



Prot. RETRORAD

Informativa Privacy Minori v1 del 01/09/2021

Informativa Privacy Minori v2 del 22/08/2022

Informativa Privacy Minori v3 del 16/06/2023 (emend. N2)

Informativa Privacy Minori v4 del 08/01/2025 (emend. N3)

Informativa Privacy Minori v5 del 18/03/2025 (secondo l'emend. N3_risp)

Informativa relativa al trattamento dei dati personali finalizzato alla partecipazione ad uno studio osservazionale di ricerca clinica ai sensi degli artt. 13 e 14 Regolamento (UE) 2016/679

Luogo e Data Milano, 18/03/2025

- **L'Ospedale Galeazzi S.p.A.**, con sede in Milano, Via Cristina Belgioioso, 173, e-mail info.ogsa@grupposandonato.it, il quale ha nominato un Responsabile per la Protezione dei Dati Personali (**"Data Protection Officer"** o **"DPO"**), contattabile all'indirizzo e-mail rp.d.ogsa@grupposandonato.it (**Centro di Sperimentazione**) in qualità di Titolare del Trattamento (di seguito solo **"Titolare"**) fornisce la presente informativa (**"Informativa"**) ai sensi degli artt. 13 del Regolamento (UE) 2016/679 (**"GDPR"**) e della normativa europea e nazionale che lo integra e/o lo modifica (**"Normativa Privacy Applicabile"**).

La presente Informativa si rivolge a pazienti che al momento delle prestazioni erano minorenni (ed ai loro Genitori/Tutori), che si sono sottoposti a radiografie, ecografie, tomografie computerizzate, risonanze magnetiche e/o mineralometria ossea computerizzata di tutti i distretti anatomici, eseguite per routine clinica presso la Radiologia dell'IRCCS Istituto Ortopedico Galeazzi (ora IRCCS Ospedale Galeazzi - Sant'Ambrogio). La presente Informativa ha lo scopo di informare sul trattamento dei dati che il Titolare intende porre in essere nell'ambito di uno studio retrospettivo osservazionale denominato **"Studio di performance diagnostica e di riproducibilità della radiografia, ecografia, tomografia computerizzata, risonanza magnetica, e mineralometria ossea computerizzata e radiologia interventistica (Studio RETROspettivo in RADiodiagnostica – RETRORAD)"**.

L'obiettivo dello studio è di rivedere retrospettivamente la casistica di radiografie, ecografie, tomografie computerizzate, risonanze magnetiche, mineralometria ossea computerizzata e procedure di radiologia interventistica ed i relativi dati clinici di tutti i distretti anatomici eseguite per routine clinica presso la Radiologia del IRCCS Istituto Ortopedico Galeazzi (ora IRCCS Ospedale Galeazzi - Sant'Ambrogio) per valutare la loro performance diagnostica loro riproducibilità ed efficacia clinica, anche avendo le informazioni cliniche (chirurgiche o di follow-up) od altre metodiche diagnostiche come standard di riferimento.

Per raggiungere tale scopo lo studio intende valutare la popolazione di pazienti sottoposti a radiografie, ecografie, tomografie computerizzate, risonanze magnetiche mineralometria ossea computerizzata e procedure di radiologia interventistica ed i relativi dati clinici di tutti i distretti anatomici presso l'IRCCS Istituto Ortopedico Galeazzi (ora IRCCS Ospedale Galeazzi - Sant'Ambrogio) dal 01/01/2006 al 31/12/2024.

I.R.C.C.S. Ospedale Galeazzi - Sant'Ambrogio
di Ospedale Galeazzi S.p.A.
Sistema di Gestione Qualità UNI EN ISO 9001

Via Cristina Belgioioso 173 - 20157 Milano (MI)
Tel. +39 02. 8350.0010 | Fax. 02.8350.1015 | info.ogsa@grupposandonato.it
C. F. e P.IVA: 05849220156 – Numero R.E.A.: MI-1040877
Capitale Sociale € 130.000 i.v.

www.grupposandonato.it



Prot. RETRORAD

Informativa Privacy Minori v1 del 01/09/2021

Informativa Privacy Minori v2 del 22/08/2022

Informativa Privacy Minori v3 del 16/06/2023 (emend. N2)

Informativa Privacy Minori v4 del 08/01/2025 (emend. N3)

Informativa Privacy Minori v5 del 18/03/2025 (secondo l'emend. N3_risp)

Per ulteriori informazioni sullo Studio, è possibile contattare il Prof. Luca Maria Sconfienza Unità Operativa Radiologia/Diagnostica per immagini con servizio di Radiologia Interventistica, e-mail io@lucasconfienza.it

1. Dati personali oggetto del trattamento

Il Titolare tratterà i dati personali di Vostro/a figlio/a o il/la Tutelato/a comuni e relativi alla salute raccolti in occasione dell'attività clinica svolta dal Titolari nei confronti di Vostro/a figlio/a o il/la Tutelato/a durante il periodo sopra indicato.

