step:

1. Inserimento delle credenziali di accesso per il software, comune a qualunque utilizzatore delle workstation di radiologia, a qualunque livello;
2. Una successiva identificazione tramite card elettronica, che ha come identificativo il codice fiscale del medico, ed inserimento del PIN associato.

Questo secondo passaggio è permesso solo ai medici, che sono gli unici in possesso di tale tessera e che sono tenuti a rimuoverla al termine della refertazione, rendendo di fatto inaccessibile questa parte del lavoro, la più delicata, al resto del personale ospedaliero. Infine, la card permette la firma digitale da parte del medico al termine della compilazione del referto; in assenza di questa firma, il referto non viene considerato valido.

6. e 7. Definitivo e Firma

Si tratta delle fasi finali del processo: una volta terminata la redazione del referto il software fornisce in automatico all'esame in svolgimento lo stato di Definitivo. A questo punto il medico appone, grazie alla propria card, la firma elettronica, ed il referto viene inviato in ritorno al sistema RIS/PACS per la sua conservazione (Repository, archivio fisico dei documenti in qualunque formato, ad es. PDF, CDA, DICOM, etc.); da lì si procede alla

stampa per la consegna al paziente. La firma elettronica è lo strumento che garantisce al supporto fisico autenticità ed integrità e, una volta firmato, il referto non è più modificabile. Il Sistema provvede ad inviare al CUP la conferma dell'esecuzione dell'esame, così da procedere con l'eventuale creazione del bollettino di pagamento per il paziente.
I referti, con le relative informazioni sugli esami svolti e le immagini mediche raccolte, vengono conservati (e restano accessibili) per un periodo di 10 anni[64], dopodiché il Sistema procede alla loro eliminazione automatica, semplicemente in base alla data di inserimento.

A sommario di quanto riportato in questo e nel precedente Capitolo, la rete di condivisione delle informazioni all'interno di un generico reparto di Radiologia (preso come riferimento in questa trattazione) è descritta schematicamente in Figura 7.

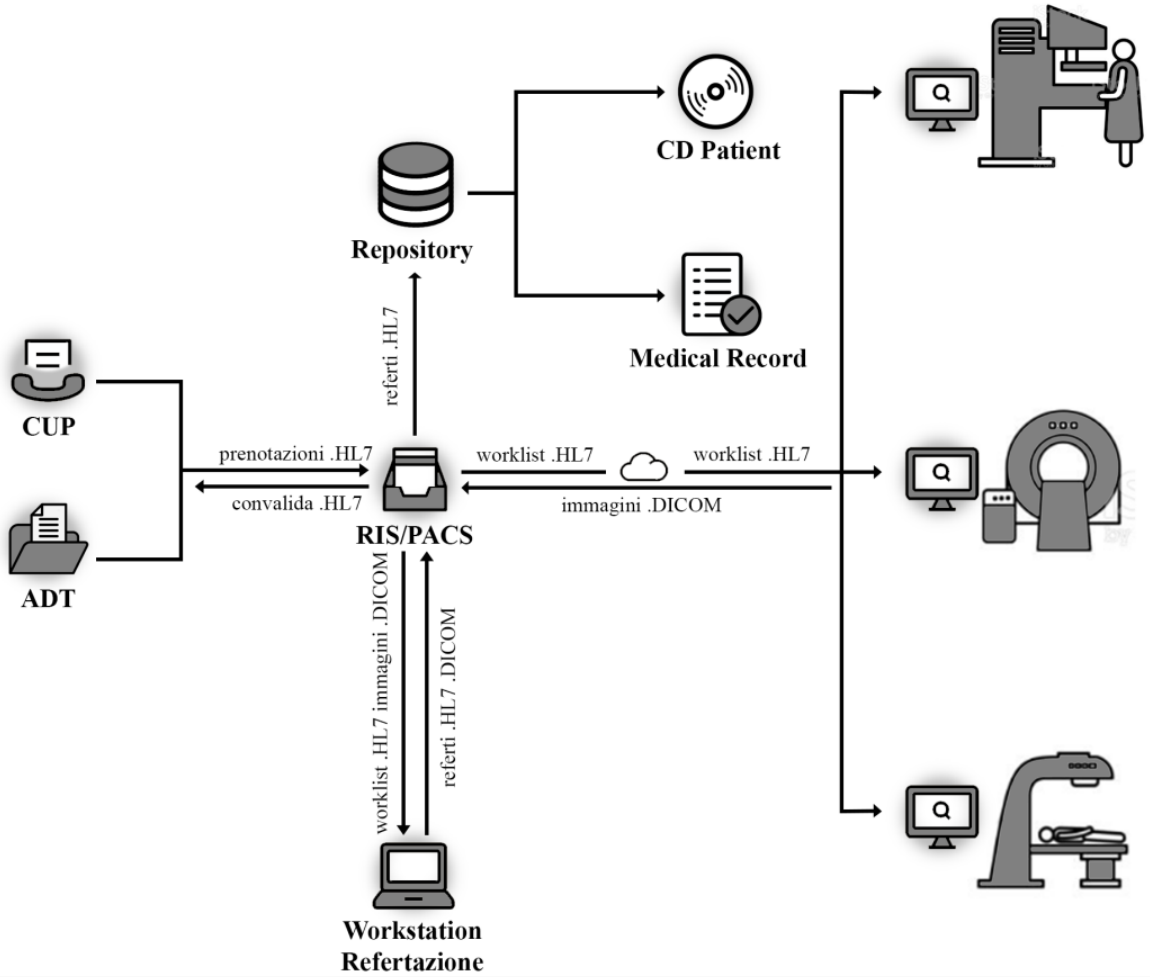


Figura 7. Rappresentazione dei flussi di dati da e verso il sistema RIS/PACS. L'architettura client/server permette di gestire un flusso bidirezionale delle informazioni, particolare attenzione è data alla scelta del protocollo di comunicazione compatibile con questo modello.

[64] La gestione delle immagini diagnostiche è regolamentata dal DM del 14 febbraio 1997, **art.4**: *Determinazione delle modalità affinché i documenti radiologici e di medicina nucleare e i resoconti esistenti siano resi tempestivamente disponibili per successive esigenze mediche.* Questa stabilisce precise direttive in relazione ad acquisizione, archiviazione e disponibilità delle immagini.

3.3 Procedura di valutazione del rischio per i trattamenti operati in Azienda

L'obiettivo finale della presente trattazione consiste nel valutare i rischi associati alla gestione dei dati in Azienda Sanitaria, un processo che per la sua realizzazione richiede delle linee metodologiche di riferimento ben precise, al fine di ottenere una valutazione chiara, e di avere standard riproducibili per ciascun trattamento. Come già riportato, nessun Regolamento o Direttiva contiene delle metodologie operative specifiche, quali ad esempio dei metodi univoci per classificare ed etichettare il rischio associato ai dispositivi medici.
Si è deciso dunque di stilare una procedura valutativa all'interno dell'Azienda Ospedaliera ULSS 5, con riferimento alle esigenze e alle modalità operative vigenti comuni a tutte le ULSS del SSR del Veneto, seguendo le direttive fornite da Azienda Zero. Questa intende essere una proposta operativa per le future indagini sui rischi associati alla trattazione del dato sanitario in ogni contesto clinico e processuale, in ottemperanza a quanto previsto dal GDPR.

La stesura si è svolta con le seguenti modalità: in primo luogo sono state identificate le diverse tipologie di trattamenti che prevedono la raccolta, la memorizzazione e la gestione dei dati dei pazienti, ed è stata effettua una valutazione preliminare dei rischi associati a detti trattamenti. Secondariamente, attraverso la scelta e la redazione di opportune scale per la valutazione dei livelli di gravità associati al rischio, è stato sviluppato un procedimento di conduzione del Data Protection Impact Assessment, per l'identificazione dei trattamenti considerati critici, da un punto di vista della possibilità di diffusione o manomissione dei dati sanitari raccolti, con conseguente rischio per i diritti e le libertà dell'Interessato. Per queste tipologie di trattamento dovranno essere individuate delle strategie di mitigazione per garantire un funzionamento sicuro del processo, conforme alla normativa vigente in tema di Protezione dei Dati Sanitari.

Prima di procedere trattando nel dettaglio i diversi passaggi di valutazione del rischio e di identificazione del livello di protezione del dato, è opportuno riportare un elenco di buone pratiche di gestione, da attuare all'interno dell'Azienda in ogni reparto, a prescindere dalla criticità dei trattamenti effettuati. Di seguito sono riportate:

1. L'inventario dei dispositivi medici presenti in azienda deve essere sempre mantenuto aggiornato;
2. Lo stesso inventario deve essere collegato ai dati e ai processi in essere nei diversi reparti, o al limite ai trattamenti erogati;

3. Va redatta e successivamente compilata una check-list di misure tecnico-organizzative, attuate allo scopo di minimizzare il rischio per ciascuna tipologia di dispositivo o per dispositivi tra loro comparabili.
4. Va considerato un inevitabile gap tra le misure attese e le misure applicate;
5. Una volta individuate le criticità - naturalmente anche la quantità di dati trattati concorre alla determinazione del livello di rischio - queste vanno valutate singolarmente o nel loro insieme, identificando possibili metodologie per la riduzione del gap individuato. L'analisi dei rischi deve tener presente tutti quelli derivanti dagli errori del software e di per sé prevedibili.
6. Le misure di contenimento del rischio possono essere effettuate o dall'ufficio tecnico dell'Azienda – che all'interno dell'ULSS5 fa capo alla UOS Ingegneria Clinica, nella quale ho operato, o a monte dal fabbricante, quest'ultimo nei casi in cui:
    a. le caratteristiche del device non siano conformi a quanto richiesto in fase di acquisto o assegnazione del bando di gara;
    b. le problematiche riscontrate si trovino ad un livello di complessità macchina troppo elevata per le competenze dei tecnici incaricati;
    c. nel caso in cui si disponga di un budget sufficiente a far apportare le modifiche necessarie direttamente all'azienda fornitrice di riferimento.
7. A conclusione, è evidente la necessità di uno studio di fattibilità della raccolta dati tramite i software installati nel parco macchine aziendale, per quantificare le risorse e i mezzi necessari ad attuare le misure di minimizzazione del rischio.

3.3.1 Definizione del valore di criticità dei trattamenti

Il Registro dei Trattamenti è il punto di partenza per l'analisi delle criticità associate ai diversi processi. Si evidenzia che, dal momento che tale Registro potrà successivamente essere ampliato in modo da riportare anche i risultati ottenuti dalla DPIA e con le modalità operative scelte per la mitigazione del rischio rilevato, la sua realizzazione costituisce un processo continuo, non definitivo, che lo porterà ad essere costantemente mantenuto aggiornato, a favore di una sempre maggiore tutela sia per i pazienti che per l'Azienda.

Per ognuno dei trattamenti mappati, rientra tra le responsabilità del Titolare del trattamento redigere una valorizzazione qualitativa per una serie di variabili utili per la definizione del livello di criticità dei trattamenti.

Tali variabili rientrano in sette categorie, che corrispondono alle principali determinanti che contribuiscono all'esposizione al rischio di ciascun trattamento:

1. Trattamento di categorie particolari di dati;

2. Trattamento di dati di minori;
3. Trattamento su altre categorie di dati;
4. Finalità del trattamento;
5. Coinvolgimento di enti o soggetti terzi;
6. Infrastruttura;
7. Utilizzo di dispositivi o supporti removibili;

Ad ognuna delle variabili oggetto di valutazione (ne sono state identificate 24) è assegnato un peso, espressione del livello di criticità associato alla variabile stessa (Tabella 3). Tutte le variabili identificate e le loro relative influenze sono riportate, per completezza, in Tabella 4.

Livelli di criticità delle variabili			
Livello di criticità	Peso delle variabili	Descrizione	Conseguenze
Basso	1	Variabile che può determinare un basso livello di criticità in termini di accessi non autorizzati, di modifica, cancellazione, furto e/o diffusione di dati personali	Impatto lieve sui diritti e sulle libertà delle persone fisiche
Medio	2	Variabile che può determinare un medio livello di criticità in termini di accessi non autorizzati, di modifica, cancellazione, furto e/o diffusione di dati personali	Medio impatto sui diritti e sulle libertà delle persone fisiche
Alto	3	Variabile che può determinare un alto livello di criticità in termini di accessi non autorizzati, di modifica, cancellazione, furto e/o diffusione di dati personali	Impatto elevato sui diritti e sulle libertà delle persone fisiche

Tabella 3. Livelli di criticità delle variabili oggetto di valutazione; il livello di criticità è ottenuto assegnando un peso che va da 1 a 3 alle variabili, dove 1 corrisponde a livello Basso di criticità, mentre 3 corrisponde a d un livello Alto di criticità.

Una volta redatte le due tabelle, si procede alla definizione del livello di criticità del trattamento nel suo complesso, ad opera del Titolare del trattamento.

Per semplicità operativa, in questa fase si è deciso di assegnare ad ognuna delle 24 variabili un valore binario, tal per cui:

- Valore pari a 0: la variabile non evidenzia criticità (assente o adeguatamente monitorata);
- Valore pari a 1: la variabile è identificata come potenzialmente critica (presente, che necessita di ulteriori valutazioni e controlli).

A livello pratico, dunque, il livello complessivo di criticità verrà dato dalla somma delle sole variabili effettivamente manifestatesi durante il trattamento.

Il livello di criticità del trattamento è ottenuto come somma del peso delle variabili, ciascuna moltiplicata per il valore binario arbitrariamente assegnato.

	Variabile	Peso della variabile
1	Dati di localizzazione	1
2	Infrastruttura o parte delle infrastrutture coinvolte nel trattamento in Cloud (Private Cloud)	1
3	MS Exchange in Private Cloud	1
4	Dati trattati attraverso l'utilizzo di device portatili anche da parte di dipendenti	1
5	Dati relativi alla salute (appartenenza a categoria protetta o info su permessi per malattia o info su permessi per Maternità senza visibilità del referto medico)	2
6	Dati di identità per altre finalità	2
7	Finalità di marketing (invio comunicazioni commerciali)	2
8	Presenza di soggetti terzi (fornitori e non) con cui possono essere condivisi i dati	2
9	Infrastruttura o parte delle infrastrutture coinvolte nel trattamento in Cloud (Cloud / SaaS)	2
10	Permesso l'utilizzo di supporto removibili per il trasferimento dei dati	2
11	Dati che rivelano l'origine razziale o etnica	3
12	Dati che rivelano le opinioni politiche	3
13	Dati che rivelano le convinzioni religiose o filosofiche	3
14	Dati che rivelano l'appartenenza sindacale	3
15	Dati genetici	3
16	Dati biometrici	3
17	Dati relativi alla salute (con evidenza del referto medico e/o informazioni su particolari disabilità)	3
18	Dati relativi alla vita sessuale o all'orientamento sessuale di una persona	3
19	Profilazione e/o marketing su minori	3
20	Tracciamento categorie particolari di dati su minori	3
21	Carte di credito / CC Bancari	3
22	Dati di videosorveglianza	3
23	Finalità di profilazione	3
24	Dati Residenti fuori dall'UE	3

Tabella 4. Si riportano i pesi associati a ciascuna variabile identificata come portatrice di potenziali criticità all'interno del trattamento effettuato. I pesi assegnati fanno riferimento alla scala di valori riportata in Tabella 3.

3.3.2 Identificazione trattamenti critici

Si passa ora alla seconda parte della valutazione del rischio associato. Lo scopo è, data una valutazione complessiva del rischio di tutti i trattamenti attuati dall'Azienda Sanitaria, identificare quelli con rischio più elevato, col fine di attuare delle strategie di mitigazione ad hoc per ciascuno di quelli rilevati.

I trattamenti vengono dunque classificati sulla base del livello di criticità complessivo rilevato, in funzione del range opportunamente scelto per ciascun livello.

Sono considerati a criticità *lieve* tutti quei trattamenti la cui somma delle variabili è inferiore o pari a 10, o tali per cui sono presenti variabili con livello di criticità 2 in numero inferiore a 2 e nessuna variabile con livello di criticità 3.

Sono considerati a criticità *media* tutti quei trattamenti la cui somma delle variabili è compresa tra 10 e 19, o tali per cui sono presenti variabili con livello di criticità 2 in numero inferiore a 2 e nessuna variabile con livello di criticità 3.

Sono infine considerati trattamenti *critici* quelli la cui somma delle variabili è superiore o pari a 20, o tali per cui sono presenti variabili con livello di criticità 3 in numero almeno pari a 1.

Il criterio di valutazione descritto viene schematicamente riportato in Tabella 5.

Livelli di criticità del trattamento		
Range	*Livello di criticità*	*Descrizione*
$\sum n: k < 10$ $X_3 = 0 \wedge X_2 < 2$	Lieve	Basso livello di criticità del trattamento, in termini di accessi non autorizzati, modifica, cancellazione, furto e/o diffusione di dati personali
$\sum n: 10 \leq k \leq 19$ $X_2 \geq 2$	Moderato	Medio livello di criticità del trattamento in termini di accessi non autorizzati, modifica, cancellazione, furto e/o diffusione di dati personali
$\sum n: k \geq 20$ $X_3 \geq 1$	Critico	Alto livello di criticità in termini di accessi non autorizzati, modifica, cancellazione, furto e/o diffusione di dati personali

Tabella 5. Classificazione dei trattamenti sulla base del livello di criticità complessivo rilevato, in funzione del range associato a ciascun livello. X_2 variabile con livello di criticità 2; X_3: variabile con livello di criticità 3.

Per i trattamenti identificati come critici, il Titolare del trattamento – o più precisamente i soggetti incaricati dall'Azienda a questo scopo – effettueranno la valutazione del rischio che gli stessi trattamenti possono comportare per i diritti e le libertà delle persone fisiche.
È doveroso richiamare il fatto che i trattamenti forniti in ambito ospedaliero, anche se altamente critici, non possono essere soppressi, in quanto facenti parte di terapie sanitarie indispensabili alla salvaguardia della salute e alla cura della persona. Si dovrà dunque optare per una mitigazione del rischio, rendendolo quantomeno accettabile rispetto all'entità del trattamento in essere. Questo si otterrà attraverso la procedura di Data Protection Impact Assessment, ovvero la già citata Valutazione d'Impatto sulla protezione dei dati sanitari.

3.3.3 Valutazione d'impatto sulla protezione dei dati

La valutazione dell'impatto del rischio, come delineato dell'HSE[65] (Healt and Safety Executive), si sviluppa sulla base di cinque distinti e successivi step metodologici - ripresi, con qualche adattamento, anche nelle linee guida Aziendali:

Step 1: Valutazione del livello di Rischio Inerente

Step 2: Identificazione della tipologia di trattamento

Step 3: Valutazione dei controlli

Step 4: Definizione del livello di Rischio Residuo

Step 5: Identificazione dei trattamenti rischiosi ed adeguamenti conseguenti

Figura 8. Rappresentazione schematica degli step metodologici per il Data Protection Impact Assessment (DPIA) in base alle linee guida di Azienda Zero.

