UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

Dipartimento di Scienze Biomediche, Metaboliche e Neuroscienze

Via Giuseppe Campi, 287
41125 - Modena, Italia

www.bmn.unimore.it

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI

VERSIONE	DATA	REDAZIONE	VISTO E VALIDATO
00	02.05.2025	Titolare del trattamento UNIMORE, per essa: • Dipartimento di Scienze Biomediche, Metaboliche e Neuroscienze • Dipartimento di Ingegneria Enzo Ferrari	Il DPO

SOMMARIO

1. INTRODUZIONE E DEFINIZIONI 4
1.1 Definizioni 4
1.2 Valutazione dei rischi 6
2. CONTESTO 6
2.1 Descrizione del trattamento 6
2.1.1 Descrizione dello Studio 6
2.1.2 Obiettivi dello Studio 7
2.1.3 Ciclo di vita del trattamento 7
2.2 Responsabilità connesse al trattamento 10
2.3 Standard applicabili al trattamento 11

2.4 Dati personali trattati 11
2.4.1 Categorie di dati personali 11
2.4.2 Modalità di raccolta 12
2.5 Interessati 12
2.6 Finalità del trattamento 12
2.7 Mezzi di trattamento – risorse di supporto al trattamento 12
2.8 Destinatari dei dati personali 13
2.9 Durata del trattamento e periodo di conservazione 13
2.10 Trasferimento di dati personali 13
3. PRINCIPI FONDAMENTALI 13
3.1 Limitazione delle finalità 14
3.2 Liceità del trattamento – base giuridica 14
3.3 Minimizzazione dei dati 14
3.4 Correttezza e aggiornamento dei dati 15
3.5 Misure a tutela dei diritti degli interessati 15
4. MISURE DI SICUREZZA ADOTTATE E APPLICABILI AL TRATTAMENTO 15
5. VALUTAZIONE DEL RISCHIO 20
5.1 Matrice di valutazione del rischio 20
5.2 Rischio di perdita di riservatezza – accesso illegittimo ai dati 22
Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare? 22
Quali sono le principali minacce che potrebbero concretizzare il rischio? 23
Quali sono le fonti di rischio? 23
Quali misure fra quelle individuate contribuiscono a mitigare il rischio? 23
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate? 23
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate? 24
5.3 Rischio di perdita di integrità – modifiche indesiderate dei dati 25

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare? 25

Quali sono le principali minacce che potrebbero concretizzare il rischio? 25

Quali sono le fonti di rischio? 25

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio? 25

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate? 26

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate? 26

5.4 Rischio di perdita di disponibilità – perdita di dati 27

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi? 27

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio? 27

Quali sono le fonti di rischio? 27

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio? 28

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate? 28

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate? 28

5.5 Valutazione complessiva 29

1. INTRODUZIONE E DEFINIZIONI

1.1 DEFINIZIONI

1) «**GDPR**»: 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);
2) «**Codice Privacy**»: D.lgs. n. 196/2003, così come modificato e dal D.lgs. n. 101/2018;
3) «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»);
4) «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
5) «**pseudonimizzazione**»: misura applicata ai dati personali trattati affinché gli stessi non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
6) «**anonimizzazione**»: operazione di de-identificazione volta a trasformare irreversibilmente i dati personali in dati anonimi, dai quali, dunque, non sia in alcun modo possibile risalire all'identità degli interessati ai quali si riferiscono;
7) «**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i

criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
9) «**autorizzati al trattamento**»: le persone fisiche, dipendenti o collaboratori, che si inseriscono nell'organizzazione del Titolare o del Responsabile del trattamento ed operano direttamente sotto la loro diretta l'autorità;
10) «**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
11) «**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
12) «**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
13) «**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
14) «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR;
15) «**rischio**»: scenario chiamato a descrivere un evento e le relative conseguenze stimato in termini di probabilità e gravità;
16) «**fonte di rischio**»: la fonte di rischio può essere umana o non umana. Per "fonte umana" si intende una persona, interna o esterna al Titolare o al Responsabile, che opera in via accidentale o intenzionale (esempio: amministratore IT, utente, dipendente, collaboratore, attaccante esterno, concorrente). Per "fonte non umana" si intende tutte le possibili fonti di rischio naturali che si verificano indipendentemente da un'azione umana (esempio: allagamento, incendio, interruzione o guasto di rete, interruzione elettrica);
17) «**minaccia**»: modalità operativa, comprendente una o più azioni individuali, applicata sulle risorse che supportano i dati. La minaccia può essere utilizzata, intenzionalmente o meno, da fonti di rischio e può quindi determinare la concretizzazione del rischio;

18) «**gestione dei rischi**»: insieme delle attività volte ad indirizzare il Titolare del trattamento in relazione a rischi individuati, analizzati, stimati, valutati e, successivamente, riesaminati;
19) «**gravità del rischio**»: rappresenta l'entità del rischio. La sua entità dipende principalmente dalla natura pregiudizievole del potenziale impatto sull'interessato;
20) «**probabilità del rischio**»: esprime la possibilità che un rischio si realizzi concretamente. La sua entità dipende principalmente dal livello di vulnerabilità delle risorse di supporto ai dati quando sono sottoposte alle minacce e dalla capacità delle fonti di rischio di sfruttare tali vulnerabilità.

1.2 VALUTAZIONE DEI RISCHI

Alla luce dell'art. 35, par. 7, lett. c del GDPR, la valutazione di impatto sulla protezione dei dati ("DPIA" acronimo di *Data Protection Impact Assessment*) deve contenere «una valutazione dei rischi per i diritti e le libertà degli interessati» e deve essere realizzata «quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche».

Inoltre, secondo l'Autorità Garante per la protezione dei dati personali, la valutazione di impatto deve sempre essere effettuata negli studi retrospettivi quando:

- il trattamento dei dati personali è su larga scala;
- vengono trattate categorie particolari di dati, ad esempio dati genetici;
- l'attività comporta il data linkage di molteplici e diversi archivi di dati;
- l'attività prevede la rilevazione di dati per individui vulnerabili (minori, soggetti con patologie psichiatriche, anziani, ecc.);
- la base giuridica per il trattamento dei dati non è riferibile al consenso al trattamento, a ricerche condotte sulla base di disposizioni di legge o regolamento o al diritto, o ad altre specifiche fattispecie previste dal GDPR e dal Codice Privacy.

2. CONTESTO

2.1 DESCRIZIONE DEL TRATTAMENTO

Il trattamento di dati personali oggetto della presente valutazione è realizzato nel contesto dello Studio "*Esposizione a fattori ambientali e rischio di tumori infantili*" (di seguito "Studio").

7363 Descrizione dello Studio

Studio caso-controllo retrospettivo population based promosso da Unimore e che coinvolge diverse strutture ospedaliere del territorio.

7.3.3.7 Obiettivi dello Studio

Lo Studio ha l'obiettivo di valutare l'associazione fra il rischio di tumori infantili e l'esposizione a fattori ambientali, in particolare in relazione:

- al benzene e altri inquinanti contenuti nelle emissioni del traffico autoveicolare e dei distributori;
- ai pesticidi derivati dall'uso agricolo;
- all'esposizione a campi elettromagnetici.

