Titolo dello studio	Radioterapia Stereotassica per il trattamento di oligomestasasi extracraniche da carcinoma mammario (ORIETTA): database retrospettivo multi-istituzionale
Promotore	IRCCS Humanitas Research Hospital
Centro di Sperimentazione	Istituto Nazionale Tumori di Napoli, IRCCS G. Pascale
Principal Investigator	Dott.ssa Sara Falivene S.C. Radioterapia Istituto Nazionale Tumori IRCCS Fondazione G. Pascale
Tipo di studio e fase	Studio Osservazionale Retrospettivo Multicentrico
Parere del Comitato Etico	Parere del CET 05.11.2025
Durata dello studio	6 mesi
DPO/RPD	Ing. Alessandro Manzoni

	Nome e Cognome	Ruolo	Firma	Data
Redazione	Roberta Fusco	Ingegnere Biomedico	Firmato digitalmente da: Roberta Fusco Ruolo: DIRIGENTE INGEGNERE Organizzazione: IRCCS FONDAZIONE G. PASCALE/00911350635 Data: 05/02/2026 20:13:38	
	Elisa Pintauro	Ricercatore Sanitario	Firmato digitalmente da: Elisa Pintauro Ruolo: RICERCATORE SANITARIO DS Organizzazione: IRCCS FONDAZIONE G.PASCALE/00911350635 Data: 24/02/2026 09:40:51	
Revisione	Gianfranco De Feo	Quality Assurance	Firmato digitalmente da: Gianfranco De Feo Ruolo: DIRIGENTE SANITARIO Organizzazione: IRCCS FONDAZIONE G. PASCALE/00911350635 Data: 08/05/2026 18:03:34	
Approvazione	Maurizio Di Mauro	Titolare del trattamento dati	Firmato digitalmente da: Maurizio Di Mauro Ruolo: DIRETTORE GENERALE Organizzazione: IRCCS FONDAZIONE G. PASCALE/00911350635 Data: 12/05/2026 15:35:19	
	Alessandro Manzoni	DPO	Firmato digitalmente da: Alessandro Manzoni Ruolo: DIRIGENTE INGEGNERE Organizzazione: IRCCS FONDAZIONE G. PASCALE/00911350635 Data: 25/05/2026 14:21:54	
	Sara Falivene	Principal Investigator		
	Gianfranco De Feo	Quality Assurance		

Tracking delle modifiche

N° Rev.	Data	Motivo della modifica	Paragrafi
1.0	02.11.2025	Prima emissione	TUTTI

Storico della rivalutazione

Revisione annuale della DPIA o a seguito di verifiche/minacce

Aggiornamento della DPIA in caso di modifiche ai sistemi informativi istituzionali o alle normative

	Data prevista	Data effettiva	Firma
Rivalutazione a cura del QA			

Tabella dei Contenuti

1. Stima del rischio e pre-assessment

Il Data Protection Impact Assessment (DPIA) o "valutazione di impatto sulla protezione dei dati" rappresenta un processo, previsto dall'art. 35 del Regolamento UE 679/2016, inteso a descrivere i rischi correlati ad un trattamento dei dati personali, valutandone la necessità e proporzionalità, nonché contribuendo a gestire, attraverso l'adozione di specifiche misure, i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei propri dati personali.

Tipologia del trattamento	**Risposta**
Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato.	NO
Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).	NO
Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.	NO
Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 Regolamento UE 2016/679 interconnessi con altri dati personali raccolti per finalità diverse.	NO

Trattamenti su larga scala di dati aventi carattere estremamente personale: si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).	NO
Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).	NO
Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).	SI
Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogni qualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 (criteri WP 29).	NO
Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).	NO
Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.	NO
Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.	NO
Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.	NO

1.1 Stima del rischio

Criteri utilizzati per la stima del rischio	**Risposta**

Il trattamento comporta la valutazione o assegnazione di un punteggio inclusiva di profilazione e previsione	NO
Il trattamento prevede un processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente	NO
Il trattamento consiste in un'attività di monitoraggio sistematico	NO
Il trattamento coinvolge dati sensibili o dati aventi carattere altamente personale	SI
Il trattamento di dati avviene su larga scala	NO
Il trattamento comporta la creazione di corrispondenze o combinazione di insiemi di dati	NO
Il trattamento coinvolge categorie di interessati vulnerabili	SI
Il trattamento coinvolge l'uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative	NO
Il trattamento impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto	NO
Medio/Elevato	

2. Quadro normativo

Regolamento (UE) 679/2016 (GDPR);
D.lgs. 196/2003 e s.m.i. per effetto del D.lgs. 101/2018;
Articolo 29 Working Party (2017), Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" in base alle disposizioni contenute nel Regolamento (UE) 679/2016;
Provvedimento 146/2019 del Garante per la protezione dei dati personali.
Provvedimento 298/2024 del Garante per la protezione dei dati personali.

3. Contesto

3.1 Titolare e Responsabile della Protezione dei Dati

Titolare dei trattamenti dei Suoi dati personali effettuati presso il Centro di Sperimentazione Istituto Nazionale dei Tumori IRCCS di Napoli Fondazione G. Pascale è il Legale Rappresentante e la dr.ssa Sara Falivene in qualità di Principal Investigator

3.2 Soggetti interessati

L'attività interessa il trattamento di dati riguardanti:

- pazienti già in precedenza assistiti presso

ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI

- pazienti che hanno fornito in precedenza propri campioni biologici presso

Non applicabile

- soggetti arruolati in studi clinici o progetti di ricerca condotti presso

Non applicabile

- Altro

Non applicabile

RICHIESTA DEL PARERE DEGLI INTERESSATI RELATIVAMENTE ALLA DPIA

☐ È stato richiesto il parere degli interessati
X Non è stato richiesto il parere degli interessati

MOTIVAZIONE DELLA MANCATA RICHIESTA DEL PARERE ALLA DPIA DEGLI INTERESSATI

Le motivazioni per la mancata raccolta delle opinioni degli interessati nella DPIA sono:

- Tutti i dati clinici dei pazienti sono stati pseudonimizzati. Non vi è alcun utilizzo di dati biometrici, sensibili o correlati a individui identificabili.
- Non vi sono attività di profilazione o decisioni automatizzate che possano influire sugli interessati.

