IRCCS
Ospedale Sacro Cuore
Don Calabria

Valutazione di Impatto
Studio: “VALUTAZIONE DELLA PLACCA ATEROSCLEROTICA IN PAZIENTI AFFETTI DA CARCINOMA DEL POLMONE NON A PICCOLE CELLULE TRATTATI O NON TRATTATI CON INIBITORI DEL CHECKPOINT IMMUNITARIO: STUDIO RETROSPETTIVO (CARDIO-ICI)”

---

ai sensi del Regolamento (UE) 2016/679 - GDPR

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE

[Vers app 7.4.8902; vers db 1.0]

1. SOMMARIO

2. PREMESSE

L'IRCCS Ospedale Sacro Cuore Don Calabria è un ospedale classificato, presidio ospedaliero accreditato con la Regione Veneto e Istituto di Ricovero e Cura a Carattere Scientifico per le malattie infettive e tropicali. Pertanto, l'Ospedale svolge, nella disciplina di propria competenza, attività di ricerca scientifica. Centrale per l'Ospedale è l'attività di ricerca scientifica, perseguita nell'ambito delle malattie infettive e tropicali secondo standard di eccellenza. L'Ospedale svolge, altresì, attività di ricerca scientifica anche in altri ambiti. La presente valutazione, dunque, mira a disciplinare il progetto di ricerca in oggetto, che l'Ospedale intende effettuare in conformità alla specifica normativa di riferimento.

Nel dettaglio il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito il "Regolamento") prevede all'articolo 35, il concetto di valutazione di impatto sulla protezione dei dati (nota anche come Data Protection Impact Assessmet – DPIA).

La valutazione di impatto deve essere effettuata quando un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche considerati la natura, l'oggetto, il contesto e le finalità del trattamento, in particolare quando prevede l'uso di nuove tecnologie.

Il titolare del trattamento, in tali casi, è tenuto ad effettuare una valutazione di impatto prima di procedere al trattamento secondo quanto previsto dall'art. 35 del GDPR

Il trattamento dei dati per finalità di Ricerca scientifica, in particolare, rientra nei casi dettati dall'art. 35, par. 3 del GDPR, per i quali è prevista la necessaria conduzione di una DPIA in quanto prevede:

a. *una 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;*
b. *il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;*

La normativa italiana ha introdotto, altresì, specifiche disposizioni nell'ambito del Codice privacy che riguardano la Ricerca:

1) l'art. 110 del Codice Privacy rubricato "Ricerca medica, biomedica ed epidemiologica".
2) l'art. 110 bis del Codice Privacy rubricato "*Trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici*"

Nel dettaglio l'art. 110 del Codice novellato, prevede che nell'ambito di un progetto di ricerca scientifica in cui risulta impossibile ottenere il consenso dell'interessato, i dati personali possono essere trattati per fini di ricerca scientifica a condizione che sia ottenuto il parere favorevole del competente comitato etico e che siano osservate le garanzie dettate dal Garante per la protezione dei dati personali (articolo 106 dello stesso Codice).

La norma, infatti, recita*: "Il consenso dell'interessato… non è necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale. Nei casi di cui al presente comma, il Garante individua le garanzie da osservare ai sensi dell'articolo 106, comma 2, lettera d), del presente codice*". In ogni caso resta salvo l'obbligo per il titolare di effettuare e rendere pubblica una valutazione di impatto ai sensi degli artt. 35 e 36 del Regolamento UE 2016/679.

A seguito dell'intervenuta modifica normativa, il Garante per la protezione dei dati personali ha, altresì, emesso il Provvedimento a carattere generale "*Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica ai sensi degli artt. 2-quater e 106 del Codice privacy – 9 Maggio 2024*". Mediante tale provvedimento, ha specificato quali sono le garanzie che il titolare del trattamento deve osservare nel trattamento dei dati per finalità di ricerca scientifica ai sensi del novellato art, 110 del Codice della privacy.