Il risultato atteso dallo Studio è l'individuazione e la quantificazione di eventuali eccessi di rischio relativo ai diversi tumori infantili presi in esame, associabile all'esposizione a fattori ambientali tra i quali le emissioni del traffico autoveicolare, con particolare riferimento al benzene, utilizzando modelli multivariati di regressione logistica condizionata e tenendo conto dei possibili fattori confondenti e di modificatori di effetto. In aggiunta, lo Studio permetterà di valutare eventuali incrementi del rischio di tali patologie associati all'esposizione ambientale a pesticidi utilizzati nelle coltivazioni site presso la residenza dei soggetti, ai campi elettromagnetici e alle emissioni di benzene provenienti da distributori di benzina.

7.3.3.8 Ciclo di vita del trattamento

A3 Raccolta dei dati relativi ai Minori-Casi e Minori-Controlli

Nello Studio saranno individuati i casi di tumori infantili diagnosticati a partire dal 1998 e sino al 31 dicembre 2024 in bambini di età inferiore o uguale ai 14 anni, residenti al momento della diagnosi nel territorio delle province di Modena e di Reggio Emilia (di seguito "Minori-Casi" o "Minore-Caso").

I dati relativi a tali Minori-Casi saranno acquisiti tramite la consultazione del Registro nazionale dell'Associazione Italiana Ematologia Oncologia Pediatrica (di seguito "*AIEOP*") e del Registro nazionale dell'Associazione Italiana Registro Tumori (di seguito "*AIRTUM*"). Tali dati verranno raccolti direttamente dalle suddette associazioni e saranno condivisi ad Unimore in forma pseudonimizzata.

A singoli Minori-Casi verrà affiancata una popolazione di controllo, costituita da minori non affetti da tumore (di seguito "Minori-Controlli" o "Minore-Controllo").

Ad ogni Minore-Caso verranno affiancati quattro Minori-Controlli, caratterizzati dal medesimo sesso, anno di nascita e provincia di residenza nel momento di diagnosi del Minore-Caso cui verranno appaiati.

I dati relativi ai Minori-Controlli saranno estratti casualmente da parte delle AUSL di Modena e AUSL di Reggio Emilia utilizzando il database storico dei residenti dei Comuni di Modena e Reggio Emilia in relazione ad ogni anno di diagnosi dei rispettivi casi di appaiamento. Una volta estratti i dati relativi ai Minori-Controlli, le suddette AUSL provvederanno a comunicarli in forma pseudonimizzata ad Unimore.

Oltre alle suddette informazioni, saranno raccolti dati relativi alla collocazione geografica dei Minori-Casi e dei Minori-Controlli presi in considerazione. Tale raccolta di dati avverrà

mediante la consultazione dei registri anagrafici comunali informatizzati e cartacei di natura pubblica e considererà i seguenti periodi di esposizione: per i Minori-Casi sarà considerato il periodo di esposizione pari a 5 anni precedenti la data di incidenza; per i Minori-Controlli si valuterà l'identico periodo di esposizione nei 5 anni precedenti la data indice di diagnosi del relativo caso appaiato.

B3Creazione dei Database GIS

I dati spaziali relativi ai Minori-Casi e Minori-Controlli saranno utilizzati per la creazione di un ambiente Geographical Information System (di seguito "GIS"), con il quale sarà possibile effettuare una valutazione espositiva agli inquinanti da traffico autoveicolare, pesticidi e campi elettromagnetici di ciascun soggetto incluso nello Studio.

La creazione di detto database sarà affidata al Dipartimento di Ingegneria "Enzo Ferrari", in collaborazione ARPA Modena e TerrAria S.r.l., e prevede il solo inserimento di dati di natura spaziale. Si precisa, infatti, che mediante il database GIS non sarà in alcun modo possibile effettuare alcuna correlazione tra i dati spaziali raccolti e il singolo Minore-Caso o Minore-Controllo considerato.

Ogni dato spaziale raccolto sarà georeferenziato tramite attribuzione delle coordinate satellitari cartografiche su un sistema Gauss-Boaga di ciascun edificio, mediante dati ottenuti dalle cartografie tecniche provinciali di Modena e di Reggio Emilia o mediante consultazione della banca dati Google Earth oppure rilevate direttamente sul posto, tramite l'utilizzazione di un dispositivo di georeferenziazione satellitare GPS Garmin in dotazione al gruppo di ricerca.

Il database GIS, oltre ai dati spaziali relativi ad entrambe le categorie di minori, sarà arricchito con ulteriori informazioni relative alle aree esposte ai fattori di rischio presi in esame nel presente Studio. In particolare, il database verrà arricchito con le seguenti informazioni:

- *Tipologia uso del suolo in stretta prossimità alla residenza dei Minori2Casi e Minori2Controlli?* Le informazioni relative alla tipologia dell'uso del suolo saranno recuperate dalla "*Mappa di uso del suolo 2003*" generata tramite ortofoto con risoluzione al suolo di 50 cm e resa disponibile per i territori comunali di Modena e Reggio Emilia dalla Regione Emilia-Romagna. In tal modo, sarà infatti possibile stimare all'interno di due aree circolari a distanza, aventi raggio di 100 e 1000 metri attorno ai dati spaziali considerati, la percentuale di terreno dedicata alle differenti tipologie di coltivazioni in essa presenti, con particolare riferimento a vitigni, frutteti, seminativi estensivi e colture orticole. L'individuazione del diverso utilizzo del suolo sarà fondamente al fine di stimare possibili esposizioni passive a pesticidi teratogeni utilizzati in aree agricole.
- *Dispersione delle emissioni autoveicolari di benzene e altri inquinanti emessi da traffico autoveicolare sull+intero territorio delle due province*: Al fine di determinare le concentrazioni di benzene e altri inquinanti da traffico autoveicolare sarà effettuata una modellizzazione dei flussi di traffico. Detta modellizzazione varrà

realizzata impiegando un software, CALINE-4[1], applicato al database dei flussi di traffico in ciascuna delle vie di maggiore rilevanza del territorio preso in esame reso disponibile dalle amministrazioni comunali e provinciali di Modena e di Reggio Emilia. I flussi di traffico in questione contengono tra l'altro il numero orario di veicoli che attraversano le zone considerate (incluse le vie di minori dimensioni relativamente alle aree maggiormente urbanizzate), nonché la tipologia di tali veicoli (veicoli leggeri e pesanti e la tipologia di carburante utilizzato). Verranno, inoltre, considerate le collocazioni dei distributori di benzina, i quali costituiscono possibili emettitori di benzene.

- ***Esposizione ai campi elettromagnetici***: Al fine di stimare l'esposizione a campi elettromagnetici saranno identificate le linee elettriche ad alta tensione (≥ 132 kilovolt) nei territori comunali di Modena e Reggio Emilia. Verrà quindi calcolata l'induzione del campo magnetico in prossimità di queste linee utilizzando il modello CAMPI[2] ed EFC400. Grazie a detti modelli sarà possibile definire la distanza alla quale, ad un'altezza di 8 m, si sono verificati i punti di taglio dell'intensità dei campi magnetici di 0,1, 0,2 e 0,4 microTesla (μT).

