

**DATA PROTECTION IMPACT ASSESSMENT**

ai sensi dell'art. 35 del Reg. UE 2016/679

**VALUTAZIONE DI IMPATTO
SULLA PROTEZIONE DEI DATI PERSONALI**

| Codice | Descrizione |
|----------------------------------|--|
| DPIA-001 | CARDIOSCORE: Valutazione retrospettiva multicentrica di fattori predittivi per lo sviluppo di cardiopatia in pazienti affetti da Linfoma Diffuso a grandi cellule (DLBCL) sottoposti a chemioterapia con antracicline |
| ELABORAZIONE DPIA PER | <input checked="" type="checkbox"/> Nuova attività trattamento <input type="checkbox"/> Aggiornamento DPIA <input type="checkbox"/> Revisione periodica DPIA |

| | | |
|------------------|-------------------------------|---------------|
| Redazione | Principal Investigator | Stefano Oliva |
|------------------|-------------------------------|---------------|

**DATA PROTECTION IMPACT ASSESSMENT**

ai sensi dell'art. 35 del Reg. UE 2016/679

| SOGGETTI COINVOLTI NELLO STUDIO | |
|---|--|
| TITOLARE promotore | IRCCS ISTITUTO TUMORI GIOVANNI PAOLO II DI BARI |
| Centri partecipanti quali Titolari del trattamento | <ul style="list-style-type: none">○ Azienda Ospedaliero Universitaria delle Marche, SOD Clinica Ematologica, Ancona○ Azienda Ospedaliero-Universitaria Careggi, SOD Ematologia, Firenze○ Azienda Ospedaliero – Universitaria Policlinico Umberto I, UOC Ematologia, Roma○ Ospedale Businco, Div. Ematologia, Cagliari○ Fondazione IRCCS Istituto Nazionale Tumori, SC Ematologia, Milano○ AOU Maggiore della Carità di Novara - SCU Ematologia, Novara○ Azienda USL – IRCCS di Reggio Emilia, SC Ematologia, Reggio Emilia○ AOU Città della Salute e della Scienza di Torino, SC Ematologia Universitaria, Torino○ Fondazione IRCCS Policlinico San Matteo, SC Ematologia, Pavia○ AOU Policlinico Modena, Centro Oncologico Modenese, Modena○ Ospedale Universitario Molinette San Giovanni Battista, U.O Ematologia, Torino○ A.O. SS. Antonio e Biagio e Cesare Arrigo - S.C. Ematologia, Alessandria○ ASST Spedali Civili di Brescia – Ematologia, Brescia○ A.O. Ospedali Riuniti Villa Sofia-Cervello - Divisione di Ematologia, Palermo○ Istituto clinico HUMANITAS IRCCS, Rozzano (MI)○ Ospedale Dell'Angelo - U.O. Ematologia, Mestre (VE)○ ASST Grande Ospedale Metropolitano Niguarda - SC |

**DATA PROTECTION IMPACT ASSESSMENT**

ai sensi dell'art. 35 del Reg. UE 2016/679

| | |
|--------------------------------------|--|
| | <p>Ematologia, Milano</p> <ul style="list-style-type: none">○ Fondazione Policlinico Campus Biomedico – SC Ematologia, Roma (RM)○ Ospedale S. Maria della Misericordia – Ematologia, Perugia (PG)○ IRCCS Centro di Riferimento Oncologico, SOC Oncologia Medica e dei Tumori Immunocorrelati, Aviano○ IRCCS CROB, UO Ematologia e Trapianto Cellule Staminali, Rionero in Vulture (PZ)○ PO "A. Perrino", UOC Ematologia, Brindisi○ Osp. Mons. Dimiccoli, Unità Operativa di Ematologia con trapianto, Barletta○ Ospedale Vito Fazzi, Ematologia, Lecce○ Azienda Ospedaliera Pia Fondazione di Culto e Religione "Car. G. Panico", UOC Ematologia e Centri Trapianti, Tricase (LE)○ Ospedale S.G. Moscati, Ematologia, Statte (TA)○ Azienda Ospedaliera Policlinico Consorziale, Unità Trapianti, Bari○ Fondazione Casa Sollievo della Sofferenza Opera di San Pio da Pietralcina – UOC Ematologia, San Giovanni Rotondo (FG)○ Fondazione IRCCS San Gerardo dei Tintori – UOC Ematologia Adulti, Monza (MB)○ IRCCS Ospedale San Raffaele – Ematologia, Milano |
| RESPONSABILE DEL TRATTAMENTO | IFC-CNR – Pisa |
| COORDINATORE E SPERIMENTATORI | PI Coordinatore: Dott. Stefano Oliva (IRCCS Istituto Tumori "Giovanni Paolo II di Bari) Sperimentatori: Dott. Attilio Guarini, SC di Ematologia e terapia Cellulare (IRCCS Istituto Tumori "Giovanni Paolo II" di Bari) |



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

| | |
|--|--|
| | Dott.ssa Carla Minoia, SC di Ematologia e terapia Cellulare (IRCCS Istituto Tumori "Giovanni Paolo II" di Bari) Study Coordinator: Dott.ssa Antonella Palmisano, SSD Cardiologia ad Interesse Oncologico (IRCCS Istituto Tumori "Giovanni Paolo II" di Bari) |
| | |

| | |
|---------------------------------|--|
| MODALITA' CONDUZIONE | <input checked="" type="checkbox"/> DPIA OBBLIGATORIA |
| | <input type="checkbox"/> DPIA VOLONTARIA |

**DATA PROTECTION IMPACT ASSESSMENT**

ai sensi dell'art. 35 del Reg. UE 2016/679

INDICE

Sommarario

| | |
|--|-----------|
| Informazioni sulla DPIA | 7 |
| ACCETTABILITA' DEL RISCHIO | 8 |
| 1 Descrizione sistematica del trattamento | 9 |
| 1.1.1 Contesto..... | 9 |
| 1.2 Panoramica del trattamento | 11 |
| 1.2.1 Quale è il trattamento in considerazione? | 11 |
| 1.2.2 Quali sono le responsabilità connesse al trattamento?..... | 13 |
| 1.2.3 Ci sono standard applicabili al trattamento? | 14 |
| 1.3 Dati, processi e risorse di supporto | 14 |
| 1.3.1 Quali sono i dati trattati e gli asset a supporto?..... | 14 |
| 1.4 Finalità del trattamento | 17 |
| 2 Principi Fondamentali..... | 17 |
| 2.1 Valutazione della necessità e proporzionalità del trattamento del trattamento | 17 |
| 2.1.1 Gli scopi del trattamento sono specifici, espliciti e legittimi? | 17 |
| 2.1.2 Quale è il flusso dei dati durante il ciclo di vita del trattamento? | 18 |
| 2.1.3 Quali sono le basi legali che rendono lecito il trattamento?..... | 19 |
| 2.1.4 I dati sono esatti e aggiornati? | 20 |
| 2.1.5 Qual è il periodo di conservazione dei dati? | 20 |
| 2.2 Misure a tutela dei diritti degli interessati | 20 |
| 2.2.1 Come sono informati del trattamento gli interessati? | 20 |
| 2.2.2 Ove applicabile: come si ottiene il consenso degli interessati?..... | 21 |
| 2.2.3 Come fanno gli interessati a esercitare i loro diritti? | 21 |
| 2.2.4 In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente? | 22 |
| I dati personali non saranno trasferiti verso Paesi Terzi extra UE. | 22 |