3.3.3.1 Valutazione del livello di Rischio Inerente

Il Data Protection Impact Assessment inizia con l'identificazione del rischio associato ad un dato trattamento, in termini di:

- Impatto, ovvero l'effetto che la diffusione dei dati potrebbe avere in primo luogo per l'interessato, e successivamente per l'Azienda;
- Probabilità di accadimento, ovvero la frequenza di accadimento di un rischio specifico, in diretta relazione dunque con la frequenza con cui il trattamento viene effettuato.

[65] La norma tecnica che ne definisce il profilo e le caratteristiche è la **UNI 11720:2018**, testo realizzato dall'Ente Italiano di Normazione.

Questa è una valutazione preliminare, che viene svolta quindi senza considerare gli eventuali presidi di controllo già attuati dall'Azienda per la sua mitigazione. Fa riferimento, infatti, alle potenzialità del rischio intrinseco di ciascun trattamento, rischio presente, come per tutti i trattamenti, per la sua particolare natura, in relazione come detto all'impatto ed alla frequenza. È compito e responsabilità del Titolare del trattamento analizzare qualitativamente l'impatto e la probabilità connessi a ciascun trattamento e determinare il livello di rischio inerente, sulla base dell'applicazione di specifiche scale di valutazione, di seguito riportate.

Criteri di valutazione dell'Impatto			
Scala	*Valutazione*	*Descrizione*	*Esempi a supporto*
4	Massimo	Informazioni che, in caso di divulgazione, avrebbero conseguenze di tipo irreversibile per l'Interessato.	Particolari giudiziari, relativi alla salute, etc. Le conseguenze rientrano nelle seguenti tipologie, o simili: elevati problemi finanziari, problemi fisici e psicologici a lungo termine, peggioramento dello stato di salute
3	Significativo	Informazioni che, in caso di divulgazione, avrebbero rilevanti, ma non irreversibili conseguenze per l'Interessato	Morosità esattoriale, dati personali limitati alle generalità o all'appartenenza etnica, politica, sindacale, etc. Le conseguenze rientrano nelle seguenti tipologie, o simili: perdita del lavoro, rischio di essere inserito in black list, discriminazione.
2	Limitato	Informazioni che, in caso di divulgazione, causerebbero problemi di carattere personale all'Interessato	Dettagli note spese, CV, retribuzione, benefit sociali. Le conseguenze rientrano nelle seguenti tipologie, o simili: danno economico, stress, impossibilità di accedere a determinati servizi/prodotti, lieve danno fisico.
1	Trascurabile	Informazioni quasi pubbliche che, in caso di divulgazione a persone o enti terzi non autorizzati, non creerebbero nessuna problematica all'interessato	Dati di dominio pubblico: numero di telefono, indirizzo, etc.

Tabella 6. Criteri di valutazione dell'impatto. Le tipologie di impatto sono state tradotte quantitativamente su una scala da 1 a 4, dove 1 corrisponde al valore minimo (Impatto = Trascurabile) e 4 corrisponde al valore massimo (Impatto = Massimo).

Criteri di valutazione della Probabilità di accadimento		
Scala	*Valutazione dell'evento*	*Descrizione*
4	Probabile	Il trattamento viene eseguito con cadenza giornaliera
3	Possibile	Il trattamento viene eseguito con cadenza settimanale
2	Improbabile	Il trattamento viene eseguito con cadenza mensile/trimestrale
1	Raro	Il trattamento viene eseguito con cadenza semestrale o annuale

Tabella 7. Criteri di valutazione delle Probabilità di accadimento. Le eventualità sono state tradotte quantitativamente su una scala da 1 a 4, dove 1 corrisponde al valore minimo (Probabilità = Evento raro) e 4 corrisponde al valore massimo (Probabilità = Evento probabile).

Il Rischio Inerente viene calcolato quantitativamente come prodotto tra i valori di Impatto e Probabilità associati a ciascun trattamento.

La valutazione dei livelli di rischio, basata su impatto e probabilità, all'interno dell'Azienda Ospedaliera Aulss 5 viene svolta per qualunque tipologia di evento avverso potenzialmente verificabile durante i trattamenti posti in essere dall'Azienda stessa. Per ogni diverso rischio (riguardante eventi avversi durante un trattamento, il rischio per la salute del paziente, per gli operatori coinvolti, il rischio di compromissione o manomissione dei dispositivi medici, etc.) si impiegano scale qualitative diverse. In questo frangente ci si limiterà a riportare quanto stabilito per il solo rischio relativo alla gestione dei dati sanitari dei pazienti.
La redazione delle tabelle di valutazione si è svolta in ottemperanza alle linee guida di Azienda Zero, tenendo conto dei dati trattati in Azienda e con riferimento ai criteri previsti dall'ULSS 5.

3.3.3.2 Identificazione della tipologia di trattamento

Questa fase consiste nell'identificazione delle modalità in cui è svolto il trattamento, ovvero il formato di raccolta dei dati appartenenti al paziente. All'interno del GDPR si riporta che i dati personali devono essere "conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati" [66]; non emerge dunque una via preferenziale di conservazione.
Ai fini della valutazione dei controlli, prevista nello step successivo, si includono le tre diverse modalità di classificazione:

- Trattamento effettuato unicamente in modalità cartacea;
- Trattamento effettuato unicamente in modalità elettronica;
- Trattamento effettuato in modalità sia cartacea che elettronica.

All'interno delle Aziende ospedaliere è questa terza categoria la più diffusa: i dati vengono raccolti ed elaborati in modo automatico dai software installati sui device medici ed il loro raggruppamento in un fascicolo elettronico comporta una notevole semplificazione della procedura; tuttavia, complice sia la necessità di renderlo consultabile a diversi operatori, spesso afferenti a diversi reparti, sia l'abitudine ad una determinata procedura, il trattamento viene redatto talvolta anche in modalità cartacea.

3.3.3.3 Valutazione dei controlli

I Titolare del trattamento effettua una valutazione qualitativa dei controlli necessari per i trattamenti, sia di quelli già svolti che di quelli ritenuti necessari, in base alla modalità in cui è

[66] Regolamento UE/2017/745, **art. 5**: *Principi applicabili al trattamento dei dati personali*, par.1

stato raccolto e catalogato il dato. Ogni controllo verrà poi valutato sulla base di una scala quantitativa, assegnando un peso a ciascuna verifica da effettuarsi.

Si utilizzerà la seguente assegnazione di valori:

- 0: Controllo nullo/assente;
- 0,5: Controllo parzialmente soddisfatto;
- 1: Controllo totalmente soddisfatto.

L'analisi del controllo per ciascun trattamento sarà poi ottenuta dalla somma pesata delle valutazioni assegnate a ciascun controllo.

Di seguito si riportano i controlli necessari per le diverse tipologie di trattamento.

- Tipologia di trattamento cartaceo

Valutazione di quattro controlli[67], di seguito elencati:

1. Identificazione chiara ed univoca di ruoli e responsabilità del controllo;
2. Svolgimento periodico delle attività di controllo, con eventuale decisione anche sulla periodicità necessaria;
3. Formale definizione di controlli e norme comportamentali nello svolgimento di procedure aziendali;
4. Verifica della presenza di misure di sicurezza fisiche per la gestione del documento cartaceo, come la presenza di armadi, casseforti, accesso alle chiavi, etc.

- Tipologia di trattamento elettronico

Valutazione di 14 controlli[68], associati a specifici obiettivi in materia di Sicurezza delle Informazioni, che possono essere riassunti come segue:

1. Politiche per la sicurezza delle informazioni - Fornire indicazioni di gestione e supporto per la sicurezza delle informazioni in accordo con i requisiti aziendali e regolamenti in essere.
2. Organizzazione della sicurezza delle informazioni - Stabilire un quadro di gestione chiaro per l'avvio ed il controllo periodico dell'implementazione di requisiti di sicurezza delle informazioni all'interno dell'organizzazione.
3. Sicurezza delle risorse umane – Formazione del personale (nel caso studio riportato, qualunque operatore sanitario, di qualunque tipologia, che abbia accesso ai dati sanitari, membri degli uffici tecnici e collaboratori esterni) per assicurare che siano comprese le responsabilità e che il comportamento sia conforme al ruolo assegnato.

[67] Definiti sulla base delle best-practice di Risk Management e tenendo conto della Metodologia di Risk Management ISO 31001.

[68] Coincidenti con i domini dello standard ISO/IEC 27001/2013.

4. Gestione degli asset - Identificare i beni di proprietà dell'Azienda e definire appropriate responsabilità per la loro protezione.
5. Controllo degli accessi - Prevenire l'accesso di utenti non autorizzati ai sistemi ed alle applicazioni.
6. Crittografia - Proteggere la riservatezza, l'autenticità o l'integrità delle informazioni attraverso strumenti di codifica del dato.

Nel corso della trattazione sono state riportare le diverse modalità attuabili per la protezione del dato sanitario; si è visto che non è necessario limitarsi alla sola crittografia, e che questa è implementabile anche assieme ad altre modalità operative. Di fatto, quanto riportato è una generalizzazione teorica, dal momento che linee guida metodologiche specifiche, per le diverse tipologie e di software di elaborazione e di dati trattati, non sono disponibili e andranno decise dalla singola Azienda in funzione delle problematiche riscontrate durante il processo di Data Risk Assessment.

7. Sicurezza fisica e ambientale - Prevenire accessi fisici non autorizzati, intromissioni e danni alle infrastrutture informative ed alle informazioni.
8. Sicurezza delle attività operative - Assicurare una gestione operativa corretta e sicura delle apparecchiature per l'elaborazione delle informazioni.
9. Sicurezza delle comunicazioni - Assicurare la salvaguardia delle informazioni in rete e la protezione dell'infrastruttura di supporto.
10. Acquisizione, sviluppo e manutenzione dei sistemi informativi - Assicurare che la sicurezza sia parte integrante dei sistemi informativi in tutto il ciclo di vita. Esso include anche i requisiti per i sistemi informativi che forniscono servizi sulle reti pubbliche.
11. Relazioni con i fornitori - Assicurare la protezione degli asset dell'Azienda accessibili ai fornitori.
12. Gestione degli incidenti relativi alla sicurezza delle informazioni - Assicurare un approccio efficace e consistente alla gestione degli incidenti di sicurezza informatica, inclusi tutti gli eventi e le vulnerabilità di sicurezza delle comunicazioni.
13. Disaster Recovery / Business Continuity - Continuità della sicurezza delle informazioni integrata nel sistema di gestione della continuità operativa dell'organizzazione.
14. Compliance - Evitare la violazione di obblighi legali, regolamentari o contrattuali relativi alla sicurezza delle informazioni.

Appare evidente che, nonostante la raccolta dei dati sanitari per ciascun paziente sia operativamente più semplice se effettuata in formato digitale / elettronico, la quantità di attenzione da prestare sia notevolmente più elevata. L'elevato numero di dispositivi, spesso interconnessi, in cui i dati possono essere gestiti e attraverso cui gli stessi dati possono viaggiare, unita alla quantità di personale che ha un accesso diretto o indiretto al dispositivo medico in uso, rendono necessaria un'analisi delle criticità che tenga conto di moltissimi aspetti relativi al trattamento dei dati.

- Tipologia di trattamento Cartaceo/Elettronico

In questo ultimo caso si tratterà di valutare controlli definiti sia per i trattamenti cartacei che per i trattamenti elettronici, per un totale di 18 controlli.

3.3.3.4 Definizione del livello di Rischio Residuo

Il valore del Rischio Residuo per ciascun trattamento è definito a partire dal valore di Rischio Inerente - calcolato quantitativamente come prodotto tra i valori di Impatto e Probabilità associati a ciascun trattamento - ed in considerazione del valore del controllo.
Si valuterà perciò, partendo dall'identificazione del rischio intrinseco del trattamento in esame, il livello di rischio che è ancora associato allo stesso trattamento in seguito alla valutazione dei controlli.

Il Rischio Residuo può essere identificato mediante l'applicazione del seguente algoritmo di calcolo:

$$R^r = R^i \cdot (1 - C)$$

dove:
R^r è il Rischio Residuo
R^i è il Rischio Inerente
C è il valore del controllo

3.3.3.5 Livelli di rischio dei trattamenti

L'identificazione dei trattamenti rischiosi è il passaggio finale del DPIA operato in Azienda. Il livello di rischio dei trattamenti viene determinato in considerazione del livello di Rischio Residuo, in base al quale viene operata una classificazione, riportata in modo riassuntivo in Tabella 8:

Trattamenti a rischio *trascurabile*: sono trattamenti con un valore di Rischio Residuo inferiore a 4 e per i quali non risulta necessario effettuare azioni di adeguamento;

Trattamenti a rischio *basso*: trattamenti che presentano un valore del Rischio Residuo compreso 4 e 8; anche per questi trattamenti non risulta necessario effettuare azioni di adeguamento; tuttavia, è sempre possibile valutare delle azioni per il miglioramento del sistema di prevenzione e protezione del rischio;

Trattamenti a rischio *medio*: trattamenti che presentano un valore di Rischio Residuo compreso tra 8 e 12. Per questa tipologia di trattamenti è consigliato, ma non obbligatorio, individuare possibili strategie di ottimizzazione del sistema di prevenzione e protezione del rischio;

Trattamenti a rischio *alto*: trattamenti che presentano un valore del Rischio Residuo superiore a 12.

È quest'ultima la tipologia di trattamenti per i quali è assolutamente indispensabile individuare e quindi attuare azioni di perfezionamento del sistema di prevenzione e protezione del rischio. In questo caso, inoltre, il Titolare del trattamento è obbligato a richiedere la consultazione preventiva dell'autorità di controllo in relazione al trattamento.

Livello di Rischio Residuo	**Intervallo numerico per l'identificazione del rischio**
Trascurabile	$0 \leq R^r < 4$
Basso	$4 < R^r < 8$
Medio	$8 < R^r < 12$
Alto	$12 < R^r \leq 16$

Tabella 8. Fasce di livello per l'identificazione del rischio associato ai trattamenti.

3.4 Valutazione di impatto e mitigazione dei rischi

In base ai dati preliminari raccolti è stata redatta una prima battuta del Registro dei Trattamenti per il reparto di Radiologia (Allegato 1) che raccoglie una descrizione sommaria delle prestazioni, delle tipologie di dati trattati e delle modalità d trattamento a cui questi sono sottoposti.

Il passaggio immediatamente successivo prevede l'inizio di un processo di valutazione del rischio per i trattamenti riportati nel registro stesso, e quindi di una conseguente valutazione di impatto sulla protezione dei dati.
Entrambe le attività dovranno necessariamente essere svolte basandosi sulle diverse tipologie di dati che vengono raccolti e gestiti e la cui comunicazione e trasmissione prevede il passaggio tra diversi sistemi a livello di rete ospedaliera.

Il procedimento che seguirà - inerente al reparto di Radiologia ma replicabile per tutte le diverse Unità - è stato svolto utilizzando le modalità operative precedentemente redatte e riportate; in breve, per la prima fase di Risk Assessment, si procederà come segue:

i. Analisi preliminare di tutte le variabili associate ai diversi trattamenti operati all'interno del reparto esaminato (riportati all'interno del Registro dei Trattamenti);
ii. Riscontro del livello di criticità nell'analisi delle variabili
iii. Assegnazione del livello di criticità complessivo del trattamento.

A questo punto, nel caso in cui dalle precedenti considerazioni il trattamento dovesse risultare ad elevata criticità – e così sarà, si procederà con lo step successivo di Data Protection Impact Assessment, secondo le modalità descritte:

i. Analisi del rischio inerente per il trattamento in esame;
ii. Valutazione dell'efficacia dei controlli necessari al monitoraggio di eventuali fattori di rischio;
iii. Stima del Rischio Residuo, a partire dal livello di Rischio Inerente, dopo opportuna valutazione dei controlli.

3.4.1 Procedura di Risk Assessment per le Workstation di Radiologia

È già stato riportato, nel corso della seguente trattazione, che è possibile realizzare sia un Registro dei Trattamenti che valuti separatamente ogni diverso trattamento, sia redigere un unico Registro che raccolga assieme trattamenti diversi ma sovrapponibili, tali per cui dunque le classificazioni dei dati raccolti e le modalità di gestione ed elaborazione degli stessi sia in parte o in tutto identica per trattamenti diversi.
Per quanto riguarda la UOC Radiologia, dal momento che la gestione dell'intera filiera è in mano tutta al medesimo programma (suitEstensa®), lo smistamento, l'elaborazione, la refertazione, le modalità di trattamento e di conseguenza i rischi associati al trattamento sono pressoché gli stessi. Per questo motivo si è scelto di operare una valutazione più snella

svolgendo, per ogni tipologia di trattamento operata dalle Workstation di Consultazione e di Refertazione, un'unica analisi complessiva.
Più precisamente, volendo procedere in considerazione alle prestazioni sanitarie erogate dal servizio in esame, è stato verificato che le Ecografie, gli esami di sala operatoria, le Densitometrie, le Radiografie, le Risonanze Magnetiche, le TAC ed infine le Ortopantomografie prevedono, per la loro corretta esecuzione, sia identici trattamenti sia la gestione delle medesime categorie di dati.
Un discorso a parte riguarda invece le Mammografie, che hanno un iter di gestione dei dati raccolti che prevede un passaggio di comunicazione aggiuntivo rispetto agli altri esami. L'analisi di questo caso particolare dovrà dunque essere integrata con ulteriori considerazioni, questo verrà illustrato in un secondo momento.

Infine, verranno svolte l'analisi del rischio e le consecutive valutazioni anche per quanto riguarda i dati raccolti dai dispositivi elettromedicali utilizzati per l'esecuzione della prestazione. Si tratterà di analizzare, per ogni device, se raccoglie e conserva dati durante lo svolgimento dell'esame e, se questo avviene, le modalità di gestione e protezione degli stessi. Questa valutazione sarà naturalmente di entità inferiore, dato che inferiore è la mole e la serietà dei dati eventualmente raccolti da questi dispositivi, e possiamo già assumere che le criticità riscontrate saranno ad un livello sufficientemente basso da non prevedere particolari strategie di miglioramento prestazionale.

3.4.1.1 Definizione del livello di criticità del trattamento

In base ad analisi svolte sul campo, le variabili associate ai trattamenti offerti dalla UOC Radiologia - per quanto concerne i dispositivi preposti alla raccolta ed alla gestione del dato – e che possono essere considerate potenzialmente critiche sono elencate in Tabella 9.

I trattamenti vengono classificati sulla base del livello di criticità complessivo rilevato. La scelta del livello di criticità si basa suoi due criteri distinti: la somma dei pesi assegnati alle variabili e la presenza di variabili a rischio elevato; il secondo criterio, in caso di incertezza nell'assegnazione, ha precedenza sul primo.