In particolare, ha stabilito che il titolare del trattamento oltre ad adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato e acquisire il parere favorevole del competente comitato etico a livello territoriale sul progetto di ricerca come previsto dall'art. 110 del Codice, deve accuratamente motivare e documentare, nel progetto di ricerca, la sussistenza delle ragioni etiche o organizzative per le quali informare gli interessati e quindi acquisire il consenso, risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, se del caso documentando altresì i ragionevoli sforzi profusi per tentare di contattarli.

Nei predetti casi, i titolari del trattamento di dati sulla salute per finalità di ricerca medica, biomedica e epidemiologica riferiti a soggetti deceduti o non contattabili devono altresì svolgere e pubblicare la valutazione di impatto, ai sensi dell'art. 35 del Regolamento, dandone comunicazione al Garante.

Quanto, invece, all'art. 110 bis del Codice Privacy, la norma al comma 4 prevede uno specifico riferimento agli IRCCS: "*Non costituisce trattamento ulteriore da parte di terzi il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell'osservanza di quanto previsto dall'articolo 89 del Regolamento*".

La norma, dunque, disciplina la possibilità per gli IRCCS di svolgere attività di ricerca scientifica su dati raccolti da soggetti diversi dagli stessi per lo svolgimento di attività clinica senza che vi sia la necessità di richiedere la preventiva autorizzazione al Garante della privacy.

A tal proposito il Garante ha emesso delle Faq specifiche per gli IRCCS relativamente all'utilizzo che possono fare dei dati raccolti per l'attività clinica per ulteriori finalità di ricerca medica inerente le linee di ricerca di propria competenza, autorizzate dal Ministero della salute. Il Garante ha, dunque, chiarito che gli IRCCS pubblici e privati, oltre che sul consenso dei partecipanti alla ricerca, possono fondare il trattamento dei dati personali raccolti a scopo di cura per ulteriori finalità di ricerca sull'art. 110-bis, comma 4 del Codice privacy, in base al quale non costituisce trattamento ulteriore dei dati raccolti per l'attività clinica, quello svolto dagli stessi a fini di ricerca.

Il Garante ha specificato, altresì, che l'art. 110-bis, comma 4 del Codice trova pertanto applicazione in relazione ad ogni tipo di ricerca medica, biomedica, epidemiologica, prospettica e retrospettiva, promossa dagli IRCCS ivi inclusi gli studi multicentrici, sia svolti nell'ambito delle reti di ricerca degli IRCCS che in quelli multicentrici promossi da tali istituti con la partecipazione di enti che non godono di tale riconoscimento.

Nel caso in cui gli IRCCS fondino il trattamento dei dati raccolti per finalità di cura per ulteriori finalità di ricerca sull'art. 110-bis, comma 4 del Codice, essi devono obbligatoriamente svolgere e pubblicare la Valutazione d'impatto sui propri siti web, in quanto tale articolo costituisce una di quelle disposizioni di legge alle quali fa riferimento l'art. 110 del Codice, prescrivendo tali ulteriori adempimenti.

L'IRCCS Ospedale Sacro Cuore Don Calabria, dunque, con il presente documento si è attivata al fine di effettuare una valutazione di impatto prima di iniziare il trattamento che la richiede, in considerazione delle caratteristiche della ricerca scientifica che intenderà svolgere. Tale valutazione è effettuata considerando, in particolare, probabilità e gravità del rischio, tenuto conto della natura, dell'ambito di applicazione, del contesto, delle finalità del trattamento e delle fonti di rischio. La valutazione di impatto verte anche sulle misure, sulle garanzie e sui meccanismi previsti per attenuare il rischio assicurando la protezione dei dati personali e dimostrando la conformità al Regolamento. Le misure in parola saranno riesaminate e aggiornate qualora necessario.

3. METODOLOGIA DI LAVORO

La valutazione di impatto sulla protezione dei dati, che si intende formalizzare nel presente documento, è stata effettuata secondo una metodologia elaborata in base al dettato dell'articolo 35 del Regolamento e articolata sulla base degli spunti di riflessione offerti dal WP29 (*Articolo 29 – Data Protection Working Party*) con il documento *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* pubblicate il 04.04.2017).

La metodologia seguita nella valutazione è ben rappresentata dalla figura sottostante, che è tratta dalle guidelines citate.

