Gentile Signora/ Egregio Signore,

Il Promotore e Centro di Sperimentazione **l'Istituto Clinico San Siro** di Ospedale Galeazzi S.p.A, con sede legale in Milano, Via Monreale, 18, e-mail **info.icss@grupposandonato.it**, in persona del suo legale rappresentante *pro-tempore*

in qualità di Titolare del trattamento dei dati personali, (il "**Titolare**"), intende fornirLe la presente informativa (la "**Informativa**") ai sensi dell' artt. 13 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 ("**GDPR**") e della normativa europea e nazionale che lo integra e/o lo modifica ("**Normativa Privacy Applicabile**"), ivi compresa la disciplina sulla protezione dei dati personali di cui al Decreto Legislativo n. 196/2003, come modificato dal Decreto Legislativo n. 101/2018 (di seguito, "**Codice Privacy**").

La presente Informativa Le viene resa in qualità di paziente del Promotore e sulla base della Sua volontaria partecipazione ad uno studio clinico osservazionale, che è in programma presso lo stesso e nelle modalità descritte dal progetto di ricerca (il "**Progetto**") che qui si intende interamente richiamato. La presente Informativa ha lo scopo di fornirLe le specifiche informazioni sul trattamento dei Suoi dati personali che si renderà necessario effettuare nel contesto dello Studio, all'interno della struttura sanitaria del Titolare nelle sue diverse articolazioni organizzative ospedaliere o territoriali. Nel prosieguo, ci si riferirà a Lei anche come l'"**Interessato**".

Titolare del trattamento e Data Protection Officer

I Suoi Dati Personali sono trattati dal **Titolare**

in accordo alle responsabilità previste dalle norme sulla buona pratica clinica.

Il Titolare ha nominato, inoltre, un responsabile per la protezione dei dati ("**Data Protection Officer**" o "**DPO**"), come previsto dal GDPR, con compiti di sorveglianza, vigilanza e consulenza specialistica in ambito *privacy*.

Il Data Protection Officer del Titolare è contattabile scrivendo al seguente indirizzo di posta elettronica **rpd.ogsa@grupposandonato.it**.

Dati personali oggetto del trattamento

Il Titolare tratterà i Suoi dati personali comuni, raccolti in occasione e nell'ambito della Sua partecipazione allo Studio, tra cui rientrano, a titolo esemplificativo e non esaustivo, nome, cognome, numero di telefono mobile, indirizzo e-mail e, in generale, i Suoi dati di contatto (i "**Dati Comuni**").

Saranno altresì trattati anche Suoi "**Dati Particolari**" ovvero dati:

☒ relativi allo stato di salute e alla vita sessuale

☐ Dati Genetici e/o campioni biologici

☒ dati idonei a rivelare l'origine razziale ed etnica

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

A. Le finalità del trattamento di Dati Personali del Titolare

FINALITÀ DEL TRATTAMENTO	BASE GIURIDICA DEL TRATTAMENTO	PERIODO DI CONSERVAZIONE DEI DATI
Partecipazione alla ricerca clinica osservazionale I Dati Personali dell'Interessato sono raccolti e trattati al fine di eseguire la ricerca clinica sopra indicata, le cui caratteristiche e modalità sono meglio esplicate nel documento "*Scheda Informativa*".	Il trattamento dei Dati Comuni è necessario per l'esecuzione di un compito di **interesse pubblico** di cui è investito il titolare del trattamento, ai sensi dell'art. 6, par. 1, lett. e) del GDPR; Il trattamento di categorie particolari di dati è **necessario a fini di ricerca scientifica** ai sensi dell'art. 9, par. 2, lett. j) del GDPR, nonché sulla base di quanto previsto dal diritto nazionale agli artt. 110 e 110 *bis*, comma 4 del Codice Privacy.	*Il promotore e Centro di sperimentazione conserveranno i dati ed i documenti essenziali relativi alla sperimentazione clinica per 5 anni.*
Tutela stragiudiziale e/o giudiziale I Suoi Dati potranno essere trattati, se necessario, per accertare, esercitare o difendere i diritti del Titolare in sede stragiudiziale e/o giudiziaria.	Il trattamento dei Dati Comuni e Categorie particolari di dati è necessario ai fini del perseguimento del legittimo interesse del Titolare alla propria tutela stragiudiziale/ giudiziaria ai sensi degli artt. 6, par. 1, lett. f) e 9, par.2, lett. f), GDPR.	Per tutta la durata del contenzioso, fino all'esaurimento dei termini di esperibilità delle azioni di impugnazione.