C3Raccolta dati di interesse epidemiologico

Ai fini della realizzazione dello Studio, saranno raccolti anche i dati relativi ai genitori dei Minori-Casi e dei Minori-Controlli. Nello specifico, verrà ricostruito un indicatore di status socioeconomico dei genitori dei Minori-Casi al momento della diagnosi (titolo di Studio, professione e reddito), mediante la consultazione della banca dati dell'anagrafe del Ministero delle Finanze, nell'ambito dell'autorizzazione rilasciata ad Unimore da detto Ministero nel dicembre 2010.

Inoltre, per ottenere risultati più precisi e con una maggiore validità scientifica, le AUSL di Modena e di Reggio Emilia forniranno ad Unimore, in forma pseudonimizzata, i seguenti dati relativi alle madri dei Minori-Casi e dei Minori-Controlli:

- Età, etnia, scolarità, occupazione, abitudine tabagica;
- Caratteristiche della gravidanza (es. durata, decorso; presentazione del feto, modalità di travaglio, modalità del parto, parti plurimi);
- Peso alla nascita del neonato, età gestazionale, sequenza di nascita (es. primogenito, secondogenito), presenza di malformazioni congenite.

Queste informazioni saranno direttamente estrapolate, da parte delle suddette AUSL, dai flussi informativi sanitari, quali CeDAP, cartelle cliniche e altri strumenti informatizzati nonché

[1] CAlifornia LINE Source Dispersion Model, version 4 è un programma realizzato dal Dipartimento di Trasporti dello Stato della California per la determinazione del monossido di carbonio, particolato, ossidi di azoto e altri inquinanti atmosferici emessi da veicoli motorizzati. È basato su un modello gaussiano che si basa a sua volta sulla numerosità dei veicoli (suddivisi in leggeri e pesanti) e sui loro livelli emissivi, nonché su dati meteorologici

[2] CAMPI è un pacchetto di simulazione software freeware sviluppato da Andreuccetti presso l'Istituto di Fisica Applicata del Consiglio Nazionale delle Ricerche di Firenze, per prevedere l'intensità della densità del flusso magnetico generata dalle linee elettriche. Il programma si basa su un modello 2D, in cui la linea di alimentazione è rappresentata con una serie di conduttori diritti, orizzontali, infiniti e paralleli.

tramite il Registro malformazioni congenite in Emilia Romagna (di seguito "IMER") e saranno condivisi in forma pseudonimizzata con l'Ateneo mediante secure large email protetta da password.

D3Modalità di trattamento e Analisi dei dati

Tutti i dati raccolti per l'esecuzione dello Studio verranno conservati in un database ospitato presso il Dipartimento di Scienze Biomediche Metaboliche e Neuroscienze (di seguito "Dipartimento BMN") e saranno suddivisi su più file criptati ed utilizzati su supporti magnetici assegnando ad ogni soggetto un codice personale (di seguito "database di Studio").
Solamente i ricercatori del gruppo di ricerca del Dipartimento BMN avranno acceso al database di Studio pseudonimizzato mediante autenticazione con username e password. Al contrario, i ricercatori del Dipartimento di Ingegneria "Enzo Ferrari" non avranno accesso completo ai dati raccolti per l'esecuzione dello Studio, ma a questi saranno unicamente forniti dati spaziali essenziali per la creazione del database GIS.
Una volta acquisiti tutti i dati, il Dipartimento BMN, utilizzando tecniche bivariate e multivariate, effettuerà un'analisi dei dati sia nell'intero campione che in singoli sottogruppi, mediante l'analisi stratificata e mediante modelli di regressione logistica condizionata. Infine, sarà modellata l'associazione tra l'esposizione agli inquinanti e il rischio dei tumori infantili presi in esame, utilizzando "spline cubiche limitate" calcolate con le routine 'mkspline' e 'xblc' del pacchetto statistico Stata-18 (Stata Corp., College Station, TX, 2023).
Una volta concluso lo Studio, i dati raccolti saranno cancellati entro sei mesi.

E3Pubblicazione dei risultati

I risultati delle attività di analisi e dell'intero Studio saranno oggetto di pubblicazioni scientifiche o di interventi in seminari, convegni o eventi di divulgazione scientifica. Tali risultati saranno resi disponibili nel solo ambito scientifico sotto forma di elaborazioni cumulative, precludendo in modo tassativo qualsivoglia riconoscimento o individuazione personale diretta od indiretta.

2.2 RESPONSABILITÀ CONNESSE AL TRATTAMENTO

Nel contesto dei trattamenti realizzati, sono identificabili le seguenti figure del trattamento

- **Titolare del trattamento:** Promotore dello Studio. Università degli Studi di Modena e Reggio Emilia e per essa il Dipartimento di Scienze Biomediche, Metaboliche e Neuroscienze e Centro di Ricerca LARMA del Dipartimenti di Ingegneria "Enzo Ferrari" dell'Università di Modena e Reggio Emilia ("Unimore" o "Promotore")
- **Titolari del trattamento:** Azienda Unità Sanitaria Locale di Modena – Servizio di Epidemiologia e Comunicazione del Rischio (di seguito "AUSL MO"); Azienda Ospedaliero Universitaria di Modena – Sezione della struttura complessa di Pediatria ad Indirizzo Oncoematologico del Dipartimento Materno-Infantile del Policlinico di

Modena (“AOU di Modena”); Azienda Unità Sanitaria Locale di Reggio Emilia – S.C. di Epidemiologia e Comunicazione del Rischio (di seguito “AUSL RE”).
congiuntamente (“Centri Partecipanti”)

- **Autorizzati al trattamento:** Team di progetto. Il Promotore, i Centri Partecipanti hanno designato al trattamento, ai sensi dell’art. 29 del GDPR, i propri Team di progetto.

2.3 STANDARD APPLICABILI AL TRATTAMENTO

Le attività dello Studio e il relativo trattamento di dati personali sono realizzati nel rispetto di:

- Good Clinical Practice [ICH Harmonized Tripartite Guidelines for Good Clinical Practice 1996 Directive
  91/507/EEC; D.M. 15.7.1997; DL 211 24/06/2003] e successive integrazioni;
- Dichiarazione di Helsinki;
- normative nazionali in materia di conduzione delle sperimentazioni cliniche;
- normative nazionali ed europee in materia di protezione dei dati personali;
- regolamenti e procedure adottate dalle singole parti in materia di protezione dei dati personali.

2.4 DATI PERSONALI TRATTATI

7393 Categorie di dati personali

Per la realizzazione dello Studio verranno trattate le seguenti tipologie di dati:

Minori2Casi

☒ dati di natura comune. In particolare: età, indirizzo di residenza, sesso

☒ dati relativi alla salute. In particolare: diagnosi di tumore, presenza di malformazioni congenite, peso alla nascita, sequenza di nascita (es. primogenito, secondogenito).

Minori2Controlli

☒ dati di natura comune. In particolare: età, indirizzo di residenza, sesso

☒ dati relativi alla salute. In particolare: assenza di diagnosi di tumore, presenza di malformazioni congenite, peso alla nascita, sequenza di nascita (es. primogenito, secondogenito).