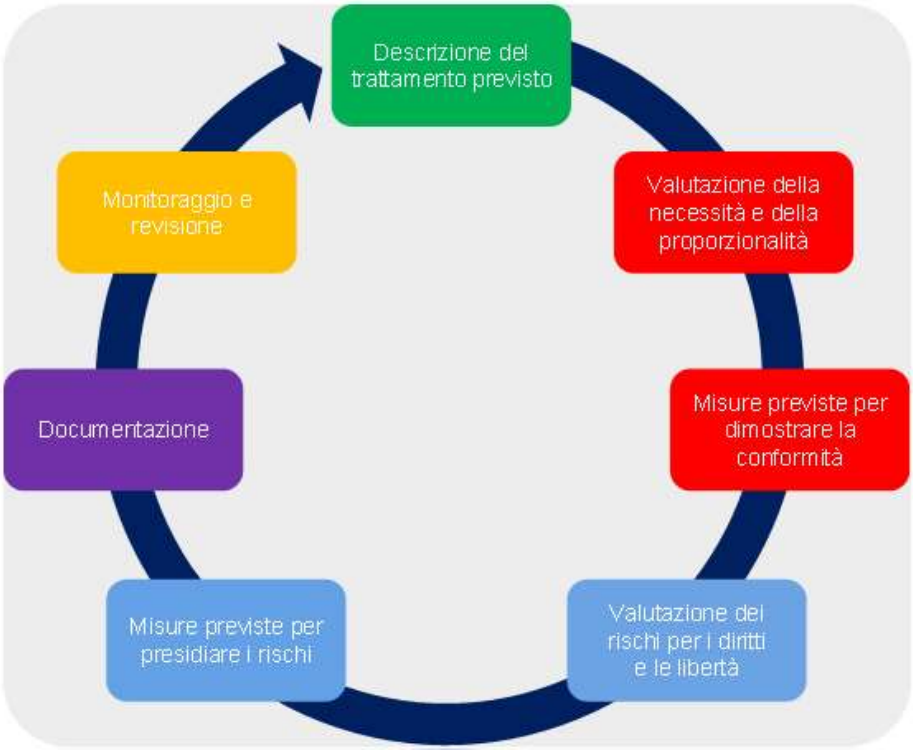

Figura 1 – Processo di svolgimento della valutazione d'impatto sulla protezione dei dati

La valutazione posta in essere dal titolare del trattamento è stata articolata nelle seguenti attività:

1. individuazione dei trattamenti che richiedono una valutazione di impatto;
2. descrizione sistematica dei trattamenti che presentano un rischio elevato per i diritti e le libertà delle persone fisiche;
3. valutazione della necessità e proporzionalità del trattamento in relazione alle finalità;
4. valutazione dei rischi per i diritti e le libertà degli interessati;
5. individuazione delle misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione;
6. piano di trattamento del rischio.

3.1. INDIVIDUAZIONE DEI TRATTAMENTI CHE RICHIEDONO UNA DPIA

L'individuazione dei trattamenti posti in essere dal titolare del trattamento per i quali è richiesta una valutazione di impatto sulla protezione dei dati è stata effettuata esaminando:

1. le considerazioni del WP29 (Articolo 29 – Data Protection Working Party) che ha definito una serie di criteri suscettibili a provocare un rischio elevato nell'ambito del documento Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. Più sono i criteri riferibili a un trattamento che il titolare pone in essere, più è probabile che il trattamento stesso presenti un rischio elevato per i diritti e le libertà delle persone fisiche e quindi richieda una valutazione di impatto per la protezione dei dati. Come regola generale il WP29 indica che un trattamento in cui siano individuabili almeno due criteri richieda una DPIA. Di seguito si riportano i criteri indicativi della necessità di condurre una valutazione di impatto così come individuati dal WP29:
    - Valutazione o assegnazione di un punteggio;
    - Decisioni automatiche con effetti giuridici o similmente significativi;
    - Controllo sistematico;
    - Dati particolari;
    - Dati elaborati su larga scala;
    - Numero di persone interessate;
    - Volume dei dati o la gamma di diversi elementi di dati in corso di elaborazione;
    - Durata e permanenza dell'attività di elaborazione dati;
    - Estensione geografica dell'attività di elaborazione;
    - Set di dati che sono stati abbinati o combinati;
    - Dati relativi ad interessati vulnerabili;
    - Uso innovativo o applicazione di soluzioni tecnologiche o organizzative;
    - Trasferimento di dati attraverso i confini al di fuori dell'Unione Europea;
    - Impossibilità da parte degli interessati di esercitare un diritto o utilizzare un servizio o un contratto.

