

## STUDIO OSSERVAZIONALE RETROSPETTIVO

### STUDIO RIFRA

#### INFORMAZIONI SULLO STUDIO E SUL TRATTAMENTO DEI DATI PERSONALI

##### Intestazione

Promotore dello studio l'Istituto di Ricovero e Cura a Carattere Scientifico, Ospedale Galeazzi-Sant'Ambrogio con sede legale in Milano, via Cristina Belgioioso, n. 173, e-mail info.ogsa@grupposandonato.it, in persona del suo legale rappresentante pro tempore, in qualità di Titolare autonomo del trattamento dei dati personali, il "Titolare, intende fornire all'Interessato le seguenti informazioni sullo studio clinico osservazionale retrospettivo che vede il trattamento di Dati Personali precedentemente raccolti per l'erogazione di attività di tipo sanitario (c.d. attività di tutela della salute). Le seguenti informazioni devono intendersi integrative di quelle tipicamente rilasciate dal Centro di Sperimentazione, mediante *Informativa sul trattamento dei dati personali* in fase di accettazione della prestazione sanitaria, che può consultare cliccando qui <https://www.grupposandonato.it/strutture/ospedale-galeazzi-sant-ambrogio/informativa-privacy-paziente>

Il presente documento vuole quindi fornirle informazioni ulteriori e di maggior dettaglio rispetto a quelle già rese ai sensi degli artt. 13 e 14 del Regolamento (UE) 2016/679 ("GDPR") e della normativa europea e nazionale che lo integra e/o lo modifica ("Normativa Privacy Applicabile").

- Titolo: *Predizione del rischio di rifrattura in pazienti con frattura da fragilità: sviluppo e validazione di uno score prognostico – studio RIFRA*
- Promotore dello studio: *IRCCS Ospedale Galeazzi – Sant'Ambrogio*
- 
- Sperimentatore Principale: *Dott. Federico Pennestrì*

##### Quali persone parteciperanno a questo studio?

Saranno inclusi in questa raccolta dati pazienti maggiorenni ricoverati per un intervento di sostituzione totale o parziale del collo del femore in seguito ad una frattura non scomposta presso l'IRCCS Istituto Ortopedico Galeazzi nel periodo intercorrente tra il 2012 al 2016 (da gennaio a dicembre) e soggetti ad una rifrattura entro due anni dal primo trauma, di cui saranno verificate eventuali recidive incrociando i dati con il database della Regione Lombardia.

##### Di quale studio si tratta?

Si tratta di uno studio osservazionale (ovvero che non altera il normale iter clinico), retrospettivo (ovvero che raccoglie dati di prestazioni già avvenute), monocentrico (ovvero che si svolge solo presso questo centro).

Lo scopo dello studio è raccogliere dati per identificare un modello la cui futura applicazione sarà aiutare i medici e gli operatori sanitari a predire anticipatamente il rischio di rifrattura in pazienti fragili già soggetti a un primo episodio di frattura.



PROTOCOLLO RIFRA

**Quali Dati personali vengono trattati nello svolgimento di questo studio?**

Il Centro di sperimentazione tratterà dati personali comuni, raccolti in occasione e nell'ambito dell'erogazione della prestazione sanitaria, tra cui rientrano, a titolo esemplificativo e non esaustivo, nome, cognome, numero di telefono mobile, indirizzo e-mail e, in generale, i dati di contatto (i "Dati Comuni").

Saranno altresì trattati anche dati relativi allo stato di salute e alla vita sessuale, nonché i dati idonei a rivelare l'origine razziale ed etnica (i "Dati Particolari").

I Dati Comuni e i Dati Particolari di seguito, congiuntamente, i "Dati Personali".

**Quanto durerà lo studio?**

Lo studio durerà 14 mesi, il tempo necessario alla raccolta retrospettiva ed all'analisi dei dati.

**Per quale motivo verranno utilizzati i miei dati i Dati Personali?**

I suoi Dati Personali sono trattati per svolgere lo studio sopra descritto. Per il trattamento dei suoi Dati Personali le basi giuridiche sono l'art. 6.1.e) e l'art. 9.2.j) del GDPR ovvero l'esecuzione di un compito di interesse pubblico qual è la ricerca clinica sulla base di una norma di legge che il titolare individua nell' art. 110bis, comma 4.

Infatti tale norma consente agli IRCCS, qual è il Titolare, di svolgere attività di ricerca scientifica mediante il trattamento ulteriore di dati personali precedentemente raccolti per attività clinica.

**Per quanto tempo verranno conservati i miei Dati Personali?**

I suoi dati verranno conservati per 10 anni dopo la chiusura dello studio. L'Interessato può chiedere ed accedere a qualsiasi informazione ulteriore scrivendo direttamente a: *Dott. Federico Pennestri* (Sperimentatore Principale) al seguente indirizzo mail [federico.pennestri@grupposandonato.it](mailto:federico.pennestri@grupposandonato.it) e al Data Protection Officer scrivendo al Data Protection Officer (DPO) [rpd.ogsa@grupposandonato.it](mailto:rpd.ogsa@grupposandonato.it)

**In che modo verranno trattati i miei Dati Personali?**

Il trattamento dei Dati Personali avverrà – secondo i principi di correttezza, liceità e trasparenza – tramite supporti e/o strumenti informatici, manuali e/o telematici, con logiche strettamente correlate allo svolgimento dello Studio come sopra descritto e, comunque, garantendo la riservatezza e sicurezza dei dati stessi e il rispetto degli obblighi specifici sanciti dalla legge.