- Valutazione di Rischio: Determinazione che il rischio per i diritti e le libertà degli interessati è basso grazie a misure di protezione implementate e riportano nella DPIA.
- Autorizzazione generale del Garante n. 9/2016 → I trattamenti di dati sanitari per finalità di ricerca scientifica non richiedono necessariamente il coinvolgimento degli interessati nella valutazione d'impatto, se sono adottate misure di sicurezza adeguate.

3.3 Descrizione del trattamento

3.3.1 Quale è il trattamento in considerazione?

Il trattamento oggetto della presente valutazione d'impatto riguarda lo svolgimento dello studio osservazionale retrospettivo multicentrico denominato *"Radioterapia stereotassica per il trattamento di oligometastasi extracraniche da carcinoma mammario (ORIETTA)"*, promosso dall'IRCCS Humanitas Research Hospital, con la partecipazione dell'INT IRCCS Fondazione G. Pascale in qualità di centro collaboratore.
Lo studio ha finalità esclusivamente scientifiche e non comporta alcuna attività clinica o interventistica sui pazienti, poiché si basa sull'analisi di dati già raccolti nell'ambito dell'attività assistenziale. L'obiettivo è valutare, in una popolazione di soggetti adulti affetti da carcinoma mammario oligometastatico extracranico, l'efficacia e la tollerabilità della radioterapia stereotassica (SBRT) in termini di sopravvivenza libera da progressione, sopravvivenza globale, controllo locale e tossicità acute o tardive correlate al trattamento.
Il trattamento consiste nell'estrazione, raccolta, pseudonimizzazione, registrazione, analisi statistica e conservazione dei dati personali e sanitari presenti nelle cartelle cliniche dei pazienti trattati con SBRT tra il 2010 e il 2023. I dati vengono resi non direttamente identificabili mediante l'assegnazione di un codice univoco e successivamente inseriti in un database dedicato, accessibile esclusivamente al personale autorizzato. Non è prevista la raccolta di nuovi dati clinici né il contatto diretto con i soggetti interessati.
Le informazioni trattate comprendono dati anagrafici, demografici e clinici, nonché dati appartenenti a categorie particolari relativi allo stato di salute, alla storia clinica, alle caratteristiche della malattia, ai trattamenti oncologici ricevuti e ai risultati delle indagini diagnostiche. Tutti i dati sono trattati nel rispetto dei principi di liceità, correttezza, minimizzazione e limitazione della conservazione, secondo quanto previsto dal Regolamento (UE) 2016/679 e dal D.Lgs. 196/2003.
Il trattamento è effettuato per finalità di ricerca scientifica in ambito medico, sanitaria e biomedica, in conformità alla missione istituzionale degli Istituti di Ricovero e Cura a Carattere Scientifico (IRCCS), e si basa su un processo standardizzato di gestione dei dati pseudonimizzati, volto a garantire la protezione dei diritti e delle libertà fondamentali dei soggetti i cui dati sono utilizzati.

3.3.2 Quali sono le responsabilità connesse al trattamento?

Nel progetto, le responsabilità connesse al trattamento dei dati personali coinvolgono vari attori e possono essere suddivise come segue:

1. Titolare del Trattamento (Data Controller)

Il Titolare del Trattamento per il Centro di Sperimentazione è l'IRCCS Fondazione G. Pascale.

Responsabilità:

- Determinare le Finalità e i Mezzi del Trattamento: Decidere come e perché i dati personali devono essere trattati.
- Garantire la Conformità al GDPR: Assicurarsi che tutte le attività di trattamento siano conformi alle disposizioni del Regolamento Generale sulla Protezione dei Dati (GDPR).
- Informativa sulla Privacy: Fornire informazioni chiare e trasparenti agli interessati riguardo al trattamento dei loro dati.
- Consenso Informato: ottenere il consenso informato per la parte prospettica. Per la parte retrospettiva potranno essere inclusi i pazienti deceduti o non contattabili ai sensi dell'art. 110-bis, comma 4, del Codice Privacy, per evitare bias di selezione, nel rispetto della volontà eventualmente espressa in vita di non voler partecipare. I dati saranno trattati in forma pseudonimizzata e con misure di sicurezza idonee a tutelare i diritti e le libertà degli interessati.
- Coordinare e pubblicare la presente Valutazione di Impatto (DPIA) ai sensi dell'art. 110-bis, comma 4, Codice Privacy per identificare e mitigare i rischi associati al trattamento
- Gestione dei Diritti degli Interessati: Assicurarsi che gli interessati possano esercitare i loro diritti (accesso, rettifica, cancellazione, ecc.).
- Sicurezza dei Dati: Implementare misure tecniche e organizzative adeguate a proteggere i dati personali.

2. Responsabile della Protezione dei Dati (Data Protection Officer - DPO)

Il DPO è una figura obbligatoria per alcuni tipi di trattamento e ha il compito di garantire che l'IRCCS INT Napoli rispetti le normative sulla protezione dei dati.

Responsabilità:

Monitoraggio della Conformità: Verificare che il progetto rispetti le normative sulla protezione dei dati.

Consulenza e Formazione: Fornire consulenza al responsabile del trattamento e ai dipendenti riguardo agli obblighi del GDPR e delle altre normative.

Punto di Contatto: Agire come punto di contatto per gli interessati e per le autorità di controllo.

3. Preposto autorizzato al trattamento

Per codesto progetto, questo ruolo è stato delegato alla dott. Sara Falivene.

Responsabilità:

Trattamento su Istruzioni: Trattare i dati personali solo su istruzioni documentate del responsabile del trattamento.

Sicurezza dei Dati: Adottare misure tecniche e organizzative adeguate a garantire la sicurezza dei dati personali.
Sub-responsabili: Informare il responsabile del trattamento e ottenere l'autorizzazione per l'eventuale coinvolgimento di sub-responsabili (sub-processors).
Assistenza al Responsabile del Trattamento: Assistere il responsabile del trattamento nel garantire la conformità alle normative, inclusa la gestione dei diritti degli interessati e la notifica delle violazioni dei dati.
Collaborare con il Titolare e con il DPO per monitorare la conformità dello studio al GDPR e per gestire le richieste degli interessati (accesso, rettifica, limitazione, opposizione)

4. Personale Coinvolto nel Trattamento
Il personale che tratta i dati personali deve essere adeguatamente formato e consapevole delle proprie responsabilità.
Responsabilità:
Riservatezza: Mantenere la riservatezza delle informazioni personali trattate.
Conformità alle Politiche Aziendali: Seguire le politiche e le procedure aziendali relative alla protezione dei dati.
Segnalazione di Incidenti: Segnalare tempestivamente eventuali incidenti di sicurezza o violazioni dei dati.

