ESTRATTO DELLA VALUTAZIONE DI IMPATTO

1. Informazioni generali

1.1 Titolare del trattamento

La presente DPIA è stata redatta dalla Fondazione IRCCS Policlinico San Matteo, in qualità di Titolare del trattamento ("Titolare del trattamento").

1.2 Contesto di riferimento

Oggetto della presente valutazione d'impatto (Data Protection Impact Assessment – DPIA) è la pubblicazione di un case report riguardante un paziente deceduto in Fondazione su rivista scientifica.

1.3 Standard di riferimento per la predisposizione della DPIA

La presente DPIA è stata realizzata utilizzando come base le informazioni contenute nel software sviluppato dall'Autorità francese per la protezione dei dati (CNIL), in conformità alle indicazioni fornite nelle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" (WP 248 rev. 01 e adottate dall'EDPB il 4 aprile 2017 e modificate il 4 ottobre 2017 – "***Linee Guida***").*
Inoltre, per la valutazione del rischio è stata utilizzata la metodologia dell'*European Union Agency For Network and Information Security* ("**ENISA**") descritta all'interno del documento "*Guidelines for SMEs on the security of personal data processing*" raggiungibile al seguente link https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing.

Sono stati, infine, tenuti in considerazione alcuni dei requisiti della norma ISO/IEC 29134 "*Information technology — Security techniques — Guidelines for privacy impact assessment":* in particolare, valutazione necessità DPIA (art. 6.2), composizione del DPIA team (art. 6.3.1), piano di trattamento del rischio residuo e revisione e verifica della DPIA (art. 6.5.3 – 6.5.4).

1.4 Descrizione del quadro normativo e regolatorio, standard e buone prassi

- Regolamento (UE) 2016 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone con riguardo al trattamento dei dati personali – Regolamento Generale sulla Protezione dei Dati (GDPR) e s.m.i.;
- D.lgs 10 agosto 2018, n. 101. "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)";
- D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e s.m.i.;
- Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" (WP 248 rev. 01 e adottate dall'EDPB il 4 aprile 2017 e modificate il 4 ottobre 2017;
- ISO/IEC 27001:2013 "Information Security Management Systems", 01/10/2013;
- ISO/IEC 27002:2013 "Code of practice for information security controls", 01/10/2013;

- Manuale ENISA (Agenzia dell'Unione europea per la cybersicurezza) sulla Sicurezza nel trattamento dei dati personali;
- Allegato A5 - 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;
- Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR Versione 2.0 Adottate il 7 luglio 2021;
- Provvedimenti Autorità Garante [provv. GPDP 497/2018 riguardante le aut. gen. 9/2016 e aut. gen. 8/2016];
- Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali - 24 luglio 2008;
- Provvedimento del 14 gennaio 2021 - Regione Veneto. Codice di condotta per l'utilizzo di dati sulla salute a fini didattici e di pubblicazione scientifica;
- Convenzione di Oviedo – "Convenzione per la protezione dei Diritti dell'Uomo e della dignità dell'essere umano nei confronti dell'applicazioni della biologia e della medicina: Convenzione sui Diritti dell'Uomo e la biomedicina", del 4 aprile 1997;
- Regolamento UE n. 536/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, *"Sulla sperimentazione clinica di medicinali per uso umano"* e che abroga la direttiva 2001/20/CE (Testo rilevante ai fini del SEE);
- GCP - ICH Harmonised Guideline – "INTEGRATED ADDENDUM TO ICH E6(R1): GUIDELINE FOR GOOD CLINICAL PRACTICE", del 9 novembre 2016;
- EDPB – "Documento sulla risposta alla richiesta della Commissione europea di chiarimenti sull'applicazione coerente del GDPR, concentrandosi sulla ricerca sanitaria", adottato il 2 febbraio 2021;
- Linee guida per la classificazione e conduzione degli studi osservazionali sui farmaci
- Linee Guida AIFA – "Definizione dei requisiti minimi per le organizzazioni di ricerca a contratto (CRO) nell'ambito delle sperimentazioni cliniche di medicinali" D.M. del 15 novembre 2011;
- GPDP – "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", pubblicate sulla G.U. n. 11 del 14 gennaio 2019.