Il trattamento è svolto ad opera di soggetti appositamente autorizzati dal Titolare del trattamento a partecipare alle attività necessarie allo svolgimento dello Studio clinico e in ottemperanza a quanto previsto dall'art. 29 del GDPR e 2-quaterdecies del Codice Privacy. In ogni caso I Dati Personali raccolti saranno trattati da o sotto la responsabilità di professionisti soggetti al segreto professionale o da altri autorizzati soggetti all'obbligo di segretezza conformemente al diritto dell'Unione Europea o del diritto nazionale o alle norme stabilite dagli organismi nazionali competenti, ai sensi dell'art. 9, par. 3, del GDPR.

### **In che modo saranno protetti i miei Dati Personali?**

I Dati Personali verranno trattati secondo quanto previsto dall'art.89 GDPR cioè adottando adeguate garanzie per i diritti e libertà dell'Interessato attraverso la predisposizione di misure specifiche quali tecniche di cifratura o di pseudonimizzazione oppure altre soluzioni che, considerato il volume dei dati trattati, la natura, l'oggetto, il contesto e le finalità del trattamento, li rendono non direttamente riconducibili all'Interessato, permettendo di identificarlo solo in caso di necessità. In questi casi, i codici utilizzati non sono desumibili dai Dati Personali identificativi salvo che ciò risulti impossibile in ragione delle particolari caratteristiche del trattamento o richieda un impiego di mezzi manifestamente sproporzionato e sia motivato, altresì, per iscritto, nel progetto di ricerca. In particolare, il medico che La seguirà nello Studio La identificherà con un codice (es. ab0001) che non permette di risalire direttamente alla sua identità e tratterà i Suoi Dati Personali solo unitamente a tale codice identificativo. Esclusivamente il medico ed i soggetti autorizzati potranno collegare questo codice al Suo nominativo e ciò sarà fatto solo in caso di effettiva necessità, impedendo così quanto più possibile la Sua diretta identificabilità.

Inoltre il Titolare del trattamento potranno comunicare i Dati Personali a:

- i. eventuali fornitori di servizi strettamente correlati e funzionali alle attività necessarie per lo svolgimento della Sperimentazione (quali consulenti esterni, la società di gestione dell'archivio delle cartelle cliniche, società di ricerca a contratto, clinical study monitor, laboratori analisi, fornitori di servizi IT per la gestione dell'infrastruttura tecnologica, dei sistemi informativi e delle reti di telecomunicazione ecc.), debitamente nominati responsabili del trattamento ai sensi dell'art. 28 del GDPR;
- ii. organismi sanitari di controllo, comitati etici, organi della pubblica amministrazione, autorità di pubblica sicurezza, autorità giudiziaria e altri soggetti, enti o autorità che agiscono nella loro qualità di titolari autonomi di trattamento, a cui sia obbligatorio comunicare i Dati Personali in forza di disposizioni di legge o di ordini delle autorità.

I Suoi Dati Personali non saranno oggetto di diffusione (intendendosi per tale, il dare conoscenza di dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione).

L'elenco completo ed aggiornato dei destinatari dei dati potrà essere richiesto al Titolare del trattamento ovvero ai rispettivi DPO, a mezzo dei recapiti sopra indicati.

### **I miei Dati Personali saranno trasferiti fuori dallo Spazio Economico Europeo?**

I Suoi Dati Personali non saranno oggetto di trasferimento verso Paesi Terzi rispetto allo Spazio Economico Europeo od organizzazioni internazionali.

Maggiori informazioni sono disponibili presso il Titolare del trattamento oppure scrivendo ai rispettivi DPO a mezzo degli indirizzi sopra indicati.



*PROTOCOLLO RIFRA*

***Quali sono i miei diritti?***

Ai sensi degli articoli dal 15 al 22 del GDPR, ove applicabile, Lei, nei confronti del titolare, ha il diritto di:

- i. ottenere, da parte del Centro di ricerca, la conferma che sia o meno in corso un trattamento di dati personali che la riguardano e in tal caso, ottenere l'accesso ai suoi dati;
- ii. conoscere le finalità del trattamento, le categorie dei dati in questione, i destinatari o le categorie di destinatari cui i dati sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali, il periodo di conservazione dei dati previsto o i criteri utilizzati per determinare tale periodo;
- iii. chiedere al Centro di ricerca la rettifica, la cancellazione dei dati o la limitazione del trattamento dei dati che la riguardano;
- iv. opporsi al trattamento dei dati, fatto salvo il diritto del Centro di ricerca o del Promotore di valutare la Sua istanza, che potrebbe non essere accettata in caso di esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgano sui Suoi interessi, diritti e libertà;
- v. essere messo a conoscenza dell'esistenza di un processo decisionale automatizzato, compresa la profilazione;
- vi. ottenere la portabilità dei dati, nei casi previsti dalla legge;
- vii. proporre reclamo ad un'autorità di controllo (Garante Privacy).