5. Partecipanti allo Studio
I partecipanti allo studio devono essere adeguatamente informati.
Responsabilità:
Seguire le procedure operative standard (SOP): Raccogliere, conservare e trasferire i dati clinici secondo le linee guida stabilite nel protocollo dello studio.
Garantire la riservatezza: Trattare i dati in modo anonimo e rispettare il principio di minimizzazione, limitando il trattamento ai dati strettamente necessari per gli scopi dello studio.
Rispettare i diritti degli interessati: Garantire che gli interessati possano esercitare i loro diritti, come l'accesso ai dati, la rettifica e il ritiro del consenso.

3.3.3 Ci sono standard applicabili al trattamento?

Ci sono diversi standard e normative applicabili al trattamento dei dati personali nel contesto del progetto. Ecco i principali:

1. Regolamento Generale sulla Protezione dei Dati (GDPR)
Il GDPR è il principale standard legale per la protezione dei dati personali nell'Unione Europea. Ecco alcuni dei requisiti chiave:
Principi del Trattamento dei Dati: I dati personali devono essere trattati in modo lecito, corretto e trasparente; raccolti per finalità determinate, esplicite e legittime; adeguati, pertinenti e limitati a quanto necessario; esatti e, se necessario, aggiornati; conservati in una forma che consenta l'identificazione degli interessati per un periodo non superiore al necessario; trattati in modo da garantire la sicurezza adeguata dei dati.

Diritti degli Interessati: Gli interessati hanno il diritto di accesso, rettifica, cancellazione, limitazione del trattamento, portabilità dei dati e opposizione al trattamento.
Valutazione d'Impatto sulla Protezione dei Dati (DPIA): Necessaria quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
Sicurezza dei Dati: Obbligo di implementare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.
Notifica di Violazione dei Dati: Obbligo di notificare le violazioni dei dati personali all'autorità di controllo entro 72 ore e, in certi casi, agli interessati.

2. Norme di sicurezza della infrastruttura e dei sistemi elettronici
Presso l'IRCCS INT Napoli sono previste delle specifiche procedura di sicurezza per i sistemi elettronici (penetration test; firewall; back-up; disaster recovery; antivirus; verifica integrità dati back-up) nonché procedure di archiviazione dati storici (abilitazione accesso, consultazione, decommissioning, migrazione del dato, ecc…).
Con cadenza semestrale viene effettuato un risk assesment da parte di un ente terzo relativamente alla sicurezza dei suddetti sistemi.

3. Linee Guida del Comitato Europeo per la Protezione dei Dati (EDPB)
Il Comitato Europeo per la Protezione dei Dati (EDPB) pubblica linee guida, raccomandazioni e best practice per l'applicazione del GDPR.
Linee guida sulla DPIA: Forniscono dettagli su quando e come condurre una DPIA.
Linee guida sulla Trasparenza: Dettagli su come fornire informazioni agli interessati in modo trasparente e comprensibile.
Linee guida sulla Sicurezza dei Dati: Raccomandazioni sulle misure di sicurezza tecniche e organizzative da adottare.

4. Direttive Nazionali e Linee Guida Specifiche per la Ricerca Clinica
A seconda del paese, possono esserci direttive nazionali aggiuntive e linee guida specifiche per la ricerca clinica che devono essere seguite.
Linee guida di AIFA (Agenzia Italiana del Farmaco): In Italia, AIFA fornisce linee guida per la conduzione di sperimentazioni cliniche, inclusi gli aspetti di protezione dei dati.
Leggi Nazionali sulla Protezione dei Dati: Ogni paese può avere leggi specifiche che integrano o dettagliano ulteriormente i requisiti del GDPR.

5. Linee Guida etiche
Dichiarazione di Helsinki: Principi etici per la ricerca medica che coinvolge soggetti umani, sviluppata dall'Associazione Medica Mondiale (WMA).
Linee Guida ICH-GCP (Good Clinical Practice): Standard internazionale per la progettazione, conduzione, registrazione e reporting di studi clinici che coinvolgono soggetti umani.

6. Standard di sicurezza e qualità applicati
- Good Clinical Practice (ICH-GCP E6 R2).
- Good Pharmacoepidemiology Practices (GPP).
- ISO/IEC 27001 per la gestione della sicurezza delle informazioni.

- ISO/IEC 27002, 27017, 27018, ove applicabili, per la protezione dei dati in ambienti cloud e sanitari.
- 21 CFR Part 11 (FDA, per sistemi elettronici conformi).
- OSSTMM e OWASP per la sicurezza delle applicazioni web (es. piattaforma eCRF).
- NIST SP 800-115 per il penetration testing e la gestione dei rischi IT.
- Standard di pseudonimizzazione e crittografia riconosciuti a livello europeo.

3.4 Dati, processi e risorse di supporto

3.4.1 Quali sono i dati trattati?

Nell'ambito dello studio osservazionale retrospettivo *ORIETTA*, vengono trattati esclusivamente i dati personali pertinenti e necessari al raggiungimento delle finalità scientifiche descritte nel protocollo di studio, nel pieno rispetto del principio di minimizzazione.
I dati trattati derivano dalle cartelle cliniche e dalla documentazione sanitaria dei pazienti affetti da carcinoma mammario oligometastatico extracranico trattati con radioterapia stereotassica (SBRT) tra il 2010 e il 2023. Essi comprendono:

- Dati identificativi e demografici, limitatamente a quelli necessari per la corretta gestione dello studio: età al momento del trattamento, sesso, altezza, peso, etnia.
- Dati clinici e anamnestici, quali: stadio della malattia, caratteristiche istologiche e molecolari del tumore, tipo di mutazioni alla diagnosi iniziale e alla seconda linea di trattamento, data di insorgenza e progressione della patologia, informazioni sulle linee terapeutiche precedenti (tipologia di trattamento, data di inizio e fine, eventuali modifiche di dose).
- Dati relativi al trattamento radioterapico, comprendenti: dose somministrata, frazionamento, sede delle lesioni trattate, effetti collaterali, valutazioni della risposta radiologica e follow-up clinico.
- Dati relativi allo stato di salute e agli esiti, come la sopravvivenza libera da progressione (PFS), la sopravvivenza globale (OS), il controllo locale della malattia e le tossicità acute e tardive correlate alla radioterapia.