I dati personali comuni di Vostro/a figlio/a o il/la Tutelato/a e quelli relativi alla salute vengono di seguito definiti congiuntamente "**Dati Personali**".

2. Finalità e base giuridica del trattamento

I Dati Personali di Vostro/a figlio/a o il/la Tutelato/a saranno trattati per le seguenti finalità e sulla base delle basi di legittimità di seguito indicate:

- a) ai fini dello svolgimento dello Studio che Vi è stato descritto e solo nella misura in cui essi siano indispensabili agli obiettivi dello stesso sulla base del combinato disposto degli artt. 9, par.2 lett. h) del GDPR e dall'art. 110-bis, comma 4, del D.Lvo 196/2003 (Codice Privacy). Infatti essendo il Titolare qualificato come Istituto di Ricovero e Cura a Carattere Scientifico (IRCSS) ai sensi del Decreto Legislativo n. 288/2003, ossia "*ente a rilevanza nazionale dotato di autonomia e personalità giuridica che, secondo standard di eccellenza, persegue finalità di ricerca, prevalentemente clinica e traslazionale, nel campo biomedico e in quello dell'organizzazione e gestione dei servizi sanitari, unitamente a prestazioni di ricovero e cura di alta specialità*", le attività di ricerca vanno ritenute come implicite, secondo quanto previsto per gli IRCCS dall'art. 110-bis, comma 4, del Codice Privacy, nei trattamenti effettuati per finalità di diagnosi e cura;
- b) per motivi di interesse pubblico nel settore della sanità pubblica, quali la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici sulla base del diritto dell'Unione Europea o del diritto nazionale, che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale, ai sensi dell'art. 9, par. 2, lett. i), del GDPR;

I.R.C.C.S. Ospedale Galeazzi - Sant'Ambrogio
di Ospedale Galeazzi S.p.A.
Sistema di Gestione Qualità UNI EN ISO 9001

Via Cristina Belgioioso 173 - 20157 Milano (MI)
Tel. +39 02. 8350.0010 | Fax. 02.8350.1015 | info.ogsa@grupposandonato.it
C. F. e P.IVA: 05849220156 – Numero R.E.A.: MI-1040877
Capitale Sociale € 130.000 i.v.

www.grupposandonato.it



Prot. RETRORAD

Informativa Privacy Minori v1 del 01/09/2021

Informativa Privacy Minori v2 del 22/08/2022

Informativa Privacy Minori v3 del 16/06/2023 (emend. N2)

Informativa Privacy Minori v4 del 08/01/2025 (emend. N3)

Informativa Privacy Minori v5 del 18/03/2025 (secondo l'emend. N3_risp)

- c) per l'adempimento di obblighi previsti da leggi, regolamenti e dalla normativa comunitaria, ai sensi degli artt. 6, lett. c) e 9, par. 2, lett. b), del GDPR (ad esempio, adempimenti fiscali; verifiche di carattere amministrativo; ispezioni di organi preposti alla vigilanza in materia sanitaria; investigazioni della polizia giudiziaria etc.);
- d) per la tutela di un diritto in giudizio o in una fase propedeutica al giudizio, ai sensi dell'art. 9 par. 2, lett. f), del GDPR;
- e) per finalità ulteriori di ricerca scientifica, in particolare per studi osservazionali, ai sensi dell'art. 9 par. 2, lett. j), del GDPR.

I Dati Personali raccolti di Vostro/a figlio/a o il/la Tutelato/a saranno in ogni caso trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale o da altri 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.

3. Modalità del trattamento

Il trattamento dei Dati Personali avverrà – secondo i principi correttezza, liceità e trasparenza – tramite supporti e/o strumenti informatici, manuali e/o telematici, con logiche strettamente correlate alle finalità del trattamento e, comunque, garantendo la riservatezza e sicurezza dei dati stessi e il rispetto degli obblighi specifici sanciti dalla legge.