Ad ogni modo, la rettificazione e l'integrazione dei Dati sono annotate senza modificare questi ultimi, quando il risultato di tali operazioni non produce effetti significativi sul risultato della ricerca, così come previsto dall'art. 110, par.2, Codice Privacy.

Le richieste vanno rivolte per iscritto al Titolare del trattamento ovvero ai rispettivi DPO a mezzo dei recapiti sopraindicati.

Qualsiasi modifica o cancellazione o limitazione al trattamento effettuata su richiesta dell'Interessato – a meno che ciò non sia impossibile o comporti uno sforzo sproporzionato – sarà comunicata dal Centro di sperimentazione al Promotore e a ciascuno dei destinatari cui sono stati comunicati i Dati Personali.

## VALUTAZIONE D'IMPATTO PER PROGETTI DI RICERCA IN AMBITO SANITARIO

### SU DATI RETROSPETTIVI

(ART. 110 D. LGS. 196/2003, Provvedimento Garante n. 146/2009)

La valutazione di impatto (DPIA) consente di identificare in modo puntuale i rischi per la protezione dei dati personali quando vengono pianificati nuovi progetti di ricerca o aggiornati progetti di ricerca in corso e di individuare le azioni necessarie per mitigare tali rischi.

**Una valutazione di impatto, secondo l'Autorità Garante per la protezione dei dati personali, 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.

#### A CURA DEL RICERCATORE

**Titolo dello studio:** Predizione del rischio di rifrattura in pazienti con frattura da fragilità: sviluppo e validazione di uno score prognostico (studio RIFRA)

**Codice di Protocollo:** RIFRA

**Titolare del trattamento:** Ospedale Galeazzi S.p.A.

**Principal Investigator:** Dott. Federico Pennestrì

**Unità:** Direzione Scientifica

**Data compilazione:** [29 Gennaio 2025]

TRATTAMENTO DEI DATI		
Descrizione del trattamento		
<i>Sinossi dello Studio</i>	<p><b>Titolo dello studio</b> <i>Predizione del rischio di rifrattura in pazienti con frattura da fragilità: sviluppo e validazione di uno score prognostico - studio RIFRA</i></p> <p><b>Centri partecipanti</b> IRCCS Ospedale Galeazzi – Sant’Ambrogio (OGSA)</p> <p><b>Obiettivo primario</b> In pazienti che hanno sperimentato una frattura da fragilità, identificare i fattori predittori del rischio di ri-frattura entro 2 anni, e sviluppare e validare uno score prognostico del rischio di ri-frattura</p> <p><b>Obiettivi secondari</b> N/A</p> <p><b>Razionale dello studio</b> Le fratture da fragilità rappresentano un carico significativo per i servizi sanitari. Due fattori principali contribuiscono all’aumento del peso delle fratture da fragilità nella popolazione:</p> <ol style="list-style-type: none"> <li>1. la crescente diffusione dell’osteoporosi, che è una malattia generalmente asintomatica fino al verificarsi di una frattura, la cui incidenza aumenta con l’invecchiamento della popolazione;</li> <li>2. sotto-diagnosi e sotto-trattamento dell’osteoporosi stessa. Sono stati sviluppati diversi strumenti di valutazione del rischio che combinano diversi fattori di rischio, con vari livelli di complessità, ma solo pochi sono stati validati seguendo approcci metodologici adeguati.</li> </ol> <p><b>Numero e tipologia degli esami previsti</b> Trattandosi di uno studio retrospettivo, i pazienti non saranno reclutati ex-novo, ma saranno utilizzati dati di pazienti sottoposti a intervento di protesi di anca già memorizzati nelle banche dati OGSA e in quelle di Regione Lombardia.</p> <p><b>Popolazione dello studio</b> Tutti i pazienti sottoposti a intervento di sostituzione totale o parziale di anca, filtrati per diagnosi di frattura chiusa del femore, presso l’IRCCS Istituto Ortopedico Galeazzi e in altre strutture lombarde, fra il 2013 e il 2017.</p> <p>In seguito al campione di pazienti OGSA (2013-2017) arruolati in prima battuta e considerata la finestra temporale di accesso ai dati ottenuta secondo la convenzione stipulata da OGSA e Regione (EIFF-48) (2011-2016), l’intervallo temporale entro cui verrà considerata la popolazione di interesse sarà 2012-2016, onde sostituire il 2017 (che verrebbe perso,</p>	