	Variabile	Peso della variabile
1	Dati di localizzazione	1
2	Infrastruttura o parte delle infrastrutture coinvolte nel trattamento in Cloud (Private Cloud)	1
3	Dati trattati attraverso l'utilizzo di device portatili anche da parte di dipendenti	1
4	Presenza di soggetti terzi (fornitori e non) con cui possono essere condivisi i dati	2
5	Permesso l'utilizzo di supporto removibili per il trasferimento dei dati	2
6	Dati che rivelano l'origine razziale o etnica	3
7	Dati relativi alla salute (con evidenza del referto medico e/o informazioni su particolari disabilità)	3
8	Dati Residenti fuori dall'UE	3

Tabella 9. Pesi associati a ciascuna variabile identificata come portatrice di potenziali criticità all'interno del trattamento effettuato, per quanto concerne i dispositivi preposti alla raccolta ed alla gestione del dato (Workstation di Elaborazione e Refertazione). L'assegnazione dei pesi fa riferimento alla *Tabella 4.*

Nel caso in esame:

- La somma delle variabili dà come risultato 16;
- Sono presenti tre variabili con livello di criticità 3.

I trattamenti effettuati presso la UOC Radiologia dell'Ospedale di Rovigo sono dunque da intendersi come critici, e per questo motivo risulta opportuno proseguire l'analisi al livello successivo, ovvero alla valutazione del rischio associato per ciascun trattamento.

3.4.2 Data Protection Impact Assessment per le Workstation di Radiologia

Prima di procedere con l'analisi si ritiene necessario ricordare la differenza che sussiste tra rischio e criticità:

> Rischio: evento o condizione incerta che, se si verifica, ha un effetto negativo su uno o più obiettivi del progetto.
>
> Criticità: condizione di pericolo potenziale che, se non adeguatamente monitorata, può portare al verificarsi di un rischio.

L'uso del termine *critico* non deve perciò destare particolare preoccupazione: ad una prima analisi, qualunque trattamento di dati che avviene all'interno del contesto ospedaliero risulta critico. Ciò è dovuto al fatto che i dati che vengono raccolti per lo svolgimento degli esami sono particolarmente delicati e, per necessità di gestione e corretta erogazione del servizio sanitario, gli stessi devono essere messi in comunicazione tra diverse realtà informatiche e

non che consentiranno ai medici di avere prontamente a disposizione il dato clinico con riferimento allo specifico paziente in caso di necessità.
È per questo motivo che è indispensabile operare una valutazione, come quella che seguirà, per verificare in primo luogo se le criticità riscontrate possono portare ad effettivi rischi per gli interessati; successivamente, la verifica riguarderà come questi rischi possono essere gestiti e le probabilità di accadimento essere minimizzate ad un livello accettabile, proporzionale al beneficio ottenuto dalla prestazione sanitaria.

3.4.2.1 Rischio Inerente

La valutazione del rischio inerente, ovvero il rischio associato ad un dato trattamento, viene effettuata in termini di impatto della diffusione e probabilità di accadimento.
Dopo un'analisi svolta con il team di Radiologia si è giunti alla conclusione che i trattamenti erogati:

- Hanno un impatto *massimo*, difatti la diffusione volontaria e/o involontaria, la manomissione o anche la perdita dei dati comportano un elevato rischio per il paziente, con conseguenze sia dal punto di vista medico che economico. Il valore numerico assegnato a questa tipologia di impatto è 4.
- Comportano una presumibilità di accadimento di eventi avversi *probabile*, dal momento che ogni tipologia di esame viene effettuata, quando non giornalmente, a giorni alterni. Il valore numerico assegnato a questa probabilità è 4.

Il livello di Rischio Inerente R_I è calcolato quantitativamente come prodotto tra i valori di Impatto v_I e Probabilità p_I associati a ciascun trattamento:

$$R_I = v_I \cdot p_I = 4 \cdot 4 = 16$$

Anche in questo contesto si ribadisce che valori così elevati sono in realtà perfettamente ragionevoli, se si pensa alla mole di dati che giornalmente vengono raccolti e gestiti per ciascuna prestazione. Il livello di Rischio Inerente identifica e raccoglie tutte le possibili cause di rischio per un singolo trattamento, legate alla natura appunto intrinseca del trattamento stesso, ed è per questo motivo che vengono effettuati una serie di controlli allo scopo di mitigare al massimo sia gli impatti, ma soprattutto le probabilità di accadimento, che rimarrebbero invariabilmente elevate se non sottoposte ad opportuni controlli.

3.4.2.2 Valutazione dei controlli

I controlli da effettuarsi sono di diversa natura e cambiano in base alle modalità di raccolta dei dati. Per quanto riguarda il reparto di Radiologia, il trattamento è svolto in modalità elettronica nella maggior parte dei casi, mentre la modalità cartacea viene impiegata principalmente in seguito a guasti, malfunzionamenti o blocchi temporanei di sistema (programmati o non).

Con lo scopo di ottenere un'analisi dei rischi il più esaustiva possibile, si è deciso di procedere con la valutazione dei controlli, sempre per quanto riguarda i software di gestione installati sulle Workstation, per entrambe le modalità.

Per quanto riguarda i controlli destinati alla corretta gestione del dato trattato in modalità cartacea, si è già detto che questa modalità riguarda solo particolari casi in cui il sistema informatico solitamente impiegato non risulta funzionante o ha subito un temporaneo blocco. In queste circostanze il personale segue delle linee guida aziendali[69] ben precise, che permettono l'esatta definizione sia di procedure per la raccolta e l'archiviazione di dati e immagini diagnostiche, sia di ruoli e responsabilità del personale ospedaliero.

Si tratta di una serie di procedure ben consolidate all'interno del reparto, questo perché il sistema centralizzato di gestione dati RIS/PACS è di relativamente recente introduzione e dunque la gestione cartacea delle cartelle-pazienti è stata la modalità operativa di elezione per molto tempo.

Le modalità operative adottate in contesti di blocco del sistema vengono descritte brevemente di seguito:

1. Gestione delle immagini: visualizzazione delle immagini DICOM tramite monitor delle consolle delle diagnostiche, con possibilità di stampa su lastra; ogni polo ospedaliero (Adria, Rovigo, Trecenta) ha a disposizione opportune stampanti nel proprio reparto.
2. Gestione della refertazione: può essere solo cartacea e, in caso di prestazione effettuata in urgenza, il referto deve essere riportato nel modulo di richiesta d'esame e inviato al servizio richiedente (trattenendo una copia presso la struttura erogante).
3. Gestione ripristino sistema RIS-PACS:
    - Trasferimento al PACS delle immagini temporaneamente memorizzate nelle relative diagnostiche ("memoria temporanea o tampone");
    - Trascrizione dei referti sul RIS, con certificazione di operazione eseguita per "fermo del sistema" (necessario indicare giorno e orario in nota al referto);

[69] "Procedura Aziendale per la gestione delle interruzioni del Sistema RIS-PACS" del 16/02/2010.

- Redazione di un elenco delle prestazioni eseguite nel periodo di "fermo del sistema" che viene trasmetto come atto ufficiale sia alla Struttura che le ha eseguite sia alla Direzione Medica;
- Attivazione, durante tutto il processo di "fermo del sistema" e relativo ripristino, di un Operatore Informatico (amministratore di Sistema interno all'Azienda o tecnico afferente alla Ditta fornitrice) per il monitoraggio delle operazioni e per svolgere verifiche di sistema.

Le modalità riportate vengono rese note agli operatori al momento dell'assunzione, ma non vengono svolti aggiornamenti periodici del personale e, per questo motivo, la valutazione per quanto riguarda la formazione del personale ha un valore più basso rispetto agli altri controlli; una formazione periodica è indispensabile per una corretta presa di coscienza dell'importanza della tematica della privacy sia da parte sia del personale neoassunto, sia per i membri attivi da più tempo.

Una considerazione conclusiva riguarda la conservazione del dato cartaceo. Nel caso in cui ci si trovasse costretti alla gestione cartacea delle informazioni del paziente ("fermo del sistema"), se da un lato le immagini sono inserite in un server provvisorio e poi spostate al server centrale una volta ripristinata l'attività, i documenti cartacei che raccolgono i dati, anche in seguito ad inserimento nel Sistema RIS/PACS, non verranno smaltiti; resteranno a disposizione (opportunamente conservati e celati) sia anagrafiche, prenotazioni, prestazioni, esiti, sia l'elenco delle operazioni svolte, anch'esso contenente dati sensibili dei pazienti trattati, in duplice copia, per un periodo di tempo equivalente al tempo di conservazione del dato in formato elettronico.

Questa modalità operativa, che si rende necessaria per scongiurare la perdita accidentale di dati essenziali per una corretta erogazione del servizio sanitario ed il monitoraggio della salute dei pazienti, porta però con sé una criticità: è noto, infatti, che più sono numerose le copie disponibili di uno stesso dato, più aumenta il rischio di manomissione, perdita o furto del dato stesso. Le uniche modalità di intervento e tutela in questo senso, a meno di modificare la procedura precedentemente descritta, e non è lo scopo della presente trattazione, consistono nell'assicurarsi che l'accesso alle casseforti contenenti queste documentazioni sia riservato al solo personale addetto e che sia protetto con misure fisiche opportune. Tutto questo è stato verificato in prima persona, constatando tuttavia la necessità che vengano incrementati i controlli relativi alla gestione fisica delle cartelle e dei dati anagrafici raccolti e conservati in formato cartaceo, considerata la mole di materiale attualmente presente in reparto.

Per quanto riguarda invece i controlli destinati alla corretta gestione del dato trattato in modalità elettronica, sono stati presi in considerazione i 14 controlli già elencati al Paragrafo 3.3.3.3, ed opportunamente valutati assieme al team Radiologico ed informatico. Seguono alcune considerazioni sulle valutazioni date.

La rete aziendale dell'ULSS 5, come già riportato in precedenza, è una rete locale che permette l'interconnessione tra i reparti e tra i poli ospedalieri, con opportuna protezione hardware e software (Firewall) che implementa le seguenti funzioni:

- Controllo degli accessi;
- Autenticazione degli utenti;
- Virtual Private Network (VPN);
- Protezione del contenuto (ma non attraverso un sistema di Crittografia);
- Reporting, ovvero rilevamento di attività illegali e tentativi di accesso indesiderati.

In quanto alla Crittografia, della quale si è accennato all'interno della trattazione e che costituisce un'utile risorsa per la protezione dei dati raccolti, questa non viene impiegata nel contesto della UOC Radiologia, né tantomeno a livello di comunicazione di dati personali e sanitari nei rimanenti reparti dell'Ospedale. Difatti, il sistema di trasmissione dati con standard HL7 non prevede by design alcun supporto per la crittografia, limitandosi a suggerire la necessità, per ogni struttura Ospedaliera che ne faccia uso, di adottare i propri sistemi di protezione, adattati alle esigenze specifiche. È già stata riportata la modalità di accesso ai diversi sistemi – con necessaria chiave di autenticazione e doppia autenticazione per i medici refertatori – nonché l'utilizzo di una LAN con rete Intranet; tuttavia, resta il fatto che le stringhe di comunicazione in formato HL7 non siano sottoposte a nessun tipo di mascheramento e che la chiave per la loro lettura sia disponibile anche online, in documenti rilasciati dalle stesse ULSS. In Figura 9 si riporta un esempio di comunicazione con standard HL7.

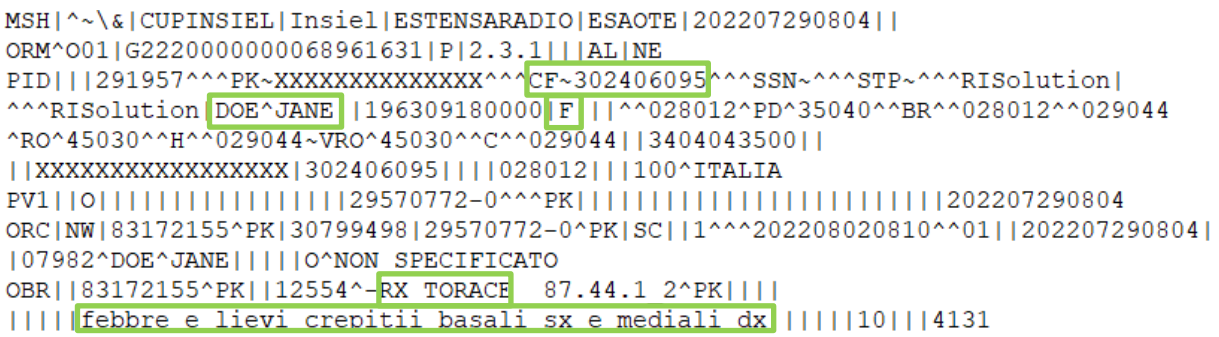


Figura 9. Esempio di Stringa HL7 generata dal Sistema Informativo RIS in uscita, verso il reparto di Radiologia, che consente la comunicazione con l'elettromedicale preposto allo svolgimento di un generico esame.
Tra i diversi segmenti di cui è costituito questo frammento di codice, si evidenziano quelli di maggiore interesse per lo scopo della trattazione: MSH (MeSsage Header), che contiene mittente e ricevente del messaggio; nel caso in esame il messaggio è stato generato dal CUP ed è diretto al software suitEstensa®, con associato dunque il codice univoco della workstation e relativo dispositivo medico al quale il messaggio è indirizzato, oltre alla data di creazione del messaggio. PID contiene le informazioni identificative del paziente, ed è possibile notare che le informazioni principali sono facilmente identificabili: è ben visibile il nome della paziente (fittizia) che verrà sottoposta ad esame, il suo codice fiscale, il sesso e l'indirizzo.
Nel segmento OBR, infine, sono visibili eventuali informazioni mediche con le quali il paziente si presenta all'esame, nonché la tipologia di esame stessa.

Quella di non utilizzare modalità di oscuramento delle informazioni attraverso codici crittografici è stata una decisione assunta non solo per l'Ospedale di Rovigo ma naturalmente per tutte le realtà ospedaliere afferenti all'ULSS5, nonché da molte altre ULSS e da cliniche di altro tipo.

È già stata riportata la necessità, in un contesto sanitario, di bilanciare quelli che sono i diritti alla riservatezza ed alla protezione dei dati personali per i pazienti che si rivolgono a questo servizio, con la capacità di garantire la corretta e funzionale (nonché celere) esecuzione delle prestazioni sanitarie erogate. Per far questo i tecnici di Radiologia, i medici e gli operatori hanno assoluta necessità di conoscere in tempi brevi esami e prestazioni associate al singolo paziente, a tutela del paziente stesso. Anche il tecnico informatico che si occupa della manutenzione del software di raccolta e gestione, nonostante sia afferente ad una ditta esterna, ha accesso ai dati sensibili del paziente, per renderli disponibili a medici ed operatori sanitari in caso di malfunzionamenti. Si ritiene che la codifica di queste informazioni, anche se a salvaguardia dei dati sensibili dei pazienti, provocherebbe un rallentamento delle operazioni per i medici e, in caso di errata decodifica, situazioni ancor più gravi. La privacy degli interessati passa dunque in secondo piano rispetto alla possibile corruzione dell'integrità dei dati, in grado di portare al peggioramento del quadro clinico del degente.

Ulteriori considerazioni riguardo alle modalità di valutazione dei controlli ed assegnazione del valore finale:

> Le politiche per la sicurezza delle informazioni sono ben redatte ma scarsamente rispettate. Un esempio di quanto appena riportato è costituito, ad esempio, dalla

possibilità, da parte del personale ospedaliero con accesso per consultazione alle immagini mediche, di effettuare un download delle stesse sul dispositivo, o di effettuare uno screeenshot della schermata e trasferire quanto raccolto su chiavetta. Questa facilità di mobilizzazione di immagini ed informazioni mediche comporta un rischio molto elevato di diffusione e dispersione; inoltre, la presenza delle medesime informazioni su dispositivi diversi da quelli utilizzati nel contesto ospedaliero renderebbe necessario l'implementazione di tecniche di sicurezza aggiuntiva su dispositivi che, essendo ad uno personale, hanno pieno accesso alla rete e non sempre dispongono di un adeguato antivirus o di una VPN. La soluzione a questa incresciosa situazione consisterà, nell'immediato futuro, nell'impossibilità di utilizzare le porte di accesso USB nelle workstation ospedaliere e di una opportuna modifica del software, in modo che il dispositivo non sia in grado di acquisire la schermata quando il software suitEstensa® è aperto ed attivo. Si sta lavorando a questo in collaborazione con il CED (Centro Elaborazione Dati) Ospedaliero.

Le indicazioni per la gestione degli eventuali rischi associati alla sicurezza delle informazioni vengono fornite alle Risorse Umane ed al personale ospedaliero di ogni tipo esclusivamente in fase di assunzione; si ritiene tuttavia siano necessari aggiornamenti frequenti del personale, in vista dell'evoluzione delle normative e delle sempre crescenti criticità associate all'ambito "privacy".

La sicurezza delle attività operative e delle comunicazioni è efficiente ma potrebbe essere migliorata, favorendo una migliore comunicazione tra l'azienda fornitrice del software di gestione delle anagrafiche ed il CED e una conseguente più efficace gestione dei processi informatici che si svolgono nel contesto ospedaliero.

In seguito alle considerazioni fatte, ogni controllo è stato valutato sulla base di una scala quantitativa, assegnando un peso a ciascuna verifica da effettuarsi.
Si ricorda la scala di valori scelta:

- 0: Controllo nullo/assente;
- 0,5: Controllo parzialmente soddisfatto;
- 1: Controllo totalmente soddisfatto.

L'assegnazione per ciascun controllo è stata effettuata in seguito a diversi colloqui sia con il capo tecnico, il dott. Fiorese, sia con il responsabile informatico della ditta Esaote, l'Ing.

Tessarollo, che ha in carico il software utilizzato per lo svolgimento degli esami, ed è riportata nelle Tabelle seguenti.

Trattamento cartaceo dei dati raccolti		
	Controlli	*Valore*
1	Identificazione di ruoli e responsabilità	1
2	Svolgimento periodico delle attività di controllo	0.5
3	Definizione di controlli e norme comportamentali	0.5
4	Presenza di misure di sicurezza fisiche per la gestione del documento cartaceo (armadi, casseforti, etc.)	1

Tabella 10. Valore assegnato ai controlli per il trattamento dei dati svolto con modalità cartacea.

Trattamento elettronico dei dati raccolti		
	Controlli	*Valore*
1	Politiche di sicurezza delle informazioni	0
2	Quadro di gestione per implementazione di requisiti di sicurezza	0.5
3	Formazione del personale	0
4	Gestione degli asset	1
5	Controllo degli accessi	1
6	Crittografia	0
7	Sicurezza fisica e ambientale	1
8	Sicurezza delle attività operative	0.5
9	Sicurezza delle comunicazioni	0.5
10	Acquisizione, sviluppo e manutenzione dei sistemi informativi	1
11	Relazioni con i fornitori	1
12	Gestione degli incidenti relativi alla sicurezza delle informazioni	1
13	Disaster Recovery e Business Continuity	1
14	Compliance in ambito di obblighi legali, regolamentari o contrattuali relativi alla sicurezza delle informazioni.	0.5

Tabella 11. Valore assegnato ai controlli per il trattamento dei dati svolto con modalità elettronica.