Subito dopo la raccolta dei Dati Personali di Vostro/a figlio/a o il/la Tutelato/a e prima di qualsiasi ulteriore trattamento, i dati di Vostro/a figlio/a o il/la Tutelato/a saranno definitivamente anonimizzati attraverso la seguente tecnica:

- al materiale clinico (nominale) verrà associato un codice del paziente;
- il codice verrà trascritto in un secondo documento e associato ad un secondo codice ottenuto mediante randomizzazione (detto “numero paziente”);
- Il “numero paziente” verrà quindi riportato in CRF e il documento intermedio verrà distrutto al termine della raccolta dei dati.

Al termine di questo processo e nel proseguo dello Studio i Suoi dati verranno trattati in modalità completamente anonima.

4. Conservazione dei dati personali

I.R.C.C.S. Ospedale Galeazzi - Sant'Ambrogio
di Ospedale Galeazzi S.p.A.
Sistema di Gestione Qualità UNI EN ISO 9001

Via Cristina Belgioioso 173 - 20157 Milano (MI)
Tel. +39 02. 8350.0010 | Fax. 02.8350.1015 | info.ogsa@grupposandonato.it
C. F. e P.IVA: 05849220156 – Numero R.E.A.: MI-1040877
Capitale Sociale € 130.000 i.v.

www.grupposandonato.it



Prot. RETRORAD

Informativa Privacy Minori v1 del 01/09/2021

Informativa Privacy Minori v2 del 22/08/2022

Informativa Privacy Minori v3 del 16/06/2023 (emend. N2)

Informativa Privacy Minori v4 del 08/01/2025 (emend. N3)

Informativa Privacy Minori v5 del 18/03/2025 (secondo l'emend. N3_risp)

I Dati Personali saranno conservati solo per il tempo necessario ai fini per cui sono raccolti, rispettando il principio di minimizzazione di cui all'articolo 5(1)(c) del GDPR nonché gli obblighi di legge cui è tenuto il Titolare.

Maggiori informazioni sono disponibili scrivendo al Titolare o al relativo DPO ai recapiti indicati in epigrafe.

5. Ambito di circolazione dei dati personali

I Dati Personali di Vostro figlio/a o *il/la Tutelato/a* 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).

Nello svolgimento della propria attività e per il perseguimento delle finalità descritte, i dati di Vostro/a figlio/a o *il/la Tutelato/a* potrebbero essere trattati da:

- soggetti appositamente autorizzati dal Titolare e in ottemperanza a quanto previsto dall'art. 29 GDPR;
- 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;
- fornitori di servizi strettamente correlati e funzionali alle attività necessarie per lo svolgimento della Sperimentazione, i quali agiscono tipicamente in qualità di responsabili del trattamento *ex art.* 28 del GDPR;
- fornitori di servizi IT per la gestione dell'infrastruttura tecnologica, dei sistemi informativi e delle reti di telecomunicazione.

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

I Dati Personali di Vostro/a figlio/a o *il/la Tutelato/a* non saranno oggetto di trasferimento verso Paesi Terzi rispetto all'Unione Europea od organizzazioni internazionali.

Maggiori informazioni sono disponibili presso il Titolare o al DPO scrivendo agli indirizzi sopraindicati.

I.R.C.C.S. Ospedale Galeazzi - Sant'Ambrogio
di Ospedale Galeazzi S.p.A.
Sistema di Gestione Qualità UNI EN ISO 9001

Via Cristina Belgioioso 173 - 20157 Milano (MI)
Tel. +39 02. 8350.0010 | Fax. 02.8350.1015 | info.ogsa@grupposandonato.it
C. F. e P.IVA: 05849220156 – Numero R.E.A.: MI-1040877
Capitale Sociale € 130.000 i.v.

www.grupposandonato.it



Prot. RETRORAD

Informativa Privacy Minori v1 del 01/09/2021

Informativa Privacy Minori v2 del 22/08/2022

Informativa Privacy Minori v3 del 16/06/2023 (emend. N2)

Informativa Privacy Minori v4 del 08/01/2025 (emend. N3)

Informativa Privacy Minori v5 del 18/03/2025 (secondo l'emend. N3_risp)

6. Diritti dell'Interessato

Voi potrete, ai sensi e per gli effetti degli artt. 15 e ss. del GDPR, accedere ai dati di Vostro/a figlio/a o il/la Tutelato/a personali, verificarne contenuto, origine, esattezza, ubicazione, chiederne copia, integrazione, aggiornamento, rettificazione e, nei casi previsti dalla Legge vigente, cancellazione, trasformazione in forma anonima, la limitazione, la portabilità dei dati; nonché proporre reclamo all'autorità di controllo competente ex articolo 77 del GDPR (Garante per la Protezione dei Dati Personali).