	<p>pregiudicando il valore numerico del campione) con il 2012 e ottenere una popolazione ragionevolmente analoga.</p> <p>Durata dello studio      14 mesi</p> <p>Dimensione del campione      Verranno reclutati circa 800 pazienti operati presso l'IRCCS Istituto Ortopedico Galeazzi nel periodo 2012 – 2016, di cui saranno verificate eventuali recidive incrociando i dati con il database lombardo</p> <p>Criteri di inclusione      Pazienti sottoposti ad intervento di sostituzione totale o parziale di anca (ICD-9-CM 81.51, 81.52) tra il 2012 ed il 2016 presso l'IRCCS Istituto</p>
<b>Tipologia di dati raccolti</b>	
<p><b>Modalità di raccolta</b> (<i>fonte dei dati</i>) (barrare anche più caselle)</p>	<p><input checked="" type="checkbox"/> da cartelle cliniche/documentazione sanitaria</p> <p><input type="checkbox"/> da archivi di dati clinici (esempio Dossier Sanitario Elettronico, RIS-PACS)</p> <p><input type="checkbox"/> da archivi di test diagnostici</p> <p><input type="checkbox"/> da dati di laboratorio</p> <p><input checked="" type="checkbox"/> da database amministrativi</p> <p><input type="checkbox"/> altro (specificare)</p> <p>_____</p>
<p><b>Trattamento dei dati</b> (<i>indicare il supporto utilizzato per la rilevazione e conservazione dei dati</i>)</p>	<p><input type="checkbox"/> In formato cartaceo</p> <p><input checked="" type="checkbox"/> In formato digitale</p> <p><input type="checkbox"/> In formato cartaceo / digitale</p> <p><input type="checkbox"/> altro (specificare)</p> <p>_____</p>
<p><b>Categorie di persone interessate</b></p>	<p><input type="checkbox"/> pazienti</p> <p><input type="checkbox"/> volontari sani</p> <p><input type="checkbox"/> operatori sanitari</p> <p><input type="checkbox"/> altro (specificare)</p> <p>_____</p>

<b>Categorie di dati trattati</b>	<input checked="" type="checkbox"/> dati sulla salute fisica o psichica <input type="checkbox"/> dati genetici <input type="checkbox"/> informazioni sulla vita sessuale <input type="checkbox"/> informazioni sull'orientamento sessuale <input type="checkbox"/> informazioni sugli stili di vita e/o le condizioni socioeconomiche <input type="checkbox"/> informazioni su istruzione e formazione professionale <input type="checkbox"/> anamnesi lavorativa <input type="checkbox"/> informazioni su religione o altre credenze <input type="checkbox"/> <i>altro (specificare)</i> <hr/>
<b>I dati personali (anche pseudonimizzati e che non siano pertanto anonimi o aggregati) vengono comunicati/condivisi con altri?</b>	<input checked="" type="checkbox"/> No <input type="checkbox"/> Sì In caso positivo, selezionare uno o più ambiti di comunicazione: <input type="checkbox"/> Promotore <input type="checkbox"/> Altri centri partecipanti <input type="checkbox"/> CRO
<b>I dati personali (anche pseudonimizzati e che non siano pertanto anonimi o aggregati) vengono trasferiti all'estero?</b>	<input checked="" type="checkbox"/> No <input type="checkbox"/> Sì Se sì <input type="checkbox"/> Paesi area UE <input type="checkbox"/> Paesi extra UE In quale/i Paese/i all'interno dell'area o extra UE <hr/>

<b>Misure di protezione dei dati</b>	
<b>Verranno conservati i dati identificativi dei partecipanti?</b>	<input checked="" type="checkbox"/> No <input type="checkbox"/> Sì Se sì, specificare le ragioni sottese a tale esigenza: <hr/> <hr/> <hr/>

<p><b><i>Descrivere le procedure utilizzate per non identificare direttamente o rendere anonimi o pseudonimizzati i dati dei partecipanti nelle diverse fasi della ricerca</i></b></p>	<p>Per non identificare direttamente l'interessato sono adottate le seguenti misure:</p> <ul style="list-style-type: none"><li><input type="checkbox"/> Adozione di tecniche crittografiche</li><li><input checked="" type="checkbox"/> Utilizzo di codici univoci per ciascun partecipante. Solo il responsabile della ricerca o altri soggetti autorizzati, possono (con l'uso di mezzi ragionevoli) collegare i codici all'identità dei partecipanti</li><li><input type="checkbox"/> Altro, specificare in dettaglio</li></ul> <p>_____</p> <p>_____</p> <p>Per anonimizzare o aggregare i dati, anche in un momento successivo alla raccolta, sono adottate le seguenti misure:</p> <ul style="list-style-type: none"><li><input checked="" type="checkbox"/> I dati personali, a seguito della raccolta sono eliminati definitivamente senza la possibilità di risalire ai dati originali</li><li><input type="checkbox"/> I dati personali sono sostituiti da uno o più identificatori, che possono essere utilizzati per un set di dati o per ogni singolo dato con distruzione del dato personale originario</li><li><input type="checkbox"/> Sono distrutti i dati che possono essere idonei a identificare gli interessati e sono conservati i soli dati aggregati</li><li><input type="checkbox"/> Altro (specificare)</li></ul> <p>_____</p>
--	---