3.4.2 Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Il trattamento dei dati nell'ambito dello studio si articola nelle seguenti fasi funzionali:

1. Raccolta
   All'atto dell'arruolamento dei partecipanti, i dati personali e sanitari vengono raccolti dai Centri clinici partecipanti. È acquisito il consenso informato, e contestualmente si procede all'attribuzione di un codice identificativo pseudonimizzato per ciascun partecipante.
2. Trasmissione / Inserimento e codifica
   I Centri inseriscono i dati nel database centralizzato o li trasmettono al promotore tramite canali sicuri (ad esempio piattaforma web protetta, protocolli crittografati). I

dati trasmessi sono pseudonimizzati: il collegamento tra codice e identità reale resta custodito presso il Centro di origine. In questa fase si può anche prevedere il trasferimento di campioni biologici o dati molecolari dove previsto (sempre secondo le modalità previste dal protocollo e con misure di sicurezza).

3. Archiviazione temporanea e gestione operativa
   Una volta acquisiti nel sistema, i dati vengono archiviati in struttura controllata (server protetti, database dedicati, oppure archivi cartacei dove necessari), e resi accessibili solo al personale autorizzato (es. data-manager dello studio, ricercatori abilitati, monitor). I dati vengono utilizzati per le attività specifiche previste dallo studio: analisi statistiche, monitoraggio della qualità, raccolta dei follow-up, generazione di report e pubblicazioni aggregate.
4. Utilizzo / elaborazione
   Durante la durata dello studio, i dati vengono elaborati ai fini della finalità di ricerca: analisi cliniche, valutazioni esiti, correlazioni, eventualmente analisi molecolari, elaborazioni statistiche. In ogni caso i dati sono trattati in forma pseudonimizzata, salvo quando è necessario mantenere il collegamento al partecipante (ad esempio in caso di aggiornamento del follow-up). Le eventuali pubblicazioni risultanti dallo studio utilizzano solo dati aggregati o non identificativi, in modo da garantire la riservatezza dell'interessato.
5. Conservazione
   Una volta terminata la raccolta attiva dei dati e concluso il periodo previsto per il follow-up, i dati resteranno conservati per il periodo indicato dal protocollo al fine di consentire controlli, audit, eventuali verifiche da parte delle autorità competenti, oppure studi secondari previsti dal piano di ricerca. Alla scadenza del periodo, oppure al termine della finalità per cui sono trattati, si procede all'anonimizzazione o cancellazione dei dati, conformemente al principio di limitazione della conservazione.
6. Verifica/audit/controllo
   Durante tutto il ciclo di vita, sono previste attività di verifica della qualità dei dati, audit interni.

3.4.3 Quali sono le risorse di supporto ai dati?

Le risorse di supporto ai dati utilizzate presso l'IRCCS "Fondazione Pascale" comprendono:

- Infrastrutture informatiche interne dell'Istituto, quali server sicuri, sistemi di archiviazione protetti e reti riservate per l'accesso ai dati pseudonimizzati.
- Sistemi di gestione documentale e clinica già in uso presso il centro, che consentono la consultazione dei dati retrospettivi.
- Supporti cartacei e fisici conservati in archivi ad accesso controllato, per eventuali documentazioni cliniche non digitalizzate.
- Il trattamento dei dati presso il centro avviene in ambiente protetto, con accesso riservato al solo personale autorizzato, in conformità alle misure tecniche e organizzative adottate per garantire la riservatezza, l'integrità e la disponibilità dei dati personali trattati.

Queste risorse costituiscono il presidio tecnico-organizzativo del trattamento e assicurano che i dati siano trattati in conformità al GDPR, al Codice Privacy e agli standard internazionali applicabili.

Inoltre, l'IRCCS INT Napoli ha effettuato una "VALUTAZIONE DI IMPATTO EX ART. 35 DEL REGOLAMENTO UE 2016/679 – RICERCA SCIENTIFICA E SPERIMENTAZIONE CLINICA" (delibera 677/2024)

4. Valutazione di necessità e proporzionalità del trattamento

4.1 Proporzionalità e necessità

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

Gli scopi del trattamento sono specifici, espliciti e legittimi, in quanto chiaramente individuati nel protocollo di studio *ORIETTA* e coerenti con la missione scientifica degli Istituti di Ricovero e Cura a Carattere Scientifico (IRCCS).
Il trattamento dei dati personali è finalizzato esclusivamente alla conduzione di una ricerca osservazionale retrospettiva multicentrica volta a valutare l'efficacia e la sicurezza della radioterapia stereotassica (SBRT) nel trattamento delle oligometastasi extracraniche da carcinoma mammario, attraverso l'analisi dei dati clinici raccolti nella normale pratica sanitaria.
In particolare, le finalità specifiche dello studio comprendono:

- la valutazione della sopravvivenza libera da progressione (PFS) come endpoint primario;
- la valutazione del controllo locale, della sopravvivenza globale (OS) e della tossicità acuta e tardiva correlata alla radioterapia come endpoint secondari;
- la produzione di conoscenze scientifiche utili al miglioramento delle strategie terapeutiche per pazienti affetti da carcinoma mammario oligometastatico, a beneficio della comunità clinica e scientifica.

Gli scopi del trattamento sono, pertanto:

- specifici, in quanto determinati in modo preciso dal protocollo approvato dal Comitato Etico e non suscettibili di utilizzi diversi da quelli di ricerca scientifica;
- espliciti, poiché chiaramente comunicati nelle informazioni fornite ai pazienti e riportati nei documenti di studio, nel rispetto dei principi di trasparenza e accountability;
- legittimi, in quanto riconducibili all'attività di ricerca scientifica in ambito sanitario, lecita ai sensi dell'art. 9, par. 2, lett. j) del Regolamento (UE) 2016/679 e dell'art. 110-bis del D.Lgs. 196/2003, che consentono agli IRCCS il trattamento dei dati raccolti per finalità di cura anche per scopi di ricerca biomedica.