Anonimizzazione dei suoi dati personali: durante il periodo di conservazione i Dati Personali dell'interessato potranno essere resi effettivamente ed irreversibilmente anonimi al fine di consentirne l'utilizzo in futuri progetti di ricerca e la divulgazione scientifica dei risultati della ricerca. I suoi dati saranno conservati solo per il tempo necessario ad effettuare il processo di anonimizzazione.

Lei potrà scegliere se conoscere o meno le scoperte inattese che emergano a suo carico durante lo studio e sempre con il Suo consenso potranno essere rese note a persone diverse, da Lei specificamente indicate.

Modalità del trattamento

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 alle finalità del trattamento come sopra riportate e, comunque, garantendo la riservatezza e sicurezza dei dati stessi e il rispetto degli obblighi specifici sanciti dalla legge.

La disponibilità, la gestione, l'accesso, la conservazione e la fruibilità dei dati è garantita dall'adozione di misure tecniche e organizzative per assicurare idonei livelli di sicurezza ai sensi degli artt. 25 e 32 del GDPR. Infatti, i Dati Personali verranno trattati 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 al 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.

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.

Ambito di circolazione dei dati personali

Nello svolgimento dello Studio e per il perseguimento delle finalità elencate nella sezione "A. Le finalità del trattamento di Dati Personali sia del Titolare", Il Titolare del trattamento potrà comunicare i Dati Personali a:

i. eventuali fornitori di servizi strettamente correlati e funzionali alle attività necessarie per lo svolgimento della Studio (quali consulenti esterni, la società di gestione dell'archivio delle cartelle cliniche, società di ricerca a contratto, 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 al DPO, a mezzo dei recapiti sopra indicati.

Trasferimento dei dati al di fuori dello 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 al DPO a mezzo degli indirizzi sopraindicati.

Diritti dell'Interessato

Ai sensi degli articoli 7 e dal 15 al 22 del GDPR, ove applicabile, Lei, nei confronti del Titolare ha il diritto di:

i. ottenere, da parte del Titolare, 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 Titolare la rettifica o la limitazione del trattamento dei dati che la riguardano;
iv. opporsi al trattamento dei dati, fatto salvo il diritto del Titolare 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. chiedere la cancellazione dei Dati Personali al verificarsi di una delle condizioni indicate all'art. 17, paragrafo 1 del GDPR, nel rispetto delle eccezioni previste al paragrafo 3 del medesimo articolo;
vi. opporsi al trattamento dei dati, con base giuridica rintracciabile all'art. 6, par. 1, lett. e) o f), fatto salvo il diritto del Titolare 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;
vii. essere messo a conoscenza dell'esistenza di un processo decisionale automatizzato, compresa la profilazione;
viii. ottenere la portabilità dei dati, nei casi previsti dalla legge;
ix. proporre reclamo ad un'autorità di controllo (Garante Privacy).

Ad ogni modo, la rettifica 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 al DPO da esso nominato 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 Titolare 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: TENOLISI ECOGUIDATA: UN APPROCCIO MININVASIVO "RETROGRADE" RELEASE