PRINCIPI, FINALITA' E BASI GIURIDICHE	
<b>Necessità e proporzionalità</b>	
<b><i>Gli scopi del trattamento sono specifici, espliciti e legittimi?</i></b>	<p>X Sì  <input type="checkbox"/> No</p> <p>Motivare la risposta:</p> <p>1. Specificità degli scopi:            Gli scopi del trattamento sono chiaramente e analiticamente definiti all'interno del protocollo. In relazione agli obiettivi dello studio il trattamento è legato esclusivamente alla ricerca così come dettagliatamente descritta e non a ulteriori scopi; pertanto, le finalità risultano circoscritte al contesto descritto. L'uso dei dati è confinato a uno scopo ben definito e non a fini generici o non correlati.</p> <p>2. Esplicitazione degli scopi:            Gli scopi del trattamento sono comunicati chiaramente negli endpoints del protocollo. Gli stessi sono funzionali a raccogliere evidenze scientifiche, migliorare la comprensione delle patologie/trattamenti descritti, e i relativi dati saranno trattati in modo proporzionale all'obiettivo.</p> <p>3. Legittimità degli scopi:            Per quanto riguarda la legittimità, lo studio osservazionale deve rispettare i requisiti legali per la ricerca scientifica previsti dal GDPR e dalle normative nazionali applicabili. Poiché il trattamento è finalizzato alla ricerca, e non a scopi commerciali, rientra nelle finalità legittime ai sensi dell'art. 9 del GDPR, che consente il trattamento di dati sanitari per motivi di ricerca scientifica, soggetto all'adozione di adeguate misure di sicurezza e minimizzazione dei dati.</p> <p>4. Proporzionalità e necessità:            Riguardo a proporzionalità e necessità, i dati trattati sono strettamente necessari a raggiungere gli obiettivi dello studio.            Nel contesto di uno studio retrospettivo, ciò implica l'uso di dati già raccolti in precedenza, riducendo al minimo il rischio di interferenze non necessarie con la protezione dei dati degli interessati.            L'utilizzo di dati anonimi o pseudonimizzati, ove applicabile, sarà sempre impiegato quale misura di mitigazione per limitare il rischio.</p>
<b><i>I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?</i></b>	<p>X Sì  <input type="checkbox"/> No</p> <p>Motivare la risposta:</p> <p>La valutazione circa la pertinenza, limitazione e necessità in relazione alle finalità dello studio in oggetto è basata sul principio di minimizzazione dei dati (art. 5(1)(c) del GDPR):</p> <p>1. Adeguatezza dei dati:            I dati raccolti sono appropriati per raggiungere le finalità dello studio.            Nello studio osservazionale retrospettivo descritto, significa che i dati selezionati oggetto di trattamento sono strettamente necessari per rispondere ai quesiti oggetto della ricerca e alle ipotesi formulate nel protocollo.</p>

	<p>I dati trattati sono scelti in base alla loro rilevanza scientifica e clinica rispetto agli obiettivi dello studio.</p> <p>2. <b>Pertinenza dei dati:</b> I dati sono pertinenti ovvero hanno un legame diretto con gli scopi dello studio. Gli stessi sono rilevanti per rispondere agli specifici quesiti scientifici che lo studio intende esplorare. Non vengono trattati dati che non hanno una connessione chiara con le finalità dichiarate, riducendo il trattamento a informazioni essenziali per la validità scientifica dello studio.</p> <p>3. <b>Limitazione dei dati (minimizzazione):</b> Il protocollo prevede la raccolta dei soli dati strettamente necessari per conseguire le finalità dello studio. I dati sono limitati per ridurre l'impatto sulla privacy degli interessati, evitando la raccolta di informazioni sovrabbondanti o ridondanti. Poiché lo studio è retrospettivo, verranno trattati dati già raccolti per altri scopi (quali la cura dei pazienti), relativamente ai quali si sono accuratamente selezionate solo le informazioni essenziali per l'analisi. Si farà ricorso a tecniche di anonimizzazione o pseudonimizzazione, ove applicabile, per limitare l'identificabilità degli individui.</p> <p>4. <b>Necessità dei dati:</b> Relativamente al principio di necessità lo studio non potrebbe essere condotto correttamente senza il trattamento dei dati previsti dal protocollo. Ogni categoria di dato trattato è necessaria per fornire risultati significativi e validi scientificamente. La raccolta di ulteriori dati fuori protocollo non essenziali non sarebbe in alcun modo giustificata. Pertanto, è possibile considerare i dati adeguati perché appropriati allo scopo dello studio, pertinenti perché direttamente legati alle finalità dichiarate e limitati in quanto raccolti solo nella misura strettamente necessaria per la ricerca, nel rispetto del principio di minimizzazione dei dati previsto dal GDPR.</p>
<b>Integrità ed esattezza</b>	
<b><i>I dati sono esatti e aggiornati?</i></b>	<p><input checked="" type="checkbox"/> Sì <input type="checkbox"/> No</p> <p>Motivare la risposta: La valutazione rispetto alla correttezza dei dati e all'aggiornamento è stata fatta in linea con il principio di esattezza previsto dall'art. 5(1)(d) del GDPR:</p> <p>1. <b>Esattezza dei dati:</b> Lo studio osservazionale retrospettivo si basa su dati già esistenti, raccolti in precedenza per finalità cliniche. Poiché originariamente utilizzati per diagnosi e trattamenti medici, i dati sono stati raccolti e registrati con un alto livello di accuratezza e precisione, in quanto necessari per garantire la cura dei pazienti. Le fonti dei dati, quali ad esempio cartelle cliniche, referti o database ospedalieri, sono dunque affidabili in quanto strumentali al corretto trattamento del paziente, il che assicura una raccolta attenta e precisa delle informazioni.</p> <p>2. <b>Validazione delle fonti dei dati:</b></p>