Genitori dei Minori2Casi e Minori2Controlli

Padre

☒ dati di natura comune. In particolare: titolo di Studio, professione, reddito, età

Madre

☒ dati di natura comune. In particolare: titolo di Studio, professione, reddito, età

☒ dati rientranti in categorie di cui all'articolo 9 del GDPR. In particolare: dati relativi all'origine etnica e alla salute, quali: etnia, abitudine tabagica, caratteristiche della gravidanza.

7393 Modalità di raccolta

I dati personali saranno raccolti mediante la consultazione di archivi pubblici nonché direttamente dai Centri Partecipanti secondo le seguenti modalità:

☒ condivisione dei dati contenuti in cartelle cliniche/documentazione sanitaria da parte dei Centri Partecipanti

☒ archivi di dati clinici (Registri di Patologia, quali AEIOP, AIRTUM, IMER)

2.5 INTERESSATI

Lo Studio prevede il trattamento di dati personali di diverse categorie di interessati. In particolare verranno trattati i dati di Minori-Casi e Minori-controlli nonché alcuni dati dei rispettivi genitori (di seguito congiuntamente "*Soggetti Interessati*").

2.6 FINALITÀ DEL TRATTAMENTO

Il trattamento di dati personali è realizzato allo specifico scopo di realizzare lo Studio che si pone gli obiettivi *supra* definiti (Par 2.1.2). Si sottolinea, in tale contesto, che l'attività di ricerca è concretizzazione dei poteri e dei compiti istituzionali di cui è investita Unimore.

2.7 MEZZI DI TRATTAMENTO – RISORSE DI SUPPORTO AL TRATTAMENTO

I dati saranno trattati su supporto

☒ digitale

☐ cartaceo

Per il trattamento dei dati vengono impiegate le seguenti risorse:

- Componente Hardware: pc utilizzati da ogni singolo membro del Team di Progetto. Sul punto si precisa che l'intero trattamento avverrà in locale presso i server del

Dipartimento di BMN e che il supporto Hardware utilizzato non sarà provvisto di alcuna connessione internet;

- Componente Software: CALINE-4, CAMPI ed EFC400.
- Risorse Umane: dipendenti e collaboratori autorizzati dai Partner di Studio. Ogni Team di Progetto è autorizzato a trattare dati personali in virtù delle specifiche attività affidate.

Inoltre, è opportuno sottolineare che tutti i dati raccolti tramite consultazione degli archivi digitali e condivisi dai Centri Partecipanti saranno condivisi al Promotore solamente in forma pseudonimizzata. Pertanto, sui sistemi informatici del Promotore non transitano né sono conservati dati personali in chiaro dei Soggetti Interessati. È dunque necessario considerare che per tutti i trattamenti realizzati presso i Centri Partecipanti rilevano i mezzi e le relative misure di sicurezza dagli stessi adottate.

2.8 DESTINATARI DEI DATI PERSONALI

a) Esterni:
   - Autorità legittimate a verificare le attività di ricerca;
   - Comitato Etico competente ove lo richieda.

b) Interni:
   - Membri del Team di progetto.

2.9 DURATA DEL TRATTAMENTO E PERIODO DI CONSERVAZIONE

Si prevede di completare lo Studio entro Dicembre 2027. Trascorsi 6 mesi dalla conclusione dello Studio tutti i dati personali raccolti verranno eliminati.

L'output finale delle attività di ricerca sarà completamente anonimizzato, dunque depurato anche dai codici identificativi assegnati ai Soggetti Interessati, e verrà conservato senza limiti temporali.

2.10 TRASFERIMENTO DI DATI PERSONALI

I dati personali non saranno in alcun modo oggetto di trasferimento verso paesi al di fuori dello Spazio Economico Europeo o verso organizzazioni internazionali. I dati saranno conservati unicamente in locale presso i server del Dipartimento BMN.

3. PRINCIPI FONDAMENTALI

3.1 LIMITAZIONE DELLE FINALITÀ

I dati raccolti saranno trattati esclusivamente al fine di realizzare gli obiettivi dello Studio indicati al paragrafo 2.1.2. Sono esclusi trattamenti che si pongano fuori dal perimetro definito dal Protocollo di Studio.

3.2 LICEITÀ DEL TRATTAMENTO – BASE GIURIDICA

Il trattamento dei dati realizzato trova fondamento in:

a. **Consenso dell'interessato** reso ai sensi dell'**art. 6, par. 1, lett. a** e dell'**art. 9, par. 2, lett. a** del **GDPR**.
   Tale base giuridica si pone a fondamento dei trattamenti realizzati nei casi in cui il Centro partecipante riesca ad avere un contatto con la paziente arruolata. In tal caso, i ricercatori dei Centri Partecipanti sottoporranno alla paziente il consenso informato alla partecipazione alla ricerca e l'informativa privacy con la raccolta del consenso al trattamento dei dati personali.

b. **Ricerca medica, biomedica ed epidemiologica** senza il consenso dell'interessato ai sensi dell'**art. 110, c.1** del **Codice della Privacy**.
   Tale base giuridica legittima i trattamenti realizzati nei casi in cui il Centro partecipante non sia in grado di instaurare un contatto con i pazienti e i relativi genitori nonché i casi-controllo, dunque non sia possibile sottoporre il consenso informato e l'informativa privacy perché

   ☐ sussistono motivi etici riconducibili alla circostanza che l'interessato ignora la propria condizione;

   ☒ sebbene sia stato svolto ogni ragionevole sforzo organizzativo, non è possibile contattare gli interessati in ragione del numero molto alto di interessati che è stato stimato;

   ☒ sebbene sia stato svolto ogni ragionevole sforzo organizzativo, non è possibile contattare gli interessati in ragione del fatto che gli interessati sono deceduti o non contattabili.

3.3 MINIMIZZAZIONE DEI DATI

Nel perimetro dello Studio sono trattati i soli dati strettamente necessari e pertinenti al perseguimento delle finalità della ricerca stessa. Infatti, ogni ulteriore dato relativo ai Soggetti Interessati rimane esclusivamente presso i Centri partecipanti ed è trattato dagli stessi per proprie autonome finalità (es. finalità di cura).

3.4 CORRETTEZZA E AGGIORNAMENTO DEI DATI

I Centri partecipanti si impegno a trasmettere al Promotore in forma pseudonimizzata i dati appropriati e completi relativi ai Soggetti Interessati.

3.5 MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

a) Informativa e raccolta del consenso

   Tale misura è di certo garantita in tutti i casi in cui sia possibile, per i Centri Partecipanti, instaurare un contatto con la paziente.

   Non sussiste, invece, nei casi in cui sebbene sia stato svolto ogni ragionevole sforzo organizzativo, non è possibile contattare gli interessati in ragione del numero molto alto di interessati che è stato stimato oppure se deceduti.

b) Procedure per garantire esercizio dei diritti degli interessati (ai sensi degli artt. 7, 15 – 22 del GDPR).