Alla fine, la valutazione del controllo complessiva per ciascun trattamento è ottenuta dalla somma ponderata delle singole valutazioni; poiché durante l'analisi non sono state riscontrate particolari differenze tra i controlli da effettuarsi, in termini di priorità o di rilevanza, per gli scopi della valutazione ad ogni controllo è stato assegnato un peso unitario.

Calcolo del Livello di Controllo:

$$C = \frac{\sum_{i=1}^{n} p_i \cdot v_i}{\sum_{i=1}^{n} v_i}$$

dove:

v_i è il controllo da effettuare

n è il numero totale di controlli, 4 per trattamenti cartacei e 14 per trattamenti elettronici

p_i è il valore assegnato al controllo, $p_i \in [0,1]$.

Poiché ogni controllo è considerato di peso unitario possiamo riscrivere la formula come:

$$C = \frac{\sum_{i=1}^{n} p_i \cdot var_i}{n}$$

Si utilizzeranno le espressioni:

$$p_0 = 0$$
$$p_{0.5} = 0.5$$
$$p_1 = 1$$

Il valore ottenuto dal calcolo del Livello di Controllo, approssimato al terzo decimale, è:

$$C = \frac{3 \cdot p_0 + 6 \cdot p_{0.5} + 9 \cdot p_1}{18} = 0.667$$

3.4.2.3 Rischio residuo per le Workstation di Radiologia

Si passa a questo punto alla valutazione del valore di rischio residuo, si ricorda la formula:

$$R^r = R^i \cdot (1 - C)$$

In base ai dati precedentemente raccolti, si giunge al risultato finale, che verrà inserito all'interno del Registro dei Trattamenti (Tabella 12):

$$R^r = 16 \cdot (1 - 0.667) = 5.328$$

Descrizione sintetica dell'attività di trattamento dati supportata dall'apparato	Dati trattati		Modalità trattamento		Suddivisione apparecchiatura in base ai rischi: - apparecchiatura stand alone - apparecchiatura con sistema proprietario collegata alla rete dati - apparecchiatura PC based collegata alla rete dati	Misure tecniche di protezione dei dati	Misure fisiche di protezione dei dati	Rischio residuo
	personali	sensibili	conservati	archiviati				
[Monitor BARCO 3MP] Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; Accesso solamente mediante rete Intranet Aziendale; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**
[PC Workstation IBM Z51] Generazione di referti con invio a RIS/PACS; Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione immagini, referti e cartelle cliniche.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Ulteriore autenticazione mediante card e secondo pin; Nessun accesso alla visualizzazione web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**

Tabella 12. Estratto del Registro dei Trattamenti che riporta la descrizione di una Workstation di Consultazione (prima riga, azzurro) e la descrizione di una Workstation di Refertazione (seconda riga, blu). Si noti che, nonostante dalle analisi sia stato appurato che il valore di Rischio Residuo è il medesimo per i due dispositivi, trattandosi del medesimo software operativo installato e di una analoga gestione dei dati personali e sanitari, all'interno del Registro devono comunque essere inserite nella descrizione le differenze operative esistenti tra i due. In questo caso, viene riportata la possibilità addizionale, per le Workstation di Refertazione, di permettere la redazione e la consultazione di referti, oltre all'assenza di una visualizzazione Web.

Si tratta di un rischio basso, che non comporta quindi la necessità di apportare modifiche rilevanti alla gestione del dato da parte sia del personale che del software di elaborazione.

Tuttavia, quello della valutazione del rischio è un processo continuo che permette (e richiede) un costante miglioramento, ed anche in casi di rischio così esiguo sono comunque operabili strategie di perfezionamento delle procedure esistenti.

Si ricorda che il presente valore di Rischio Residuo è relativo alle sole Workstation – di refertazione e di consultazione - del reparto di Radiologia, e non del reparto nel suo complesso. Seguiranno infatti ulteriori valutazioni tecniche per quanto riguarda i singoli dispositivi medici che vengono impiegati per lo svolgimento degli esami radiologici: in questo modo sarà possibile ottenere un Registro dei Trattamenti che fornisca un'idea complessiva delle modalità di protezione dei trattamenti operati nel reparto in esame.

3.4.2.4 Primo complemento all'analisi: Microfoni di refertazione e Robot di masterizzazione

Associati alle Workstation di Refertazione è possibile trovare i microfoni modello "Speech Mike" che, collegati tramite cavo a tali monitor, permettono al medico di comporre il referto tramite registrazione vocale. Tali dispositivi costituiscono esclusivamente un tramite per rendere più agevole la refertazione e non sono in grado di mantenere in memoria dati personali e sanitari: l'unica informazione che riescono a memorizzare è un numero limitato di parole ripetute, che variano in base al medico che li utilizza e che non sono in alcun modo collegabili ad un paziente specifico. Il medico può infatti utilizzare il microfono per riportare considerazioni di carattere sanitario, ma le generalità del paziente non possono essere registrate e vanno inserite manualmente.

Il microfono non ha collegamenti alla rete e si spegne automaticamente una volta appoggiato sul tavolo, grazie ad un sensore di movimento. In base a queste considerazioni, svolgendo la medesima procedura precedentemente adottata per le workstation, risulterà che non ci sono variabili che evidenziano criticità, dal momento che appunto in nessun modo è possibile utilizzarli per conservare la registrazione. Per tale motivo il rischio associato è pari a 0 (come riportato in Tabella 13).

Descrizione sintetica dell'attività di trattamento dati supportata dall'apparato	Dati trattati		Modalità trattamento		Suddivisione apparecchiatura in base ai rischi: - apparecchiatura stand alone - apparecchiatura con sistema proprietario collegata alla rete dati - apparecchiatura PC based collegata alla rete dati	Misure tecniche di protezione dei dati	Misure fisiche di protezione dei dati	Rischio residuo
	personali	sensibili	conservati	archiviati				
[Microfono SpeechMike PRO] Microfono di dettatura per la stesura di referti. Possibilità di mantenere in memoria i termini più utilizzati.	Sì	Sì	No	No	Apparecchiatura stand-alone con software proprio dedicato; collegamento con le Workstation attraverso cavo USB. Nessun collegamento alla rete.	Time-out della sessione automatico a cessato utilizzo. I dati passano dal microfono alla workstation senza conservazione della registrazione sul dispositivo; nessun collegamento con la rete.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**0**

Tabella 13. Estratto del Registro dei Trattamenti che riporta la descrizione di un microfono da refertazione. Tale dispositivo non ha accesso alcuno alla rete e trasmette le informazioni raccolte mediante un collegamento alla Workstation di Refertazione con cavo USB. Non è in grado né di archiviare né di conservare alcuna informazione che costituisca un rischio per la sicurezza e la privacy dei pazienti e pertanto il suo valore di Rischio Residuo è da considerarsi nullo.

Per quanto riguarda invece i Robot di masterizzazione, si tratta di particolari dispositivi che, collegati direttamente al Sistema RIS/PACS attraverso il medesimo software di gestione presente sulle Workstation, permettono la copiatura su CD delle immagini e del referto del medico. Tali dispositivi sono associati ad un PC che gestisce le informazioni che devono masterizzare e non conservano in memoria nessuna informazione. L'accesso a questi monitor – non sono identificabili come Workstation ma presentano le medesime caratteristiche informatiche - è riservato al personale ospedaliero dell'ufficio preposto. Trattandosi dunque sempre dello stesso software e non avendo considerazioni aggiuntive da fare sulla sicurezza fisica delle postazioni e sul controllo degli accessi, in linea con quanto riportato nell'analisi precedente, si ritiene di poter associare a tali dispositivi il medesimo valore di Rischio Residuo assegnato alle Workstation, pari quindi a 5.83 (Tabella 14), perché le criticità individuate sono perfettamente sovrapponibili, così come i controlli che vengono effettuati.

Descrizione sintetica dell'attività di trattamento dati supportata dall'apparato	Dati trattati		Modalità trattamento		Suddivisione apparecchiatura in base ai rischi: - apparecchiatura stand alone - apparecchiatura con sistema proprietario collegata alla rete dati - apparecchiatura PC based collegata alla rete dati	Misure tecniche di protezione dei dati	Misure fisiche di protezione dei dati	Rischio residuo
	personali	sensibili	conservati	archiviati				
[Robot di masterizzazione RIMAGE 2000I] Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni mediche associate.	No	No	No	No	Apparecchiatura PC based collegata alla rete dati; medesimo software di gestione anagrafiche ed immagini installato sulle workstation.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; Accesso solamente mediante rete Intranet Aziendale; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**

Tabella 14. Estratto del Registro dei Trattamenti che riporta la descrizione di un Robot di masterizzazione. Il software installato sul pc collegato al Robot è sempre suitEstensa®, pertanto la modalità di gestione del dato è sovrapponibile a quella riportata durante l'analisi delle Workstation. Tali dispositivi vengono impiegati per limitare il numero di personale che può avere accesso ad informazioni particolarmente sensibili.

3.4.2.5 Secondo complemento all'analisi: Iter di gestione degli esami mammografici

Come precedentemente introdotto, le prestazioni mammografiche che vengono svolte nel contesto del reparto di Radiologia richiedono una narrazione a complemento di quanto è già stato riportato a livello generale per gli altri esami; si premette già che queste ulteriori considerazioni non comporteranno una modifica del procedimento o dei risultati della Valutazione del Rischio Associato.

Gli esami di screening mammografico, infatti, al netto degli elettromedicali utilizzati per lo svolgimento fisico dell'esame, possiedono una procedura di gestione dei dati raccolti (anagrafiche ed informazioni mediche rilevate) distinta rispetto alle altre prestazioni erogate dal reparto di Radiologia, principalmente per due aspetti cardine: refertazione e comunicazione dell'esito.

Per le diverse ULSS del Veneto è stato adottato nel 2013 il progetto "Sistema Rete Mammografica", che vede l'utilizzo di un software regionale centralizzato per la gestione delle campagne di screening e la raccolta di tutte le informazioni cliniche e amministrative da esse derivate, sfruttando il sistema informativo per gli screening oncologici. Grazie all'adozione di questo sistema, presso l'Azienda Ospedaliera si effettua una tipologia di

refertazione degli esami mammografici a “singolo cieco” o a “doppio cieco”, prevista dal protocollo scientifico dettato dalle Linee Guida Nazionali[70].

Il giorno previsto per l’esame il sistema RIS/PACS fornisce, alle workstation collegate agli elettromedicali coinvolti, le informazioni della paziente – nelle stesse modalità già descritte. Una volta svolto l’esame, un medico radiologo fa la prima refertazione ed un secondo medico, all’oscuro del contenuto della refertazione del collega, effettua una seconda refertazione indipendente: si tratta di refertazione a *singolo cieco*. Nel caso in cui gli esiti siano discordanti un terzo medico fornisce un ulteriore referto indipendente – è il caso della refertazione a *doppio cieco* – e questo stabilisce un esito definitivo che deve essere comunicato alla paziente.
I dati sanitari raccolti vengono quindi inviati all’Ufficio Screening, che si occupa della gestione delle lettere di risposta, mentre referti ed immagini vengono conservati nel Sistema Informatico Ospedaliero nelle stesse modalità riservate agli altri trattamenti.
Il passaggio attraverso l’ufficio di screening fornisce la duplice possibilità, per il Sistema Sanitario territoriale, di informare periodicamente le utenti interessate della possibilità di svolgere degli esami preventivi e di monitorare le percentuali di persone affette da questo tumore sul territorio, conoscendo però solo l’esito e non avendo il possesso fisico dei referti e delle immagini raccolte.

[70] Linee guida AIOM (Associazione Italiana Oncologia Medica) “Neoplasie della Mammella”, pubblicata nel Sistema Nazionale Linee Guida; Roma, 13 luglio 2020 - Aggiornamento 17 novembre 2021.

Capitolo 4.

Complemento all'analisi: Procedura di Risk Assessment e DPIA per gli elettromedicali radiologici

4.1 Il Defibrillatore

Nel corso della seguente analisi conclusiva, prima di applicare la procedura di valutazione del rischio ai dispositivi medici classificati come "elettromedicali" - i dispositivi attraverso i quali vengono svolti fisicamente gli esami sui pazienti – si rende necessario operare tra questi una differenziazione. Nella fattispecie, occorre considerare separatamente i device che, mantenendo in memoria dati sensibili del paziente, anche se per un breve periodo, costituiscono un rischio per i diritti e le libertà del paziente e necessitano di controlli ottimali per ridurlo, dai dispositivi che per caratteristiche di progettazione non possono mantenere in memoria alcuna informazione sensibile. Tra questi, all'interno della seguente analisi, figura il defibrillatore portatile.

Il defibrillatore non è un elettromedicale di scopo propriamente radiologico, è in dotazione a ciascun reparto, secondo le diverse necessità e caratteristiche, per garantire la sicurezza clinica del paziente in caso di arresto cardiaco. All'interno del reparto di Radiologia sono presenti 4 defibrillatori di tipo portatile (Figura 10); tali dispositivi, in caso di emergenza, si attivano in automatico all'apertura e registrano all'interno di una scatola nera solo tre informazioni:

- La data;
- Il tracciato ecografico del paziente;
- La registrazione vocale di ciò che dicono gli operatori coinvolti.

Figura 10. Defibrillatore portatile Saver One 200J semi-automatico, destinato al reparto di Radiologia, in manutenzione presso l'Ufficio Tecnico.

I dati anagrafici del paziente non vengono raccolti e, di conseguenza, non potranno essere collegati al suo tracciato. La registrazione vocale degli operatori non costituisce dato personale o sensibile ed è obbligatoria per poter certificare, in caso di dubbio, che tutte le operazioni siano state svolte a dovere.

Per i motivi descritti, non mostrando il dispositivo in esame di possedere variabili che costituiscono potenziale rischio per il trattamento di dati sanitari, si è stabilito di assegnare, all'interno del Registro dei Trattamenti, un valore di Rischio Residuo pari a 0. Un riassunto delle informazioni principali associate a tale dispositivo viene riportato in Tabella 15.

Descrizione sintetica dell'attività di trattamento dati supportata dall'apparato	**Dati trattati**		**Modalità trattamento**		**Suddivisione apparecchiatura in base ai rischi:** **- apparecchiatura stand alone** **- apparecchiatura con sistema proprietario collegata alla rete dati** **- apparecchiatura PC based collegata alla rete dati**	**Misure tecniche di protezione dei dati**	**Misure fisiche di protezione dei dati**	**Rischio residuo**
	personali	sensibili	conservati	archiviati				
[Defibrillatore DEFIGARD] Raccolta tracciati e registrazione vocale delle operazioni eseguite; Nessuna associazione dei dati raccolti con le anagrafiche paziente; Archiviazione su memoria fisica.	No	Sì	No	Sì	Apparecchiatura stand-alone con software proprio dedicato. Nessun collegamento con il Sistema Informativo.	Ritenute non necessarie	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**0**

Tabella 15. Estratto del Registro dei Trattamenti che riporta la descrizione di un Defibrillatore Portatile. Questo dispositivo non è collegato alla rete e non memorizza informazioni sanitarie correlabili al paziente, per questo motivo è di default non rischioso per i diritti e le libertà degli interessati. Le misure fisiche atte alla sua protezione vengono realizzate per il valore del device e la sua importanza all'interno del reparto, non per tutela alla privacy del paziente.

Si può procedere quindi alla valutazione – che necessita di analisi aggiuntive - degli elettromedicali che effettuano una memorizzazione temporanea dei dati sanitari raccolti e dei dati anagrafici associati.

4.2 Elettromedicali per gli esami radiologici

Segue, a complemento, una breve descrizione dei device più rilevanti all'interno di un reparto di Radiologia.

Ecografo: L'ecografia è un sistema di indagine diagnostica medica ad ultrasuoni che consente lo studio di diverse parti del corpo e si basa sul principio dell'emissione di

eco e della trasmissione delle onde ultrasonore. Un ecografo è tipicamente formato da una sonda che trasmette e riceve il segnale, un sistema elettronico e un monitor di visualizzazione. Si tratta di un elettromedicale che non ha esclusivo utilizzo all'interno del reparto di Radiologia; al contrario: la sua versatilità, la facilità di utilizzo, il funzionamento senza radiazioni lo rendono un device particolarmente versatile. Un esempio è riportato in Figura 11.

L'esame è particolarmente utile per la valutazione degli organi dell'addome come fegato, pancreas, milza, organi dell'apparato urinario, utero, ovaie e prostata, ma anche nella valutazione dei tessuti molli come la tiroide e la mammella, o nello studio superficiale di muscoli e articolazioni.

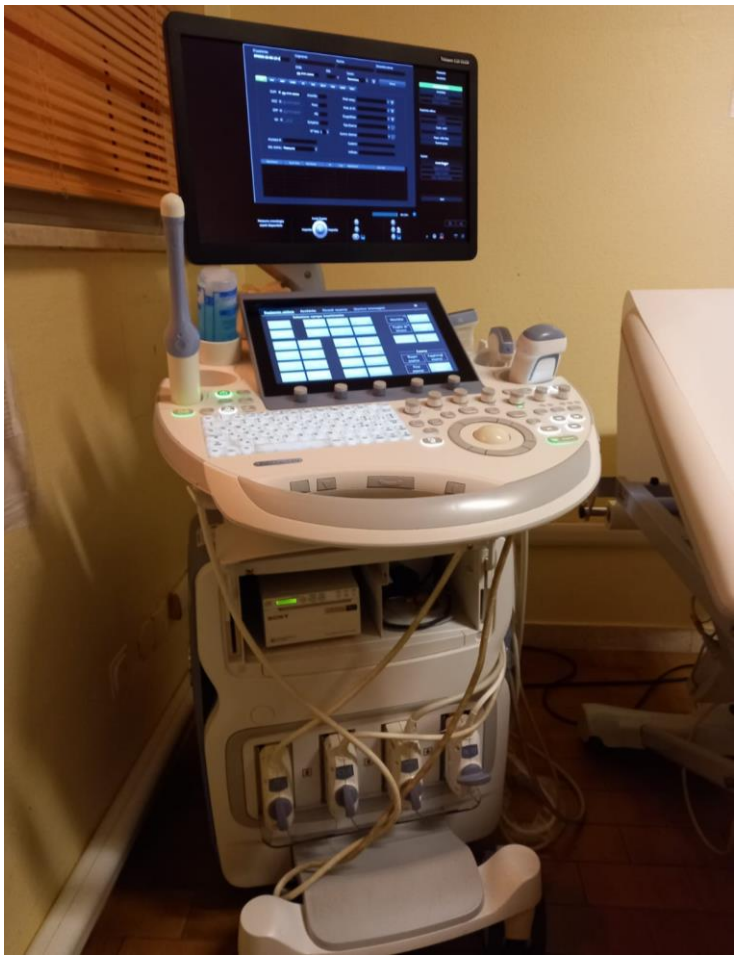


Figura 11. Ecografo impiegato dall'ambulatorio di Ginecologia. È possibile notare il monitor di visualizzazione, che è parte integrante del dispositivo medico: l'ecografo infatti non necessita di una Workstation per accedere alle informazioni anagrafiche e alle prenotazioni del paziente. Il software integrato nell'ecografo (non si tratta di suitEstensa®) riceve direttamente dal Sistema RIS-PACS le informazioni necessarie per lo svolgimento dell'esame e, una volta completato, invia le immagini nuovamente al Sistema – che provvederà a renderle disponibili al medico in una Workstation di Refertazione. Si tratta di un procedimento di comunicazione analogo a quanto accade per gli altri dispositivi, fatta eccezione per il passaggio attraverso la Workstation di Consultazione, che per questi esami viene bypassato. In Tabella 19 è riportata la descrizione di questi dispositivi all'interno del Registro dei Trattamenti.