2. Fase 0: Determinazione della necessità di condurre la DPIA e costituzione del team DPIA

2.1 Necessità di svolgere la DPIA

In questo caso la necessità di svolgere la DPIA deriva dall'art. 110-bis, comma 4, dlgs. 196/2003, come previsto dal Garante nelle FAQ sulla ricerca scientifica nell'ambito degli IRCCS: "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 (VIP) 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."

Nella redazione del presente documento si è provveduto a seguire i principi fondamentali relativi alla valutazione d'impatto sulla protezione dei dati di cui al Regolamento (UE) 2016/679 (di seguito GDPR) così come schematizzati nelle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" del 4 ottobre 2017 pubblicate dal Gruppo di lavoro Articolo 29 (WP29), e si è riscontrato che i trattamenti presi in considerazione possono presentare rischi elevati.

Il trattamento preso in esame, rispetto a quelli individuati nell'allegato 1 al provvedimento del Garante della protezione dei dati personali n. 467 dell'11 ottobre 2018, "Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto", rientra nel:

- Trattamenti non occasionali di dati relativi a soggetti vulnerabili/deceduto (rif. 6);
- Criterio n.4 del WP248: dati sensibili o dati aventi carattere altamente personale

Preso atto che il sopracitato provvedimento asserisce che la valutazione d'impatto sulla protezione dei dati debba essere effettuata ogniqualvolta ricorra almeno un criterio in quanto è indice di un trattamento che presenta un rischio elevato per i diritti e le libertà degli interessati, si è ritenuto opportuno procedere all'esecuzione della valutazione d'impatto.

2.2 Piano delle attività

Al termine della predisposizione della DPIA, il documento verrà sottoposto al parere del DPO.

Il team dovrà recepire almeno parzialmente le osservazioni del DPO, evidenziando eventuali scostamenti, per l'approvazione da parte del Legale Rappresentante.

3. Fase 1: Descrizione del trattamento

3.1.1 Il trattamento oggetto della Valutazione di Impatto

Utilizzo di campioni biologici del paziente *post mortem*, attività laboratoristica di analisi e pubblicazione dei risultati.
In particolare, il paziente oggetto di studio è affetto da leucemia mieloide acuta, con un assetto citogenetico, alla diagnosi, normale. Il paziente è stato trattato e durante i followup sono stati raccolti campioni biologici per le analisi cliniche. Il paziente è deceduto, e il materiale biologico precedentemente prelevato a scopo clinico, è utilizzato per indagini di ricerca. La ricerca è effettuata mediante indagini di citogenetica, affiancate dallo studio in FISH, dall'analisi di biologia molecolare e dal sequenziamento nucleotidico.

3.1.2 Ruoli e responsabilità collegate al trattamento.

Non ci sono altri soggetti che possono intervenire oltre il Titolare.

Lo studio è stato in parte finanziato da un grant da parte del Ministero della Salute italiano per giovani ricercatori-GR-2016-02361272-.

3.1.2.1.1 Persone fisiche che intervengono nel trattamento

Il gruppo di Sperimentatori è costituito da biologi adeguatamente istruiti sul trattamento e sulle misure tese a garantire una adeguata protezione dei dati personali.

3.2 Dati, processi e beni di supporto

3.2.1 Dati trattati

DATI COMUNI data di nascita
DATI CLINICI peso altezza, età alla diagnosi, esiti di esami di laboratorio, esami di citogenetica e FISH, analisi citofluorimetriche e molecolari, campioni biologici del paziente. Diagnosi di patologia, terapie, dati di follow up (terapie successive, sopravvivenza).

3.2.2 Fonti dei dati

I dati personali del paziente sono acquisiti dalla cartella clinica.

3.2.3 Descrizione del flusso dei dati

3.2.3.1 Flusso dei dati

I dati personali oggetto del trattamento sono già presenti nelle cartelle cliniche e nell'ulteriore documentazione sanitaria in possesso del Titolare e sono stati precedentemente e lecitamente acquisiti per finalità di diagnosi, cura e prevenzione.
In particolare, i dati relativi alla salute e i campioni biologici del paziente saranno utilizzati come previsto da (inserire il riferimento al documento che descrive le analisi).