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

Il trattamento dei dati personali svolto nell'ambito dello studio è lecito ai sensi della normativa europea e nazionale in materia di protezione dei dati personali, e si fonda sulle seguenti basi giuridiche:

1. Per i dati personali comuni:
    - Art. 6, par. 1, lett. e) del GDPR – Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico, in quanto lo studio è finalizzato alla ricerca scientifica in ambito sanitario, condotta da un ente pubblico (IRCCS "Fondazione Pascale") ai sensi del proprio mandato istituzionale.
2. Per i dati particolari (dati relativi alla salute):
    - Art. 9, par. 2, lett. j) del GDPR – Il trattamento è necessario per finalità di ricerca scientifica, nel rispetto delle condizioni e delle garanzie previste dall'art. 89 del GDPR.
3. Normativa nazionale di riferimento:
    - Art. 110-bis del Codice Privacy (D.lgs. 196/2003 e s.m.i.) – Il trattamento è consentito anche in assenza del consenso per i pazienti deceduti o non contattabili, qualora lo studio sia stato approvato da un Comitato Etico competente e vengano rispettate le misure di garanzia individuate dal Garante per la Protezione dei Dati Personali (es. pseudonimizzazione, minimizzazione, limitazione dell'accesso).
4. Consenso informato (se previsto):
    - Per i soggetti raggiungibili, il trattamento è effettuato anche sulla base del consenso informato scritto, ai sensi dell'art. 7 del GDPR, nel quale è illustrata la finalità scientifica e il trattamento dei dati.

4.1.3 I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

I dati personali trattati nell'ambito dello studio *ORIETTA* sono adeguati, pertinenti e limitati a quanto strettamente necessario per perseguire le finalità scientifiche previste dal protocollo, in conformità al principio di minimizzazione di cui all'art. 5, par. 1, lett. c) del Regolamento (UE) 2016/679.
Il trattamento riguarda esclusivamente le informazioni indispensabili per valutare l'efficacia e la sicurezza della radioterapia stereotassica (SBRT) nel carcinoma mammario oligometastatico extracranico. I dati vengono selezionati in base agli endpoint dello studio (sopravvivenza libera da progressione, sopravvivenza globale, controllo locale e tossicità) e includono solo le variabili cliniche e demografiche necessarie a tali analisi.
Non sono raccolti né trattati dati eccedenti, non pertinenti o non correlati agli obiettivi della ricerca. In particolare:

- i dati anagrafici sono utilizzati unicamente per consentire l'identificazione interna e la corretta gestione della codifica dei soggetti;
- i dati clinici derivano dalle cartelle sanitarie preesistenti e sono limitati a quelli utili per l'analisi statistica prevista.

Prima dell'inserimento nei database di studio, i dati sono pseudonimizzati, riducendo così al minimo le informazioni identificative. La chiave di collegamento è conservata separatamente e accessibile solo al personale clinico autorizzato.
L'approccio metodologico previsto dal promotore e adottato anche dal centro partecipante (IRCCS Pascale) garantisce che ogni fase del trattamento sia improntata alla riduzione al minimo dei dati, assicurando che non vengano raccolte informazioni aggiuntive rispetto a quelle strettamente necessarie e che ogni trattamento sia proporzionato alle finalità di ricerca dichiarate.

4.1.4 I dati sono esatti e aggiornati?

I dati personali trattati nello studio osservazionale retrospettivo *ORIETTA* sono esatti, completi e coerenti con la documentazione sanitaria originale, in conformità al principio di accuratezza di cui all'art. 5, par. 1, lett. d) del Regolamento (UE) 2016/679.
Poiché lo studio ha natura retrospettiva, le informazioni derivano da cartelle cliniche, referti diagnostici e registrazioni sanitarie ufficiali già presenti nei sistemi informativi dei centri partecipanti. Tali fonti sono ritenute affidabili e validate, in quanto prodotte e conservate nell'ambito dell'attività assistenziale secondo le regole di buona pratica clinica e le normative sanitarie vigenti.
Durante la fase di estrazione dei dati, il personale clinico e di ricerca appositamente autorizzato effettua un controllo di coerenza e congruenza tra i dati riportati nella documentazione sorgente (source documents) e quelli inseriti nella base dati pseudonimizzata dedicata allo studio. Eventuali incongruenze o errori vengono verificati e corretti prima della validazione finale, garantendo l'affidabilità del dataset utilizzato per l'analisi scientifica.

4.1.5 Qual è il periodo di conservazione dei dati?

I dati personali trattati nell'ambito dello studio osservazionale retrospettivo ORIETTA vengono conservati per un periodo massimo di sette anni successivo alla conclusione dello studio e alla redazione dei risultati scientifici.

Tale periodo è determinato in conformità alle prassi di conservazione previste per gli studi clinici e osservazionali e risponde all'esigenza di garantire la verificabilità e la tracciabilità dei dati utilizzati a fini scientifici, regolatori e di rendicontazione.

Durante tutto il periodo di conservazione, i dati restano pseudonimizzati e custoditi in archivi elettronici protetti, accessibili esclusivamente al personale autorizzato dal promotore e dai centri partecipanti. Decorso il termine previsto, i dati saranno cancellati o definitivamente anonimizzati, secondo le procedure interne del promotore e nel rispetto della normativa vigente in materia di protezione dei dati personali e di buona pratica clinica.

4.2 Misure a tutela dei diritti degli interessati

4.2.1 Come sono informati del trattamento gli interessati?

Gli interessati sono informati in modo chiaro, completo e trasparente mediante:

1. Scheda informativa e modulo di consenso informato
   Ai soggetti raggiungibili viene consegnata una scheda informativa (Informativa privacy conforme agli artt. 13 e 14 del GDPR), redatta in linguaggio comprensibile e approvata dal Comitato Etico competente.
   L'informativa descrive:
   - le finalità del trattamento;
   - le categorie di dati trattati (clinici, radiologici);
   - le basi giuridiche del trattamento;
   - le modalità di conservazione e trasferimento;
   - i diritti dell'interessato (accesso, rettifica, limitazione, opposizione, cancellazione ove applicabile);
   - i riferimenti del Titolare e del DPO.
2. Accesso informato e consenso esplicito
   Il paziente può porre domande e ricevere chiarimenti prima della firma del consenso informato. Il consenso al trattamento dei dati è acquisito separatamente da quello alla partecipazione allo studio clinico, come previsto dagli artt. 7 e 13 del GDPR.
3. Per i soggetti deceduti o non contattabili si applicano le deroghe previste dagli artt. 14.5 e 110-bis del Codice Privacy, in presenza di approvazione del Comitato Etico e garanzie adeguate (pseudonimizzazione, minimizzazione, limitazione dell'accesso).