4. MISURE DI SICUREZZA ADOTTATE E APPLICABILI AL TRATTAMENTO

È opportuno premettere che in tale sezione sono riportate le misure tecniche ed organizzative garantite da Unimore.

In un'ottica di Studio tali misure andranno certamente integrate con quelle dichiarate dai singoli Centri Partecipanti, in ordine ai dati da questi trasmessi. Infatti, si ricorda che i dati personali relativi dei Soggetti Interessati sono trattati in chiaro esclusivamente presso ogni singolo Centro Partecipante e vengono trasmessi al Promotore in forma pseudonimizzata.

È dunque necessario considerare che per tutti i trattamenti realizzati presso i Centri partecipanti rilevano i mezzi e le relative misure di sicurezza dagli stessi adottate.

MISURA	**Esistenti**	**Note**
Organigramma interno	X	Predisposto con regolamento interno.
Nomine responsabili esterni	X	Unimore è dotata di template per la nomina a responsabile del trattamento e, talvolta, valuta eventuali modelli proposti dalle controparti.
Nomina DPO	X	Contratto Rep. nr. 19/2022 del 26 luglio 2022.

Informativa	X	Nel caso di specie, per tutti i casi non classificabili come "retrospettivi", viene predisposta dai Centri partecipanti un'informativa privacy con la raccolta del relativo consenso al trattamento dei dati personali. Per i casi di Studio "retrospettivi" non è possibile fornire l'informativa all'interessato.
Istruzioni persone autorizzate trattamento	X	Il personale coinvolto riceve adeguate istruzioni in sede di incarico al trattamento e mediante le policy adottate e circolarizzate dal titolare.
Formazione	X	Il personale coinvolto è sensibilizzato e formato in materia di data protection.
Registri	X	Il titolare ha predisposto i registri dei trattamenti realizzati ai sensi dell'art. 30 GDPR e delle Linee guida CODAU.
Procedure	X	Il Titolare ha adottato le necessarie procedure per garantire un'adeguata compliance GDPR.
Politiche di tutela della privacy	X	L'attività del titolare è orientata ad una strutturata compliance GDPR: > designato DPO esterno con il quale intercorre uno stretto confronto; > adottate misure tecniche ed organizzative; > implementate misure tecniche di sicurezza ICT richieste da AGID; > adottati regolamenti e procedure interni in materia di *data protection;*
Distruzione/smaltimento sicuro cartaceo		Non applicabile nel caso di specie
Inventario degli asset	X	• <u>Inventario dei dispositivi autorizzati e non autorizzati</u>: Sono gestiti attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia permesso solo ai dispositivi autorizzati e che i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso. Sono adottate misure per ridurre il rischio che le caratteristiche delle apparecchiature (server, postazioni, portatili, periferiche, dispositivi, supporti removibili ecc.) siano utilizzate per danneggiare dati personali. <u>Inventario dei software autorizzati e non autorizzati</u>: Sono gestiti attivamente tutti i software sulla rete in

		modo che sia installato ed eseguito solo il software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione. Sono adottate misure per ridurre la possibilità che le caratteristiche del software (sistemi operativi, applicazioni, software ecc.) vengano sfruttate per danneggiare i dati personali trattati. Si tratta di: aggiornamenti, protezione fisica e accessi, lavoro su spazio di rete protetto, controlli di integrità, logging ecc.
Misure anti – intrusive (cartelli di divieto di accesso ai locali, strumenti per la rilevazione degli accessi, guardiania, portineria, serrature armadi, schedari, ecc.)	X	• Sono adottate misure per il controllo degli accessi fisici agli uffici universitari, nonché ai "locali strategici" (es. locali server, locali pc, archivi). • Sono implementati sistemi di protezione adeguati volti a garantire la sicurezza della rete (es. firewall e antivirus).
Politiche di sicurezza informatica	X	• Istituita, implementata e gestita attivamente (tracciata, segnalata, corretta) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni. • Acquisite, valutate e intraprese continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.
Controllo accessi (log)	X	• Sono adottati Regolamenti e Procedure per la gestione degli incarichi al trattamento del personale, nonché delle relative credenziali di accesso ai sistemi/file autorizzati. • Sono adottate regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.

		L’accesso al database di Studio è consentito unicamente a tre dei membri del Team di Progetto tramite l’inserimento di credenziali di autenticazione (username e password).
Antivirus / firewall	X	• Sono implementati sistemi di protezione adeguati volti a garantire la sicurezza della rete (es. firewall e antivirus). • Sono adottate misure volte a proteggere l'accesso alla rete, le postazioni ed i server contro malware che potrebbero compromettere la sicurezza dei dati personali trattati.
Back – up dei dati	X	• L'università adotta politiche di backup tali da assicurare la disponibilità e l'integrità dei dati personali. • Come richiesto da AGID, sono adottate procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.
Crittografia	X	I dati in forma pseudonimizzata riferibili ai Soggetti Interessati conservati presso il Dipartimento di BMN sono protetti mediante tecniche di crittografia.
Anonimizzazione	X	Misura applicata decorsi 6 mesi dalla conclusione dello Studio prevista per Dicembre 2027. Il Promotore non entra mai in possesso del file con le chiavi di decodifica, che rimane presso i Centri Partecipanti. Seppur nell’ottica soggettiva del Promotore il data set è di fatto anonimo, lo stesso non può dirsi oggettivamente tale sino a quando i Centri Partecipanti, in qualità di Autonomi titolari del trattamento, non eliminino definitivamente e irreversibilmente il file con le chiavi di decodifica. I centri Partecipanti provvedono ad eliminare tale file secondo le proprie procedure interne.

Pseudonimizzazione	X	Dopo la raccolta dei dati presso i Centri Partecipanti, i ricercatori responsabili presso gli stessi assegnano ad ogni paziente un codice identificativo. Ogni dato trasmesso al Promotore sarà identificato esclusivamente con quel codice, senza alcun riferimento all'identità della paziente. Dunque, i dati che pervengono al Promotore non possono più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive. Queste ultime sono conservate separatamente ed esclusivamente presso il Centro partecipante di origine, in qualità di autonomo titolare del trattamento.
Sicurezza dei documenti cartacei		Non applicabile nel caso di specie
Gestione postazioni	X	In generale, le postazioni sono accessibili dai soli utenti universitari. È adottato un regolamento sul corretto utilizzo delle postazioni informatiche.
Autenticazione	X	Sono creati, affidati e gestisti diversi profili utente in virtù delle mansioni svolte. In particolare, ogni utente dei sistemi del titolare è dotato di un User e di una password creata nel rispetto dei regolamenti interni.
Policy di gestione data breach	X	• Sono adottate adeguate procedure di gestione dei data breach; In via preventiva sono acquisite, valutate e intraprese continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.

Minimizzazione	X	Il processo di trattamento dei dati effettuato nello Studio è tarato sui soli dati considerati necessari al raggiungimento degli obiettivi della ricerca. Ciò in considerazione: • della selezione "*by design*" a monte dei soli dati effettivamente pertinenti e adeguati al raggiungimento delle finalità dello Studio. • della limitazione dell'accesso ai dati; • della realizzazione delle attività di ricerca su un data set pseudonimizzato.