**DATA PROTECTION IMPACT ASSESSMENT**

ai sensi dell'art. 35 del Reg. UE 2016/679

| | | |
|------------|--|-----------|
| 2.3 | Misure esistenti o pianificate per la protezione del dato | 22 |
| 3 | <i>Rischi</i> | 24 |
| 3.1 | Panoramica dei rischi per diritti e libertà | 24 |
| 3.2 | Accesso illegittimo ai dati..... | 26 |
| 3.2.1 | Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare? | 26 |
| 3.2.2 | Quali sono le principali minacce che potrebbero concretizzare il rischio?..... | 26 |
| 3.2.3 | Quali sono le fonti di rischio? | 27 |
| 3.2.4 | Quali misure fra quelle individuate contribuiscono a mitigare il rischio?..... | 27 |
| 3.2.5 | Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate? | 27 |
| 3.2.6 | Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate? | 27 |
| 3.3 | Modifiche indesiderate dei dati | 27 |
| 3.3.1 | Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare? | 27 |
| 3.3.2 | Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio? | 27 |
| 3.3.3 | Quali sono le fonti di rischio? | 27 |
| 3.3.4 | Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio? | 28 |
| 3.3.5 | Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate? | 28 |
| 3.3.6 | Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate? | 28 |
| 3.4 | Perdita di dati..... | 28 |
| 3.4.1 | Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?..... | 28 |
| 3.4.2 | Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio? | 28 |
| 3.4.3 | Quali sono le fonti di rischio? | 28 |
| 3.4.4 | Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio? | 28 |



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

| | | |
|------------|---|-----------|
| 3.4.5 | Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate? | 29 |
| 3.5 | METRICHE PER ANALISI RISCHIO | 29 |
| 4 | <i>Panoramica dei rischi</i>..... | 31 |

Informazioni sulla DPIA

La DPIA, acronimo di *Data Protection Impact Assessment*, è una valutazione preliminare, eseguita dal Titolare del trattamento dei dati personali, relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati. In linea con l'approccio basato sul rischio adottato dal Regolamento generale sulla protezione dei dati, è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento" può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35 del Regolamento 2016/679).

Ai sensi dell'articolo 35, paragrafo 3 del Regolamento 2016/679 la valutazione è effettuata nei casi in cui un trattamento può presentare rischi elevati, ossia quando:

- 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;
- 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 sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

In particolare, preso atto della tipologia di Studio (retrospettivo) in argomento, è condotta e resa pubblica una valutazione d'impatto sulla protezione dei dati, in forza dell'art. 35 del Reg. UE 2016/679, riguardo al trattamento dei dati ai sensi e per gli effetti del combinato disposto degli artt. 9, par. 2, lett. j) del GDPR, 110 e 110 bis, comma 4 del Codice Privacy.

Il presente documento contiene:



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

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

ACCETTABILITA' DEL RISCHIO

Tenuto conto della natura, del contesto, delle finalità e dell'ambito di applicazione del trattamento in esame, il **livello di rischio residuo**, considerato accettabile indicato dal Titolare, sentito anche il parere del DPO, è risultato **BASSO** MEDIO ALTO

Di seguito sono illustrati i dettagli della valutazione d'impatto sulla protezione dei dati.



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

1 Descrizione sistematica del trattamento

1.1.1 Contesto

Lo Studio in argomento si propone di identificare e validare un punteggio di rischio relativo all'insorgenza di tossicità cardiaca acuta e tardiva in una coorte storica di pazienti sottoposti a trattamento CHOP-Rituximab, includente antraciclina convenzionale a seguito di prima diagnosi di Linfoma diffuso a grandi cellule (DLBCL). Lo score verrà individuato dalla combinazione di una serie di fattori biologici e voluttuari indipendenti che siano predittivi dello sviluppo di tossicità cardiaca. La validità di tale punteggio sarà testata in una seconda coorte di pazienti che presenterà le stesse caratteristiche di quella identificata per lo sviluppo dello score.

A tal fine il contributo dei centri partecipanti allo studio si riassume di seguito:

- coordinamento attività di ricerca:
 - IRCCS Istituto Tumori "Giovanni Paolo II" di Bari.
- collazionamento dati di una coorte storica relativa pazienti afferenti all'Istituto di appartenenza secondo i criteri di arruolamento:
 - Azienda Ospedaliero Universitaria delle Marche, SOD Clinica Ematologica, Ancona
 - Azienda Ospedaliero-Universitaria Careggi, SOD Ematologia, Firenze
 - Azienda Ospedaliero – Universitaria Policlinico Umberto I, UOC Ematologia, Roma
 - Ospedale Businco, Div. Ematologia, Cagliari
 - Fondazione IRCCS Istituto Nazionale Tumori, SC Ematologia, Milano
 - AOU Maggiore della Carità di Novara - SCU Ematologia, Novara
 - Azienda USL – IRCCS di Reggio Emilia, SC Ematologia, Reggio Emilia
 - AOU Città della Salute e della Scienza di Torino, SC Ematologia Universitaria, Torino
 - Fondazione IRCCS Policlinico San Matteo, SC Ematologia, Pavia
 - AOU Policlinico Modena, Centro Oncologico Modenese, Modena