   A questi criteri si aggiungono, o sovrappongono, le circostanze individuate a livello normativo nel comma 3 dell'articolo 35 del Regolamento.
2. Il Provvedimento dell'Autorità Garante per la protezione dei dati personali dell'11 ottobre 2018 contenente l'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, (di seguito "**Provvedimento**").
3. Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (aut. gen. n. 9/2016).
4. Provvedimento a carattere generale "*Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica ai sensi degli artt. 2-quater e 106 del Codice privacy – 9 maggio 2024*"
5. Codice in materia di protezione dei dati personali, D Lgs. n. 196/2003 aggiornato con le modifiche apportate dalla L. 29 aprile 2024, n. 56.

3.2. DESCRIZIONE SISTEMATICA DEI TRATTAMENTI

La prima attività da svolgersi laddove si decida di intraprendere un processo di valutazione di impatto consiste nella descrizione sistematica dei trattamenti che richiedono lo svolgimento.

Il considerando 90 al Regolamento prevede che la valutazione di impatto deve infatti tenere conto anzitutto "*della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio*" insite nel processo di trattamento.

Il titolare del trattamento ha, preliminarmente all'attivazione del processo di valutazione di impatto, già provveduto ad effettuare un esame approfondito dei trattamenti di dati personali posti in essere nell'ambito attività previste dal Regolamento.

Tale attività è stata svolta per redigere il Registro dei trattamenti. Nello specifico, per ciascun trattamento rilevato, il Registro dei trattamenti riporta:

- una descrizione del trattamento;
- le categorie di interessati e le categorie di dati personali;
- le modalità di raccolta e di trattamento dei dati;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- 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 del Regolamento, la documentazione delle garanzie adeguate;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- le risorse attraverso cui sono trattati i dati personali (hardware, software, reti, persone, mezzi cartacei o di trasmissione cartacea);
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

3.3. VALUTAZIONE DELLA NECESSITÀ E PROPORZIONALITÀ DEL TRATTAMENTO

La valutazione della necessità e della proporzionalità dei trattamenti deve essere applicata, nell'ambito del processo di valutazione di impatto per la protezione dei dati personali, rispetto ai trattamenti individuati e quindi descritti nell'ambito delle attività di cui al punto 3.2 precedente.

La valutazione in parola è stata effettuata dal titolare del trattamento in base ai criteri definiti dal WP29 (*Articolo 29 – Data Protection Working Party*) sempre all'interno delle "*Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679"*.

Il trattamento è da ritenersi **necessario e proporzionale** se sono soddisfatti tutti i requisiti riportati di seguito. Qualora un requisito non sia soddisfatto:

- o il trattamento non può essere effettuato in quanto non necessario / proporzionale;
- o verrà specificata la motivazione per cui tale requisito non può essere soddisfatto.

Di seguito si riportano i criteri definiti dal WP29 (*Articolo 29 – Data Protection Working Party*) indicatori di un trattamento necessario e proporzionale:

- Il trattamento ha finalità specifiche, esplicite e legittime;
- Il trattamento è lecito, ovvero è posto in essere in presenza di una delle condizioni individuate dall'articolo 6 del Regolamento;
- Il trattamento è adeguato, pertinente e limita l'utilizzo dei dati a quando necessario;
- È stata definita una tempistica di conservazione dei dati personali trattati.

Poiché il WP29 sottolinea come contribuiscano in maniera significativa a configurare un trattamento come proporzionale e lecito anche le misure che assicurano i diritti agli interessati, il titolare del trattamento ha inserito anche specifiche valutazioni a riguardo nell'iter valutativa dell'impatto sulla protezione dei dati.