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

Per i pazienti contattabili, il consenso al trattamento dei dati personali, inclusi quelli appartenenti a categorie particolari (dati sanitari e genetici), viene ottenuto in forma scritta attraverso la procedura di consenso informato, in conformità agli articoli 6(1)(a) e 9(2)(a) del GDPR.

Modalità di acquisizione del consenso

- Il personale sanitario del centro fornisce al paziente:
  - Il foglio informativo contenente le finalità dello studio e i dettagli sul trattamento dei dati,
  - Il modulo di consenso informato (ICF) da firmare.
- Il consenso è raccolto prima dell'inizio di qualsiasi trattamento o inserimento dati nello studio.
- Viene garantito che:
  - Il paziente comprenda appieno le informazioni ricevute,
  - Il consenso sia libero, specifico, informato e inequivocabile.
- Il modulo firmato viene archiviato localmente presso il centro sperimentale, in copia cartacea o digitale, in conformità alle regole interne dell'Istituto.

Revoca del consenso

- Il paziente ha diritto a revocare il consenso in qualsiasi momento, senza pregiudicare la liceità del trattamento già effettuato.
- La revoca è comunicata per iscritto al centro, che provvede alla cessazione del trattamento e alla relativa annotazione nel sistema.

Questa modalità garantisce il pieno rispetto del principio di liceità del trattamento, così come previsto dall'art. 5 del GDPR.

4.2.3 Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

Nel contesto dello studio in oggetto, gli interessati (pazienti partecipanti) hanno il diritto di esercitare i loro diritti di accesso e di portabilità dei dati in conformità con il Regolamento Generale sulla Protezione dei Dati (GDPR). Ecco come possono esercitare questi diritti:

Diritto di Accesso

Il diritto di accesso consente ai pazienti viventi di ottenere conferma se i loro dati personali sono trattati e, in tal caso, di accedere a tali dati insieme ad alcune informazioni aggiuntive.

Procedura per Esercitare il Diritto di Accesso

1. **Richiesta di Accesso**:
   - I pazienti possono presentare una richiesta di accesso ai loro dati personali. La richiesta può essere effettuata al DPO.
   - Informazioni di contatto per le richieste di accesso sono generalmente fornite nel documento di informativa al trattamento dei dati e includono l'indirizzo e-mail del DPO.
2. **Verifica dell'Identità**:
   - Prima di fornire l'accesso ai dati, l'Istituto verificherà l'identità del richiedente per garantire che i dati personali siano rilasciati alla persona corretta. Questo può includere la richiesta di una copia di un documento d'identità.
3. **Fornitura delle Informazioni**:
   - Una volta verificata l'identità, l'Istituto fornirà una copia dei dati personali richiesti. Questo include le informazioni sui dati specifici raccolti, le finalità del trattamento, le categorie di dati trattati e qualsiasi altra informazione richiesta dal GDPR.
   - Le informazioni saranno fornite in un formato chiaro e comprensibile.

Diritto di Portabilità dei Dati

Il diritto di portabilità dei dati consente ai pazienti di ottenere i loro dati personali in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e di trasmetterli a un altro titolare del trattamento senza impedimenti.

Procedura per Esercitare il Diritto di Portabilità dei Dati

1. **Richiesta di Portabilità**:
   - I pazienti possono presentare una richiesta per ottenere i loro dati personali in un formato portabile. La richiesta può essere effettuata al DPO.

- Informazioni di contatto per le richieste di accesso sono generalmente fornite nel documento di informativa al trattamento dei dati e includono l'indirizzo e-mail del DPO.

2. **Verifica dell'Identità**:
   - Come per il diritto di accesso, l'Istituto verificherà l'identità del richiedente per garantire che i dati personali siano rilasciati alla persona corretta.
3. **Fornitura dei Dati**:
   - I dati personali saranno forniti in un formato strutturato, di uso comune e leggibile da dispositivo automatico (ad esempio, formato CSV o XML).
   - Se richiesto, i dati possono essere trasmessi direttamente a un altro titolare del trattamento indicato dal paziente, a condizione che ciò sia tecnicamente fattibile.

Contatti per Esercitare i Diritti

- **DPO**: Ing. Alessandro Manzoni
  - **E-mail**: a.manzoni@istitutotumori.na.it
- **Principal Investigator**: Dott. Sara Falivene
  - **E-mail**: sara.falivene@istitutotumori.na.it

Gli interessati possono esercitare i loro diritti di accesso e di portabilità dei dati attraverso una procedura chiara e strutturata. Le informazioni necessarie per effettuare queste richieste sono fornite nel documento di consenso informato e attraverso i contatti del personale dello studio. L'Istituto assicura che tutte le richieste siano gestite in conformità con le normative del GDPR, garantendo che i dati personali siano accessibili e portabili in modo sicuro e trasparente.

4.2.4 Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Gli interessati possono esercitare i propri diritti di rettifica (art. 16 GDPR) e cancellazione (art. 17 GDPR, "diritto all'oblio") rivolgendosi:

Al Titolare locale (Centro sperimentale – Istituto Pascale)

- Gli interessati possono presentare una richiesta scritta al Responsabile della Protezione dei Dati (RPD/DPO) del centro.
- La richiesta deve contenere l'indicazione del diritto che si intende esercitare (es. rettifica, cancellazione, limitazione) e i riferimenti necessari all'identificazione del paziente.
- Il centro, in quanto titolare autonomo del trattamento, è responsabile della gestione iniziale della richiesta.

Limiti applicabili al diritto all'oblio
In conformità all'art. 17(3)(d) GDPR e all'art. 110 del Codice Privacy, il diritto alla cancellazione può essere limitato nei casi in cui il trattamento sia necessario per fini di ricerca scientifica, a condizione che:

- I dati siano pseudonimizzati e
- L'ulteriore trattamento non comporti rischi elevati per i diritti e le libertà dell'interessato.

In questi casi, la richiesta può non essere accolta, ma deve comunque essere valutata e formalmente riscontrata entro 30 giorni.

4.2.5 Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Gli interessati possono esercitare i propri diritti di limitazione del trattamento (art. 18 GDPR) e di opposizione al trattamento (art. 21 GDPR) rivolgendosi al centro sperimentale secondo modalità chiare e accessibili.