5. VALUTAZIONE DEL RISCHIO

La valutazione dei rischi si focalizza in particolar modo sulle attività di trattamento realizzate dal Promotore. Pertanto, in ottica di Studio, la presente valutazione può essere integrata con le valutazioni effettuate, in qualità di autonomi titolari del trattamento, dai singoli Centri Partecipanti.

5.1 MATRICE DI VALUTAZIONE DEL RISCHIO

Il calcolo del rischio si focalizza in particolar modo sulle attività di trattamento dei dati acquisiti dalle Road Side Unit, secondo la seguente modalità di valutazione: **R = IMPATTO * PROBABILITÀ.**

Per valutare l'impatto è necessario tenere in considerazione gravità che rappresenta l'entità del rischio e dipende principalmente dalla natura pregiudizievole del potenziale impatto.

Per la determinazione dei *livelli di impatto* sugli interessati, si prende in considerazione quanto segue:

IMPATTO PRIVACY	DESCRIZIONE
Molto basso	Gli interessati non subiranno alcun impatto
Trascurabile (Basso)	Gli interessati possono incontrare alcuni piccoli inconvenienti, che supereranno senza difficoltà (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).

Limitato (Medio)	Gli interessati potrebbero sperimentare inconvenienti significativi, superabili nonostante alcune difficoltà (costi aggiuntivi, impossibilità di accesso a servizi, timore o mancanza di comprensione, stress, disagi o disturbi fisici minori, ecc.).
Importante (Alto)	Gli interessati potrebbero subire conseguenze significative, che dovrebbero essere in grado di superare anche se con difficoltà reali e significative (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita del posto di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
Massimo (Molto Alto)	Gli interessati potrebbero subire conseguenze significative, anche irrimediabili, che potrebbero non superare (incapacità di lavorare, gravissima perdita economica, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Per la determinazione dei *livelli di probabilità* che si concretizzino si prende in considerazione quanto segue:

PROBABILITÀ	**DESCRIZIONE**
Molto bassa	Appare impossibile che la fonte di rischio concretizzi una minaccia considerando le caratteristiche del trattamento (ad esempio: accesso non autorizzato ad un file anonimizzato)
Bassa/Trascurabile	Appare di fatto quasi impossibile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti, tuttavia, potrebbe verificarsi in caso di coincidenze (ad esempio: furto di supporti cartacei conservati in un locale dell'organizzazione il cui accesso è controllato tramite badge e codice d'ingresso).
Media/Limitata	Appare difficile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti (ad esempio: furto di supporti cartacei conservati in un locale dell'organizzazione il cui accesso è controllato tramite badge).
Alta/Importante	Appare possibile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti (ad esempio: furto di supporti cartacei conservati in uffici dell'organizzazione ove l'accesso è controllato da un incaricato all'ingresso).

Molto Alta/Massima	Appare estremamente facile per le fonti di rischio considerate concretizzare una minaccia basandosi sulle caratteristiche dei supporti (ad esempio: furto di supporti cartacei conservati in un locale dell'organizzazione pubblicamente accessibile).

		IMPATTO				
		MOLTO BASSO	**BASSO**	**MEDIO**	**ALTO**	**MOLTO ALTO**
PROBABILITÀ	**MOLTO BASSA**	**1**	**2**	**3**	**4**	**5**
	BASSA	**2**	**4**	**6**	**8**	**10**
	MEDIA	**3**	**6**	**9**	**12**	**15**
	ALTA	**4**	**8**	**12**	**16**	**20**
	MOLTO ALTA	**5**	**10**	**15**	**20**	**25**

PROBABILITA÷-P.	*IMPATTO -I.*	*RISCHIO -R] P/I.*
Probabilità molto bassa: 1	Impatto molto basso: 1	Rischio basso: R< 7
Probabilità bassa: 2	Impatto basso: 2	Rischio medio: 7<R<11
Probabilità media: 3	Impatto medio: 3	Rischio alto: R>11
Probabilità alta: 4	Impatto alto: 4	Rischio Elevato: 12<R<16
Probabilità molto alta: 5	Impatto molto alto: 5	

5.2 RISCHIO DI PERDITA DI RISERVATEZZA – ACCESSO ILLEGITTIMO AI DATI

*Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare_*

L'accesso illegittimo ai dati trattati dal Promotore sarebbe suscettibile di determinare un impatto sui Soggetti Interessati unicamente nel caso in cui tale accesso si verificasse da parte del medesimo agente in concomitanza ad un accesso illegittimo alle chiavi di decodifica. Si ricorda, infatti, che il Promotore tratta unicamente dati pseudonimizzati e che le chiavi di

decodifica sono conservate presso ogni Centro Partecipante, dunque, in sistemi del tutto separati rispetto a quello del Promotore.
Nel caso in cui tale eventualità si verifichi, gli impatti potrebbero essere: perdita di riservatezza dei dati personali coperti da segreto professionale; perdita del controllo dei propri dati; decifratura non autorizzata dei dati pseudonimizzati e possibile diffusione dei dati non autorizzata.

*Quali sono le principali minacce che potrebbero concretizzare il rischio_*

Utilizzo inappropriato delle password di accesso ai computer dell'Ateneo e al relativo database di raccolta dati impiegato per lo studio; sottrazione delle password di accesso da parte di un terzo; operatori abilitati che sfruttano i privilegi di accesso per accedere illegittimamente alle informazioni; attacco informatico; errata profilazione degli utenti; errata o incauta trasmissione dei dati ad opera dei Centri Partecipanti.

*Quali sono le fonti di rischio_*

Soggetti non autorizzati o terzi malintenzionati "attaccanti" (hacker) che prendono di mira il database di raccolta dati; Soggetti non autorizzati o terzi malintenzionati che tentino di accedere ai sistemi con privilegi di accesso; errore umano; malfunzionamento e/o incidente informatico.

*Quali misure fra quelle individuate contribuiscono a mitigare il rischio_*

Istruzioni persone autorizzate trattamento; Formazione; Procedure; Politiche di tutela della privacy; Misure anti – intrusive; Politiche di sicurezza informatica; Controllo accessi (log); Antivirus/firewall; Autenticazione; Crittografia; Pseudonimizzazione.

*Come stimereste la gravità del rischio1 specialmente alla luce degli impatti potenziali e delle misure pianificate_*

La gravità del rischio è **BASSA/TRASCURABILE**.

Nella stima della gravità è necessario considerare l'impatto derivante dall'eventualità, remota ma ipotizzabile, di un contestuale accesso non autorizzato al database pseudonimizzato e al file con le chiavi di decodifica. In tale caso, infatti, l'impatto sui Soggetti Interessati potrebbe essere rilevante, considerando la natura dei dati trattati nello Studio. Tuttavia, le valutazioni in merito alla gravità del rischio devono tenere in considerazione anche le misure pianificate. Nel trattamento di specie, le misure adottate sono tali da limitare ai minimi termini la concretizzazione di un possibile impatto sui Soggetti Interessati.

*Come stimereste la probabilità del rischio1 specialmente con riguardo alle minacce1alle fonti di rischio e alle misure pianificate_*

La probabilità di concretizzazione del rischio è **BASSA/TRASCURABILE**.