Sono indici di un trattamento rispettoso dei diritti dell'interessato (e pertanto che non impatterà negativamente sui diritti e le libertà fondamentali dello stesso) circostanze quali:

- la messa a disposizione di informazioni chiare e complete alla persona interessata;
- la possibilità per l'interessato di esercitare il diritto di accesso e portabilità dei dati;
- la possibilità per l'interessato di esercitare il diritto di rettificare, cancellare, opporsi o limitare il trattamento;
- la chiara identificazione dei soggetti a cui i dati personali possono essere comunicati;
- la chiara identificazione di responsabile/i del trattamento;
- il fatto che, in caso di trasferimento di dati extra UE, siano soddisfatte le condizioni di legittimità del trasferimento.

3.4. VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTÀ DEGLI INTERESSATI

Il passaggio successivo, che metodologicamente va a comporre il processo di valutazione di impatto dei trattamenti previsti sulla la protezione dei dati personali, è relativo all'individuazione dei rischi che effettivamente incombono sui diritti e le libertà delle persone fisiche tenuto conto dei dati personali trattati.

Ai fini dell'analisi sono considerati i seguenti parametri:

- Identificazione dei trattamenti che richiedono una valutazione di impatto;
- Identificazione delle minacce rispetto a ciascun trattamento;
- Valutazione della probabilità di accadimento delle singole minacce per ogni trattamento assegnando a ciascuna un valore probabilistico circa il verificarsi, in base ai seguenti parametri:
  - Storia o statistica aziendale;
  - Valutazioni motivazionali;
- Valutazione del livello di vulnerabilità di ciascun trattamento;
- Valutazione del potenziale impatto che la realizzazione di una minaccia può causare (per ciascun trattamento) considerando i possibili:
  - Danni Patrimoniali;
  - Danni non Patrimoniali;
  - Lesioni ai diritti ed alle libertà fondamentali;
- Identificazione delle contromisure applicabili e applicate (fisiche, logiche, organizzative o qualitative);
  - **Contromisure logiche**: sono quelle che prevedono l'implementazione o una particolare configurazione di strumenti tecnologici (ad esempio una particolare configurazione dei browser o l'implementazione di un antivirus o un firewall opportunamente configurato integrano una misura tecnologica).
  - **Contromisure fisiche**: sono quelle che prevedono l'implementazione di una protezione fisica dalle minacce (ad esempio per quanto riguarda il rischio di incendio, una contromisura fisica è costituita dall'estintore o dall'uso di mobilio ignifugo).
  - **Contromisure organizzative**: sono quelle che prevedono l'implementazione di una strategia aziendale, come una policy o una procedura (ad es. la procedura che disciplina l'utilizzo degli strumenti informatici).
  - **Contromisure di tipo qualitativo**: sono quelle che fanno riferimento ad una determinata tipologia di trattamento e, in particolare, al trattamento sottoposto a valutazione d'impatto.
- Valutazione degli effetti preventivi e mitigativi in relazione all'applicazione delle contromisure;
- Misurazione e classificazione dei rischi, evidenziando il rischio per ciascun trattamento.

La valutazione del rischio effettuata dal titolare è sinteticamente riassumibile nella seguente formula matematica che individua il modo in cui il titolare del trattamento individua il cosiddetto **Rischio Residuo**:

$$R = P \times V \times \left(\frac{100 - CP}{100}\right) \times I \times \left(\frac{100 - CM}{100}\right)$$

dove:

		FASCE DI RISCHIO		
LEGENDA		**VALORE NUMERICO**	**FASCIA**	**DESCRIZIONE**
R	Rischio residuo (in termini di valore)	>= 0,1 e <= 3	1	Irrilevante
		> 3 e <= 26	2	Basso
		> 26 e < 63	3	Medio
		>= 63 e < 99	4	Alto
		>= 99 e <= 125	5	Critico
P	Probabilità di accadimento (in termini di valore)			
V	Vulnerabilità dell'asset (in termini di valore)			
CP	Capacità Preventiva delle Contromisure (in termini percentuali su una scala compresa tra 0 e 100)			
I	Impatto (in termini di valore)			
CM	Capacità Mitigativa delle Contromisure (in termini percentuali su una scala compresa tra 0 e 100)			