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

- o Ospedale Universitario Molinette San Giovanni Battista, U.O Ematologia, Torino
- o A.O. SS. Antonio e Biagio e Cesare Arrigo - S.C. Ematologia, Alessandria
- o ASST Spedali Civili di Brescia – Ematologia, Brescia
- o A.O. Ospedali Riuniti Villa Sofia-Cervello - Divisione di Ematologia, Palermo
- o Istituto clinico HUMANITAS IRCCS, Rozzano (MI)
- o Ospedale Dell'Angelo - U.O. Ematologia, Mestre (VE)
- o ASST Grande Ospedale Metropolitano Niguarda - SC Ematologia, Milano
- o Fondazione Policlinico Campus Biomedico – SC Ematologia, Roma (RM)
- o Ospedale S. Maria della Misericordia – Ematologia, Perugia (PG)
- o IRCCS Centro di Riferimento Oncologico, SOC Oncologia Medica e dei Tumori Immunocorrelati, Aviano
- o IRCCS CROB, UO Ematologia e Trapianto Cellule Staminali, Rionero in Vulture (PZ)
- o PO "A. Perrino", UOC Ematologia, Brindisi
- o Osp. Mons. Dimiccoli, Unità Operativa di Ematologia con trapianto, Barletta
- o Ospedale Vito Fazzi, Ematologia, Lecce
- o Azienda Ospedaliera Pia Fondazione di Culto e Religione "Car. G. Panico", UOC Ematologia e Centri Trapianti, Tricase (LE)
- o Ospedale S.G. Moscati, Ematologia, Statte (TA)
- o Azienda Ospedaliera Policlinico Consorziale, Unità Trapianti, Bari
- o Fondazione Casa Sollievo della Sofferenza Opera di San Pio da Pietralcina – UOC Ematologia, San Giovanni Rotondo (FG)
- o Fondazione IRCCS San Gerardo dei Tintori – UOC Ematologia Adulti, Monza (MB)
- o IRCCS Ospedale San Raffaele – Ematologia, Milano
- analisi dei dati secondo le finalità dello studio
 - o IFC-CNR – Pisa.

Tutti i dati collezionati verranno quindi centralizzati presso il sistema di raccolta dati predisposto dal centro promotore come di seguito dettagliato. Nello specifico, i dati pseudonimizzati, raccolti



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

presso i Centri partecipanti, saranno trasferiti mediante l'utilizzo della piattaforma RedCAP. IFC-CNR – Pisa, avrà accesso alla stessa piattaforma per l'estrazione dei dati funzionale all'elaborazione degli stessi.

1.2 Panoramica del trattamento

1.2.1 Quale è il trattamento in considerazione?

Lo studio si configura come osservazionale non interventistico di lungo periodo su coorte storica e verrà condotto mediante la raccolta di dati anamnestici e di successivo outcome relativi a un gruppo di pazienti trattati fra il 1998 e il 2015 per nuova diagnosi di Linfoma non Hodgkin diffuso a grandi cellule presso i Centri afferenti alla FIL (Fondazione Italiana Linfomi).

I pazienti inclusi nello studio saranno caratterizzati dalla presenza di diagnosi di linfoma diffuso a grandi cellule e dal trattamento con schema chemioterapico comprendente antracicline CHOP-Rituximab. Saranno invece esclusi i pazienti che abbiano sperimentato un precedente trattamento chemio-radioterapico.

Per l'identificazione dello score di rischio saranno necessari circa 800 pazienti.

Tenendo in considerazione una composizione per genere che prevede il 46% di donne e il 54% di uomini, una deviazione standard dell'età di 15 anni, un overall event rate del 7% sui gradi di tossicità più severi (livelli 3-5 secondo il criterio CTCV 2.0), la numerosità campionaria stimata permetterà di evidenziare, con una potenza statistica dell'80% e un livello di significatività pari al 5%, un Hazard Ratio a due code pari a 2 relativamente al genere, e pari a 1.03 anni relativamente all'età.

Per ottenere le informazioni complete su almeno 800 soggetti è previsto identificare un campione lordo di 1000 pazienti.



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

Per la fase di validazione verrà identificata una seconda coorte di circa 400 pazienti, con le stesse caratteristiche dei soggetti analizzati in precedenza.

Per i pazienti inclusi nello studio verranno raccolti i seguenti dati:

- Età al momento di iniziare la terapia;
- Sesso;
- BMI;
- L'eventuale presenza di fattori di rischio cardiovascolare al momento di iniziare la terapia antitumorale con particolare attenzione alla ipertensione arteriosa (identificazione del grado di ipertensione e della efficacia della terapia) e diabete;
- Familiarità per cardiopatia ischemica e scompenso cardiovascolare nei familiari di primo grado (genitori) e secondo grado (fratelli e sorelle);
- L'abitudine tabagica (> o < 10 sigarette/die);
- L'eventuale terapia cardiologica in uso al momento di iniziare la terapia antitumorale;
- Il valore di LVEF al basale (prima di iniziare la terapia), se disponibile;
- La dose totale di Doxorubicina (dose cumulativa) somministrata;
- La presenza di ricadute di malattia;
- L'eventuale radioterapia sul mediastino effettuata e la dose;
- I valori di LVEF disponibili misurati al follow up;
- La comparsa al follow up di eventi cardiovascolari così come definiti dagli end point primari e secondari.



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

Verrà registrata, inoltre, l'insorgenza dei seguenti endpoints:

- Riduzione della frazione di eiezione ventricolare sinistra (LVEF: left ventricular ejection fraction) < 50%;
- Comparsa di segni e sintomi di CHF (edemi periferici, dispnea da sforzo);
- Insorgenza di aritmie ventricolari o sopraventricolari correlate alla infusione di antracicline che richiedano intervento farmacologico;
- Insorgenza di ipertensione arteriosa di grado moderato o severo secondo la definizione della WHO,
- Insorgenza di ischemia miocardica (angina da sforzo o a riposo, infarto miocardico);
- Ospedalizzazione per cause cardiovascolari;
- Morte per cause cardiovascolari.

Tipologia di Studio

Trattasi di studio osservazionale retrospettivo, multicentrico.

1.2.2 Quali sono le responsabilità connesse al trattamento?

Gli sperimentatori coinvolti nello Studio sono appositamente autorizzati al trattamento dei dati, ai sensi dell'art. 29 del Reg. UE 2016/679 e dell'art. 2 quaterdecies del Dlgs 196/2003, così come novellato dal D.lgs 101/2018. Nell'ambito dello Studio risultano designati soggetti terzi in qualità di Responsabili del trattamento dati ai sensi dell'art. 28 del GDPR (IFC-CNR).



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

1.2.3 Ci sono standard applicabili al trattamento?

- La linea guida di Buona Pratica Clinica [Good Clinical Practice (GCP)] è uno standard internazionale di etica e qualità scientifica per progettare, condurre, registrare e relazionare gli studi clinici che coinvolgono soggetti umani. La GCP ha l'obiettivo di fornire, in conformità con i principi per la tutela dei diritti dell'uomo stabiliti dalla Dichiarazione di Helsinki, uno standard comune ad Unione Europea, Giappone e Stati Uniti per facilitare la mutua accettazione dei dati clinici da parte delle autorità regolatorie di queste aree geografiche;
- La linea guida recepita dall'Italia (G.U.R.I. n.191 del 18 agosto 1997) è stata messa a punto sulla base delle GCP attualmente adottate da Unione Europea, Giappone e Stati Uniti, oltre che da Australia, Canada, Paesi Nordici e dall'Organizzazione Mondiale della Sanità (OMS);
- Il trattamento di dati personali per scopi di ricerca scientifica è effettuato nel rispetto del Regolamento UE 2016/679, del Codice, delle Prescrizioni relative al trattamento dei dati genetici e delle Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica, nonché le Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, che costituiscono condizione essenziale di liceità e correttezza dei trattamenti.