All’esito delle attività di analisi, i risultati potranno essere oggetto di pubblicazione in ambito scientifico. I dati sono oggetto di pubblicazione previa opportuna anonimizzazione.

3.2.3.2

Si veda il capitolo 3 - Fase 1: Descrizione del trattamento

3.2.3.3 Tipo di operazioni

La tipologia delle operazioni effettuate sono:

Operazioni standard: Raccolta, Registrazione, organizzazione, conservazione, consultazione, elaborazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione.

Comunicazione mediante trasmissione: mediante caricamento sulla piattaforma dell’editore

Diffusione: I dati potranno essere diffusi in forma anonima. I risultati della analisi di ricerca saranno oggetto di pubblicazione nell’ambito di riviste scientifiche internazionali indicizzate.

3.2.4 Beni di supporto

I beni di supporto possono essere raggruppati in:

- Fonti dei dati:
    - Cartella clinica e risultati degli esami di laboratorio

4. Fase 2: Valutazione necessità, proporzionalità e legittimità del trattamento

4.1 Proporzionalità e necessità

Lo scopo di miglioramento del processo di cura/prevenzione e più in generale della salute della collettività si viene a contrappore al diritto alla riservatezza dei singoli. Il miglioramento è tanto più urgente quanto le patologie hanno effetti socio economici importanti. D'altra parte gli impatti sui pazienti è tanto maggiore quanto le patologie destano allarme social e potenziale discriminazione.

I dati personali sono indispensabili per la qualità della ricerca. Le fasi di verifica dei risultati sono un requisito fondamentale di un processo di qualità. Queste quindi richiedono una collegabilità del dato alle informazioni cliniche primarie e di conseguenza all'identità del paziente. La strategia principale per rendere il trattamento il meno impattante possibile sulla riservatezza è la minimizzazione della collegabilità tramite tecniche di minimizzazione e pseudonimizzazione dei dati. La necessità di chiedere un nuovo consenso per studi successivi può rendere più complessa questa strategia.

4.1.1 Finalità esplicite e legittime

Le finalità del trattamento sono:

1) Di ricerca scientifica
2) Di pubblicazione scientifica

Esse vengono esplicitate nell'informativa (cfr. Allegata al presente documento).

4.1.2 Fondamenti legali del trattamento

La base giuridica del trattamento si fonda su:

Articolo 110 bis comma 4 codice privacy.

4.1.3 I dati raccolti sono adeguati, rilevanti e limitati a quanto è necessario al conseguimento delle finalità del trattamento ("Minimizzazione dei dati")

Ogni dato raccolto è direttamente e specificatamente funzionale alle necessità per le quali è stato raccolto ed è pertanto pertinente rispetto alle finalità sopra esplicitate.

4.1.4 Accuratezza ed aggiornamento dei dati

Gli Sperimentatori verificano la correttezza dei dati raccolti sulla scheda raccolta dati confrontandoli con quelli presenti sulla cartella clinica del partecipante. I dati sono raccolti e trattati da un numero ristretto di persone biologi e medici.
Si assume che la documentazione clinica di origine (cartella clinica) sia accurata (documento di fede privilegiata).

4.1.5 Durata della conservazione dei dati

Tipologia di dati	Tempo di conservazione
Dati dell'utente	5 anni dalla pubblicazione della ricerca

I dati in forma direttamente identificabile sono conservati a norma di legge nella documentazione clinica.

I dati di autorizzazione, identificazione ed accesso ai sistemi sono conservati per 5 anni.

4.2 Controlli per proteggere i diritti degli interessati

4.2.1 Come sono informati gli interessati circa il trattamento

Si procederà alla pubblicazione dell'informativa sul sito web istituzionale.

4.2.2 Esercizio dei diritti da parte degli interessati

Per esercitare i diritti previsti dagli artt. da 15 a 22 del GDPR, l'interessato può rivolgersi al titolare del trattamento, anche per il tramite del DPO. I diritti possono essere esercitati con le modalità indicate nell'informativa.
Inoltre, come precisato nell'informativa, l'interessato può sempre esercitare, qualora ritenga che il trattamento dei Suoi dati personali avvenga in violazione di quanto previsto dal GDPR, il diritto di proporre reclamo all'Autorità di controllo, seguendo le indicazioni pubblicate sul sito della stessa (https://www.garanteprivacy.it/modulistica-e-servizi-online/reclamo) o di ricorrere avanti la competente autorità giudiziaria (artt. 77 e 79 del GDPR).