Contatto con il Centro sperimentale (Istituto Pascale)

- L'interessato può presentare richiesta scritta al Responsabile della Protezione dei Dati (RPD/DPO) del centro, indicando:
  - Il diritto che intende esercitare (limitazione o opposizione),
  - Il motivo specifico (es. contestazione dell'esattezza dei dati, motivi personali o etici).
- Il centro valuta la richiesta come titolare autonomo e, se necessario, coordina l'applicazione del diritto con il promotore.

Eccezioni e limiti

- Il diritto di opposizione può essere limitato se il trattamento è effettuato per finalità di ricerca scientifica, come previsto dall'art. 21(6) e 89(2) GDPR, salvo che l'interessato non dimostri motivi legittimi prevalenti.
- Il diritto alla limitazione può essere esercitato, ad esempio, durante la verifica di accuratezza dei dati o in attesa di una decisione sulla richiesta di cancellazione.

4.2.6 Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Nel contesto dello studio, qualora vengano coinvolti soggetti terzi con la funzione di responsabile del trattamento o sub-responsabile, è previsto che tali soggetti siano formalmente incaricati tramite un contratto o altro atto giuridico conforme alla normativa applicabile.

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

Non è previsto il trasferimento dei dati al di fuori dell'Unione europea.

5. Motivi della valutazione d'impatto

La valutazione d'impatto sulla protezione dei dati (DPIA) è stata condotta in quanto il trattamento dei dati personali previsto dallo studio *ORIETTA* presenta caratteristiche che, in base al Regolamento (UE) 2016/679 e alle Linee guida del Gruppo di lavoro Articolo 29 (WP 248 rev.01), possono comportare un rischio elevato per i diritti e le libertà degli interessati.
In particolare, il trattamento soddisfa più di due dei criteri individuati dall'European Data Protection Board per cui la DPIA risulta necessaria, e precisamente:

- trattamento di categorie particolari di dati, in quanto vengono utilizzati dati relativi alla salute dei pazienti oncologici, talvolta associati a informazioni genetiche o cliniche sensibili;
- presenza di soggetti vulnerabili, trattandosi di pazienti oncologici in condizioni cliniche delicate;
- uso di sistemi informatici dedicati e piattaforme elettroniche per la raccolta, pseudonimizzazione e gestione dei dati di ricerca.

Inoltre, la DPIA si rende opportuna in ragione della natura retrospettiva dello studio, che comporta il riutilizzo di dati clinici originariamente raccolti per finalità di cura e successivamente trattati per scopi di ricerca scientifica. Tale modalità richiede una valutazione puntuale delle misure tecniche e organizzative adottate per garantire la riservatezza, la sicurezza e la minimizzazione del rischio di reidentificazione.
La DPIA è pertanto finalizzata a:

- analizzare i rischi connessi al trattamento di dati sanitari e genetici su larga scala;
- valutare la correttezza e adeguatezza delle misure tecniche e organizzative adottate dai centri partecipanti e dal promotore;
- garantire la piena conformità dello studio al Regolamento (UE) 2016/679, al D.lgs. 196/2003 s.m.i. e alle Linee guida del Garante per la protezione dei dati personali in materia di ricerca scientifica.

6. Valutazione dei Rischi

Per ogni trattamento vengono individuati gli asset direttamente o indirettamente ad esso collegati. Per ognuno di essi, il processo di analisi dei rischi esamina le vulnerabilità, le relative minacce, e le contromisure, dirette o indirette, attuate, fornendo il livello di rischio. Tale livello tiene anche conto della probabilità e dell'impatto che l'attuazione della minaccia avrebbe sui dati personali trattati, per mezzo degli specifici asset.
In tal senso si procede ad individuare una scala di indice dei rischi da un livello di rischio molto basso sino ad un livello molto alto.

6.1 Accesso illegittimo ai dati

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

Violazione della privacy, Implicazioni psicologiche e sociali, Discriminazione, Costi, Diffusione risultati della ricerca

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

Vulnerabilità informatiche, attacco basato su chiave compromessa, attacco denial of service di rete, spoofing d'identità, attacco man in the middle, attacco di riproduzione RTP, virus, worm, phishing, malware.
Locale lasciato aperto o non custodito.
Trasmissione informatica o comunicazione verbale di dati personali a soggetti non autorizzati.
Accesso e/o trattamento dei dati personali per finalità diverse da quelle autorizzate.
Allontanarsi dalla propria postazione lasciando il PC connesso.
Copiare i dati su dispositivi removibili e trasportabili all'esterno senza autorizzazione.
Modifica accidentale dei dati.
Cancellazione accidentale dei dati.
Inoltro di dati a soggetti non autorizzati a conoscerli.
Emergenza non sanitaria con impatto sul sistema informatico (incendio, alluvione, terremoto).

6.1.3 Quali sono le fonti di rischio?

Umano, Strumenti vulnerabili.

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

Pseudonimizzazione, Sicurezza dei canali informatici, Procedure di sicurezza dei sistemi elettronici, Controllo degli accessi logici, Formazione e Sensibilizzazione, Tracciabilità, Politica di tutela della privacy, Minimizzazione dei dati, Limitazione dell'Accesso ai Dati, Accesso controllato ai locali, Audit e monitoraggi periodici; Contrattualizzazione con Responsabili Esterni.

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

Importante/Grave

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

Poco Probabile

6.2 Modifiche indesiderate dei dati

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

Violazione della privacy, Implicazioni psicologiche e sociali, Discriminazione, Costi, Diffusione risultati della ricerca

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

Vulnerabilità informatiche, attacco basato su chiave compromessa, attacco denial of service di rete, spoofing d'identità, attacco man in the middle, attacco di riproduzione RTP, virus, worm, phishing, malware.
Locale lasciato aperto o non custodito.
Trasmissione informatica o comunicazione verbale di dati personali a soggetti non autorizzati.
Accesso e/o trattamento dei dati personali per finalità diverse da quelle autorizzate.
Allontanarsi dalla propria postazione lasciando il PC connesso.
Copiare i dati su dispositivi removibili e trasportabili all'esterno senza autorizzazione.
Modifica accidentale dei dati.
Cancellazione accidentale dei dati.
Inoltro di dati a soggetti non autorizzati a conoscerli.
Emergenza non sanitaria con impatto sul sistema informatico (incendio, alluvione, terremoto).