Vi informiamo, inoltre, che voi potrete opporvi al trattamento dei dati personali di Vostro/a figlio/a o il/la Tutelato/a ai sensi dell'art. 21 del Regolamento.

La modifica dei dati originari può avere effetti significativi sui risultati dello studio, per cui in caso di esercizio di diritti che comportano variazione/integrazione dei dati registrati, le modifiche richieste potranno essere annotate e registrate a margine dei dati originari senza modificare questi ultimi.

I diritti di Vostro/a figlio/a o il/la Tutelato/a potranno essere esercitati solo in una prima fase, in quanto dopo la raccolta essi verranno anonimizzati, con la conseguente impossibilità del Titolare di risalire alle informazioni che riguardano Vostro/a figlio/a o il/la Tutelato/a.

Per esercitare i diritti di privacy di Vostro/a figlio/a o il/la Tutelato/a potete contattare il DPO o il Titolare del trattamento ai recapiti sopra indicati.

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: Studio di performance diagnostica e di riproducibilità ed efficacia clinica della radiografia, ecografia, tomografia computerizzata, risonanza magnetica, e mineralometria ossea computerizzata e radiologia interventistica (Studio RETROspettivo in RADiodiagnostica – RETRORAD)

Codice di Protocollo: RETRORAD

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

Principal Investigator: Prof. Luca Maria Sconfienza

Unità: Unità Operativa Radiologia/Diagnostica per immagini con servizio di Radiologia Interventistica

Data compilazione: 14/01/2025

TRATTAMENTO DEI DATI	
Descrizione del trattamento	
Sinossi dello Studio	<p><i>L'obiettivo del nostro studio è di rivedere retrospettivamente la casistica di radiografie, ecografie, tomografie computerizzate, risonanza magnetica, mineralometria ossea computerizzata e procedure di radiologia interventistica ed i relativi dati clinici di tutti i distretti anatomici eseguite per routine clinica presso la Radiologia del IRCCS Ospedale Galeazzi Sant'Ambrogio per valutare la loro performance diagnostica, riproducibilità ed efficacia clinica, anche avendo le informazioni cliniche (chirurgiche o di follow-up) od altre metodiche diagnostiche come standard di riferimento.</i></p> <p><i>L'imaging è quasi sempre il primo approccio diagnostico alla patologia di tutti i distretti corporei, sia essa traumatica, degenerativa, infiammatoria o neoplastica con risultati di performance diagnostica variabili a seconda della metodica utilizzata (radiografie, ecografie, tomografie computerizzate, risonanza magnetica e/o mineralometria ossea computerizzata), del tipo di patologia e/o regione corporea. Accanto a questa accuratezza diagnostica dimostrata per molti distretti anatomici e strutture, ci sono altrettanti ambiti in cui la performance diagnostica o la riproducibilità dell'imaging non è ancora stata dimostrata. Analogamente, le procedure di radiologia interventistica vengono utilizzate di routine per il trattamento mini-invasivo di diverse procedure ed in molti ambiti l'efficacia diagnostica non è ancora dimostrata chiaramente.</i></p> <p><i>A seconda della regione anatomica e della metodica di imaging oggetto dello studio o del trattamento mini-invasivo (radiografia, ecografia, tomografia computerizzata, risonanza magnetica e/o mineralometria ossea computerizzata), saranno valutate le lesioni/strutture anatomiche di interesse e saranno messi in relazione con i relativi dati clinici del paziente (anamnesi, chirurgia, follow-up, ecc.) o con i reperti risultanti da altre metodiche diagnostiche (vedi tabelle allegate). Per ogni paziente, saranno valutati il primo esame eseguito ed eventualmente anche gli ulteriori controlli successivi, se disponibili, per studiare l'evoluzione del quadro patologico. Le valutazioni saranno eseguite da uno o possibilmente più radiologi esperti nel relativo ambito con diversi livelli di esperienza.</i></p> <p><i>Saranno inclusi tutti i pazienti che hanno eseguito almeno un esame/procedura diagnostica di radiologia, ecografia, tomografia computerizzata, risonanza magnetica, mineralometria ossea computerizzata e/o di radiologia interventistica presso l'IRCCS Ospedale Galeazzi-Sant'Ambrogio conservato in formato digitale sul nostro archivio informatico. Non sono previsti criteri di esclusione.</i></p>