Allo specifico trattamento oggetto di valutazione di impatto vengono attribuiti i valori di rischio della coppia “trattamento-minaccia”. Tali valori vengono convertiti in due soglie riportate nella tabella seguente:

VALORE NUMERICO	RISCHIO
>= 0,1 e <= 26	**RISCHIO ACCETTATO**
> 26 e <= 125	**RISCHIO NON ACCETTATO**

Tabella – Fasce di accettazione del rischio residuo

La differenza fra il Rischio inerente e il Rischio residuo rappresenta il livello di resilienza del trattamento.

3.5. INDIVIDUAZIONE DELLE MISURE PREVISTE PER AFFRONTARE I RISCHI

L'individuazione delle 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 air requisiti normativi vigenti, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione) è indicata dal considerando 90 del Regolamento come conseguenza diretta della valutazione dei rischi.

Il Titolare del Trattamento è infatti chiamato a intervenire su quei rischi che sono risultati "non accettati" (ovvero un rischio che si colloca nella fascia "**Rischio non accettato**" della tabella riportata nel paragrafo precedente) per porvi adeguata mitigazione o prevenzione.

L'individuazione di ulteriori misure di sicurezza atte a prevenire e mitigare i rischi "non accettati", al fine di mutarli in rischi "accettabili", viene effettuata attraverso delle simulazioni al fine di definire la tipologia di contromisure (fisiche, logiche, organizzative o qualitative) che il Titolare del trattamento può mettere in atto.

3.6. PIANO DI TRATTAMENTO DEL RISCHIO

Le misure identificate per affrontare i rischi "non accettati" sono riportate all'interno del Piano di trattamento del Rischio in cui è definito un costo per la loro implementazione ed una tempistica di attuazione prima della quale il trattamento non può iniziare.

Se dalla valutazione delle simulazioni emerge che il rischio per la protezione dei dati **non può essere ragionevolmente attenuato mediante l'uso delle tecnologie disponibili o per gli elevati costi di attuazione**, il Titolare del trattamento dovrà consultare l'Autorità di controllo prima dell'inizio dell'attività di trattamento.

4. VALUTAZIONE

I paragrafi seguenti riportano le analisi effettuate per ciascun trattamento sottoposto a valutazione di impatto.

4.1. RICERCA MEDICA, BIOMEDICA ED EPIDEMIOLOGICA

DESCRIZIONE DEL TRATTAMENTO
Il progetto oggetto di valutazione è uno studio osservazionale retrospettivo, ossia uno studio clinico osservazionale in cui la raccolta dei dati clinici avviene a partire dalle cartelle cliniche, dopo che i pazienti siano stati sottoposti nell'ambitodella normale pratica clinica a visita medica, esame diagnostico o trattamento. Più nello specifico, nel presente studioretrospettivo sono previste la raccolta e l'analisi dei dati di pazienti ricontattabili e non ricontattabili per la raccolta delconsenso al trattamento dei dati personali. È rilevante, per lo studio in oggetto, l'arruolamento di pazienti non contattabili. Al fine di avere risultati affidabili e significativi è necessario infatti raggiungere una numerosità campionaria non ottenibile solo considerando pazienti contattabili. Il non raggiungimento della numerosità stimata (escludendo pazienti non raggiungibili) indebolirebbe la solidità dello studio

4.1.1. SODDISFACIMENTO DEI REQUISITI DI NECESSITÀ E PROPORZIONALITÀ

Le tabelle seguenti riportano il soddisfacimento dei requisiti di necessità e di proporzionalità.