Le attività di trattamento del Promotore si svolgono su dati preventivamente pseudonimizzati. Pertanto, tale aspetto limita già di per la probabilità di accesso illegittimo a dati personali. Infatti, un soggetto terzo che acceda solo al file pseudonimizzato, senza le chiavi di decodifica, sarebbe in grado di ottenere solo un elenco di informazioni non riconducibili a persone fisiche identificate o identificabili.
Anche nel caso in cui si verificasse un accesso simultaneo al dataset pseudonimizzato e ai file con le chiavi di decodifica, conservati presso i singoli Centri Partecipanti, la probabilità che la minaccia si concretizzi, considerando le caratteristiche del trattamento, è da ritenersi bassa. Ciò in virtù del fatto che:

- a tutela degli ambienti e dei sistemi del Promotore, in cui è conservato il database di Studio, sono adottate tutte le misure di sicurezza ICT considerate minime e necessarie dall'AGID. Tali misure sono periodicamente aggiornate in linea con il progresso tecnologico;
- Al database di Studio possono accedere solo tre dei membri del Team di progetto afferenti al Dipartimento di BMN con proprie credenziali di autenticazione;
- Il file con le chiavi di decodifica è conservato presso i Centri Partecipanti con le relative misure di sicurezza e il relativo accesso riservato è regolamentato dalle procedure interne previste da ogni singolo centro.

Classificazione	***Intervallo del rischio***
Assenza Rischio	Valore finale tra 0 e 1 compresi
Rischio Basso	Valore finale tra 2 e 6 compresi
Rischio Medio	Valore finale tra 7 e 11 compresi
Rischio Elevato	Valore finale tra 12 e 16 compresi

Alla luce delle valutazioni operate in precedenza nonché della relativa assegnazione sulla base della matrice di valutazione, il rischio di impatto del trattamento descritto sui diritti e le libertà degli interessati è **BASSO**.

5.3 RISCHIO DI PERDITA DI INTEGRITÀ – MODIFICHE INDESIDERATE DEI DATI

*Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare_*

L'impatto principale, in caso di modifiche indesiderate dei dati, si riverserebbe unicamente sui risultati dello Studio, determinando un'alterazione della qualità e dell'affidabilità dell'attività di ricerca e degli esiti della stessa.
Ciò in quanto, in caso di concretizzazione del rischio non vi sarebbe alcun impatto sugli interessati, i quali non subirebbero conseguenze pregiudizievoli da una modifica indesiderata dei dati trattati dal Promotore.
Al più, potrebbero essere ipotizzati impatti sull'interessata solo nel caso in cui la modifica non autorizzata sia preceduta da un accesso non autorizzato. Per tale evenienza (di difficile concretizzazione), si ritiene opportuno richiamare le valutazioni operate nel punto precedente: *: 3 Rischio di perdita di riservatezza " accesso illegittimo ai dati*.

*Quali sono le principali minacce che potrebbero concretizzare il rischio_*

Utilizzo inappropriato delle password di accesso ai computer del Promotore e al relativo database di raccolta dati; sottrazione delle password di accesso da parte di un terzo; operatori abilitati che sfruttano i privilegi di accesso per accedere illegittimamente alle informazioni; attacco informatico; errata profilazione degli utenti; intervento non accurato sul database da parte degli autorizzati.

*Quali sono le fonti di rischio_*

Soggetti non autorizzati o terzi malintenzionati "attaccanti" (hacker) che prendono di mira il database di raccolta dati; Soggetti non autorizzati o terzi malintenzionati che tentino di accedere ai sistemi con privilegi di accesso; errore umano; malfunzionamento e/o incidente informatico.

*Quali misure1fra quelle individuate1contribuiscono a mitigare il rischio_*

In ordine alle misure individuate, la tecniche più significativa volta ed evitare la concretizzazione di detto rischio è la limitazione dell'accesso al database contenente i dati dello Studio esclusivamente al PI e a due dei propri collaboratori, mediante dispositivi e spazi di conservazione connessi all'utenza universitaria. Oltre a dette misure, si tengono in considerazione le ulteriori misure previste, quali: Istruzioni persone autorizzate trattamento (con particolare riferimento alla corretta gestione e utilizzo delle credenziali di accesso ai dispositivi e ai file utilizzati nella ricerca); Formazione; Procedure; Politiche di tutela della

privacy; Autenticazione; Misure anti – intrusive; Politiche di sicurezza informatica; Crittografia; Controllo accessi (log); antivirus/firewall; Back – up dei dati.

*Come stimereste la gravità del rischio1 specialmente alla luce degli impatti potenziali e delle misure pianificate_*

La gravità del rischio è **MOLTO BASSA**.

Infatti, nel caso di modifica indesiderata dei dati non si verificherebbe alcun impatto in capo ai Soggetti Interessati. Infatti, ogni inconveniente ricadrebbe esclusivamente sulla qualità e sull'affidabilità dell'attività dello Studio nonché sugli esiti dello stesso. L'impatto sui Soggetti Interessati è di fatto limitato al solo caso di accesso non autorizzato seguito da modifica indesiderata. Tale eventualità deve necessariamente essere descritta in termini meramente ipotetici e la relativa valutazione è operata nel precedente punto ***:3 Rischio di perdita di riservatezza " accesso illegittimo ai dati***.

*Come stimereste la probabilità del rischio1 specialmente con riguardo alle minacce1alle fonti di rischio e alle misure pianificate_*

La probabilità di concretizzazione del rischio è **MOLTO BASSA**. Con riferimento ad eventuali modifiche indesiderate:

- sono adottate misure di sicurezza ICT considerate minime e necessarie dall'AGID, aggiornate periodicamente in linea con il progresso tecnologico, poste a tutela dei sistemi universitari in cui sono conservati i file utilizzati per lo studio.
- sono adottate misure di sicurezza degli accessi ai dispostivi e ai profili universitari e i singoli file inseriti nel database di Studio sono protetti con apposite password di accesso;
- viene effettuato un backup periodico dei sistemi e del materiale conservato nei server messi a disposizione dall'università;

Per evitare, o in ogni caso limitare, possibili modifiche indesiderate ad opera dei membri del gruppo di ricerca o del personale del Promotore coinvolto nello Studio, sono adottate a livello universitario procedure, regolamenti e policy in materia di protezione e corretto trattamento dei dati. Tale materiale è integrato dagli iter e dalle procedure delineate ad hoc per la realizzazione dello Studio.

Classificazione	Intervallo del rischio
Assenza Rischio	Valore finale tra 0 e 1 compresi
Rischio Basso	Valore finale tra 2 e 6 compresi
Rischio Medio	Valore finale tra 7 e 11 compresi

Rischio Elevato	Valore finale tra 12 e 16 compresi

Alla luce delle valutazioni operate in precedenza nonché della relativa assegnazione sulla base della matrice di valutazione, il rischio di impatto del trattamento descritto sui diritti e le libertà degli interessati è **ASSENZA DI RISCHIO**.