Codice di Protocollo: RETROGRADE

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

Principal Investigator: Dr.ssa Alessandra Scalese

Unità: Chirurgia della mano III

Data compilazione: 14/01/2026

TRATTAMENTO DEI DATI

Descrizione del trattamento

Sinossi dello Studio

RIASSUNTO DELLO STUDIO – SINOSSI

Titolo dello studio	**TENOLISI ECOGUIDATA: UN APPROCCIO MININVASIVO "RETROGRADE" RELEASE**
Centri partecipanti	ISTITUTO CLINICO SAN SIRO
Obiettivo primario	VALUTAZIONE DEI TEMPI DI RECUPERO POST TENOLISI ECOGUIDATA: Valutazione della guarigione della ferita e relativa chiusura a pugno a 7 giorni dall'intervento tramite valutazione clinica.
Obiettivi secondari	1.Valutazione ecografica pre op dello spessore della puleggia A1 per stabilire una eventuale correlazione tra spessore della puleggia e risultato post op e valutazione della ripresa delle attività quotidiane abituali con appositi score test (quick DASH) e SANE score. Valutazione del dolore percepito tramite scala VAS. 2. Eventuali complicanze insorte in seguito a tale tecnica e paragone con quelle presentate in letteratura per la tecnica a cielo aperto.
Razionale dello studio	La tecnica di tenolisi ecoguidata permette una più rapida ripresa delle attività rispetto ai dati relativi alla tecnica a cielo aperto presenti in letteratura.
Numero e tipologia degli esami previsti	Esame ecografico pre operatorio di prassi clinica.
Popolazione dello studio	Pazienti affetti da tenosinovite stenosante di II-III-IV e V dito con indicazione chirurgica.
Durata dello studio	3 anni
Dimensione del campione	189
Criteri di inclusione	Pazienti maggiorenni, affetti da tenosinovite stenosante che interessi II-III-IV e V dito Firma del consenso informato
Criteri di esclusione	Pazienti affetti da I dito a scatto. Pazienti con abbondante tenosinovite flessori riscontrata alla eco pre operatoria. Presenza di altri stati patologici locali in cui la semplice tenolisi non sia sufficiente. Pazienti in gravidanza o allattamento o che presentino delle controindicazioni cliniche sistemiche all'atto chirurgico
Metodi statistici e calcolo della grandezza del campione	Per il calcolo della numerosità campionaria viene considerato l'outcome primario "guarigione della ferita" e relativa chiusura a pugno a 7 giorni. Dalla letteratura e dall'esperienza del ricercatore, la percentuale di pazienti sottoposte a tenolisi ecoguidata con guarigione della ferita a 7 giorni è del 98%. Considerando tale proporzione, sarà necessaria una dimensione campionaria di 189 soggetti, che permetterà di stimare un intervallo di confidenza bilaterale al 95% con margine di errore del 2% . Per il calcolo

		della sample size è stata utilizzata la formula $n = p * (1 - p) * \left(\frac{z_{\frac{\alpha}{2}}}{E}\right)^2$, dove p è la percentuale di pazienti attesa, α è il livello di significatività, E è il margine di errore. Verrà eseguita l'analisi descrittiva delle variabili e dei parametri clinici valutati nei pazienti inclusi nello studio. L'analisi delle variabili quantitative continue verrà eseguita previa analisi della distribuzione dei dati, tramite il D'Agostino Pearson omnibus normality test: dati con distribuzione normale saranno espressi come media e deviazione standard, dati con distribuzione non normale saranno espressi come mediana e range interquartile. Le variabili qualitative verranno espresse in termini di frequenze assolute e valore percentuale. Verrà calcolata la percentuale di pazienti con guarigione della ferita e relativa chiusura a pugno a 7 giorni e il relativo intervallo di confidenza al 95%, e varrà fatta una valutazione della rilevanza clinica dei risultati ottenuti. Per l'analisi degli endpoint secondari, verranno valutati i tempi di ripresa funzionale e della ripresa delle attività quotidiane abituali mediante SANE score e dolore percepito su scala VAS a 7 e 30 giorni e quick DASH score a 30 giorni. Medie e deviazioni standard verranno utilizzati se i dati sono distribuiti normalmente, in alternativa si utilizzeranno mediane e range interquartili. I valori ottenuti da questi score verranno confrontati inoltre valutati rispetto ai lo spessore della puleggia a1 al basale. Il confronto e la valutazione dell'associazione verrà fatta graficamente mediante scatterplot e calcolando il coefficiente di correlazione lineare di Bravais-Pearson (se i dati sono distribuiti normalmente) o il coefficiente di Spearman sedati non sono distribuiti normalmente). Infine verranno descritte le eventuali complicanze insorte in seguito alla tecnica ecoguidata e verrà calcolata la percentuale di pazienti con complicanze. Verranno fatti una valutazione e confronto descrittivo di tali complicanze rispetto a quelle riportate in letteratura per la tecnica a cielo aperto. La percentuale stimata di complicanze, corredata dal relativo intervallo di confidenza, verrà confrontata con la percentuale di complicanze riportata in letteratura per la tecnica a cielo aperto.
	Safety Data	Non applicabile
	Calendario previsto per lo studio	Data di inizio studio: al ricevimento delle autorizzazioni da parte del Comitato Etico Tempo di reclutamento soggetti: 30 mesi Raccolta dei dati ed analisi: 6 mesi Durata totale dello studio: 36 mesi
Tipologia di dati raccolti		