	<p>Tutte le fonti dei dati sono istituzionalmente validate e soggette a rigorosi controlli di qualità. Vengono applicate procedure per la revisione e la verifica dei dati clinici, riducendo così il rischio di errori. I dati utilizzati sono stati raccolti in conformità a questi protocolli di qualità, assicurando la loro precisione.</p> <p>3. Controlli e verifiche incrociate: All'interno dello studio, sono attuati meccanismi di controllo per garantire l'esattezza dei dati utilizzati. Processi di revisione e pulizia dei dati sono posti in essere per assicurare che non vi siano errori evidenti o duplicazioni [selezionare se del caso tra 4-Eyes Check, Double Data Entry, Source Data Verification (SDV), Query Management, Edit Checks, Audit Trail, Risk-Based Monitoring, Statistical Data Cleaning, Validation and Cross-Validation]</p> <p>4. Aggiornamento dei dati: Lo studio retrospettivo utilizza dati storici, pertanto i dati utilizzati sono pertinenti per il periodo temporale di riferimento dello studio. L'aggiornamento dei dati si riferisce alla loro coerenza rispetto al momento storico e al contesto clinico in cui sono stati raccolti. In quest'ottica, i dati non devono pertanto essere "aggiornati" nel senso tradizionale, ma devono riflettere fedelmente lo stato di salute o il trattamento del paziente in quel determinato periodo.</p> <p>5. Misure di mitigazione del rischio: Esclusivamente i dati accurati e affidabili vengano inclusi nelle analisi finali: lo studio adotta misure di mitigazione come l'esclusione di record non completi o poco chiari. Pertanto i dati trattati nello studio sono esatti perché raccolti da fonti affidabili e soggette a controlli di qualità, accurati nel contesto clinico originario e aggiornati rispetto al periodo storico di interesse. Inoltre, lo studio prevede misure per verificare la correttezza dei dati e garantire che qualsiasi eventuale errore venga identificato e corretto.</p>
<b>Limitazione della conservazione</b>	
<p><b><i>Per quanto tempo verranno conservati i dati raccolti?</i></b></p>	<p>Indicare il numero di anni: <b>10</b></p> <p>Decorso tale termine i dati verranno:</p> <p><input type="checkbox"/> Anonimizzati completamente</p> <p><input checked="" type="checkbox"/> Distrutti</p> <p><input type="checkbox"/> altro (<i>specificare</i>)</p>

Basi giuridiche	
<b>Quali sono le basi giuridiche del trattamento?</b>	<input checked="" type="checkbox"/> art. 9, par. 2, lett. j) GDPR <sup>1</sup> <input type="checkbox"/> art. 110, co. 1 primo periodo Codice Privacy <sup>2</sup> <input type="checkbox"/> art. 110, co. 1, secondo periodo Codice Privacy <sup>3</sup>
MISURE A TUTELA DEI DIRITTI DELL'INTERESSATO	
Informativa e consenso	
<b>SOLO SE LA BASE GIURIDICA È L'ART. 110, CO. 1, SECONDO PERIODO</b> <i>Indicare i motivi per i quali non è possibile fornire l'informativa ai partecipanti allo Studio (soggetti interessati) e acquisirne il consenso</i>	<input type="checkbox"/> motivi etici riconducibili alla circostanza che l'interessato ignora la propria condizione <input type="checkbox"/> sebbene sia stato svolto ogni ragionevole sforzo organizzativo, non è possibile contattare gli interessati in ragione del numero molto alto di interessati non contattabili/non raggiungibili <input type="checkbox"/> deceduti o non contattabili <input checked="" type="checkbox"/> NA
<b>Come sono informati del trattamento gli interessati?</b>	<input checked="" type="checkbox"/> E' stata pubblicata una informativa per pubblici proclami sul sito del promotore <input type="checkbox"/> E' stata pubblicata una informativa per pubblici proclami sul sito di tutti i centri partecipanti
<b>E' stata predisposta una valutazione di impatto ai sensi dell'art. 35 del GDPR?</b>	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
<b>E' stata pubblicata la valutazione di impatto?</b>	<input type="checkbox"/> sul sito del promotore <input type="checkbox"/> sul sito di tutti i centri partecipanti

<sup>1</sup> il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

<sup>2</sup> Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), del Regolamento, ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento.

<sup>3</sup> Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale e deve accuratamente motivare e documentare, nel progetto di ricerca, la sussistenza delle ragioni etiche o organizzative per le quali informare gli interessati e quindi acquisire il consenso, risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, se del caso documentando altresì i ragionevoli sforzi profusi per tentare di contattarli.