1.3 Dati, processi e risorse di supporto

1.3.1 Quali sono i dati trattati e gli asset a supporto?

| Tipologia di dati personali | Categoria interessati |
|--|--|
| <input checked="" type="checkbox"/> Dati identificativi comuni (es. nome, cognome, indirizzo) <input checked="" type="checkbox"/> Dati di contatto (recapiti email, telefono, cellulare, etc.) <input type="checkbox"/> Credenziali di autenticazioni, chiavi di accesso | <ul style="list-style-type: none">• Pazienti vivi in visita presso il nostro Istituto• Pazienti deceduti o non reperibili |



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

| | |
|--|--|
| <input type="checkbox"/> Dati raccolti da strumenti audiovisivi, videosorveglianza <input type="checkbox"/> Dati raccolti da tecnologie traccianti e/o di monitoraggio <input type="checkbox"/> Dati raccolti da tecnologie IoT <input type="checkbox"/> Dati su abitudini di vita, consumi e comportamento <input type="checkbox"/> Dati su familiari/stato familiari <input type="checkbox"/> Dati bancari <input type="checkbox"/> Dati sulla localizzazione <input type="checkbox"/> Dati sulla solvibilità economica | |
| <input type="checkbox"/> Appartenenza sindacale <input type="checkbox"/> Convinzioni politiche, religiose o filosofiche <input type="checkbox"/> Origine razziale o etnica <input checked="" type="checkbox"/> Dati sulla salute <input type="checkbox"/> Orientamento e vita sessuale <input type="checkbox"/> Dati genetici <input type="checkbox"/> Dati biometrici <input type="checkbox"/> Dati "giudiziari" (diritto penale) | |
| <input checked="" type="checkbox"/> dati soggetti a maggior tutela: dati relativi alle infezioni da HIV (l. 15 febbraio 1996, n. 66; l. 3 agosto 1998, n. 269; l. 6 febbraio 2006, n. 38; l. 5 giugno 1990, n. 135; d.P.R. 9 ottobre 1990, n. 309; l. 22 maggio 1978, n. 194; d.m. 16 luglio 2001, n. 349; l. 29 luglio 1975, n. 405) | |
| Altro:..... | |

COMPONENTI ORGANIZZATIVE

**DATA PROTECTION IMPACT ASSESSMENT**

ai sensi dell'art. 35 del Reg. UE 2016/679

| | |
|--------------------------------|--|
| Soggetti interni | Lo staff dello studio è composto dal Principal Investigator e da uno a due Study Coordinator, specificamente individuati. Al Principal Investigator Autorizzato alla gestione delle attività di trattamento dei dati personali per i compiti relativi alla protezione dei dati personali necessari per la conduzione dello studio. Gli altri componenti dello staff sono delegati al trattamento di dati personali da parte del P.I. tramite apposito atto di nomina individuale |
| Soggetti esterni | Ciascun Centro Partecipante allo studio fornisce i dati pseudonimizzati mediante attribuzione di un codice. Il Responsabile del Trattamento riceve ed elabora, pertanto, solo dati pseudonimizzati. Tra il Promotore ed i Centri Partecipanti, e tra il Promotore ed il Responsabile del Trattamento rapporti sono regolati dal protocollo e dal Data Transfer Agreement. |
| COMPONENTI TECNOLOGICHE | |
| Applicazioni | Per l'elaborazione dei dati sono utilizzati sistemi di office automation quali RedCap, IBM SPSS Statistics, Prism. |
| Infrastrutture ICT | Per la conservazione dei dati in formato elettronico sono utilizzati i sistemi di storage aziendali opportunamente protetti sia per quanto riguarda l'accesso fisico che l'accesso ai database che sono opportunamente criptati secondo le regole tecniche usuali e politiche di backup specifiche. |
| Reti informatiche | I computer utilizzati per il trattamento dei dati si trovano su rete dedicata e messa in sicurezza su apposita VLAN. I trasferimenti avvengono mediante protocolli criptati. |
| COMPONENTI FISICHE | |
| Asset | Per l'elaborazione dei dati sono utilizzati appositi strumenti software aziendali. I PC su cui sono installati tali software sono muniti di idonei sistemi di autenticazione, autorizzazione e tracciabilità delle operazioni. |
| Sedi | Il trattamento dei dati avviene attraverso postazioni di lavoro presso la sede aziendale della ricerca scientifica con accesso riservato. |
| Archivi | I dati personali sono conservati in sicurezza presso l'archivio corrente aziendale o su IaaS (Infrastructure as a Service) in cloud opportunamente protetta. |



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

1.4 Finalità del trattamento

Il trattamento dei dati personali identificativi risulta necessario per le seguenti finalità dello Studio: identificare e validare un punteggio di rischio relativo all'insorgenza di tossicità cardiaca acuta e tardiva in una coorte storica di pazienti sottoposti a trattamento CHOP-Rituximab, includente antraciclina convenzionale a seguito di prima diagnosi di Linfoma diffuso a grandi cellule (DLBCL).

2 Principi Fondamentali

2.1 Valutazione della necessità e proporzionalità del trattamento del trattamento

Il trattamento è effettuato nel rispetto delle prescrizioni previste dall'art. 5 del GDPR e pertanto saranno trattati secondo i principi di:

1. liceità, correttezza e trasparenza
2. limitazione della finalità
3. minimizzazione dei dati
4. esattezza
5. limitazione della conservazione
6. integrità e riservatezza

Lo Studio in argomento comporta il trattamento di dati personali riconducibili allo stato di salute degli assistiti in cura presso l'IRCCS, secondo i criteri di inclusione dello Studio.

2.1.1 Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento correlato allo Studio è effettuato nel rispetto del principio di liceità e trasparenza. A tal proposito è stata predisposta e pubblicata sul sito internet istituzionale, unitamente alla presente VIP, l'informativa Privacy sullo studio in parola. Lo scopo dello Studio è esplicito ed è descritto dettagliatamente nella documentazione di presentazione del medesimo Studio approvato dal Comitato Etico competente.