Modalità di raccolta *(fonte dei dati) (barrare anche più caselle)*	☒ da cartelle cliniche/documentazione sanitaria ☒ da archivi di dati clinici (esempio Dossier Sanitario Elettronico, RIS-PACS) ☐ da archivi di test diagnostici ☐ da dati di laboratorio ☐ da database amministrativi ☒ direttamente presso l'interessato (paziente) ☐ direttamente presso terzi (es. familiari del paziente) ☐ altro (specificare) _____
Trattamento dei dati *(indicare il supporto utilizzato per la rilevazione e conservazione dei dati)*	☐ In formato cartaceo ☐ In formato digitale ☒ In formato cartaceo / digitale ☐ altro (specificare) _____
Categorie di persone interessate	☒ pazienti ☐ volontari sani ☐ operatori sanitari ☐ *altro (specificare)* _____
Categorie di dati trattati	☒ dati sulla salute fisica o psichica ☐ dati genetici ☐ informazioni sulla vita sessuale ☐ informazioni sull'orientamento sessuale ☐ informazioni sugli stili di vita e/o le condizioni socioeconomiche ☐ informazioni su istruzione e formazione professionale ☒ anamnesi lavorativa ☐ informazioni su religione o altre credenze ☐ *altro (specificare)* _____

I dati personali (anche pseudonimizzati e che non siano pertanto anonimi o aggregati) vengono comunicati/condivisi con altri?	☒ No ☐ Sì In caso positivo, selezionare uno o più ambiti di comunicazione: ☐ Promotore ☐ Altri centri partecipanti ☐ CRO
I dati personali (anche pseudonimizzati e che non siano pertanto anonimi o aggregati) vengono trasferiti all'estero?	☒ No ☐ Sì Se sì ☐ Paesi area UE ☐ Paesi extra UE In quale/i Paese/i all'interno dell'area o extra UE _____

Misure di protezione dei dati	
Verranno conservati i dati identificativi dei partecipanti?	☒ No ☐ Sì Se sì, specificare le ragioni sottese a tale esigenza: _____ _____ _____
Descrivere le procedure utilizzate per non identificare direttamente o rendere anonimi o pseudonimizzati i dati dei partecipanti nelle diverse fasi della ricerca	Per non identificare direttamente l'interessato sono adottate le seguenti misure: ☐ Adozione di tecniche crittografiche ☒ 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 ☐ Altro, specificare in dettaglio _____ _____ Per anonimizzare o aggregare i dati, anche in un momento successivo alla raccolta, sono adottate le seguenti misure: ☐ I dati personali, a seguito della raccolta sono eliminati definitivamente senza la possibilità di risalire ai dati originali

	☐ I dati personali sono sostituti 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 ☒ Sono distrutti i dati che possono essere idonei a identificare gli interessati e sono conservati i soli dati aggregati ☐ Altro (specificare) _____

PRINCIPI, FINALITA' E BASI GIURIDICHE	
Necessità e proporzionalità	
Gli scopi del trattamento sono specifici, espliciti e legittimi?	X Sì ☐ No Motivare la risposta: 1. Specificità degli scopi: Gli scopi del trattamento sono definiti in modo dettagliato all'interno del protocollo. In relazione agli obiettivi dello studio, il trattamento dei dati è finalizzato esclusivamente alla ricerca scientifica, come descritto, e non a scopi differenti. Nel contesto di questo studio, che comprende sia una raccolta retrospettiva sia prospettica, gli scopi risultano circoscritti al miglioramento della comprensione delle patologie/trattamenti, con un uso limitato dei dati al solo ambito della ricerca. 2. Esplicitazione degli scopi: Gli scopi del trattamento sono comunicati chiaramente negli endpoints del protocollo. Tali scopi includono la raccolta di evidenze scientifiche utilizzando dati storici già disponibili (retrospettiva) e la raccolta di nuove informazioni cliniche da pazienti durante il follow-up (prospettiva), previa acquisizione di consenso informato specifico per la partecipazione allo studio. Entrambe le modalità di raccolta contribuiscono a fornire un quadro completo per rispondere agli obiettivi dello studio in maniera proporzionale. 3. Legittimità degli scopi: La legittimità dello studio osservazionale si basa sul rispetto dei requisiti legali per la ricerca scientifica previsti dal GDPR e dalle normative nazionali applicabili. Poiché il trattamento dei dati, sia retrospettivo che prospettico, è finalizzato alla ricerca e non ha scopi commerciali, esso rientra nelle finalità legittime ai sensi dell'art. 9 del GDPR. Il trattamento dei dati sanitari per motivi di ricerca scientifica è quindi permesso, a condizione che siano adottate misure di sicurezza e minimizzazione dei dati adeguate. 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 e prospettico, 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 e la raccolta di dati prospettici per ottenere ulteriori informazioni scientificamente rilevanti con il consenso diretto degli interessati. L'utilizzo di dati anonimi o pseudonimizzati, ove applicabile, sarà sempre impiegato quale misura di mitigazione per limitare il rischio.