CONDIZIONI DI NECESSITA' DPIA		
CRITERI	**EVIDENZA**	**Note**
Combinazione o raffronto di insiemi di dati *Per esempio combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato.*	X	Nell'ambito dell'attività di ricerca scientifica è necessario mettere in collegamento più basi dati.
Dati relativi a interessati vulnerabili *Per esempio minori, dipendenti, soggetti vulnerabili e meritevoli di specifiche tutele e ogni interessato per il quale si possa identificare una situazione di disequilibrio nel rapporto con il rispettivo titolare del trattamento*	X	I dati personali oggetto di trattamento sono relativi a pazienti.
Dati particolari o dati di natura estremamente personale *A titolo di esempio, un ospedale che conserva le cartelle cliniche dei pazienti, o un investigatore privato che conserva informazioni su soggetti responsabili di reati*	X	I dati personali oggetto di trattamento riguardano lo stato di salute dei pazienti.
Decisioni automatizzate che producono significativi effetti giuridici o di analoga natura *Per esempio, il trattamento può comportare l'esclusione di una persona fisica da determinati benefici ovvero la sua discriminazione quali concessioni prestiti, stipula assicurazioni*		
Monitoraggio sistematico *Ad esempio trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti, la videosorveglianza, l'analisi invasiva mediante app o siti web*		
Trattamenti di dati su larga scala *Definita in considerazione: del numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; del volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; della durata, ovvero la persistenza, dell'attività di trattamento; della portata geografica dell'attività di trattamento*		

CONDIZIONI DI NECESSITA' DPIA		
CRITERI	**EVIDENZA**	**Note**
Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici *Sono ricompresi i sistemi di videosorveglianza e di geolocalizzazione, ma anche atri sistemi dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti*		
Trattamenti sistematici di dati biometrici o genetici *tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento*		
Trattamenti valutativi o di scoring *Ad esempio la profilazione e attività predittive (compresa la profilazione), in particolare a partire da aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato*		
Trattamento che, di per sé, impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto *A titolo di esempio, allo screening dei clienti di una banca attraverso i dati registrati in una centrale rischi al fine di stabilire se ammetterli o meno a un finanziamento*	X	Nei casi in cui non sia possibile contattare il paziente è limitato il diritto di opporsi al trattamento in quanto il paziente, nonostante gli sforzi profusi, potrebbe non essere raggiunto dalla notizia relativa al trattamento dei suoi dati personali nell'ambito della ricerca medica retrospettiva.
Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative *Ad esempio l'associazione fra tecniche dattiloscopiche e riconoscimento del volto per migliorare il controllo degli accessi fisici, e così via*		

VALUTAZIONE DI NECESSITA' E PROPORZIONALITA'		
CRITERI	**EVIDENZA**	**Note**
Alla persona interessata sono messe a disposizione di informazioni chiare e complete	X	Il Titolare del trattamento ha messo a disposizione degli interessati informazioni chiare e complete attraverso la condivisione e pubblicazione di un'informativa ai sensi dell'art. 13 GDPR.
È data all'interessato la possibilità di esercitare il diritto di accesso e portabilità dei dati	X	L'interessato ha la possibilità di essere informato dei suoi diritti attraverso specifica informativa resa ai sensi dell'art. 13 del GDPR consultabile sul sito web dell'Ospedale. La portabilità, considerate la base giuridica che legittima il trattamento, non è contemplata.
È data all'interessato la possibilità di esercitare il diritto di rettificare, cancellare, opporsi o limitare il trattamento	X	L'interessato ha la possibilità di essere informato dei suoi diritti attraverso specifica informativa resa ai sensi dell'art. 13 del GDPR consultabile sul sito web dell'Ospedale.
È stata definita una tempistica di conservazione dei dati personali trattati	X	I tempi di conservazione dei dati personali trattati in relazione alla ricerca medica, biomedica ed epidemiologica sono definiti nell'ambito del Protocollo di Ricerca approvato dal Comitato Etico e sono riportati nella specifica informativa resa ai sensi dell'art. 13 del GDPR.
Il trattamento è adeguato, pertinente e limita l'utilizzo dei dati a quando necessario	X	Il trattamento dei dati personali avviene in osservanza del Protocollo di Ricerca approvato dal Comitato Etico.