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

<b><i>E' stata comunicato l'avvenuto svolgimento e pubblicazione della valutazione di impatto al Garante Privacy?<sup>4</sup></i></b>	<input type="checkbox"/> si <input type="checkbox"/> no <input checked="" type="checkbox"/> non necessario
<b>Esercizio da parte dell'interessato dei diritti ex artt.15-22 DPR</b>	
<b><i>E' stata predisposta una procedura ad hoc da parte del Titolare?</i></b>	<input checked="" type="checkbox"/> Si <input type="checkbox"/> No
<b><i>Come fanno gli interessati a esercitare i loro diritti</i></b>	Rivolgendosi direttamente ai titolari del trattamento o ai rispettivi dpo così come indicato nell'informativa

---

<sup>4</sup> Solo nel caso in cui la base giuridica sia art. 110, co. 1, secondo periodo Codice Privacy<sup>4</sup>

MISURE DI SICUREZZA APPLICATE AL TRATTAMENTO		
MISURA	Esistenti	Note
Organigramma interno	X	<ul style="list-style-type: none"> <li>○ Ruoli e Responsabilità</li> </ul>
Controllo accessi	X	<ul style="list-style-type: none"> <li>○ L'accesso avviene tramite account personali.</li> <li>○ Sono applicate politiche di minimizzazione e restrizione dell'accesso ai dati personali.</li> <li>○ L'autenticazione è effettuata tramite password e, in alcuni casi, tramite autenticazione a due fattori.</li> <li>○ Sono adottate delle politiche di complessità delle password in coerenza con le buone pratiche di settore</li> </ul>
Gestione dei cambiamenti	X	<ul style="list-style-type: none"> <li>○ Ogni modifica ai sistemi IT è valutata, registrata e monitorata.</li> <li>○ E' stata definita una procedura generale per la protezione dei dati personali, comprensiva di valutazioni in ottica by design e by default, volta a individuare i requisiti di protezione dei trattamenti e a implementare e mantenere i sistemi e le applicazioni garantendo livelli di sicurezza adeguati.</li> <li>○ L'acquisizione di componenti del sistema informativo tiene conto dei requisiti di sicurezza dei trattamenti che dovranno essere supportati e delle garanzie offerte dal fornitore.</li> </ul>
Strumenti di sicurezza e protezione	X	<ul style="list-style-type: none"> <li>○ Firewall, anti-malware centralizzati e strumenti di protezione per le postazioni di lavoro.</li> <li>○ Monitoraggio continuo del sistema IT per rilevare incidenti di sicurezza.</li> </ul>
Gestione degli incidenti	X	<ul style="list-style-type: none"> <li>○ Le violazioni dei dati personali vengono gestite tramite procedure di escalation, coinvolgendo il DPO.</li> <li>○ È attivo un sistema di monitoraggio continuo (SIEM e SOC) per raccogliere e analizzare i log.</li> <li>○ Il titolare mantiene un registro delle violazioni dei dati personali.</li> </ul>
Rapporti con i Responsabili	X	<ul style="list-style-type: none"> <li>○ Il titolare gestisce i rapporti con i propri Responsabili del trattamento attraverso accordi formalizzati che comprendono specifiche clausole per assicurare la riservatezza dei dati trattati e l'obbligo per i Responsabili di operare in conformità alla normativa sul trattamento dei dati personali, in particolare, per quanto riguarda le misure di sicurezza, in riferimento agli art. 28 e 32.</li> </ul>

Pseudonimizzazione e cifratura	X	<ul style="list-style-type: none"> <li>○ Pseudonimizzazione e cifratura sono utilizzate per limitare l'identificabilità dei dati.</li> <li>○ Viene applicata la cifratura nelle connessioni VPN, nei servizi HTTPS e nelle comunicazioni machine-to-machine.</li> </ul>
Continuità operativa	X	<ul style="list-style-type: none"> <li>○ L'infrastruttura IT è progettata per garantire la continuità operativa tramite due datacenter distanti almeno 20 km.</li> <li>○ I dati di backup sono conservati in un sito di recupero dati a oltre 100 km.</li> </ul>
Formazione e gestione del personale	X	<ul style="list-style-type: none"> <li>○ Il personale riceve formazione istituzionale con corsi FAD sulla protezione dei dati e sicurezza informatica, con incontri di aggiornamento periodici awareness e sensibilizzazione.</li> <li>○ Il personale con ruoli specifici nell'ambito della data protection (Local Privacy Executive e Local Privacy Contact) riceve una formazione specifica ulteriore.</li> </ul>
Sicurezza delle postazioni di lavoro e delle reti	X	<ul style="list-style-type: none"> <li>○ Le postazioni di lavoro sono aggiornate regolarmente e protette da sistemi anti-malware.</li> <li>○ Le reti sono protette da firewall e strumenti di monitoraggio delle intrusioni.</li> </ul>
Backup e Vulnerability Assessment	X	<ul style="list-style-type: none"> <li>○ Backup giornalieri dei dati e test periodici del sistema di ripristino.</li> <li>○ Valutazioni periodiche della vulnerabilità per identificare possibili rischi di sicurezza.</li> </ul>
Sicurezza fisica	X	<ul style="list-style-type: none"> <li>○ I datacenter sono protetti da misure fisiche e ambientali (protezione da incendi, allagamenti, controllo accessi fisici).</li> <li>○ I datacenter sono certificati TIER3 e TIER4.</li> </ul>