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?	X Sì ☐ No Motivare la risposta: 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): 1. Adeguatezza dei dati: I dati raccolti, sia retrospettivi sia prospettici, sono appropriati per raggiungere le finalità dello studio. Per la componente retrospettiva, ciò significa che i dati selezionati sono quelli già disponibili e strettamente necessari per rispondere ai quesiti di ricerca definiti nel protocollo. Per la componente prospettica, i dati raccolti durante le visite di follow-up con consenso specifico sono scelti per la loro rilevanza scientifica e clinica rispetto agli obiettivi dello studio. 2. Pertinenza dei dati: ☒ I dati trattati sono pertinenti, in quanto hanno un legame diretto con gli scopi dello studio. Sia i dati storici già raccolti che quelli ottenuti dai pazienti in follow-up sono rilevanti per rispondere ai quesiti scientifici che lo studio intende esplorare. Non vengono raccolti o trattati dati che non abbiano una chiara connessione con le finalità dichiarate, limitando il trattamento alle informazioni essenziali per la validità scientifica dello studio. 3. Limitazione dei dati (minimizzazione): 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. Per la componente prospettica, la raccolta di nuove informazioni è limitata alle sole necessarie per il follow-up e per raggiungere gli obiettivi di ricerca, minimizzando l'impatto sulla privacy degli interessati. Si farà ricorso a tecniche di anonimizzazione o pseudonimizzazione, ove applicabile, per limitare l'identificabilità degli individui. 4. Necessità dei dati: 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, siano essi retrospettivi o prospettici, 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.

Integrità ed esattezza	
I dati sono esatti e aggiornati?	X Sì ☐ No 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: 1. Esattezza dei dati: 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. 2. Validazione delle fonti dei dati: 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. 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] 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. 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.
Limitazione della conservazione	

Per quanto tempo verranno conservati i dati raccolti?	Indicare il numero di anni: 3 Decorso tale termine i dati verranno: ☐ Anonimizzati completamente ☒ Distrutti ☐ altro (*specificare*) _____

Basi giuridiche	
Quali sono le basi giuridiche del trattamento?	☒ art. 9, par. 2, lett. j) GDPR[1] ☐ art. 110, co. 1 primo periodo Codice Privacy[2] ☐ art. 110, co. 1, secondo periodo Codice Privacy[3]
MISURE A TUTELA DEI DIRITTI DELL'INTERESSATO	
Informativa e consenso	
SOLO SE LA BASE GIURIDICA È L'ART. 110, CO. 1, SECONDO PERIODO Indicare i motivi per i quali non è possibile fornire l'informativa ai partecipanti allo Studio (soggetti interessati) e acquisirne il consenso	☐ 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 non contattabili/non raggiungibili ☐ deceduti o non contattabili
Come sono informati del trattamento gli interessati?	☒ E' stata pubblicata una informativa per pubblici proclami sul sito del promotore ☐ E' stata pubblicata una informativa per pubblici proclami sul sito di tutti i centri partecipanti
E' stata predisposta una valutazione di impatto ai sensi dell'art. 35 del GDPR?	☒ si ☐ no
E' stata pubblicata la valutazione di impatto?	☒ sul sito del promotore ☐ sul sito di tutti i centri partecipanti

[1] 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.

[2] 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.

[3] 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.