5.4 RISCHIO DI PERDITA DI DISPONIBILITÀ – PERDITA DI DATI

*Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi_*

In caso di concretizzazione del rischio non vi sarebbe alcun impatto generale sui Soggetti Interessati. Infatti, l'eventuale perdita di dati trattati nel contesto dello Studio non determinerebbe alcuna perdita dei dati trattati dai Centri Partecipanti per le proprie autonome finalità di cura nonché degli archivi digitali impiegati.

Un eventuale impatto potrebbe essere ipotizzato solo nel caso in cui la perdita sia preceduta e determinata da un accesso non autorizzato. Per tale evenienza (di difficile concretizzazione), si ritiene opportuno richiamare le valutazioni operate al punto *:373"Rischio di perdita di riservatezza " accesso illegittimo ai dati*".

Nell'eventualità in cui si verifichi tale ipotesi, occorre innanzitutto evidenziare che tale rischio potrebbe concretizzarsi unicamente in forma informatica, essendo esclusa ogni attività di trattamento in forma cartacea. In ogni caso, tale ipotesi determinerebbe impatti solo in termini di alterazione dei risultati dello Studio o di impossibilità di proseguire lo Studio, ma non produrre effetti negativi sui Soggetti Interessati.

*Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio_*

Utilizzo inappropriato delle password di accesso ai computer del Promotore e al relativo database di raccolta dati che può portare ad una cancellazione erronea o volontaria dei dati; sottrazione delle password di accesso da parte di un terzo; operatori abilitati che sfruttano i privilegi di accesso per accedere illegittimamente alle informazioni; attacco informatico; errata profilazione degli utenti; intervento non accurato sul database da parte degli autorizzati; vulnerabilità dei sistemi a possibili incidenti o guasti tecnici o naturali.

*Quali sono le fonti di rischio_*

Soggetti non autorizzati o terzi malintenzionati "attaccanti" (hacker) che prendono di mira il database di raccolta dati; Soggetti non autorizzati o terzi malintenzionati che tentino di

accedere ai sistemi con privilegi di accesso; errore umano; malfunzionamento e/o incidente informatico; accadimenti naturali (es. incendio, inondazioni, sovraccarico elettrico, terremoti).

*Quali misure1fra quelle individuate1contribuiscono a mitigare il rischio_*

Back – up dei dati; Controllo accessi (log); Misure anti – intrusive; antivirus/firewall; Gestione postazioni; Crittografia; Politiche di tutela della privacy¸ Politiche di sicurezza informatica; Autenticazione; Istruzioni persone autorizzate trattamento (con particolare riferimento alla corretta gestione e utilizzo delle credenziali di accesso ai dispositivi e ai file utilizzati nella ricerca).

*Come stimereste la gravità del rischio1 specialmente alla luce degli impatti potenziali e delle misure pianificate_*

La gravità del rischio è **MOLTO BASSA**.

Una perdita di dati nel database oggetto dello Studio non avrebbe impatti sostanziali sui diritti dei Soggetti Interessati, in quanto gli impatti si produrrebbero unicamente sui risultati dello Studio.
Al contrario, il verificarsi di detto rischio sarebbe suscettibili di avere un impatto sui Soggetti Interessati unicamente laddove la perdita di dati avesse ad oggetto la fonte originaria presso i Centri Partecipanti. Tuttavia, detto rischio non è in alcun modo connesso al trattamento realizzato nello Studio.
L'impatto sui Soggetti Interessati è di fatto limitato al solo caso di accesso non autorizzato seguito da perdita di dati. Tale eventualità deve necessariamente essere descritta in termini meramente ipotetici e la relativa valutazione è operata nel punto ***:3*** *"Rischio di perdita di riservatezza " accesso illegittimo ai dati*".

*Come stimereste la probabilità del rischio1specialmente con riguardo alle minacce1alle fonti di rischio e alle misure pianificate_*

La probabilità di concretizzazione del rischio è **MOLTO BASSA**.

Le misure adottate limitano in modo importante la possibilità per le fonti di rischio di sfruttare possibili vulnerabilità degli strumenti utilizzati concretizzando il rischio di perdita dei dati. Per limitare o evitare perdite di dati:

- sono adottate misure di sicurezza ICT considerate minime e necessarie dall'AGID, aggiornate sistematicamente in linea con il progresso tecnologico, poste a tutela dei sistemi in cui è conservato il database di Studio;
- sono adottate misure di sicurezza degli accessi ai dispostivi e ai profili universitari e i singoli file inseriti nel database di Studio sono protetti con apposite password di accesso;

- viene effettuato un backup periodico dei sistemi e del materiale conservato nei server e negli spazi cloud messi a disposizione dall'università;

In ogni caso, l'eventuale perdita dei dati nel database di Studio non sarebbe mai definitiva in virtù delle procedure menzionate.

Classificazione	Intervallo del rischio
Assenza Rischio	Valore finale tra 0 e 1 compresi
Rischio Basso	Valore finale tra 2 e 6 compresi
Rischio Medio	Valore finale tra 7 e 11 compresi
Rischio Elevato	Valore finale tra 12 e 16 compresi

Alla luce delle valutazioni operate in precedenza nonché della relativa assegnazione sulla base della matrice di valutazione, il rischio di impatto del trattamento descritto sui diritti e le libertà degli interessati è **ASSENZA DI RISCHIO**.

5.5 VALUTAZIONE COMPLESSIVA

PROBABILITA÷-P.	*IMPATTO -I.*	*RISCHIO -R] P/I.*
Probabilità molto bassa: 1 Probabilità bassa: 2 Probabilità media: 3 Probabilità alta: 4 Probabilità molto alta: 5	Impatto molto basso: 1 Impatto basso: 2 Impatto medio: 3 Impatto alto: 4 Impatto molto alto: 5	Rischio basso: R< 7 Rischio medio: 7<R<11 Rischio alto: R>11

		IMPATTO				
		MOLTO BASSO	**BASSO**	**MEDIO**	**ALTO**	**MOLTO ALTO**
PROBABILITÀ	**MOLTO BASSA**	**1**	**2**	**3**	**4**	**5**
	BASSA	**2**	**4**	**6**	**8**	**10**
	MEDIA	**3**	**6**	**9**	**12**	**15**
	ALTA	**4**	**8**	**12**	**16**	**20**
	MOLTO ALTA	**5**	**10**	**15**	**20**	**25**

EVENTO – RISCHIO	**VALORE DEL RISCHIO (P*I)**	**LIVELLO DI RISCHIO**	**VALUTAZIONE COMPLESSIVA**
ACCESSO ILLEGITTIMO	2*2	4	6
MODIFICHE INDESIDERATE DEI DATI	1*1	1	
PERDITA DI DATI	1*1	1	

Classificazione	**Intervallo del rischio**
Assenza Rischio	Valore finale tra 0 e 1 compresi

Rischio Basso	Valore finale tra 2 e 6 compresi
Rischio Medio	Valore finale tra 7 e 11 compresi
Rischio Elevato	Valore finale tra 12 e 16 compresi

Alla luce delle valutazioni operate nell'intero punto 5 del presente documento nonché della relativa assegnazione sulla base della matrice di valutazione, il rischio di impatti del trattamento descritto sui diritti e le libertà degli interessati è **BASSO**.