	<p>Saranno inclusi nello studio gli esami di radiologia, ecografia, tomografia computerizzata, risonanza magnetica, mineralometria ossea computerizzata e/o di radiologia interventistica eseguiti dal 1/1/2006 al 31/12/2024 presso l'IRCCS Ospedale Galeazzi-Sant'Ambrogio, circa:</p> <p>Esami radiografici: 1.200.000</p> <p>Ecografie: 90.000</p> <p>Tomografie computerizzate: 120.000</p> <p>Risonanze magnetiche: 190.000</p> <p>Mineralometria ossea computerizzata: 31.000</p> <p>Procedure interventistiche: circa 7.000</p> <p>Criteri di inclusione: Saranno inclusi tutti i pazienti che hanno eseguito almeno un esame/procedura diagnostica di radiologia, ecografia, tomografia computerizzata, risonanza magnetica, mineralometria ossea computerizzata e/o di radiologia interventistica presso l'IRCCS Ospedale Galeazzi-Sant'Ambrogio, conservato in formato digitale sul nostro archivio informatico</p> <p>Criteri di esclusione: Nessuno.</p> <p>Non è prevista una valutazione della dimensione campionaria ad hoc.</p> <p>Avendo la chirurgia il follow-up o altre metodiche di imaging come standard di riferimento, per ogni variabile presa in esame potranno essere calcolati sensibilità, specificità, valore predittivo positivo, valore predittivo negativo ed accuratezza diagnostica di radiologia, ecografia, tomografia computerizzata, risonanza magnetica, mineralometria ossea computerizzata e/o radiologia interventistica. Quando le valutazioni saranno eseguite da più radiologi, si calcolerà anche la riproducibilità intra- ed interosservatore utilizzando la k di Cohen per variabili discrete ed il metodo di Bland-Altman per variabili continue.</p> <p>Raccolta dati relativa al periodo: 1/01/2006-31/12/2024</p> <p>Tempo per la raccolta e l'analisi dei dati: circa 20 anni</p>
Tipologia di dati raccolti	
<p>Modalità di raccolta (fonte dei dati) (barrare anche più caselle)</p>	<p><input checked="" type="checkbox"/> da cartelle cliniche/documentazione sanitaria</p> <p><input checked="" 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 type="checkbox"/> da database amministrativi</p> <p><input type="checkbox"/> altro (specificare)</p> <p>_____</p>

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

Misure di protezione dei dati	
Verranno conservati i dati identificativi dei partecipanti?	<input checked="" type="checkbox"/> No <input type="checkbox"/> Sì Se sì, specificare le ragioni sottese a tale esigenza: <hr/> <hr/> <hr/>
Descrivere le procedure utilizzate per non identificare direttamente o rendere anonimi o pseudonimizzati i dati dei partecipanti nelle diverse fasi della ricerca	<p>Per non identificare direttamente l'interessato sono adottate le seguenti misure:</p> <input type="checkbox"/> Adozione di tecniche crittografiche <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 <input checked="" type="checkbox"/> Altro, specificare in dettaglio <ul style="list-style-type: none"> - Al materiale radiografico (nominale) verrà associato un codice del paziente; - il codice verrà trascritto in un secondo documento e associato ad un secondo codice ottenuto mediante randomizzazione (detto "numero paziente"); - Il "numero paziente" verrà quindi riportato in CRF e il documento intermedio verrà distrutto al termine della raccolta dei dati <p>Per anonimizzare o aggregare i dati, anche in un momento successivo alla raccolta, sono adottate le seguenti misure:</p> <input type="checkbox"/> I dati personali, a seguito della raccolta sono eliminati definitivamente senza la possibilità di risalire ai dati originali <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 <input checked="" type="checkbox"/> Sono distrutti i dati che possono essere idonei a identificare gli interessati e sono conservati i soli dati aggregati <input type="checkbox"/> Altro (specificare) <hr style="width: 50%; margin-left: 0;"/>