E' stata comunicato l'avvenuto svolgimento e pubblicazione della valutazione di impatto al Garante Privacy?[4]	☐ si ☐ no ☒ non necessario
Esercizio da parte dell'interessato dei diritti ex artt.15-22 DPR	
E' stata predisposta una procedura ad hoc da parte del Titolare?	☒ Sì ☐ No
Come fanno gli interessati a esercitare i loro diritti	Rivolgendosi direttamente ai titolari del trattamento o ai rispettivi dpo così come indicato nell'informativa

[4] Solo nel caso in cui la base giuridica sia art. 110, co. 1, secondo periodo Codice Privacy[4]

MISURE DI SICUREZZA APPLICATE AL TRATTAMENTO		
MISURA	Esistenti	Note
Organigramma interno	X	o Ruoli e Responsabilità
Controllo accessi	X	o L'accesso avviene tramite account personali. o Sono applicate politiche di minimizzazione e restrizione dell'accesso ai dati personali. o L'autenticazione è effettuata tramite password e, in alcuni casi, tramite autenticazione a due fattori. o Sono adottate delle politiche di complessità delle password in coerenza con le buone pratiche di settore
Gestione dei cambiamenti	X	o Ogni modifica ai sistemi IT è valutata, registrata e monitorata. o 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. o 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.
Strumenti di sicurezza e protezione	X	o Firewall, anti-malware centralizzati e strumenti di protezione per le postazioni di lavoro. o Monitoraggio continuo del sistema IT per rilevare incidenti di sicurezza.
Gestione degli incidenti	X	o Le violazioni dei dati personali vengono gestite tramite procedure di escalation, coinvolgendo il DPO. o È attivo un sistema di monitoraggio continuo (SIEM e SOC) per raccogliere e analizzare i log. o Il titolare mantiene un registro delle violazioni dei dati personali.
Rapporti con i Responsabili	X	o 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.

Pseudonimizzazione e cifratura	X	○ Pseudonimizzazione e cifratura sono utilizzate per limitare l'identificabilità dei dati. ○ Viene applicata la cifratura nelle connessioni VPN, nei servizi HTTPS e nelle comunicazioni machine-to-machine.
Continuità operativa	X	○ L'infrastruttura IT è progettata per garantire la continuità operativa tramite due datacenter distanti almeno 20 km. ○ I dati di backup sono conservati in un sito di recupero dati a oltre 100 km.
Formazione e gestione del personale	X	○ Il personale riceve formazione istituzionale con corsi FAD sulla protezione dei dati e sicurezza informatica, con incontri di aggiornamento periodici awareness e sensibilizzazione. ○ Il personale con ruoli specifici nell'ambito della data protection (Local Privacy Executive e Local Privacy Contact) riceve una formazione specifica ulteriore.
Sicurezza delle postazioni di lavoro e delle reti	X	○ Le postazioni di lavoro sono aggiornate regolarmente e protette da sistemi anti-malware. ○ Le reti sono protette da firewall e strumenti di monitoraggio delle intrusioni.
Backup e Vulnerability Assessment	X	○ Backup giornalieri dei dati e test periodici del sistema di ripristino. ○ Valutazioni periodiche della vulnerabilità per identificare possibili rischi di sicurezza.
Sicurezza fisica	X	○ I datacenter sono protetti da misure fisiche e ambientali (protezione da incendi, allagamenti, controllo accessi fisici). ○ I datacenter sono certificati TIER3 e TIER4.

APPENDICE

MINACCE

ACCESSO ILLEGITTIMO AI DATI

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

Impatti Potenziali
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?

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

Quali sono le fonti di rischio?

Fonte
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?

Impatti Potenziali
Dati non esatti e/o non aggiornati

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Minaccia
Errore operativo

Fonte
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; Back – up dei dati

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?	Limitato
Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?	Trascurabile

PERDITA DI DATI

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

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

Impatti Potenziali
Costi aggiuntivi

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

Minaccia
Errore operativo

Quali sono le fonti di rischio?

Fonte
Eventi tecnologici (es. guasti, malfunzionamenti, etc.)
Fonti umane interne accidentali (es. collaboratori negligenti)

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

Back – up dei dati; Controllo accessi (log); Misure anti – intrusive; antivirus/firewall; Tracciabilità, Gestione postazioni; Politiche di tutela della privacy¸ Politiche di sicurezza informatica

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?	Trascurabile
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?	Trascurabile

VALUTAZIONE DEL RISCHIO

PROBABILITA' (P)	*IMPATTO (I)*	*RISCHIO (R=P*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§§			
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;

MINACCIA	**VALORE DEL RISCHIO (P*I)**	**LIVELLO DI RISCHIO**	**VALUTAZIONE COMPLESSIVA** (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 Importanto	Valore finale tra 7 e 11 compresi
Rischio Massimo	Valore finale tra 12 e 16 compresi