Ortopantomografo: L'ortopantomografo è un'apparecchiatura che consente di eseguire un radiogramma panoramico dell'intera struttura delle arcate dentarie. Tale dispositivo è costituito da una struttura meccanica in cui il paziente può essere disposto, posizionato in modo che le arcate dentarie si trovino in una particolare posizione rispetto a un braccio rotante che supporta, da un lato, la sorgente radiogena, e dall'altro un tamburo rotante contenente la pellicola radiografica.

Mammografo: È uno strumento radiologico che proietta un fascio di raggi X direttamente sulla mammella, fornendone una valutazione morfologica e strutturale. Il Mammografo (Figura 12) è costituito essenzialmente da una colonna con alimentatore, da un braccio a C per supporto per il tubo radiogeno e da sistema di rilevazione immagine che trasmette i segnali elettronici a un computer per fornire una o più immagini digitale.

Figura 12. Device medico impiegato per lo svolgimento delle Mammografie (a sx) e postazione del tecnico radiologo (a dx). I due monitor sono la Consolle collegata con il Sistema RIS/PACS e il monitor associato all'elettromedicale, parte dello stesso, che riceve dalla consolle le informazioni necessarie allo svolgimento dell'esame. La consolle – o Workstation di Consultazione – è collegata grazie al software suitEstensa® al Sistema RIS/PACS, dal quale riceve le informazioni ed al quale, al termine dell'esame, invia le immagini mediche raccolte, di modo che queste vengano sia conservate che inviate alla Workstation di Refertazione per permettere al medico radiologo di concludere l'esame. In Tabella 19 è riportata la descrizione di questi dispositivi all'interno del Registro dei Trattamenti.

Macchina per RMN (Risonanza Magnetica Computerizzata): Si tratta di un apparecchio cui si ricorre nell'ambito della diagnostica per immagini, si basa sull'applicazione di un campo magnetico di elevata intensità al distretto corporeo di interesse; la sua esecuzione può richiedere la somministrazione in vena di un mezzo di contrasto.

Macchina per TC (Tomografia Computerizzata): La TC è una tecnica di diagnostica che utilizza le radiazioni ionizzanti per ottenere delle immagini tridimensionali. Durante l'esame le aree del corpo da studiare vengono attraversate da un fascio di raggi X che, grazie ad un sistema di elaborazione, si trasformerà in immagini tridimensionali digitali. In alcuni casi è necessario iniettare il mezzo di contrasto.

Figura 13. Macchina per TAC Optima durante la preparazione per un nuovo paziente. La consolle di questa apparecchiatura, assieme alla Workstation di Consultazione alla quale è associata, si trovano fuori da locale utilizzato per le analisi, per proteggere gli operatori dalle radiazioni emesse dalla macchina. In alto a dx nell'immagine è riportato in dettaglio l'iniettore angiografico; esso è considerato un device a sé stante e pertanto all'interno del Registro dei Trattamenti viene riportata una sua valutazione indipendente. Un iniettore angiografico dispone di un software integrato che permette all'operatore esclusivamente di inserire manualmente per ogni esame la quantità di dose da erogare (indicazione fornita dal Sistema RIS/PACS alla Workstation), non registra o necessita di informazioni relative al paziente, né private né sanitarie, e pertanto il valore di Rischio Residuo non sarà determinabile. In Tabella 19 è riportata la descrizione di questi dispositivi all'interno del Registro dei Trattamenti.

4.2.1 Risk Assessment per gli elettromedicali radiologici

Pur tenendo conto delle differenze costitutive e di scopo, il funzionamento della maggior parte degli elettromedicali è pressoché il medesimo: ciascun elettromedicale è dotato di un software proprio integrato, che comunica con il software suitEstensa® di gestione delle anagrafiche installato sulla Workstation dedicata, in modo da ricevere dal Sistema Informativo le corrette indicazioni sugli esami da svolgere. Una volta effettuata la procedura e

raccolte le immagini radiologiche, queste, mediante lo stesso collegamento, vengono inviate alla Workstation e da lì al Sistema RIS/PACS per la loro conservazione, nonché per il successivo accesso al Sistema tramite Workstation di Refertazione per la conclusione dell'esame.

Ogni dispositivo ha la possibilità di archiviare nella propria memoria un certo quantitativo di immagini ed informazioni sull'esame, in base alla capacità della macchina: in genere l'arco temporale varia dalle 24 ore, per i device più piccoli, fino a 7 giorni per le Risonanze e le TAC. Passato questo periodo le informazioni vengono eliminate direttamente.

Dal momento che le modalità di azione di tali dispositivi sono pressoché le medesime - raccolta delle immagini radiografiche e conservazione in memoria della loro associazione con le anagrafiche del paziente per un periodo compreso tra le 24h e 7 giorni, nessun accesso ai referti – si è scelto di svolgere un'analisi complessiva per tali dispositivi, eccezion fatta naturalmente per i defibrillatori, di cui si è già trattato in precedenza.

In base alle analisi svolte, le variabili associate ai trattamenti offerti dalla UOC Radiologia - per quanto concerne gli elettromedicali di diagnosi e raccolta di immagini – e che possono essere considerate potenzialmente critiche sono elencate in Tabella 13.

	Variabile	**Peso della variabile**
1	Dati di localizzazione	1
2	Dati relativi alla salute (appartenenza a categoria protetta o info su permessi per malattia o info su permessi per Maternità senza visibilità del referto medico)	2
3	Dati che rivelano l'origine razziale o etnica	3
4	Dati Residenti fuori dall'UE	3

Tabella 16. Pesi associati a ciascuna variabile identificata come portatrice di potenziali criticità all'interno del trattamento effettuato. L'assegnazione dei pesi fa riferimento alla *Tabella 4.*

Nel caso in esame:

- La somma delle variabili dà come risultato 9;
- Sono presenti due variabili con livello di criticità 2.

Si ricorda che, poiché la scelta del livello di criticità si basa sia sulla somma dei pesi assegnati alle variabili, sia sula presenza di variabili a rischio elevato, e poiché il secondo criterio, in caso di incertezza nell'assegnazione, ha precedenza sul primo, i trattamenti effettuati attraverso elettromedicali sono da intendersi come critici, e per questo motivo anche in questo caso risulta opportuno proseguire l'analisi al livello successivo, ovvero alla valutazione del rischio associato per ciascun trattamento.

4.2.2 Data Protection Impact Assessment per gli elettromedicali radiologici

Procedendo con l'analisi, si passa alla definizione del livello di Rischio Inerente associato al trattamento svolto dagli elettromedicali, effettuata in termini di impatto della diffusione e probabilità di accadimento.

Anche in questo caso i trattamenti erogati hanno un impatto *massimo* e presentano una presumibilità di accadimento di eventi avversi *probabile*.

Il livello di Rischio Inerente R_I è anche in questo caso pari a:

$$R_I = v_I \cdot p_I = 4 \cdot 4 = 16$$

Una volta noto il livello di Rischio Inerente si procede con la valutazione dei controlli che vengono effettuati allo scopo di mitigare impatti e probabilità di accadimento.

I controlli da effettuarsi sono di diversa natura e cambiano in base alle modalità di raccolta dei dati - modalità elettronica, eseguita nella maggior parte dei casi, e cartacea, impiegata in seguito a blocchi temporanei di sistema (programmati o non). Si effettuerà dunque la valutazione dei controlli per entrambe le modalità riportate.

- *Controlli per la modalità cartacea*

Non si tratta propriamente di modalità cartacea, in quanto gli elettromedicali, in situazione di blocco del sistema, ritornano alla modalità analogica di stampaggio su pellicola. Una volta che il sistema sarà tornato in funzione, il personale si occuperà di digitalizzare le immagini stampate, conservando fisicamente anche la pellicola originale per lo stesso arco temporale in cui viene conservato il file DICOM digitalizzato. In queste circostanze il personale segue delle linee guida aziendali già citate, così come per la valutazione sono stati presi in esame i 4 controlli precedentemente riportati, e sui quali dunque non ci si soffermerà ulteriormente.

Si riporta di seguito la valutazione effettuata.

Trattamento cartaceo dei dati raccolti		
	Controlli	*Valore*
1	Identificazione di ruoli e responsabilità	1
2	Svolgimento periodico delle attività di controllo	0.5
3	Definizione di controlli e norme comportamentali	0.5
4	Presenza di misure di sicurezza fisiche per la gestione del documento cartaceo (armadi, casseforti, etc.)	1

Tabella 17. Valore assegnato ai controlli per il trattamento dei dati svolto con modalità cartacea.

- *Controlli per la modalità elettronica*

Sono stati presi in considerazione ed opportunamente valutati i 14 controlli che raccolgono le principali aree di monitoraggio di un trattamento digitale; di seguito vengono riportati i valori assegnati.

Trattamento elettronico dei dati raccolti		
	Controlli	*Valore*
1	Politiche di sicurezza delle informazioni	1
2	Quadro di gestione per implementazione di requisiti di sicurezza	1
3	Formazione del personale	0
4	Gestione degli asset	1
5	Controllo degli accessi	0.5
6	Crittografia	0
7	Sicurezza fisica e ambientale	1
8	Sicurezza delle attività operative	0.5
9	Sicurezza delle comunicazioni	1
10	Acquisizione, sviluppo e manutenzione dei sistemi informativi	1
11	Relazioni con i fornitori	1
12	Gestione degli incidenti relativi alla sicurezza delle informazioni	1
13	Disaster Recovery e Business Continuity	1
14	Compliance in ambito di obblighi legali, regolamentari o contrattuali relativi alla sicurezza delle informazioni.	1

Tabella 18. Valore assegnato ai controlli per il trattamento dei dati svolto con modalità elettronica.

Alcune considerazioni riguardo alle modalità di valutazione dei controlli ed assegnazione del valore finale:

Si sta trattando, in questo contesto, di dati raccolti ed elaborati per mezzo di dispositivi elettromedicali i quali, per loro caratteristica di progettazione, non danno la possibilità di accedere al numero elevato di informazioni alle quali si ha invece accesso tramite le Workstation. Queste sono infatti caratterizzate dalla presenza di un software (suitEstensa®) che gestisce una serie molto più elevata di dati, personali e sensibili, fornite dal Sistema RIS/PACS, mentre le apparecchiature ricevono dalle Workstation solo le informazioni utili allo svolgimento dell'esame.

Inoltre, è importante notare che, non avendo gli elettromedicali collegamenti con le Workstation di refertazione, le tipologie di dati trattati sono meno rischiose e, di conseguenza, i controlli associati ai trattamenti richiederanno una quantità inferiore di azioni per essere ritenuti soddisfatti.

È possibile notare, infatti, che nella seguente analisi, svolta considerando gli elettromedicali, i valori associati ai controlli sono più elevati rispetto a quelli ottenuti dall'analisi precedente, relativa alle Workstation. Con tutto ciò, questo accade anche

perché il personale è molto più istruito sul corretto utilizzo delle apparecchiature di raccolta delle immagini radiologiche rispetto ai monitor di gestione delle anagrafiche, sia per formazione accademica che per una cultura - maggiormente orientata alla tutela del paziente dal punto di vista della salute fisica che non della protezione delle sue informazioni personali - ancora notevolmente radicata nel contesto ospedaliero.

Gli unici punti che manifestano controlli non completamente rispettati, com'è possibile notare in Tabella 15, sono quelli che riguardano la sicurezza delle attività operative: mentre le Workstation hanno implementato un sistema di controllo degli accessi molto rigido, la maggior parte degli elettromedicali, soprattutto quelli mobili (Portatili Radiologici ed Ecografi), non sono integrati con modalità di accesso particolarmente vincolanti e spesso all'operatore è sufficiente una card (situata in prossimità del dispositivo) per effettuare l'accesso quando questo è in stand by. Si tratta di una modalità operativa che garantisce un facile accesso e la celerità delle operazioni, attuata in considerazione del fatto che i dati trattati non hanno il medesimo livello di sensibilità di quelli gestiti dalle Workstation e che l'apparecchiatura non è in alcun modo connessa alla rete o accessibile dall'esterno; tuttavia, si ritiene in questa sede che dovrebbero comunque essere implementate delle modalità di accesso ulteriori o più rigide, come ulteriore protezione ai dati in gestione alla macchina.

La valutazione del controllo complessiva per ciascun trattamento è ottenuta dalla somma ponderata delle singole valutazioni; anche in questa analisi ad ogni controllo è stato assegnato un peso unitario.

Calcolo del Livello di Controllo:

$$C = \frac{\sum_{i=1}^{n} p_i \cdot var_i}{n}$$

dove:

v_i è il controllo da effettuare

n è il numero totale di controlli, 4 per trattamenti cartacei e 14 per trattamenti elettronici

p_i è il valore assegnato al controllo, $p_i \in [0,1]$.

Il valore ottenuto dal calcolo del Livello di Controllo, approssimato al terzo decimale, è:

$$C = \frac{2 \cdot p_0 + 5 \cdot p_{0.5} + 11 \cdot p_1}{18} = 0.778$$

Si passa a questo punto alla valutazione del valore di Rischio Residuo, tramite l'espressione:

$$R^r = R^i \cdot (1 - C)$$

In base ai dati precedentemente raccolti, si giunge al risultato finale, che verrà inserito all'interno del Registro dei Trattamenti:

$$R^r = 16 \cdot (1 - 0.75) = 3.556$$

L'analisi svolta ha portato al raggiungimento di un livello di rischio definito trascurabile, che non comporta (in base al Regolamento UE 2016/679 e alle linee guida di Azienda Zero) l'obbligo da parte del Titolare del Trattamento di implementare ulteriori procedure a minimizzazione dei rischi associati alla gestione dei dati sensibili presso la UOC Radiologia.

Descrizione sintetica dell'attività di trattamento dati supportata dall'apparato	**Dati trattati**		**Modalità trattamento**		**Suddivisione apparecchiatura in base ai rischi:** **- apparecchiatura stand alone** **- apparecchiatura con sistema proprietario collegata alla rete dati** **- apparecchiatura PC based collegata alla rete dati**	**Misure tecniche di protezione dei dati**	**Misure fisiche di protezione dei dati**	**Rischio residuo**
	personali	sensibili	conservati	archiviati				
[Ecografo LOGOS HI VISION GOLD] Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di archiviazione una settimana ca, eliminazione progressiva dei file in ordine di acquisizione. Possibilità di consultazione di immagini. (a)	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati. Il software è installato sul dispositivo medico, rientra nella classificazione di on-board.	Utilizzo tramite card di accesso disponibile per il personale addetto, non è richiesta autenticazione; Nessun collegamento web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) attraverso la workstation dedicata e ivi mantenuti per le tempistiche di legge. Presenza di Firewall di protezione all'HIS.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**

[Mammografo SENOGRAPHE DMR V2] Raccolta informazioni anagrafiche paziente ed immagini radiologiche mammografiche; Memoria di archiviazione una settimana ca, eliminazione progressiva dei file in ordine di acquisizione. (b)	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati; Il software è incorporato nel dispositivo medico, rientra nella classificazione di Embedded.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) attraverso la workstation dedicata e ivi mantenuti per le tempistiche di legge, con passaggio ulteriore del risultato all'Ufficio Screening. Presenza di Firewall di protezione all'HIS.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**
[Risonanza Magnetica OASIS] Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di archiviazione una settimana ca, eliminazione progressiva dei file in ordine di acquisizione. (c)	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati; Il software è incorporato sul dispositivo medico, rientra nella classificazione di Embedded.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) attraverso la workstation dedicata e ivi mantenuti per le tempistiche di legge. Firewall di protezione all'HIS.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**
[Iniettore angiografico] Nessuna raccolta dati (d)	No	No	No	No	Non applicabile	Non applicabile	Non applicabile	**X**

Tabella 19. Esempio di tre dispositivi elettromedicali inseriti con un valore di Rischio Residuo pari a 3.556 all'interno del Registro dei Trattamenti. La prima riga della tabella (a) riporta la descrizione di un ecografo, per il quale le informazioni necessarie per l'esecuzione dell'esame – anagrafiche e prestazionali – vengono inviate direttamente dal Sistema RIS/PACS al monitor integrato, senza il passaggio intermedio di una Workstation di Consultazione. La seconda riga della tabella (b) riporta le informazioni relative ad un device mammografico; viene inteso l'elettromedicale, non la Workstation dedicata, per la quale valgono le analisi svolte nel capitolo precedente. I risultati degli esami svolti con questo elettromedicale necessitano di un passaggio ulteriore all'Ufficio Screening (come descritto al Paragrafo 3.4.2.5). Nelle righe terza e quarta della tabella sono riportate informazioni di gestione della Risonanza Magnetica (c) e dell'iniettore angiografico associato (d), per il quale, dato che non gestisce alcun dato, non è possibile tantomeno necessario individuare un valore di Rischio Residuo: tale dispositivo non comporta alcun rischio per le procedure svolte dal reparto.

Sono stati esclusi dall'analisi tutti i dispositivi che, non avendo collegamento diretto con il paziente e non disponendo di un sistema informatico, associato o integrato, non sono in grado di raccogliere nessun tipo di informazione personale o sanitaria. Questo accade perché sono device che non raccolgono né gestiscono (fisicamente o elettronicamente) i dati dei pazienti sottoposti ad esami. Si tratta dunque di strumenti passivi, che non contribuiscono in nessun

modo, e secondo nessuna modalità di utilizzo, a un rischio per il dato personale o sanitario. Tali dispositivi medici, nel Registro dei Trattamenti realizzato, presenteranno alla voce Rischio Residuo la dicitura "X".

4.3 Il Registro delle Attività di Trattamento

Il risultato finale dell'analisi svolta presso la UOC Radiologia durante il periodo di tirocinio, vale a dire Il Registro delle Attività di Trattamento di tutti i dispositivi inventariati presenti in reparto, è disponibile integralmente all'Allegato 2. Si ritiene necessario riportare alcune informazioni a titolo di chiarificazione:

Come richiesto dalle direttive Aziendali, sono stati presi in considerazione tutti i dispositivi medici che vengono impiegati in tale reparto, ordinati in base al numero di inventario che è stato assegnato loro dal dipartimento di Ingegneria Clinica in fase di collaudo.