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

2.1.2 Quale è il flusso dei dati durante il ciclo di vita del trattamento?

Il ciclo di vita del dato ha origine dall'acquisizione delle informazioni di interesse per lo studio attinenti lo stato di salute del paziente, attraverso la documentazione sanitaria e gli archivi presenti presso le Unità Operative dell'IRCCS ai sensi dell'art. 110Bis, 4 comma, Cod. Privacy.

Successivamente, previa:

- pseudonimizzazione dell'identità come descritto al punto 2.3;
- memorizzazione delle associazioni codice pseudonimizzato (generatore casuale) e nome/cognome del paziente in un file separato (tabella di transcodifica), per l'eventuale necessità di dover rintracciare il paziente nei casi previsti dal protocollo;

si provvede:

- all'annotazione di tali dati in una piattaforma di raccolta dati (eCRF) ovvero RedCap, cifrato in corrispondenza del dato pseudonimizzato;
- memorizzazione della corrispondenza tra l'anagrafica del soggetto ed il relativo pseudonimo su supporto informatico separato custodito in armadio accessibile fisicamente solo al Data Manager

Su tali dati verranno effettuate le attività delle elaborazioni statistiche peculiari dello Studio.

La trasmissione dei dati cifrati, dai centri partecipanti al Promotore e dal Promotore al Responsabile del Trattamento, avverrà solo tramite la suddetta piattaforma web istituzionale RedCap. Ad ogni centro partecipante saranno assegnate credenziali specifiche.

I dati clinici sono introdotti su sistema informativo di raccolta delle eCRF "RedCAP" ospitato sulla IAAS di InnoVaPuglia (Cloud Sanità). L'introduzione dello pseudonimo è eseguita attraverso sistema di regole autonomamente gestito da ciascun centro con la preposizione nelle prime 2 cifre dello pseudonimo di codice di identificazione del centro di provenienza.

La Web Application è sita nel layer DMZ, non raccoglie dati, ma consente l'accesso agli utenti autorizzati ed è protetta dalla rete internet esterna tramite firewall. Il database che colleziona i dati è accessibile esclusivamente dalla DMZ, la connessione è protetta da un apposito firewall.

I dati relativi all'identità dei pazienti sono sottoposti a pseudonimizzazione eseguita secondo una delle due procedure descritte nel paragrafo relativo alle misure tecniche.



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

I dati provenienti da centri collaboranti avranno accesso alla eCRF che espone i propri servizi secondo quanto descritto nel paragrafo delle misure tecniche. Per quanto attiene alle immagini esse vengono trasferite mediante collegamento in VPN (con protocollo IPSec) su server FTPS ospitato su rete interna all'Istituto con accesso controllato tramite apposite credenziali.

L'infrastruttura prevede uno spazio di archiviazione dedicato (NAS), cu cui viene effettuato un backup completo dei dati con frequenza giornaliera, dal provider del servizio cloud (InnovaPuglia s.p.a.).

L'accesso al sistema cloud è basato su connessione VPN con protocollo IPsec, che garantisce l'autenticazione dell'utente, preservando l'integrità dei dati e la confidenzialità.

Al sistema cloud possono accedere solo i ricercatori individuati per lo studio in oggetto, per i quali verranno messe a disposizione delle apposite credenziali di accesso.

2.1.3 Quali sono le basi legali che rendono lecito il trattamento?

Basi giuridiche del trattamento di dati

Paziente in vita e rintracciabile

Art. 6 par. 1, lett a) e Art. 9 par. 2 lett. a) del GDPR (**acquisizione del consenso**).

Pazienti deceduti o non rintracciabili

Art. 9 par. 2 lett. j) del GDPR e artt. 110-110 bis c. 4 del d.lgs 196/03 e Aut. Gen. 9/2016 e ss aggiornamenti:

Il trattamento è necessario a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea, ed è condotta e resa pubblica una valutazione d'impatto sulla protezione dei dati.

Il paziente è qualificato come non rintracciabile dopo almeno 3 tentativi (tracciati) di contatto non riusciti.



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

L'interessato deceduto viene rilevato dalla CC (in caso di decesso durante il periodo di degenza) o dal sistema TS (tessera sanitaria).

Ulteriori garanzie:

art. 8, comma 5-bis del d.lgs. n. 288 del 2003

2.1.4 I dati sono esatti e aggiornati?

I dati personali sono acquisiti dagli archivi aziendali con ulteriori controlli interni in caso di omonimie o omocodie.

2.1.5 Qual è il periodo di conservazione dei dati?

| Tipologia di dati personali | Tempi di conservazione |
|---|---|
| Dati pseudonimizzati | I dati pseudonimizzati saranno conservati per la durata dello studio, decorsi i quali saranno anonimizzati. |
| Tabella di corrispondenza Codice ID/Paziente | La tabella di corrispondenza sarà cancellata in modalità permanente al termine della durata dello studio in parola. |

2.2 Misure a tutela dei diritti degli interessati

2.2.1 Come sono informati del trattamento gli interessati?

A beneficio dei pazienti deceduti o per quelli irreperibili sono pubblicate nell'apposita sezione del sito internet istituzionale, le informazioni sul trattamento dei dati relative allo specifico studio in



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

parola, ai sensi dell'art. 14, par. 5, lett. b) del Reg. UE 2016/679. È altresì pubblicato l'avviso di assenza di consenso con relativa valutazione d'impatto.

2.2.2 Ove applicabile: come si ottiene il consenso degli interessati?

Paziente in vita e rintracciabile

Art. 6, par. 1, lett. A) e art. 9 par. 2 lett. a) del GDPR

Il consenso, ove possibile, è raccolto dal paziente in fase di arruolamento, tramite l'acquisizione di firma autografa su modello "Consenso Informato Privacy specifico della Ricerca rev 3.0 del 28 ottobre 2024".

Paziente deceduti/non rintracciabili

Per tale categoria di pazienti, il consenso non può essere raccolto pertanto per il nostro IRCCS ci si avvale dell'art. **110 e 110 bis, comma 4 del Codice Privacy e art. 9, par 2, lett j), GDPR.**

2.2.3 Come fanno gli interessati a esercitare i loro diritti?

I diritti degli interessati di cui agli artt. 15-22 del GDPR sono sempre garantiti nelle modalità indicate nell'informativa ex artt. 13-14 del GDPR rese al momento dell'arruolamento o della pubblicazione. Altresì sono resi disponibili sul sito internet istituzionale (<https://www.sanita.puglia.it/web/irccs/privacy1>) i modelli da poter utilizzare per l'esercizio di tali diritti.

I diritti di cui agli articoli da 15 a 22 del Reg. UE 2016/679 riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce quale avente diritto o per ragioni familiari meritevoli di protezione. Le informazioni sul trattamento dei dati circa gli Studi condotti in assenza del consenso sono rese pubbliche sul sito internet istituzionale, nell'apposita sezione dedicata alla ricerca scientifica, ivi comprese le valutazioni d'impatto sulla



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

protezione dati.