VALUTAZIONE DI NECESSITA' E PROPORZIONALITA'		
CRITERI	**EVIDENZA**	**Note**
Il trattamento è lecito	X	Il trattamento è da considerarsi legittimo in quanto effettuato sulla base del consenso espresso dall'interessato ai sensi degli artt. 6, par. 1, lett. a) e 9, par. 2, lett. a) del Regolamento per i pazienti raggiungibili e con esimente ex art. 110 comma 1 secondo periodo per i pazienti non raggiungibili. Al fine di raggiungere il campione statistico necessario per ottenere risultati validi, non è possibile fare riferimento a soli pazienti ricontattabili.
Il trattamento ha finalità specifiche, esplicite e legittime	X	Le finalità e modalità del trattamento sono espressamente riportate nel documento di informativa consultabile dagli interessati sul sito web dell'Ospedale. L'Ospedale ha adottato opportune procedure operative standard per la gestione e lo svolgimento degli studi clinici.
Sono stati chiaramente identificati i soggetti a cui i dati personali possono essere comunicati	X	All'interno dell'informativa messa a disposizione degli interessati sono indicate le categorie di destinatari a cui i dati possono essere comunicati (comprese ad esempio le autorità regolatorie). Le misure tecniche ed organizzative adottate prevedono che i dati personali oggetto di trattamento rispettino le Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018 e le Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (aut. gen. n. 9/2016) e il Provvedimento a carattere generale "*Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica ai sensi degli artt. 2-quater e 106 del Codice privacy – 9 Maggio 2024*".

4.1.2. ELENCO DEGLI ASSET ASSOCIATI AL TRATTAMENTO

La tabella successiva riporta gli asset utilizzati a supporto del trattamento ed estrapolati dal Registro dei trattamenti predisposto.

BANCHE DATI					
NOME BANCA DATI	**ASSET DI RIFERIMENTO**	**UBICAZIONE**	**PAESE EXTRA U.E.**	**TIPOLOGIA DI DATO**	**Note**
Software di raccolta dati (CRF)		U.E.	--	Dati Personali e Dati Particolari	--

4.1.3. CONTROMISURE APPLICATE

Di seguito si riportano le contromisure applicate al trattamento oggetto di valutazione.

[OMISSIS]

4.1.4. RISULTATI DELLA VALUTAZIONE DI IMPATTO

La tabella seguente illustra il livello di rischio per ciascuna minaccia incombente sul trattamento oggetti di valutazione.

[OMISSIS]

4.1.5. TIPOLOGIA DI IMPATTO (RISERVATEZZA, DISPONIBILITÀ ED INTEGRITÀ)

La seguente tabella rappresenta le relazioni tra le Minacce afferenti al trattamento oggetto di valutazione e la tipologia di impatto in termini di riservatezza, disponibilità ed integrità.

MINACCIA	TIPO IMPATTO		
	Disp.	Int.	Ris.
Accesso illegittimo ai dati	Basso	Basso	
Modifiche indesiderate ai dati	Basso	Basso	
Perdita di dati			Basso

5. PARERE DEL DPO

Il presente documento è stato sottoposto alla valutazione del DPO che ha rilasciato parere favorevole ritenendo, pertanto, che il trattamento possa essere implementato.

6. PARERE DEGLI INTERESSATI

Relativamente alla specifica ricerca il titolare non ha potuto sentire il parere di tutti gli interessati per la sussistenza di ragioni, considerate del tutto particolari e/o eccezionali, per cui informare gli stessi sarebbe risultato impossibile per cui è stata redatta la presente valutazione in quanto gli stessi risultano non più contattabili e/o deceduti.

Coerentemente con le pronunce dell'Autorità Garante, l'impossibilità di informare gli interessati e acquisire il relativo consenso è stata accertata successivamente a tre tentativi infruttuosi di raccolta.

7. CONCLUSIONI

La matrice successiva riassume le valutazioni effettuate

Trattamento	Rischio residuo max	*Rischio DPIA*
Ricerca medica, biomedica ed epidemiologica (studi retrospettivi)	5,10	Rischio accettato

*Rischio Residuo associato alla minaccia afferente al trattamento oggetto di valutazione con il valore peggiore

ALLEGATO 1 - LEGENDA

[OMISSIS]