Da Regolamento UE 2016/679 non sono previste linee guida specifiche per lo svolgimento delle procedure di analisi del rischio e di redazione del Registro dei Trattamenti, anche se naturalmente sono riportate le informazioni fondamentali da integrare perché questo abbia valore giuridico. Nel presente lavoro di tesi si è deciso di svolgere, per i dispositivi che presentavano sovrapponibili modalità di trattamento dei dati, una valutazione unica di Risk Assessment e DPIA, che viene, in fase di redazione del Registro, attribuita ad ogni elettromedicale presente nell'elenco. Resta inteso che, ad ogni inserimento di nuovi dispositivi e sostituzione o aggiornamento di software tra quelli presenti seguirà uno corrispondente aggiornamento del Registro riportato (ed ufficialmente utilizzato nella documentazione aziendale), con un ricalcolo del rischio residuo associato, utilizzando la medesima sequenza di passaggi di analisi dei controlli e valutazione del rischio proposta e redatta in questo elaborato.

I termini riportati in tabella, *archiviazione* e *conservazione*, sono spesso utilizzati come sinonimi, ma in questa trattazione è rilevante sottolinearne la differenza:

- Per archiviazione si intende la collocazione di un documento in uno spazio dedicato per renderlo reperibile in futuro.
- Per conservazione si intende invece un processo che permette di prolungare nel tempo la validità legale di un documento, con procedure ed elementi in grado di autenticare e certificare il documento stesso.

In pratica: i singoli device medici possono archiviare informazioni, ma solo il Sistema Informativo Ospedaliero le conserva.

Conclusioni

L'analisi presentata in questa tesi ha messo in evidenza come la complessità delle tecnologie riguardanti i Sistemi Ospedalieri integrati di telecomunicazione (ICT) stia crescendo rapidamente e come le interdipendenze siano numerose, complesse a volte nascoste e pericolose. L'effetto dell'informatica e dell'automazione sulle procedure medico-sanitarie si sta manifestando in maniera sempre più ampia, portando notevoli vantaggi per la salute e il benessere di tutti i pazienti, ma al tempo stesso l'impatto del trattamento dei dati sanitari può determinare severe conseguenze sotto diversi profili, in materia di privacy e sicurezza delle informazioni, ponendo sfide sempre più complesse alle istituzioni sanitarie e ai produttori di dispositivi medico-sanitari.

Le Aziende Ospedaliere, pubbliche e private, in qualità di Titolari del trattamento, sono tenute a mettere in atto misure tecniche ed organizzative atte a garantire un livello di sicurezza adeguato ai rischi in cui i dati sensibili possono incorrere durante il loro impiego.

In coerenza con l'approccio della gestione del rischio che caratterizza tutto l'impianto del Regolamento Europeo sulla Protezione del Dato, si impone al Titolare di effettuare una valutazione di impatto (o DPIA – *Data Protection Impact Assessment*) allorché un tipo di trattamento o più trattamenti simili fra di loro, possano costituire un rischio elevato per i diritti e le libertà delle persone fisiche.

Per la sensibilità dei dati circolanti all'interno di una qualsiasi azienda sanitaria appare evidente la necessità di sviluppare una procedura di Valutazione del Rischio calata nella realtà ospedaliera in cui si sta operando.

Nel corso della trattazione, sono stati analizzati gli aspetti del nuovo Regolamento europeo più rilevanti sia per i fabbricanti di dispositivi medici sia, particolarmente, per gli operatori sanitari, e conseguentemente è stato realizzato ed attuato un protocollo di Analisi e Valutazione dei Rischi, il quale ha permesso di costruire infine il Registro delle Attività di Trattamento svolte nel Reparto di Radiologia, presso l'Azienda Ospedaliera Aulss5, nel Polo Ospedaliero di Rovigo.

Una volta definiti e caratterizzati i sistemi medicali con cui si opera in un contesto Ospedaliero – con particolare interesse ai software integrati nel device medico - sono state studiate delle modalità operative attuabili presso l'Azienda per l'identificazione dei livelli di criticità e di rischio per i diritti e le libertà personali degli interessati per i trattamenti implementati. La DPIA deve identificare gli scenari di rischio e, per ciascuno di essi, stimare

il livello di rischio effettivo connesso al trattamento in esame, con riguardo alla natura, all'ambito di applicazione, al contesto ed alle finalità del trattamento.
La linea metodologica presentata, che utilizza parametri di valutazione quantitativi, prevede, in breve:

1. L'assegnazione di un livello di criticità per ciascuna variabile associata al trattamento;
2. La conseguente determinazione del livello di criticità del trattamento nella sua interezza;
3. Per i trattamenti identificati come critici, la valutazione del Rischio Intrinseco, ossia il rischio connesso al trattamento, in termini di impatto dell'evento avverso e di periodicità con cui il trattamento viene eseguito.

Per ciascuna minaccia identificata come associata al trattamento in esame, in base alle differenti tipologie riscontrate, occorre effettuare dei controlli a tutela dei dati personali e sanitari, relativamente ad ambiti quali le politiche di sicurezza delle informazioni adottate dall'Azienda, le protezioni fisiche a tutela dei dati conservati e la corretta ed attenta gestione del software che governa a livello informatico il trattamento. Deve essere quindi esaminato il livello di implementazione di tali controlli.

4. Si procede infine al calcolo del Rischio Residuo, verificando quanto il Rischio Intrinseco sia stato mitigato o ridotto (mai eliminato) dai controlli eseguiti per le diverse modalità di trattamento.

In base al valore del Rischio Residuo, il rischio a cui il trattamento continua ad essere soggetto anche dopo l'effettuazione dei controlli, vengono rilevate le tipologie di trattamento che perseverano nel presentare un alto rischio per i diritti e le libertà degli Interessati.
La soglia di accettabilità del rischio è tarata su un livello trascurabile o basso – nella graduatoria riportata nel Capitolo 3 si fa riferimento a trattamenti che presentano un valore del Rischio Residuo compreso 0 e 8, per i quali non risulta necessario effettuare azioni di adeguamento. Nei casi in cui invece il livello di rischio riscontrato abbia un valore pari o superiore ad 8 dovranno essere valutate delle strategie di mitigazione e minimizzazione, attraverso la collaborazione degli operatori coinvolti, dei tecnici aziendali e dell'ente responsabile della gestione del rischio.

In ultimo, è stato riportato il Registro dei Trattamenti, che restituisce in via schematica i principali elementi emersi dalle analisi svolte, individuati per ciascun dispositivo medico; tale Registro rappresenta un documento ufficiale, che viene utilizzato per tenere traccia di quanto

svolto in Azienda, per avere un punto di partenza nelle eventuali strategie di mitigazione dei rischi associati ai trattamenti svolti e, in caso di controversie, attesta la conformità dell'Azienda alla normativa vigente.

Portando l'attenzione al reparto di Radiologia, obiettivo di studio di questa trattazione, due sono gli ambiti principali per i quali è stato necessario svolgere una procedura di Risk Assessment e Data Protection Impact Assessment:

- Le Workstation di consultazione e refertazione;
- Gli elettromedicali impiegati per lo svolgimento fisico dell'esame.

Di seguito alcune considerazioni sui risultati ottenuti.

La valutazione dei rischi associati all'esecuzione delle prestazioni mediche con i dispositivi elettromedicali ha richiesto, da un lato, una conoscenza non solo dello scopo del dispositivo ma anche e soprattutto delle sue particolari modalità di funzionamento. La valutazione dei rischi associati, dei controlli, e quindi il valore di rischio residuo riscontrato, testimoniano per che il rischio riscontrato è di molto inferiore rispetto a quello ottenuto dall'analisi delle Workstation. Questo avviene perché, se da un lato la buona riuscita di un esame dal punto di vista cinico è strettamente correlata al funzionamento dell'elettromedicale impiegato, sono le Workstation; quindi, le consolle associate a tali device che si occupano della raccolta e della diffusione nella rete ospedaliera dei dati estrapolati, lasciando all'apparecchiatura il solo compito di eseguire l'esame. I software incorporati negli elettromedicali non sono dunque di una complessità tale da poter gestire, immagazzinare ed indirizzare il flusso di lavoro di un intero reparto e si limiteranno, al massimo, a conservare in memoria un numero relativamente ridotto di prestazioni, che verranno eliminate via via che i pazienti si susseguono, e che non sono interpretabili senza l'intermediazione della consolle di lavoro.

La valutazione delle Workstation ha rappresentato il punto più impegnativo del lavoro, dal momento che è l'interconnessione tra le diverse apparecchiature presenti in reparto con il sistema RIS/PACS, nonché l'interazione di questo con i Sistemi satelliti, che comporta i maggiori rischi di diffusione, dolosa o accidentale, sia di informazioni anagrafiche, che come è stato visto rimangono visibili con lo standard di comunicazione utilizzato HL7, sia, anche se ovviamente maggiormente tutelate, le informazioni mediche relative a referti ed immagini medicali radiologiche. Per questo motivo le Workstation, le quali hanno installato di default il software di gestione dati suitEstensa®, sono i dispositivi medici che raccolgono il maggior numero di informazioni sensibili e sono chiamati a gestirli nel rispetto delle misure di

sicurezza adottate dal reparto, per scongiurare il pericolo di diffusione e furto. La procedura effettuata ha mostrato che, per quanto riguarda le Workstation, il valore di Rischio Residuo associato ai trattamenti di dati sanitari e personali dei pazienti è molto basso, pari a 5.328. In base alla scala di valori riportata non si presenterebbe dunque la necessità di effettuare ulteriori valutazioni integrative, per migliorare il software gestionale o per variare le modalità operative adottate dal personale operante nel reparto di Radiologia.

Nonostante, tuttavia, la presenza di misure di sicurezza, sia fisica che informatica, a tutela dei dati trattati, si ritiene in questa sede necessario aggiungere una considerazione conclusiva che esula – ma non poi di molto – dalle valutazioni meramente tecniche di DPIA svolte per il reparto di Radiologia.

Durante i sopralluoghi in tale reparto è purtroppo emersa la scarsa attenzione che ancora oggi, dopo 4 anni dall'introduzione del Regolamento Europeo 2016/679, si riserva alle questioni legate alla privacy nel contesto sanitario. Le aziende ospedaliere sono molto in ritardo nell'adeguamento a questa normativa, sia da un punto di vista di uniformazione delle procedure di valutazione di impatto e di redazione di un Registro dei Trattamenti per ciascun dispositivo medico presente presso i reparti, sia per quanto riguarda la formazione del personale addetto al trattamento.

Ciò è dovuto, oltre che ad una evoluzione molto rapida delle tecnologie medicali, ad una posizione molto diffusa che vede i servizi di cura al paziente prioritari rispetto al garantirne la riservatezza dei dati forniti. Questa idea, più che condivisibile sotto certi aspetti, deve però essere secolarizzata e rivista alla luce del contesto sociale in cui ci si trova a lavorare: i dati personali, grazie alle stesse tecnologie che permettono di sfruttarli al meglio per l'esecuzione degli esami, sono sottoposti ad un rischio molto elevato e la loro perdita, ma ancora di più la loro diffusione, comporta un impatto considerevole sul benessere dell'interessato. Il settore sanitario è uno dei settori più esposti sul versante della sicurezza informatica, e tali problematiche di sicurezza evidenziano come l'attenzione sugli aspetti tecnologici non può essere disgiunta dall'attenzione degli aspetti organizzativi delle risorse umane. Tra i fattori di rischio che incidono maggiormente è stato infatti possibile riscontrare:

- L'ampia diversificazione delle figure professionali coinvolte, con diverse formazioni e diversi profili di autorizzazione nei sistemi e che spesso accedono a più applicativi o attrezzature collegate in rete;
- La necessità di integrare applicativi e attrezzature fortemente diversificate, soprattutto nei casi in cui i dispositivi siano stati acquistati in momenti diversi o presso ditte diverse.

In conclusione, le procedure di Risk Assessment e Data Protection Impact Assessment realizzate in questo percorso di tesi magistrale possono essere applicate a tutti i reparti ospedalieri, dopo aver scelto in modo opportuno le variabili da inserire nell'analisi, ed è quindi necessaria una conoscenza approfondita dei reparti, del loro funzionamento operativo e dei dispositivi presenti. Le pratiche di gestione del rischio, perché siano efficaci, devono interessare tutte le aree in cui si possono manifestare criticità durante il processo clinico-assistenziale: solo una gestione integrata può portare a cambiamenti nella pratica clinica, promuovere la crescita di una cultura della salute più attenta e vicina al paziente e che tenga in opportuna considerazione il suo diritto alla privacy, oltre che quello alla salute. I processi, non solo tecnologici ma anche organizzativi, dovranno dunque essere revisionati e potenziati nel corso del tempo, anche se non formalmente richiesto dalla Normativa, e la gestione del rischio clinico dovrà essere affidata ad una sola figura professionale – nella persona dell'ingegnere clinico o biomedico, bensì ad un gruppo di lavoro in cui si arrivi ad una buona integrazione di diversi background professionali ed umani.

Bibliografia

Agenzia per l'Italia Digitale AGID: Linee Guida per la modellazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del Secure/Privacy by Design (2020)

AIIC, Il ruolo dell'ingegnere clinico nel SSN, 2010

Article 29 Working Party: *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely result in high risk" for the purposes of Regulation 2016/679*, WP248 rev.01 (2017)

Article 29 Working Party: Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force. WP 209 (2013).

Article 29 Working Party: Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications. WP 175 (2010).

Bassini M., *Le tecnologie avanzano, le norme passano ma le costituzioni rimangono*, in "Diritti Comparati", 2014

Berti P., Ciuffi D., Messina G., *La digitalizzazione in radodiagnostica. Aspetti operativi e gestionali*, in "Mondo Sanitario" - n.01-02, 2011

Bieker, F., Friedewald, M. et al., *A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation*, in: Schiffner, Privacy Technologies and Policy. APF 2016. Lecture Notes in Computer Science(), vol 9857. Springer, Cham. https://doi.org/10.1007/978-3-319-44760-5_2

Borasi G., Nitrosi A. et al., *Efficienza ed efficacia del sistema PACS nella realtà dell'Ospedale filmless di Reggio Emilia*, in "Fisica in Medicina", 2/2004

Calzolaio S., *Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, in ""Federalismi"", 2017."

Carrino J.A., Unkel P.J. et al., *Large-scale PACS implementation*, J Digit Imaging. 1998;11(3 Suppl 1):3-7. doi: 10.1007/BF03168246.

Centonse M., Fileni A., Dalla Palma F., *Il Codice della Privacy: istruzioni per l'uso*, Supplemento de "Il Radiologo", SIRM Società Italiana di Radiologia Medica, 3/2005.

Charlesworth M., van Zundert AAJ., *Medical device regulation: the need for clinical vigilance and oversight*. Anaesthesia. 2019;74(6):693-695. doi: 10.1111/anae.14603.

Clunie D. A., *DICOM implementations for digital radiography*, Digital Radiogr.: RSNA Categorical Course in Diagn. Radiol. Phys, 2003, 163-172.

Crabtree A., Urquhart L., Chen J., *Right to an Explanation Considered Harmful*. Social Science Research Network (SSRN), 2019.

D'Cuncha C., *Una nuova visione per l'Europa*, Garante per la protezione dei dati personali, International Association of Privacy Professionals, 2019.

Dameff C., Bland M., Levchenko K., Tully F., *Pestilential Protocol: How Unsecure HL7 Messages Threaten Patient Lives*, 2018

Danezis G., Domingo-Ferrer J. Et al., *Privacy and Data Protection by Design - from policy to engineering*, ENISA (2014).

Donnelly M, McDonagh M., Health Research, *Consent and the GDPR Exemption*, Eur J Health Law. 2019;26(2):97-119. doi: 10.1163/15718093-12262427.

Drummond M., Velasco M. et al., *Best practice in undertaking and reporting health technology assessments*. Working group 4 report. Int J Technol Assess Health Care. 2002;18(2):361-422. doi: 10.1017/s0266462302000284.

Ehlers L., Vestergaard M. et al., *Doing mini-health technology assessments in hospitals: a new concept of decision support in health care?*, Int J Technol Assess Health Care. 2006;22(3):295-301. doi: 10.1017/s0266462306051178.

European Commission, Clinical Evaluation: G*uidelines on the Qualification and classification of Stand Alone Software used in Healthcare within the Regulatory Framework of Medical Devices*, Medical Devices: Guidance Document, MEDDEV 2.1/6(2016).

Feng D.D., *Biomedical Information Technology*, in "Biomedical Engineering", Academic Press, 2008. doi:10.1016/B978-012373583-6.50001-3.

Finck M., *Blockchain and the General Data Protection Regulation*, EPRS | European Parliamentary Research Service, Scientific Foresight Unit (STOA), PE 634.445 – July 2019; doi: 10.2861/535

Hansen, M., Jensen, M., Rost, M.: *Protection goals for privacy engineering*. In: 2015 International Workshop on Privacy Engineering (IWPE), Security and Privacy Workshops (SPW), pp. 159–166. IEEE (2015)

Hasselgren A, Kralevska K, Gligoroski D, Faxvaag A., *GDPR Compliant Blockchain and Distributed Ledger Technologies in the Health Sector*, Stud Health Technol Inform. 2020;270:1293-1294. doi: 10.3233/SHTI200408.

Iaselli M., *Protezione dei dati personali: le novità del nuovo Regolamento europeo*, Altalex, 2016

ISO 31000: Risk management – Guidelines, International Organization for Standardization (2018)

ISO/IEC 29134: Information technology – Security techniques – Privacy impact assessment – Guidelines. ISO/IEC, International Organization for Standardization (2018)

Kloza, Dariusz, et al., *Towards a Method for Data Protection Impact Assessment: Making Sense of GDPR Requirements*, Policy Brief D.PIA.LAB, vol. 1, 2019, pp. 1–8, doi:10.31228/osf.io/es8bm.

Lien, Chung-Yueh L., Chia-Hung H. et al., *Integrity and Authenticity of Quality Assurance and Control in an Imaging Examination Workflow*, HEALTHINF 2010 - 3rd International Conference on Health Informatics, Proceedings, 2010.

McKee D., Nordeck S., *80 to 0 in Under 5 Seconds: Falsifying a Medical Patient's Vitals*, https://doi.org/10.5446/39683

National Electrical Manufacturers Association: Digital Imaging and Communications in Medicine (DICOM). PS 3.1-3.15, 2008

Noumeir R., *Benefits of the DICOM Modality Performed Procedure Step*, Journal of Digital Imaging 18(4), 260-269, 2005.

Oemig F., *HL7 Version 2.x Goes FHIR*. Stud Health Technol Inform. 2019 Sep 3;267:93-98. doi: 10.3233/SHTI190811.

Orel A, Bernik I., *GDPR and Health Personal Data; Tricks and Traps of Compliance*, Stud Health Technol Inform. 2018;255:155-159. PMID: 30306927.

Pesapane F., Volonté C. et al., *Artificial intelligence as a medical device in radiology: ethical and regulatory issues in Europe and the United States*, Insights Imaging. 2018; 9(5):745-753. doi: 10.1007/s13244-018-0645-y.