2.2.4 In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

I dati personali non saranno trasferiti verso Paesi Terzi extra UE.

2.3 Misure esistenti o pianificate per la protezione del dato

- **garanzie** (adozione di tecniche di pseudonimizzazione, minimizzazione, implementazione della privacy by design e by default, previsione di procedure volte a testare, verificare e valutare l'efficacia delle garanzie e misure adottate)
- **misure di sicurezza organizzative** (es: norme e procedure che disciplinano l'aspetto organizzativo della sicurezza)
- **misure di sicurezza fisiche** (es: misure di protezione di aree, apparecchiature, dati)
- **misure di sicurezza logiche** (backup, piano di continuità operativa, piano di disaster recovery) sia in relazione al corretto utilizzo degli strumenti elettronici, sia in relazione alla loro gestione e manutenzione

Di seguito le principali misure tecniche applicate, ai sensi dell'art. 32 del Reg. UE 2016/679:

- **Endpoint protection:** Antivirus e firewall sulle singole postazioni di lavoro costantemente aggiornati mediante server ed associazioni a dominio. L'IRCCS ha acquisito un sistema di sicurezza integrato che comprende la gestione del *firewall* e del SOC. Per il monitoraggio e il controllo della rete viene utilizzato lo strumento Manage Engine Central che individua, gestisce e tiene traccia delle risorse poste sotto il dominio. Il SOC funge da primo soccorso in caso di incidente di sicurezza. Si possono eseguire operazioni come: isolare gli *endpoint*, terminare i processi dannosi, impedire l'esecuzione di processi dannosi ed eliminare i *files*.
- Implementazione di un Piano Operativo del servizio di sicurezza;
- Adozione del *cloud* di Regione Puglia, gestito dalla società *in-house* Innovapuglia, come *cloud* aziendale. Per i dati migrati sui menzionati *cloud* sono garantiti ridondanza dei dati e *backup*.
- Accesso alle postazioni di lavoro mediante password a dominio aggiornata secondo i criteri



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

di sicurezza adeguati al trattamento dei dati sensibili

- Separazione del server applicativo per la compilazione della eCRF dal database che contiene i dati della eCRF stessa;
- Collocazione del server applicativo in zona demilitarizzata "DMZ" e del server database in zona protetta con protocolli di comunicazione tra loro di tipo "secure";
- Installazione dell'infrastruttura di elaborazione su IAAS regionale (Cloud Sanità) in architettura in alta affidabilità su siti fisicamente separati e contemporaneamente aggiornati e backup giornaliero al fine del *disaster recovery*
- Intrusion detection system sia a livello applicativo che sullo strato dei dati
- Tecniche di pseudonimizzazione dell'identità dei pazienti realizzate alla volta con:
 1. tabella fisica di associazione pseudonimo/identità custodita in armadio a chiave dal PI e solo da questi accessibile
 2. esecuzione di algoritmi di hashing non reversibili a chiave
- Registrazione dei log di accesso al server applicativo e database, È altresì prevista la possibilità di verificare i log dall'Event Viewer di ciascuna postazione degli utenti abilitati come Amministratori di Sistema.
- Aggiornamento costante dei sistemi operativi e dei software di sistema e di ambiente. Predisposizione di un *asset inventory* tecnologico attraverso lo strumento di Manage Engine Central che individua, gestisce e tiene traccia delle risorse poste sotto dominio.
- Backup quotidiano della base dei dati su supporto ottico custodito separatamente in armadio ad accesso fisico ad uso esclusivo del PI. È presente un data center virtuale con servizi Backup As A Service presso Innovapuglia e PSN.
- Utilizzo di utenze nominative
- Meccanismi di identificazione ed autenticazione degli utenti
- Classificazione strutturata delle informazioni che tenga conto delle informazioni riservate/contenenti particolari categorie di dati ex art. 9 GDPR, attraverso sw dotati di certificazione di sicurezza.
- Password Policy adeguate al trattamento dei dati sensibili. L'ente ha sviluppato una policy sull'assegnazione delle password e che prescriva come tutte le macchine sotto dominio dell'ente richiedano periodicamente l'aggiornamento delle password.
- Erogazione di contenuti formativi per i dipendenti dell'ente che operano nel campo della ricerca.



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

Misure di sicurezza specifiche per campioni biologici:

Non applicabile

3 Rischi

3.1 *Panoramica dei rischi per diritti e libertà*

Il processo di **valutazione del rischio** parte dalla determinazione dell'impatto sull'interessato (cioè sulla persona fisica a cui il dato si riferisce) in caso di distruzione, perdita, modifica, divulgazione non autorizzata o altri avvenimenti negativi che possono compromettere la sicurezza del trattamento.

L'impatto derivante dalla perdita di una o più delle caratteristiche della sicurezza delle informazioni, ossia riservatezza, integrità e disponibilità, rappresenta la gravità del danno diretto o indiretto causato agli interessati.

Nel valutare i rischi per le libertà e diritti degli interessati, però, come suggerisce la norma ISO/IEC 29134 si dovrebbero considerare anche altri aspetti, oltre alla sicurezza dei dati; e che pertanto devono essere considerati gli effetti complessivi del trattamento.

I rischi pertanto sono identificati in base ai seguenti quattro parametri:

- 1) conformità ai principi applicabili al trattamento dei dati (art. 5 del Reg. UE 2016/679)
- 2) riservatezza
- 3) integrità
- 4) disponibilità.

A tal fine, nella determinazione del livello di impatto sono incluse valutazioni sulle possibili conseguenze derivanti da mancanza di trasparenza, mancato rispetto dei tempi di conservazione dei dati, o dalla violazione degli altri principi fondamentali applicabili alla protezione dei dati personali.

- **Quali sono le principali minacce che potrebbero concretizzare il rischio?**



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

Una minaccia potrebbe concretizzarsi solo al momento dell'acquisizione dei dati durante la consultazione della documentazione sanitaria, che però è effettuata da personale esercente la professione sanitaria, tenuta al segreto professionale, ed istruita in materia di protezione dei dati personali.

- **Quali sono le fonti di rischio?**

Una fonte di rischio potrebbe essere rappresentata dalla tabella di transcodifica che è gestita separatamente e che se sottratta insieme al database centralizzato dello Studio, consentirebbe di risalire allo stato di salute ed alle patologie dei soggetti inclusi nello Studio.

Non si ravvisano rischi per l'assistito in merito alla perdita di disponibilità del dato in quanto, in caso di evento avverso, non saranno compromessi i dati acquisiti e conservati per finalità di diagnosi, assistenza e cura. Anche in caso di perdita di integrità non saranno compromessi dati acquisiti e conservati per finalità di diagnosi, assistenza e cura, ma solo per la finalità dello Studio.