4.2.2.1 Diritto di accesso

Con riferimento al diritto di accesso, l'interessato può ottenere la conferma che sia o meno in corso un trattamento di dati che lo riguardano e in tal caso ottenere l'accesso agli stessi e alle informazioni riportate in dettaglio all'art. 15 del GDPR (es. finalità, destinatari, periodo di conservazione).

4.2.2.2 Diritto di rettifica

L'interessato, inoltre, ha sempre il diritto di ottenere – senza ingiustificato ritardo e comunque entro 30 gg - la rettifica dei dati personali inesatti che lo riguardano ovvero l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

4.2.2.3 Diritto di cancellazione

Per il trattamento in oggetto che si fonda sul consenso, l'interessato potrà richiedere la cancellazione dei dati personali nell'ambito del presente studio, ai sensi dell'art. 17 del GDPR.

4.2.2.4 Diritti di limitazione

L'interessato ha il diritto di chiedere la limitazione del trattamento quando:

a. contesta l'esattezza dei dati personali, chiedendo quindi la rettifica, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
b. ritiene che il trattamento sia illecito e chiede che ne sia limitato l'utilizzo;
c. i dati personali sono necessari per l'accertamento, l'esercizio o la difesa di un diritto dell'interessato in sede giudiziaria;

d. si è opposto al trattamento, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

4.2.2.5 Diritto di opposizione

L'interessato ha il diritto di opporsi al trattamento per motivi connessi alla sua situazione particolare. Il Titolare dovrà astenersi dal trattare ulteriormente i dati personali salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. (art. 21 del GDPR).

4.2.3 Obbligazioni dei responsabili del trattamento

Non ci sono responsabili del trattamento.

4.3 Trasferimenti al di fuori dello SEE

Non vengono effettuati trasferimenti extra SEE.

4.4 Rispetto dei principi di Privacy by Design

4.4.1 Rispetto delle strategie

1. Minimizzare: sono trattati soltanto i dati necessari per raggiungere le finalità
2. Nascondere: il trattamento dei dati personali è limitato soltanto a soggetti autorizzati
3. Informare: all'interessato sono fornite tutte le informazioni pertinenti al trattamento in oggetto (informative ex art. 13 GDPR)
4. Controllare: all'interessato è garantito l'esercizio dei diritti previsti dalla normativa (artt. 15-22 GDPR). Si rinvia alla procedura di gestione dei diritti degli interessati.
5. Dimostrare: si rinvia alle policy del Titolare del trattamento

5. Fase 3: Calcolo del livello del rischio

Il livello del rischio viene calcolato moltiplicando il valore dell'Impatto (conseguenze negative per gli Interessati di una determinata minaccia) per la Probabilità che una determinata minaccia si possa verificare.
Pertanto, il livello del rischio è pari:

LIVELLO DEL RISCHIO = IMPATTO X PROBABILITÀ OCCORRENZA DELLA MINACCIA

5.1 Calcolo dell'impatto

Si considerano i seguenti livelli di Impatto:

Tabella 1

LIVELLO DI IMPATTO	VALORE	DESCRIZIONE
BASSO	1	Gli individui possono andare incontro a **disagi minori**, che supereranno **senza alcun problema** (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).
MEDIO	2	Gli individui possono andare incontro a **significativi disagi**, che saranno in grado di superare nonostante **alcune difficoltà** (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).
ALTO	3	Gli individui possono andare incontro a **conseguenze significative**, che dovrebbero essere in grado di superare anche se con **gravi difficoltà** (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
MOLTO ALTO	4	Gli individui possono subire **conseguenze significative**, o addirittura irreversibili, **non superabili** (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Il livello d'Impatto deve essere valutato in relazione alle seguenti variabili:

- perdita di riservatezza dei dati;
- perdita d'integrità dei dati;
- perdita di disponibilità dei dati.

Tabella 2

Il più alto dei tre livelli (perdita di riservatezza, integrità e disponibilità) deve essere considerato come il risultato finale della valutazione dell'Impatto.