**APPENDICE**

**MINACCE**

**ACCESSO ILLEGITTIMO AI DATI**

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

<b>Impatti Potenziali</b>
Perdita di controllo dei propri dati
Utilizzo da parte di terzi di dati dell'interessato

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

<b>Minaccia</b>
Comportamenti sleali/fraudolenti
Attacco informatico (es. social engineering, man in the middle, denial of service, brute force, etc.)
Furto e/o perdita di dispositivi, supporti di memorizzazione, documenti

**Quali sono le fonti di rischio?**

<b>Fonte</b>
Fonti umane esterne (es. criminali informatici, fornitori, utenti)
Fonti umane interne accidentali (es. collaboratori negligenti)

**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; Politiche di trasmissione dei dati; Crittografia; Pseudonimizzazione

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

Importante

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

Limitato

**MODIFICHE INDESIDERATE DEI DATI**

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

<b>Impatti Potenziali</b>
Dati non esatti e/o non aggiornati

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

<b>Minaccia</b>	
Errore operativo	
<b>Fonte</b>	
Fonti umane interne accidentali (es. collaboratori neglienti)	
<b>Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?</b>	
Istruzioni persone autorizzate trattamento; Formazione; Procedure; Politiche di tutela della privacy; Misure anti – intrusive; Politiche di sicurezza informatica; Controllo accessi (log); antivirus/firewall; Back – up dei dati	
<b>Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?</b>	Limitato
<b>Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?</b>	Trascurabile
<b>PERDITA DI DATI</b>	
<b>Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?</b>	
Una perdita dei dati potrebbe causare l’alterazione dei risultati dello Studio o la impossibilità di proseguire lo Studio; tuttavia non si tratta di dati originali	
<b>Impatti Potenziali</b>	
Costi aggiuntivi	
<b>Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?</b>	
<b>Minaccia</b>	
Errore operativo	
<b>Quali sono le fonti di rischio?</b>	
<b>Fonte</b>	
Eventi tecnologici (es. guasti, malfunzionamenti, etc.)	
Fonti umane interne accidentali (es. collaboratori neglienti)	
<b>Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?</b>	
Back – up dei dati; Controllo accessi (log); Misure anti – intrusive; antivirus/firewall; Tracciabilità, Gestione postazioni; Politiche di tutela della privacy, Politiche di sicurezza informatica	
<b>Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?</b>	Trascurabile
<b>Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?</b>	Trascurabile

### VALUTAZIONE DEL RISCHIO

<i>PROBABILITA' (P)</i>	<i>IMPATTO (I)</i>	<i>RISCHIO (R=P*I)</i>
Probabilità trascurabile: 1 Probabilità limitato: 2 Probabilità importane: 3 Probabilità massima: 4	Impatto trascurabile: 1 Impatto limitato: 2 Impatto importante: 3 Impatto massimo: 4	Rischio basso: $R < 6$ Rischio medio: $7 < R < 11$ Rischio alto: $R > 11$

### MATRICE DI VALUTAZIONE DEL RISCHIO

		IMPATTO <sup>§§</sup>			
PROBABILITA' §	MASSIMO	4	8	12	16
	IMPORTANTE	3	6	9	12
	LIMITATO	2	4	6	8
	TRASCURABILE	1	2	3	4
		TRASCURABILE	LIMITATO	IMPORTANTE	MASSIMO

§ Frequenza con la quale si possono verificare criticità nel trattamento dei dati: **Rischio molto basso**: è probabile che non si verifichi mai; **Basso**: non è probabile che si verifichi, ma può accadere; **Medio**: si può verificare occasionalmente; **Alto**: è probabile che si verifichi, ma non in modo persistente/stabile;

§§ Impatto atteso: **Molto basso**: è improbabile che possa avere un qualsiasi impatto; **Basso**: può avere un impatto; **Medio**: è probabile che abbia un impatto; **Alto**: molto probabile che abbia un impatto significativo;

<u>MINACCIA</u>	<u>VALORE DEL RISCHIO</u> (P*I)	<u>LIVELLO DI RISCHIO</u>	<u>VALUTAZIONE</u> <u>COMPLESSIVA</u> (SOMMA COLONNA LIVELLO RISCHIO)
ACCESSO ILLEGITTIMO	3*2	6	6
MODIFICHE INDESIDERATE DEI DATI	1*2	2	
PERDITA DI DATI	1*1	1	

Classificazione	Intervallo del rischio
Assenza di Rischio	Valore finale tra 0 e 2 compresi
Rischio Limitato	Valore finale tra 3 e 6 compresi
Rischio Importante	Valore finale tra 7 e 11 compresi
Rischio Massimo	Valore finale tra 12 e 16 compresi