Pillon S., *La sicurezza dei dispositivi medici è diventato un problema serio: come rimediare*, in "Agenda Digitale EU", 2018.

Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, L119/1, Gazzetta Ufficiale dell'Unione Europea.

Regolamento (UE) 2017/745 del Parlamento Europeo e del Consiglio del 5 aprile 2017, L117/1, Gazzetta Ufficiale dell'Unione Europea.

Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019, L151/15, Gazzetta Ufficiale dell'Unione Europea.

Riba M, Sala C, Toniolo D, Tonon G., *Big Data in Medicine, the Present and Hopefully the Future*, Front Med (Lausanne). 2019 Nov 15;6:263. doi: 10.3389/fmed.2019.00263.

Riccomagno A., *La privacy dei dati sanitari al tempo della pandemia*, in "PHCC: Policy and Procurement in Healthcare", 2021.

Riccomagno A., *Nuova strategia europea sui dati: quale impatto sulla sanità*, in "PHCC: Policy and Procurement in Healthcare", 2022.

Saetta B., *Sanità e Privacy*, in "Protezione dei dati personali", 2018.

Schüze B., Kroll M. et al*., Patient data security in the DICOM standard*, European Journal of Radiology 51(3), 286-289, 2004

Shah A., *10 Ways GDPR Will Affect Engineers*, in "Mechanical Engineering magazine", 2018

Vashkover A., *After the Dust Has Settled: GDPR in Healthcare*, Cyber MDX, 2021.

Wilkinson B., van Boxtel R., *The Medical Device Regulation of the European Union Intensifies Focus on Clinical Benefits of Devices*, Ther Innov Regul Sci. 2020;54(3):613-617. doi: 10.1007/s43441-019-00094-2.

Sitografia

https://www.agendadigitale.eu/sanita/

https://www.agid.gov.it

https://www.aiic.it/

https://www.altalex.com/documents/codici-altalex/2018/03/05/regolamento-generale-sulla-protezione-dei-dati-gdpr

https://www.aulss5.veneto.it/

https://www.azero.veneto.it/

https://www.buonepratichesicurezzasanita.it/

https://www.esaote.com/it-IT/healthcare-it/

https://www.garanteprivacy.it

https://healthmanagement.org/c/hospital/issuearticle/general-data-protection-regulation-and-healthcare

https://www.ingegnereclinico.it

https://www.iso.org

https://www.medicaldevicenews.eu/

https://www.medicalimaging.org/

www.medical.nema.org

https://www.riskmanagement360.it/analisti-ed-esperti/

https://www.salute.gov.it/portale/home.html

Ringraziamenti

A conclusione di questo elaborato, ritengo doveroso ringraziare alcune delle persone che mi hanno accompagnato in questi sei mesi di tirocinio e che hanno permesso la realizzazione del presente lavoro. In primo luogo, desidero ringraziare il Prof. Facchinetti, mio relatore, per l'interesse mostrato verso l'argomento trattato e per la costanza e attenzione con le quali sono stata seguita.

Ringrazio il mio tutor, l'Ing. Tenan, per aver accolto la mia proposta di tirocinio ed avermi così dato l'occasione non solo di realizzare questo lavoro, ma anche e soprattutto di acquisire un'esperienza altamente formativa all'interno dell'ambiente ospedaliero. Assieme a lui, i miei ringraziamenti vanno anche ai miei colleghi, un gruppo energico e sempre allegro, che ha reso il luogo di lavoro piacevole e sempre stimolante, e naturalmente tale riconoscenza si estende a tutta l'Azienda Ospedaliera ULSS 5.

Ringrazio il Dott. Favat, primario di Radiologia, che per primo mi ha proposto il suo reparto per lo svolgimento della tesi e mi ha messo in comunicazione attiva con tutto il personale di supporto. Ringrazio quindi la Dott.ssa Piga, il Dott. Fiorese, il Dott. Franceschetti e il Dott. Marchetto, i tecnici radiologi che mi hanno fatto da guida all'interno del reparto di Radiologia e hanno trovato sempre il tempo per rispondere alle mie domande e sciogliere i miei dubbi. Il mio ringraziamento finale va all'Ing. Tessarollo, della ditta Esaote, che ha collaborato con me nell'identificazione di tutte le possibili criticità del Sistema Informativo Radiologico del Polo Ospedaliero.

Allegato 1

Registro dei trattamenti generalizzato per il reparto di Radiologia, contenente le informazioni principali inerenti ai trattamenti svolti presso la struttura; queste sono state impiegate per una valutazione più approfondita e la realizzazione del Registro dei Trattamenti.

Unità Operativa	*Tipologia di trattamento*	*Finalità e liceità del trattamento*	*Tipologia di dati trattati*	*Categorie di interessati*	*Categorie di destinatari*	*Conserva-zione*	*Misure di sicurezza*	*Dati di contatto del titolare del trattamento*
UOC Radiologia	[X] raccolta [X] registrazione [X] organizzazione [X] strutturazione [X] conservazione [ ] adattamento o modifica [ ] estrazione [X] consultazione [X] uso [X] comunicazione mediante trasmissione [X] diffusione o qualsiasi altra forma di messa a disposizione [X] raffronto o interconnessione [ ] limitazione [ ] cancellazione o distruzione [ ] profilazione [ ] pseudonimizzazione [ ] altro	Regolamento UE 2016/679, art. 6, par.1, lett. a, b. Prestazioni erogate: • Ecografia • Esami di sala Operatoria • Densitometria • Mammografia* • Radiografia • Risonanza Magnetica • Tomografia Computerizzata (TAC) • Ortopantomografia	[X] Dati di localizzazione [X] Dati relativi alla salute (con evidenza del referto medico e/o informazioni su particolari disabilità) [ ] Dati relativi alla salute (appartenenza a categoria protetta o info su permessi per malattia o info su permessi per Maternità senza visibilità del referto medico) [X] Dati che rivelano l'origine razziale o etnica [ ] Dati che rivelano le opinioni politiche [ ] Dati che rivelano le convinzioni religiose o filosofiche [ ] Dati genetici [ ] Dati biometrici [ ] Dati relativi alla vita sessuale o all'orientamento sessuale di una persona	Pazienti, degenti, ospedalizzati, da pronto soccorso	Medici refertatori, personale ospedaliero autorizzato, pazienti, tecnico informatico autorizzato.	10 anni DM del 14 febbraio 1997, art.4	Conservazione dei dati in triplice copia presso sistema RIS/PACS. In caso di guasti, malfunzionamenti o blackout la prestazione può essere erogata in modalità analogica. Presenza continuata di un tecnico informatico sul posto in assistenza a servizio CED per un celere ripristino delle funzioni.	Azienda ULSS 5 POLESANA Sede legale: Viale tre martiri, 89 - 45100 Rovigo Codice Fiscale/Partita Iva: 01013470297 PEC: protocollo.aulss5@pecveneto.it Direttore Generale - Dr.ssa Patrizia Simionato- email: direzione.generale@aulss5.veneto.it

Allegato 2

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO PER LA VALUTAZIONE DELLA UOC RADIOLOGIA - Valutazione dei device medicali

Azienda U.L.S.S. n .5 - Polesana - P.O. Rovigo
Rilevazione a cura di: Dott.ssa Elena Crepaldi

Inventario	Tipologia	Descrizione sintetica dell'attività di trattamento dati supportata dall'apparato	Dati trattati		Modalità trattamento		Suddivisione apparecchiatura in base ai rischi: - apparecchiatura stand alone - apparecchiatura con sistema proprietario collegata alla rete dati - apparecchiatura PC based collegata alla rete dati	Misure tecniche di protezione dei dati	Misure fisiche di protezione dei dati	Rischio residuo
		Generazione e eventuale archiviazione di documenti (referti, esami, immagini, etc.) contenenti dati sensibili di tipo sanitario	personali	sensibili	conservati	archiviati				
111769	TAVOLO TOMOGRAFICO	Nessuna raccolta dati	X	X	X	X	Non applicabile	Non applicabile	Non applicabile	X
119022	DIAFANOSCOPIO	Nessuna raccolta dati	X	X	X	X	Non applicabile	Non applicabile	Non applicabile	X
119159	DIAFANOSCOPIO	Nessuna raccolta dati	X	X	X	X	Non applicabile	Non applicabile	Non applicabile	X
124247	DEFIBRILLATORE	Raccolta tracciati e registrazione vocale delle operazioni eseguite; Nessuna associazione dei dati raccolti con le anagrafiche paziente; Archiviazione su memoria fisica.	No	Sì	No	Sì	Apparecchiatura stand-alone con software proprio dedicato. Nessun collegamento con il Sistema Informativo.	Ritenute non necessarie	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**0**
149774	SIST. PORTATILE C-ARM MOBILE OEC 9600 ASP	Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di archiviazione una settimana ca, eliminazione progressiva dei	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati; Il software è incorporato nel dispositivo medico, rientra nella classificazione di Embedded.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; I dati fomiti sono inviati al Sistema RIS/PACS (principale ed ausiliari) attraverso la workstation dedicata e ivi mantenuti	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**

		file in ordine di acquisizione.						per le tempistiche di legge. Presenza di Firewall di protezione all'HIS.		
166995	ORTOPANTOMOGRAFO "PM 2002 CC" PLANMECA	Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di archiviazione una settimana ca, eliminazione progressiva dei file in ordine di acquisizione.	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati; Il software è incorporato nel dispositivo medico, rientra nella classificazione di Embedded.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) attraverso la workstation dedicata e ivi mantenuti per le tempistiche di legge. Presenza di Firewall di protezione all'HIS.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**
202825	GENERATORE RADIOLOGICO MGR50LP	Nessuna raccolta dati	X	X	X	X	Non applicabile	Non applicabile	Non applicabile	**X**
202826	GENERATORE RADIOLOGICO MGR50LP	Nessuna raccolta dati	X	X	X	X	Non applicabile	Non applicabile	Non applicabile	**X**
204063	COMPLESSO RADIOGENO RTM	Nessuna raccolta dati	X	X	X	X	Non applicabile	Non applicabile	Non applicabile	**X**
204064	COMPLESSO RADIOGENO RTM	Nessuna raccolta dati	X	X	X	X	Non applicabile	Non applicabile	Non applicabile	**X**
204791	MAMMOGRAFO SENOGRAPHE DMR V2	Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di archiviazione una settimana ca, eliminazione progressiva dei file in ordine di	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati; Il software è incorporato nel dispositivo medico, rientra nella classificazione di Embedded.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) attraverso la workstation dedicata e ivi mantenuti per le tempistiche di legge,	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**

		acquisizione.						con passaggio ulteriore del risultato all'Ufficio Screening. Presenza di Firewall di protezione all'HIS.		
205280	STAMPANTE B/N SONY UP 890	Nessuna raccolta dati	X	X	X	X	Non applicabile	Non applicabile	Non applicabile	**X**
205570	SCHERMO DI PROTEZIONE ANTI-X	Nessuna raccolta dati	X	X	X	X	Non applicabile	Non applicabile	Non applicabile	**X**
205824	NEGATIVOSCOPIO MOTORIZZ.PLANILUX	Nessuna raccolta dati	X	X	X	X	Non applicabile	Non applicabile	Non applicabile	**X**
207114	STAMPANTE TERMICA SONY UP-89X	Nessuna raccolta dati	X	X	X	X	Non applicabile	Non applicabile	Non applicabile	**X**
225681	MONITOR BARCO 3MP MOD.MFGD3420	Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; Accesso solamente mediante rete Intranet Aziendale; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**

225682	MONITOR BARCO 3MP MFGD3420	Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; Accesso solamente mediante rete Intranet Aziendale; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**
225684	ROBOT DI MASTERIZ.RIMAGE 2000I	Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni mediche associate; Possibilità di consultazione immagini e referti (per tecnici autorizzati).	No	No	No	No	Apparecchiatura PC based collegata alla rete dati; medesimo software di gestione anagrafiche ed immagini installato sulle workstation.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; Accesso solamente mediante rete Intranet Aziendale; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**

225693	MONITOR PLANAR 17"	Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni mediche associate; Possibilità di consultazione immagini e referti.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Ulteriore autenticazione mediante card e secondo pin; Nessun accesso alla visualizzazione web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**
225700	MICROFONO SPEECH MIKE PRO	Microfono di dettatura per la stesura di referti. Possibilità di mantenere in memoria i termini più utilizzati.	Sì	Sì	No	No	Apparecchiatura stand-alone con software proprio dedicato; collegamento con le Workstation attraverso cavo USB. Nessun collegamento alla rete.	Time-out della sessione automatico a cessato utilizzo. I dati passano dal microfono alla workstation senza conservazione della registrazione sul dispositivo; nessun collegamento con la rete.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**0**
225732	RIPRODUTTORE LASER	Nessuna raccolta dati	X	X	X	X	Non applicabile	Non applicabile	Non applicabile	**X**
226437	RIPRODUTTORE LASER	Nessuna raccolta dati	X	X	X	X	Non applicabile	Non applicabile	Non applicabile	**X**
227890	MICROFONO PHILIPS SPEECH MIKE CLASSIC USB	Microfono di dettatura per la stesura di referti. Possibilità di mantenere in memoria i termini più utilizzati.	Sì	Sì	No	No	Apparecchiatura stand-alone con software proprio dedicato; collegamento con le Workstation attraverso cavo USB. Nessun collegamento alla rete.	Time-out della sessione automatico a cessato utilizzo. I dati passano dal microfono alla workstation senza conservazione della registrazione sul dispositivo; nessun collegamento con la rete.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**0**

227891	MICROFONO PHILIPS SPEECH MIKE CLASSIC USB	Microfono di dettatura per la stesura di referti. Possibilità di mantenere in memoria i termini più utilizzati.	Sì	Sì	No	No	Apparecchiatura stand-alone con software proprio dedicato; collegamento con le Workstation attraverso cavo USB. Nessun collegamento alla rete.	Time-out della sessione automatico a cessato utilizzo. I dati passano dal microfono alla workstation senza conservazione della registrazione sul dispositivo; nessun collegamento con la rete.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**0**
227892	MICROFONO PHILIPS SPEECH MIKE CLASSIC USB	Microfono di dettatura per la stesura di referti. Possibilità di mantenere in memoria i termini più utilizzati.	Sì	Sì	No	No	Apparecchiatura stand-alone con software proprio dedicato; collegamento con le Workstation attraverso cavo USB. Nessun collegamento alla rete.	Time-out della sessione automatico a cessato utilizzo. I dati passano dal microfono alla workstation senza conservazione della registrazione sul dispositivo; nessun collegamento con la rete.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**0**
227924	PC WORKSTATION IBM Z51 SISTEMA PACS-RIS	Generazione di referti con invio a RIS/PACS; Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione immagini e referti.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Ulteriore autenticazione mediante card e secondo pin; Nessun accesso alla visualizzazione web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**

227926	PC WORKSTATION IBM Z52 SISTEMA PACS-RIS	Generazione di referti con invio a RIS/PACS; Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione immagini e referti.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Ulteriore autenticazione mediante card e secondo pin; Nessun accesso alla visualizzazione web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**
227930	MONITOR IBM LENOVO	Generazione di referti con invio a RIS/PACS; Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione immagini e referti.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Ulteriore autenticazione mediante card e secondo pin; Nessun accesso alla visualizzazione web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**

227931	MONITOR IBM LENOVO	Generazione di referti con invio a RIS/PACS; Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione immagini e referti.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Ulteriore autenticazione mediante card e secondo pin; Nessun accesso alla visualizzazione web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**
227932	MONITOR IBM LENOVO MOD.9417-AB6	Generazione di referti con invio a RIS/PACS; Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione immagini e referti.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Ulteriore autenticazione mediante card e secondo pin; Nessun accesso alla visualizzazione web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**

227949	PC WORKSTATION IBM Z51	Generazione di referti con invio a RIS/PACS; Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione immagini e referti.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Ulteriore autenticazione mediante card e secondo pin; Nessun accesso alla visualizzazione web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**
227952	PC WORKSTATION IBM Z51	Generazione di referti con invio a RIS/PACS; Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione immagini e referti.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Ulteriore autenticazione mediante card e secondo pin; Nessun accesso alla visualizzazione web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**

227956	PC WORKSTATION IBM Z51 - Muletto	Generazione di referti con invio a RIS/PACS; Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione immagini e referti.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Ulteriore autenticazione mediante card e secondo pin; Nessun accesso alla visualizzazione web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**
228011	MONITOR BARCO 5MP	Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione immagini.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; Accesso solamente mediante rete Intranet Aziendale; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**

228012	MONITOR BARCO 5MP	Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; Accesso solamente mediante rete Intranet Aziendale; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**
228013	MONITOR BARCO 3MP MOD.MFGD3420 SISTEMA PACS-RIS	Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; Accesso solamente mediante rete Intranet Aziendale; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**

228014	MONITOR BARCO 3MP MOD.MFGD3420	Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; Accesso solamente mediante rete Intranet Aziendale; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**
228572	SIST.X RADIOL.DIGIT.CR REGIUS 190 E ACCESSORI	Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di archiviazione una settimana ca, eliminazione progressiva dei file in ordine di acquisizione.	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati; Il software è incorporato nel dispositivo medico, rientra nella classificazione di Embedded.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) attraverso la workstation dedicata e ivi mantenuti per le tempistiche di legge, con passaggio ulteriore del risultato all'Ufficio Screening. Presenza di Firewall di protezione all'HIS.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**

231344	SIST.X RADIOL.DIGIT.CR REGIUS 190 E ACCES.E SOTW.MAMMOG RAFICO MAMMO HQ	Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di archiviazione una settimana ca, eliminazione progressiva dei file in ordine di acquisizione.	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati; Il software è incorporato nel dispositivo medico, rientra nella classificazione di Embedded.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) attraverso la workstation dedicata e ivi mantenuti per le tempistiche di legge, con passaggio ulteriore del risultato all'Ufficio Screening. Presenza di Firewall di protezione all'HIS.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**
235589	MACCHINA GENERATRICE DI OZONO OZO2	Nessuna raccolta dati	X	X	X	X	Non applicabile	Non applicabile	Non applicabile	**X**
290681	CONSOLLE DI REFERTAZIONE	Generazione di referti con invio a RIS/PACS; Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione immagini, referti e cartelle cliniche.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Ulteriore autenticazione mediante card e secondo pin; Nessun accesso alla visualizzazione web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**
290682	GRUPPO CONTINUITA'	Nessuna raccolta dati	X	X	X	X	Non applicabile	Non applicabile	Non applicabile	**X**