PRINCIPI, FINALITA' E BASI GIURIDICHE	
Necessità e proporzionalità	
<i>Gli scopi del trattamento sono specifici, espliciti e legittimi?</i>	<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>
<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>	<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. Pertinenza dei dati: 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. 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. Si farà ricorso a tecniche di anonimizzazione o pseudonimizzazione, ove applicabile, per limitare l'identificabilità degli individui.</p> <p>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 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>
Integrità ed esattezza	
<p><i>I dati sono esatti e aggiornati?</i></p>	<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. 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.</p> <p>2. Validazione delle fonti dei dati:</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>
Limitazione della conservazione	
<p><i>Per quanto tempo verranno conservati i dati raccolti?</i></p>	<p>Indicare il numero di mesi/anni: 5 anni</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> <p>_____</p>

Basi giuridiche	
Quali sono le basi giuridiche del trattamento?	<input checked="" type="checkbox"/> art. 9, par. 2, lett. j) GDPR ¹ <input type="checkbox"/> art. 110, co. 1 primo periodo Codice Privacy ² <input type="checkbox"/> 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 <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
Come sono informati del trattamento gli interessati?	<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
E' stata predisposta una valutazione di impatto ai sensi dell'art. 35 del GDPR?	<input checked="" type="checkbox"/> si <input type="checkbox"/> no
E' stata pubblicata la valutazione di impatto?	<input type="checkbox"/> sul sito del promotore <input type="checkbox"/> 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.

<i>E' stata comunicato l'avvenuto svolgimento e pubblicazione della valutazione di impatto al Garante Privacy?⁴</i>	<input type="checkbox"/> si <input type="checkbox"/> no <input checked="" type="checkbox"/> non necessario
Esercizio da parte dell'interessato dei diritti ex artt.15-22 DPR	
<i>E' stata predisposta una procedura ad hoc da parte del Titolare?</i>	<input checked="" type="checkbox"/> Si <input type="checkbox"/> No
<i>Come fanno gli interessati a esercitare i loro diritti</i>	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 Privacy⁴

MISURE DI SICUREZZA APPLICATE AL TRATTAMENTO		
MISURA	Esistenti	Note
Organigramma interno	X	<ul style="list-style-type: none"> ○ Ruoli e Responsabilità
Controllo accessi	X	<ul style="list-style-type: none"> ○ L'accesso avviene tramite account personali. ○ Sono applicate politiche di minimizzazione e restrizione dell'accesso ai dati personali. ○ L'autenticazione è effettuata tramite password e, in alcuni casi, tramite autenticazione a due fattori. ○ Sono adottate delle politiche di complessità delle password in coerenza con le buone pratiche di settore
Gestione dei cambiamenti	X	<ul style="list-style-type: none"> ○ Ogni modifica ai sistemi IT è valutata, registrata e monitorata. ○ 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. ○ 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	<ul style="list-style-type: none"> ○ Firewall, anti-malware centralizzati e strumenti di protezione per le postazioni di lavoro. ○ Monitoraggio continuo del sistema IT per rilevare incidenti di sicurezza.
Gestione degli incidenti	X	<ul style="list-style-type: none"> ○ Le violazioni dei dati personali vengono gestite tramite procedure di escalation, coinvolgendo il DPO. ○ È attivo un sistema di monitoraggio continuo (SIEM e SOC) per raccogliere e analizzare i log. ○ Il titolare mantiene un registro delle violazioni dei dati personali.
Rapporti con i Responsabili	X	<ul style="list-style-type: none"> ○ 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	<ul style="list-style-type: none"> ○ 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	<ul style="list-style-type: none"> ○ 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	<ul style="list-style-type: none"> ○ 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	<ul style="list-style-type: none"> ○ 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	<ul style="list-style-type: none"> ○ Backup giornalieri dei dati e test periodici del sistema di ripristino. ○ Valutazioni periodiche della vulnerabilità per identificare possibili rischi di sicurezza.
Sicurezza fisica	X	<ul style="list-style-type: none"> ○ 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 middle, denial of service, 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 neglienti)	
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 neglienti)	
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

<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 ^{§§}			
		TRASCURABILE	LIMITATO	IMPORTANTE	MASSIMO
PROBABILITA' §	MASSIMO	4	8	12	16
	IMPORTANTE	3	6	9	12
	LIMITATO	2	4	6	8
	TRASCURABILE	1	2	3	4

§ 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