Tabella 3

LIVELLO FINALE DELL'IMPATTO	**Basso**

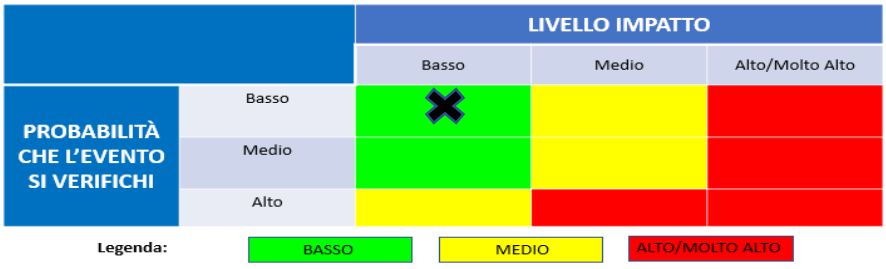
5.2 Calcolo della probabilità di accadimento della minaccia

Tabella 8

LIVELLO FINALE DELLA PROBABILITÀ DELLE MINACCE	**basso**

5.3 Calcolo del livello di rischio

Il livello del rischio sarà dato dalla moltiplicazione del risultato del livello d'Impatto riportato nella **Tabella 3** del paragrafo 5.1 per il risultato del livello di probabilità riportato nella **Tabella 8** del paragrafo 5.2.



LIVELLO DEL RISCHIO	**basso**

6. Fase 6: Calcolo del rischio residuo, piano di remediation e parere del DPO

6.1 Rischio residuo

Si ritiene che il rischio residuo collegato al trattamento di dati personali per le finalità dello studio in oggetto sia accettabile in quanto sono state adottate misure di sicurezza tecniche e organizzative idonee a contenere il rischio per i diritti e le libertà degli interessati.

6.2 Piano di remediation

Per la minimizzazione del rischio residuo, non sono al momento previste ulteriori misure di sicurezza.

6.3 Opinione del DPO

L'indice di questo documento e relativi contenuti rispecchiano quanto indicato nell'allegato 2 del WP 248 *(Criteri per una valutazione d'impatto sulla protezione dei dati accettabile)* (cfr. Comitato Europeo per la protezione dei dati, Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248rev.01).
Il DPO, consultato dal Titolare in conformità all'art. 35, par. 2, del GDPR in merito alla Valutazione d'impatto ex artt. 35-36 GDPR (cd. DPIA) sulle attività di trattamento sopramenzionate ha valutato che**:**

Alla luce di quanto descritto nella presente DPIA e della documentazione sottoposta al DPO, si ritiene che il trattamento in questione, laddove effettivamente realizzato nei termini indicati, possa essere considerato rispettoso dei principi di cui all'art. 5 del GDPR.
La DPIA descrive in maniera sufficiente il trattamento oggetto della valutazione d'impatto, sia dal punto di vista dello studio, che dal punto di vista degli strumenti (anche informatici) a supporto dello stesso.
Inoltre, le misure di sicurezza applicate, in rapporto alla tipologia di dati trattati e alle caratteristiche del caso specifico, appaiono adeguate a rispettare i dettami dell'art. 32 del GDPR nonché, più in generale, i diritti e le libertà fondamentali degli individui.
Il calcolo dell'impatto e della probabilità del rischio, sia di quello assoluto che di quello residuo, appare ben strutturato e motivato, mediante ricorso alla metodologia ENISA.
Il DPO si riserva, comunque, successive valutazioni anche a seguito dei possibili riscontri che potrebbero pervenire dagli interessati. In quest'ottica, qualora la concreta applicazione del trattamento lo richiedesse, dovranno essere implementate eventuali misure correttive che, nel caso, condurranno altresì ad un aggiornamento della presente DPIA.

7. Fase 7: Eventuale consultazione dell'Autorità Garante per la protezione dei dati personali ai sensi dell'art. 36 GDPR

Dato che il trattamento dei dati personali rientra nei casi previsti dall'art. 110 bis comma 4 del D.lgs 196/2003, il Titolare non procederà alla consultazione dell'Autorità Garante per la protezione dei dati personali ai sensi dell'art. 36 GDPR.