298807	MICROFONO PHILIP SPEECH MIKE	Microfono di dettatura per la stesura di referti. Possibilità di mantenere in memoria i termini più utilizzati.	Sì	Sì	No	No	Apparecchiatura stand-alone con software proprio dedicato; collegamento con le Workstation attraverso cavo USB. Nessun collegamento alla rete.	Time-out della sessione automatico a cessato utilizzo. I dati passano dal microfono alla workstation senza conservazione della registrazione sul dispositivo; nessun collegamento con la rete.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**
302204	STAMPANTE DIGITALE SONY	Nessuna raccolta dati	X	X	X	X	Non applicabile	Non applicabile	Non applicabile	**X**
302888	ECOGRAFO LOGOS HI VISION GOLD	Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di archiviazione una settimana ca, eliminazione progressiva dei file in ordine di acquisizione. Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati. Il software è installato sul dispositivo medico, rientra nella classificazione di on-board.	Utilizzo tramite card di accesso disponibile per il personale addetto, non è richiesta autenticazione; Nessun collegamento web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) direttamente dal monitor installato sull'elettromedicale e ivi mantenuti per le tempistiche di legge. Presenza di Firewall di protezione all'HIS.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**
302889	STAMPANTE TERMICA SONY	Nessuna raccolta dati	X	X	X	X	Non applicabile	Non applicabile	Non applicabile	**X**
305768	RISONANZA MAGNETICA OASIS	Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di archiviazione una settimana ca, eliminazione progressiva dei file in ordine di acquisizione.	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati; Il software è incorporato sul dispositivo medico, rientra nella classificazione di Embedded.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; I dati forniti sono inviati al Sistema RIS/PACS attraverso la workstation dedicata e ivi mantenuti per le tempistiche di legge. Firewall di protezione all'HIS.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**

305995	INIETTORE MEZZO DI CONTRASTO	Nessuna raccolta dati	X	X	X	X	Non applicabile	Non applicabile	Non applicabile	**X**
307704	DEFIBRILLATORE DEFIGARD 972500821	Raccolta tracciati e registrazione vocale delle operazioni eseguite; Nessuna associazione dei dati raccolti con le anagrafiche paziente; Archiviazione su memoria fisica.	No	Sì	No	Sì	Apparecchiatura stand-alone con software incorporato (Embedded); nessun collegamento alla rete dati.	Ritenute non necessarie	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**0**
307705	MONITOR AMAGNETICO MAGLIFE SERENITY	Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; Accesso solamente mediante rete Intranet Aziendale; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**

307706	MONITOR MAGSCREEN	Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; Accesso solamente mediante rete Intranet Aziendale; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**
316328	DEFIBRILLATORE	Raccolta tracciati e registrazione vocale delle operazioni eseguite; Nessuna associazione dei dati raccolti con le anagrafiche paziente; Archiviazione su memoria fisica.	No	Sì	No	Sì	Apparecchiatura stand-alone con software proprio dedicato. Nessun collegamento con il Sistema Informativo.	Ritenute non necessarie	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**0**
316329	DEFIBRILLATORE	Raccolta tracciati e registrazione vocale delle operazioni eseguite; Nessuna associazione dei dati raccolti con le anagrafiche paziente; Archiviazione su memoria fisica.	No	Sì	No	Sì	Apparecchiatura stand-alone con software proprio dedicato. Nessun collegamento con il Sistema Informativo.	Ritenute non necessarie	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**0**

317880	SERVER E SOFTWARE TAC TC64	Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; Accesso solamente mediante rete Intranet Aziendale; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**
319585	INSUFFLATORE C02	No	X	X	X	X	Non applicabile	Non applicabile	Non applicabile	**X**
320699	ECOGRAGO	Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di archiviazione una settimana ca, eliminazione progressiva dei file in ordine di acquisizione. Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati. L'ecografo è costituito da un monitor di visualizzazione integrato: il software è integrato sul dispositivo medico, rientra nella classificazione di on-board.	Utilizzo tramite card di accesso disponibile per il personale addetto, non è richiesta autenticazione; Nessun collegamento web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) direttamente dal monitor installato sull'elettromedicale e ivi mantenuti per le tempistiche di legge. Presenza di Firewall di protezione all'HIS.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**
320836	ECOGRAFO	Raccolta informazioni anagrafiche paziente ed immagini radiologiche;	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati. Il sistema radiologico portatile è costituito da un monitor di visualizzazione	Utilizzo tramite card di accesso disponibile per il personale addetto, non è richiesta autenticazione; Nessun collegamento web; I dati forniti sono inviati al	Device situato in locali ad accesso riservato al personale	**3.556**

		Memoria di archiviazione una settimana ca, eliminazione progressiva dei file in ordine di acquisizione. Possibilità di consultazione di immagini.					integrato: il software è integrato sul dispositivo medico, rientra nella classificazione di on-board. Collegamento con software di gestione delle anagrafiche tramite integrazioni.	Sistema RIS/PACS (principale ed ausiliari) direttamente dal monitor installato sull'elettromedicale e ivi mantenuti per le tempistiche di legge. Presenza di Firewall di protezione all'HIS.	ospedaliero autorizzato.	
324533	RADIOLOGICO PORTATILE	Raccolta informazioni anagrafiche paziente, immagini radiologiche ed informazioni mediche associate; Possibilità di conservazione immagini 24-48h.	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati. Il sistema radiologico portatile è costituito da un monitor di visualizzazione integrato: il software è integrato sul dispositivo medico, rientra nella classificazione di on-board. Collegamento con software di gestione delle anagrafiche tramite integrazioni.	Utilizzo tramite card di accesso disponibile per il personale addetto, non è richiesta autenticazione; Nessun collegamento web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) attraverso la workstation dedicata e ivi mantenuti per le tempistiche di legge,	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**
325419	INIETTORE ANGIOGRAFICO	Nessuna raccolta dati	X	X	X	X	Non applicabile	Non applicabile	Non applicabile	**X**
326252	APPARECCHIA-TURA RADIOLOGICA OPTIMA XR200	Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di archiviazione una settimana ca, eliminazione progressiva dei file in ordine di acquisizione.	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati; Il software è incorporato nel dispositivo medico, rientra nella classificazione di Embedded.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) attraverso la workstation dedicata e ivi mantenuti per le tempistiche di legge. Presenza di Firewall di protezione all'HIS.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**

328568	BARELLA AMAGNETICA 3 TESLA RM108	Nessuna raccolta dati	X	X	X	X	Non applicabile	Non applicabile	Non applicabile	**X**
328601	SISTEMA RADIOLOGICO TELECOMANDA-TO SIREVIX	Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di archiviazione una settimana ca, eliminazione progressiva dei file in ordine di acquisizione.	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati; Il software è incorporato nel dispositivo medico, rientra nella classificazione di Embedded.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) attraverso la workstation dedicata e ivi mantenuti per le tempistiche di legge. Presenza di Firewall di protezione all'HIS.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**
328909	ECOGRAFO EÈKOQ 5G	Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di archiviazione una settimana ca, eliminazione progressiva dei file in ordine di acquisizione. Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati. Il sistema radiologico portatile è costituito da un monitor di visualizzazione integrato: il software è integrato sul dispositivo medico, rientra nella classificazione di on-board. Collegamento con software di gestione delle anagrafiche tramite integrazioni.	Utilizzo tramite card di accesso disponibile per il personale addetto, non è richiesta autenticazione; Nessun collegamento web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) direttamente dal monitor installato sull'elettromedicale e ivi mantenuti per le tempistiche di legge. Presenza di Firewall di protezione all'HIS.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**
328909	ECOGRAFO EÈKOQ 5G	Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di archiviazione una	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati. Il sistema radiologico portatile è costituito da un monitor di visualizzazione integrato: il software è integrato sul dispositivo	Utilizzo tramite card di accesso disponibile per il personale addetto, non è richiesta autenticazione; Nessun collegamento web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari)	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**

		settimana ca, eliminazione progressiva dei file in ordine di acquisizione. Possibilità di consultazione di immagini.					medico, rientra nella classificazione di on-board. Collegamento con software di gestione delle anagrafiche tramite integrazioni.	direttamente dal monitor installato sull'elettromedicale e ivi mantenuti per le tempistiche di legge. Presenza di Firewall di protezione all'HIS.		
328990	STAMPANTE	No	X	X	X	X	Non applicabile	X	X	**X**
329031	PROTEZIONI RX	No	X	X	X	X	Non applicabile	X	X	**X**
329212	RIVELATORE FERR.	No	X	X	X	X	Non applicabile	X	X	**X**
329662	TAC SOMATOM DEFINITION EDGE	Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di archiviazione una settimana ca, eliminazione progressiva dei file in ordine di acquisizione.	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati; Il software è incorporato nel dispositivo medico, rientra nella classificazione di Embedded.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) attraverso la workstation dedicata e ivi mantenuti per le tempistiche di legge. Presenza di Firewall di protezione all'HIS.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**
329663	WORKSTATION SYNGO.VIA	Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni mediche associate; Possibilità di	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; Accesso solamente mediante rete Intranet Aziendale; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge;	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**

		consultazione immagini.						Time-out della sessione con necessità di reinserimento password; Firewall di protezione.		
330256	WORKSTATION SHARE 7 M81521KA	Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni mediche associate; Possibilità di consultazione immagini.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; Accesso solamente mediante rete Intranet Aziendale; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**
330257	TAC REVOLUTION EVO B75632RE	Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di archiviazione una settimana ca, eliminazione progressiva dei file in ordine di acquisizione.	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati; Il software è incorporato nel dispositivo medico, rientra nella classificazione di Embedded.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) attraverso la workstation dedicata e ivi mantenuti per le tempistiche di legge. Presenza di Firewall di protezione all'HIS.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**

332574	ECOGRAFO MYLAB ALPHA EHD	Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di archiviazione una settimana ca, eliminazione progressiva dei file in ordine di acquisizione. Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati. Il sistema radiologico portatile è costituito da un monitor di visualizzazione integrato: il software è integrato sul dispositivo medico, rientra nella classificazione di on-board. Collegamento con software di gestione delle anagrafiche tramite integrazioni.	Utilizzo tramite card di accesso disponibile per il personale addetto, non è richiesta autenticazione; Nessun collegamento web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) direttamente dal monitor installato sull'elettromedicale e ivi mantenuti per le tempistiche di legge. Presenza di Firewall di protezione all'HIS.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**
332575	ECOGRAFO MYLAB ALPHA EHD	Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di archiviazione una settimana ca, eliminazione progressiva dei file in ordine di acquisizione. Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati. Il sistema radiologico portatile è costituito da un monitor di visualizzazione integrato: il software è integrato sul dispositivo medico, rientra nella classificazione di on-board. Collegamento con software di gestione delle anagrafiche tramite integrazioni.	Utilizzo tramite card di accesso disponibile per il personale addetto, non è richiesta autenticazione; Nessun collegamento web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) direttamente dal monitor installato sull'elettromedicale e ivi mantenuti per le tempistiche di legge. Presenza di Firewall di protezione all'HIS.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**
332576	ECOGRAFO MYLAB ALPHA EHD	Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di archiviazione una settimana ca,	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati. Il sistema radiologico portatile è costituito da un monitor di visualizzazione integrato: il software è integrato sul dispositivo medico, rientra nella	Utilizzo tramite card di accesso disponibile per il personale addetto, non è richiesta autenticazione; Nessun collegamento web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) direttamente dal monitor	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**

		eliminazione progressiva dei file in ordine di acquisizione. Possibilità di consultazione di immagini.					classificazione di on-board. Collegamento con software di gestione delle anagrafiche tramite integrazioni.	installato sull'elettromedicale e ivi mantenuti per le tempistiche di legge. Presenza di Firewall di protezione all'HIS.		
332577	ECOGRAFO MYLAB ALPHA EHD	Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di archiviazione una settimana ca, eliminazione progressiva dei file in ordine di acquisizione. Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati. Il sistema radiologico portatile è costituito da un monitor di visualizzazione integrato: il software è integrato sul dispositivo medico, rientra nella classificazione di on-board. Collegamento con software di gestione delle anagrafiche tramite integrazioni.	Utilizzo tramite card di accesso disponibile per il personale addetto, non è richiesta autenticazione; Nessun collegamento web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) direttamente dal monitor installato sull'elettromedicale e ivi mantenuti per le tempistiche di legge. Presenza di Firewall di protezione all'HIS.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**
332916	SISTEMADRX REVOLUTION NANO PORTATILE RADIOLOGICO	Raccolta informazioni anagrafiche paziente, immagini radiologiche ed informazioni mediche associate; Possibilità di conservazione immagini 24-48h.	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati. Il sistema radiologico portatile è costituito da un monitor di visualizzazione integrato: il software è integrato sul dispositivo medico, rientra nella classificazione di on-board. Collegamento con software di gestione delle anagrafiche tramite integrazioni.	Utilizzo tramite card di accesso disponibile per il personale addetto, non è richiesta autenticazione; Nessun collegamento web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) attraverso la workstation dedicata e ivi mantenuti per le tempistiche di legge,	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**
333991	INIETTORE PER TAC	No	X	X	X	X	Non applicabile	Non applicabile	Non applicabile	**X**

334594	ECOGRAFO GE VIVID T8	Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di archiviazione una settimana ca, eliminazione progressiva dei file in ordine di acquisizione. Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati. Il sistema radiologico portatile è costituito da un monitor di visualizzazione integrato: il software è integrato sul dispositivo medico, rientra nella classificazione di on-board. Collegamento con software di gestione delle anagrafiche tramite integrazioni.	Utilizzo tramite card di accesso disponibile per il personale addetto, non è richiesta autenticazione; Nessun collegamento web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) direttamente dal monitor installato sull'elettromedicale e ivi mantenuti per le tempistiche di legge. Presenza di Firewall di protezione all'HIS.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**
334594	ECOGRAFO GE VIVID T8	Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di archiviazione una settimana ca, eliminazione progressiva dei file in ordine di acquisizione. Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati. Il sistema radiologico portatile è costituito da un monitor di visualizzazione integrato: il software è integrato sul dispositivo medico, rientra nella classificazione di on-board. Collegamento con software di gestione delle anagrafiche tramite integrazioni.	Utilizzo tramite card di accesso disponibile per il personale addetto, non è richiesta autenticazione; Nessun collegamento web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) direttamente dal monitor installato sull'elettromedicale e ivi mantenuti per le tempistiche di legge. Presenza di Firewall di protezione all'HIS.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**

336689	SISTEMA TELECOMANDATO G800IQ OPERA SWING	Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di archiviazione una settimana ca, eliminazione progressiva dei file in ordine di acquisizione.	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati; Il software è incorporato nel dispositivo medico, rientra nella classificazione di Embedded.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) attraverso la workstation dedicata e ivi mantenuti per le tempistiche di legge. Presenza di Firewall di protezione all'HIS.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**
338670	PORTATILE RADIOLOGICO CARESTREAM	Raccolta informazioni anagrafiche paziente, immagini radiologiche ed informazioni mediche associate; Possibilità di conservazione immagini 24-48h.	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati. Il sistema radiologico portatile è costituito da un monitor di visualizzazione integrato: il software è integrato sul dispositivo medico, rientra nella classificazione di on-board. Collegamento con software di gestione delle anagrafiche tramite integrazioni.	Utilizzo tramite card di accesso disponibile per il personale addetto, non è richiesta autenticazione; Nessun collegamento web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) attraverso la workstation dedicata e ivi mantenuti per le tempistiche di legge,	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**
338677	MAMMOGRAFO SELENIA DIMENSIONS 3000	Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di conservazione 24h.	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati; Il software è incorporato nel dispositivo medico, rientra nella classificazione di Embedded.	Utilizzo tramite card di accesso disponibile per il personale addetto, non è richiesta autenticazione; Nessun collegamento web; I dati forniti sono inviati al Sistema RIS/PACS attraverso la workstation dedicata e ivi mantenuti per le tempistiche di legge, con passaggio ulteriore del risultato all'Ufficio Screening.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**

339686	CARESTREAM DRX-REVOLUTION PORTATILE RADIOLOGICO	Raccolta informazioni anagrafiche paziente, immagini radiologiche ed informazioni mediche associate; Possibilità di conservazione immagini 24-48h.	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati. Il sistema radiologico portatile è costituito da un monitor di visualizzazione integrato: il software è integrato sul dispositivo medico, rientra nella classificazione di on-board. Collegamento con software di gestione delle anagrafiche tramite integrazioni.	Utilizzo tramite card di accesso disponibile per il personale addetto, non è richiesta autenticazione; Nessun collegamento web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) attraverso la workstation dedicata e ivi mantenuti per le tempistiche di legge,	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**
339716	BARCO CORONIS FUSION COD. K9602943	Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; Accesso solamente mediante rete Intranet Aziendale; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**
345402	BARCO CORONIS FUSION COD. K9602943	Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; Accesso solamente mediante rete Intranet Aziendale; I dati forniti sono inviati al Sistema	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**

		esse associate; Possibilità di consultazione di immagini.					svolgerà l'esame.	RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.		
345403	BARCO CORONIS FUSION COD. K9602943	Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; Accesso solamente mediante rete Intranet Aziendale; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**
345404	BARCO CORONIS FUSION COD. K9602943	Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; Accesso solamente mediante rete Intranet Aziendale; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**

345405	BARCO CORONIS FUSION COD. K9602943	Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; Accesso solamente mediante rete Intranet Aziendale; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**
345406	BARCO CORONIS FUSION COD. K9602943	Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; Accesso solamente mediante rete Intranet Aziendale; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**

345407	BARCO MDCG-5221 CB MKII	Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; Accesso solamente mediante rete Intranet Aziendale; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**
345408	BARCO CORONIS FUSION COD. K9602943	Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; Accesso solamente mediante rete Intranet Aziendale; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**

345409	BARCO MDCG-5221 CB MKII	Raccolta e gestione di informazioni anagrafiche dei pazienti; Raccolta ed elaborazione delle immagini radiologiche ed informazioni ad esse associate; Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura PC based collegata alla rete dati. Le workstation di elaborazione e di refertazione (che rientrano nella classificazione informatica di console e terminali) sono dotate di un software di tipo accessorio, sono associati all'elettromedicale che svolgerà l'esame.	Utilizzo vincolato al possesso di credenziali di accesso fornite dall'amministratore di sistema; Necessità di autenticazione all'avvio; Accesso solamente mediante rete Intranet Aziendale; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) e ivi mantenuti per le tempistiche di legge; Time-out della sessione con necessità di reinserimento password; Firewall di protezione.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**5.328**
346892	ECOGRAFO APLIO CUS AA000/S3	Raccolta informazioni anagrafiche paziente ed immagini radiologiche; Memoria di archiviazione una settimana ca, eliminazione progressiva dei file in ordine di acquisizione. Possibilità di consultazione di immagini.	Sì	Sì	No	Sì	Apparecchiatura con sistema proprietario collegata alla rete dati. L'ecografo è costituito da un monitor di visualizzazione integrato: il software è integrato sul dispositivo medico, rientra nella classificazione di on-board.	Utilizzo tramite card di accesso disponibile per il personale addetto, non è richiesta autenticazione; Nessun collegamento web; I dati forniti sono inviati al Sistema RIS/PACS (principale ed ausiliari) direttamente dal monitor installato sull'elettromedicale e ivi mantenuti per le tempistiche di legge. Presenza di Firewall di protezione all'HIS.	Device situato in locali ad accesso riservato al personale ospedaliero autorizzato.	**3.556**