- **Quali misure fra quelle individuate contribuiscono a mitigare il rischio?**

Oltre alle istruzioni operative fornite agli sperimentatori, è implementato un sistema crittografico sull'archivio centralizzato che prevede crittografia AES 256 bit con 14 round o cicli di elaborazione crittografica.

- **Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?**

Il rischio residuo calcolato, dopo l'adozione delle misure di sicurezza pianificate, è BASSO, anche per l'applicazione delle misure di sicurezza dirette sul dato come la pseudonimizzazione e cifratura e misure tecniche generali dell'ente.

Le fonti di rischio possono essere categorizzate in:

- **Violazioni dei principi applicabili ai trattamenti di dati personali**
- **Minacce alla sicurezza dei trattamenti**



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

- **Eventi con danni fisici/materiali**
- **Eventi naturali**
- **Perdita o indisponibilità di servizi essenziali**
- **Compromissione di dati e informazioni**
- **Problemi tecnici**
- **Azioni non autorizzate**
- **Compromissione di funzioni / servizi per errori o azioni malevole**

Il livello di rischio è direttamente proporzionale alla probabilità che si verifichino le diverse minacce e alla gravità dell'impatto per gli interessati. Può essere mitigato con l'applicazione delle necessarie misure di mitigazione.

Se l'applicazione delle misure di mitigazione riduce il livello di rischio, fornendo un primo livello di rischio residuo, il governo dei processi e il presidio di controlli efficaci può fornire un ulteriore livello di ponderazione. Ecco perché oltre alle specifiche contromisure, la metodologia utilizzata inserisce, mediante un self assessment, degli obiettivi di controllo specifici per diverse categorie e ambiti, e dei controlli sullo svolgimento del processo di Valutazione di impatto.

Per la data protection si fa riferimento ai controlli della ISO/IEC 29151, estensione di quelli della ISO/IEC 27001 Annex A, a quelli della ISO/IEC 27701:2019 e della ISDP10003:2018.

3.2 Accesso illegittimo ai dati

3.2.1 Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Danno immateriale, perdita dignità, perdita di controllo sui propri dati personali, irritazione, perdita della fiducia nella sanità pubblica, perdita finanziaria

3.2.2 Quali sono le principali minacce che potrebbero concretizzare il rischio?

Accessi esterni non autorizzati, Uso improprio del software, Corruzione dei dati, Comunicazione illegale dei dati e dei documenti, Uso non autorizzato dei dati, attacco hacker.



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

3.2.3 Quali sono le fonti di rischio?

Fonti di rischio umane interne, fonti di rischio umane esterne

3.2.4 Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia AES 256 bit sugli archivi elettronici dello Studio e dei relativi backup, Controllo degli accessi logici, Tracciabilità, Lotta contro il malware, Gestione postazioni, Politica di tutela della privacy, Firewalling, EDR, Registrazione dei log di accesso al server applicativo e *database*.

3.2.5 Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Significativa. La gravità del rischio potenziale di accesso illecito ai dati è stimata come ALTA, in considerazione della tipologia di dati raccolti.

3.2.6 Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

La probabilità di accadimento è stimata come BASSA in considerazione delle misure di garanzia implementate con particolare riferimento alla tecniche di pseudonimizzazione e crittografia applicate, oltre che a tutte le misure di natura tecnica e organizzativa implementate dall'ente.

3.3 Modifiche indesiderate dei dati

3.3.1 Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Modifiche ai dati raccolti per finalità di ricerca non comportano un impatto diretto all'interessato.

3.3.2 Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Accessi esterni non autorizzati, Azione di virus informativi o di codici malefici, Uso non autorizzato dei dati, Sabotaggio, Alterazione dolosa o colposa dati

3.3.3 Quali sono le fonti di rischio?



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

Fonti di rischio umane interne, fonti di rischio umane esterne

3.3.4 Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Crittografia, Controllo degli accessi logici, Tracciabilità, Lotta contro il malware, Gestione postazioni, Backup, Manutenzione, Politica di tutela della privacy, Firewalling, EDR, Registrazione dei log di accesso al server applicativo e *database*.

3.3.5 Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Limitata. La gravità del rischio potenziale di modifica illecita dei dati è stimata come BASSA, in considerazione della presenza di dati originali già raccolti per finalità di diagnosi e cura.

3.3.6 Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

La probabilità di accadimento è stimata come BASSA in considerazione delle misure di garanzia implementate.

3.4 Perdita di dati

3.4.1 Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

perdita di fiducia, irritazione, perdita reputazione, perdita di controllo sui propri dati personali

3.4.2 Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Azione di virus informativi o di codici malefici, Sabotaggio, attacco hacker, Uso non autorizzato dei dati, Uso improprio del software, Accessi esterni non autorizzati

3.4.3 Quali sono le fonti di rischio?

fonti di origine naturale, fonti di rischio umane esterne, fonti di rischio umane interne

3.4.4 Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Backup, Disaster Recovery plan, Manutenzione, Politica di tutela della privacy, Controllo degli accessi



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

logici, Crittografia, Tracciabilità, Lotta contro il malware, Firewalling, EDR, Registrazione dei log di accesso al server applicativo e *database*.

3.4.5 Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

La probabilità di accadimento è stimata come BASSA in considerazione delle misure di garanzia implementate.

3.5 METRICHE PER ANALISI RISCHIO

Valori dei livelli di rischio

| <u>Livello</u> | <u>Descrizione</u> |
|----------------|--|
| BASSO | Il rischio per gli interessati è accettabile dall'organizzazione mediante misure organizzative e tecniche idonee, ma deve continuare ad essere monitorato per controllare che cambiamenti non incrementino il livello di rischio |
| MEDIO | Il rischio medio per gli interessati potrebbe essere accettabile ma l'adozione delle misure tecnico-organizzative deve essere monitorata su base regolare, e il trattamento può essere sottoposto a ulteriori considerazioni |
| ALTO | Il rischio per le persone interessate al trattamento è ad un livello non accettabile e necessita un rafforzamento delle misure di mitigazione |
| ELEVATO | Il rischio per gli interessati si presenta elevato o molto critico, mantenendo un livello non accettabile per l'organizzazione e necessitando l'aggiunta di ulteriori controlli a prevenzione/mitigazione dello stesso |

Valori dei livelli di probabilità

**DATA PROTECTION IMPACT ASSESSMENT**

ai sensi dell'art. 35 del Reg. UE 2016/679

| Livello | Descrizione |
|----------------|--|
| BASSO | Evento/Minaccia poco probabile/frequente, o raro; è improbabile che la minaccia si concretizzi in condizioni normali o può verificarsi con frequenza inferiore rispetto alle tendenze riportate da studi, ricerche, statistiche di settore |
| MEDIO | Evento/Minaccia possibile; è un evento che si è già verificato o che può verificarsi con frequenza in media con le tendenze riportate da studi, ricerche, statistiche di settore |
| ALTO | Evento/Minaccia probabile; è un evento che si è già verificato o che può verificarsi con frequenza superiore rispetto alla media con riferimento alle tendenze riportate da studi, ricerche, statistiche di settore |

Valori dei livelli di impatto

| Livello | Descrizione |
|----------------------|--|
| IRRILEVANTE | Gli interessati possono incontrare alcuni piccoli inconvenienti, che supereranno senza troppi problemi |
| LIMITATO | Gli interessati possono incontrare disagi significativi, che riusciranno comunque a superare a dispetto di alcuni problemi |
| SIGNIFICATIVO | Gli interessati possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà |
| CRITICO | Gli interessati possono avere conseguenze gravi, o addirittura irreversibili, che potrebbero non superare |

**DATA PROTECTION IMPACT ASSESSMENT**

ai sensi dell'art. 35 del Reg. UE 2016/679

4 Panoramica dei rischi

| Rischio Privacy | Descrizione delle conseguenze per gli interessati derivanti dalla vulnerabilità del trattamento | Livello di impatto |
|---|---|---------------------------|
| Perdita dei dati personali | La perdita dei dati potrebbe comportare un danno agli interessati in termini di perdita di controllo sui propri dati | MEDIO |
| Distruzione non autorizzata o indisponibilità | La distruzione dei dati o l'indisponibilità degli archivi dello Studio non comporta un impatto diretto sugli interessati | BASSO |
| Modifica non autorizzata | La modifica dei dati per finalità di ricerca non comporta un impatto diretto sugli interessati | BASSO |
| Divulgazione non autorizzata | La divulgazione di dati personali dei partecipanti allo Studio potrebbe comportare un danno rilevante agli interessati | ALTO |
| Accesso ai dati non autorizzato | L'accesso illecito ai dati personali dei partecipanti allo Studio potrebbe comportare un danno rilevante agli interessati | ALTO |

**DATA PROTECTION IMPACT ASSESSMENT**

ai sensi dell'art. 35 del Reg. UE 2016/679

| | | |
|---|--|--------------|
| Eccessiva raccolta di dati personali | Utilizzare più dati personali del dovuto implicherebbe un'esposizione di dati personali all'utilizzo per scopi non pertinenti e non compatibili | BASSO |
| Collegamenti o raffronti inappropriati o non autorizzati a dati personali | Collegamenti o raffronti con altre banche dati potrebbe comportare danni immateriali agli interessati | BASSO |

| Rischio Privacy | Descrizione delle conseguenze per gli interessati derivanti dalla vulnerabilità del trattamento | Livello di impatto |
|---|---|---------------------------|
| Perdita di controllo dei dati da parte degli interessati | La mancanza di trasparenza e sicurezza dei trattamenti potrebbe comportare un impatto per gli interessati | BASSO |
| Riuso per finalità diverse dei dati personali senza la consapevolezza e/o il consenso degli interessati | I dati personali potrebbero essere utilizzati per altre finalità sconosciute all'interessato con danno immateriale agli interessati (mancanza di trasparenza e consenso) | BASSO |
| Disequità o difettosità dell'elaborazione o del processo | In caso di errata elaborazione delle informazioni, errori di registrazione etc. gli interessati potrebbero subire nocumento | BASSO |



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

| | | |
|---|---|--------------|
| Conservazione immotivatamente prolungata dei dati personali | La conservazione dei dati oltre il periodo prestabilito e motivato potrebbe comportare un danno immateriale agli interessati | BASSO |
| Inesattezza o perdita di qualità dei dati personali | Eventuali inesattezze o perdita della qualità dei dati raccolti non presenta un impatto diretto sui pazienti | BASSO |
| Re-identificazione dei soggetti interessati | Il processo di anonimizzazione potrebbe non eliminare la probabilità di re-identificazione dei partecipanti allo Studio, con particolare riferimento a malattie rare, con conseguente nocumento agli interessati | BASSO |

**DATA PROTECTION IMPACT ASSESSMENT**

ai sensi dell'art. 35 del Reg. UE 2016/679

| CATEGORIE DI MINACCE CONSIDERATE | Livello MAX Prob. |
|--|--------------------------|
| Minacce alla conformità del trattamento | BASSO |
| Eventi con danni fisici | BASSO |
| Eventi naturali | BASSO |
| Indisponibilità dei servizi essenziali | BASSO |
| Violazioni di dati per azioni deliberate | MEDIO |
| Problemi tecnici | BASSO |
| Violazioni di dati per azioni involontarie | BASSO |

| CATEGORIE DI MINACCE | EFFICACIA MISURA ESISTENTE |
|---|-----------------------------------|
| Minacce alla conformità del trattamento | MISURE ESISTENTI ADEGUATE |
| Eventi con danni fisici/materiali/immateriali | MISURE ESISTENTI ADEGUATE |
| Eventi Naturali | MISURE ESISTENTI ADEGUATE |
| Indisponibilità di Servizi essenziali | MISURE ESISTENTI ADEGUATE |
| Compromissione di dati e informazioni per azioni deliberate | MISURE ESISTENTI ADEGUATE |



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

| | |
|--|---------------------------|
| Problemi tecnici | MISURE ESISTENTI ADEGUATE |
| Compromissione di dati o servizi per azioni involontarie | MISURE ESISTENTI ADEGUATE |

A seguito della ponderazione del livello di rischio calcolata mediante l'applicazione della mitigazione delle misure tecniche ed organizzative, il **rischio residuo** risulta **BASSO**, pertanto

| | |
|---|--|
| ACCETTABILE <input checked="" type="checkbox"/> | NON ACCETTABILE <input type="checkbox"/> |
|---|--|



DATA PROTECTION IMPACT ASSESSMENT

ai sensi dell'art. 35 del Reg. UE 2016/679

Il Titolare del trattamento, in persona del Direttore Generale *pro tempore*, preso atto delle valutazioni sopra riportate in ordine all'analisi del potenziale impatto per i diritti e le libertà degli interessati, con l'adozione della presente VIP, dispone che il documento:

- a) sia reso pubblico sul sito internet istituzionale nell'apposita sezione della Ricerca Scientifica (pubblicazione obbligatoria se lo Studio rientra nell'ambito del programma di ricerca nazionale, ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502)
- b) sia resa disponibile agli interessati, su istanza dei medesimi.

Data.....

Firma del Direttore Generale.....