6.2.3 Quali sono le fonti di rischio?

Strumenti vulnerabili, Umano

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

Pseudonimizzazione, Formazione e Sensibilizzazione, Minimizzazione dei dati, Limitazione dell'Accesso ai Dati, Sicurezza dei canali informatici, Procedure di sicurezza dei sistemi elettronici, Controllo degli accessi logici, Tracciabilità, Politica di tutela della privacy, Accesso controllato ai locali, Audit e monitoraggi periodici, Conservazione e archiviazione dei dati.

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

Importante/Grave

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

Poco probabile

6.3 Perdita di dati

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

Implicazioni psicologiche e sociali, Violazione della privacy, Costi, Diffusione risultati della ricerca

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

Cancellazione accidentale dei dati.
Emergenza non sanitaria con impatto sul sistema informatico (incendio, alluvione, terremoto).
Modifica accidentale dei dati, vulnerabilità informatiche, attacco basato su chiave compromessa, attacco denial of service di rete, spoofing d'identità, attacco man in the middle, attacco di riproduzione RTP, virus, worm, phishing, malware.
Locale lasciato aperto o non custodito.
Allontanarsi dalla propria postazione lasciando il PC connesso.

6.3.3 Quali sono le fonti di rischio?

Strumenti vulnerabili, Umano.

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

Formazione e Sensibilizzazione, Sicurezza dei canali informatici, Limitazione dell'Accesso ai Dati, Controllo degli accessi logici, Accesso controllato ai locali, Procedure di sicurezza dei sistemi elettronici; Conservazione e archiviazione dei dati.

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

Grave/Importante

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

Poco Probabile

7. Piano d'azione

7.1 Mitigazione dei rischi con Misure esistenti o pianificate

7.1.1 Pseudonimizzazione

Nel contesto dello studio osservazionale retrospettivo *ORIETTA*, i dati personali dei pazienti vengono pseudonimizzati, come descritto nei documenti di riferimento del progetto.
Dopo la selezione dei soggetti eleggibili, ai dati viene assegnato un codice univoco che non corrisponde all'ID paziente e non consente l'identificazione diretta dell'interessato (ad esempio tramite nome, cognome o codice fiscale). La chiave di collegamento tra tale codice e i dati identificativi è conservata in modo separato, in una cartella di rete protetta e ad accesso limitato, disponibile solo al personale clinico autorizzato del centro sperimentale o al Principal Investigator.
Tutti i dati utilizzati per le analisi statistiche e scientifiche sono quindi pseudonimizzati, e nessuna informazione direttamente identificativa (nome, indirizzo, contatti, ecc.) viene trasmessa al promotore o agli altri centri partecipanti.
Questa modalità di trattamento, come riportato nei documenti, garantisce che le informazioni raccolte siano utilizzabili per le finalità di ricerca, mantenendo al tempo stesso un elevato livello di tutela della riservatezza e della sicurezza dei pazienti coinvolti.

7.1.2 Formazione e Sensibilizzazione

Il personale coinvolto nel trattamento dei dati riceve formazione regolare sulla protezione dei dati e sulla sicurezza delle informazioni, assicurando che siano consapevoli delle loro responsabilità e delle migliori pratiche da seguire.

7.1.3 Tracciabilità

Nel corso dello studio osservazionale retrospettivo *ORIETTA*, la tracciabilità dei dati è garantita mediante procedure standardizzate che assicurano la corretta gestione, verifica e rintracciabilità di tutte le operazioni effettuate sui dati personali trattati.
Ogni soggetto incluso nello studio è identificato attraverso un codice numerico o alfanumerico univoco, attribuito al momento della pseudonimizzazione. Tale codice consente di collegare in modo controllato i dati pseudonimizzati alla documentazione clinica originale, garantendo la possibilità di verifica e validazione delle informazioni, ma senza compromettere l'anonimato del paziente.
La chiave di collegamento tra il codice e l'identità del soggetto è conservata in un archivio elettronico sicuro, protetto da credenziali e accessibile esclusivamente al personale clinico e di ricerca autorizzato del centro partecipante.
I flussi informativi tra i centri partecipanti e il promotore avvengono in modo controllato e documentato, attraverso piattaforme dedicate per la raccolta e la gestione delle CRF.

7.1.4 Politica di tutela della privacy

L'esercizio dei diritti di privacy da parte degli interessati sarà consentito conformemente a quanto descritto nella procedura aziendale e pubblicato nella sezione privacy del sito istituzionale.

7.1.5 Gestione delle politiche di tutela della privacy

Il titolare del trattamento segue la procedura istituzionale che garantisce la tutela della privacy: Regolamento per la protezione dei dati personali in attuazione del D. Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali".
Il titolare garantisce Trasparenza e Comunicazione:

- Informazione chiara e trasparente sulle finalità del trattamento e sulle modalità di esercizio dei diritti degli interessati.
- Pubblicazione di informazioni relative allo studio e ai suoi scopi, quando possibile, per mantenere la trasparenza con il pubblico e con gli interessati.

Inoltre, sono definite procedure di sicurezza dei sistemi elettronici ed è stata effettuata la valutazione di impatto specifica per gli studi clinici di cui alla delibera 677/2024.

7.1.6 Minimizzazione dei dati

Il centro raccoglie solo le variabili essenziali per le finalità dello studio, in conformità al principio di necessità e minimizzazione (art. 5.1.c GDPR).

7.1.7 Controllo degli accessi logici

Il sistema dove è localizzato il database consente l'accesso solo a utenti autorizzati con autenticazione mediante credenziali individuali (user/password).

7.1.8 Limitazione dell'Accesso ai Dati

Solo i ricercatori direttamente coinvolti nello studio e con un ruolo specifico hanno accesso ai dati pseudonimizzati.

7.1.9 Audit e monitoraggi periodici

Saranno condotti audit periodici e controlli interni per verificare la conformità alle politiche di sicurezza e alle normative sulla protezione dei dati.

7.1.10 Sicurezza dei canali informatici

La rete ospedaliera prevede l'implementazione di sistemi di protezione adeguati: firewall, antivirus volti a garantire la sicurezza della rete.
Per maggiori dettagli vedi sezione 3.4.3

7.1.11 Procedure di sicurezza dei sistemi elettronici

I server (centrali o in cloud) sono collocati in ambienti protetti, con controlli ambientali (clima, accessi fisici) e ridondanza hardware.
Policy di physical access control impediscono l'accesso non autorizzato ai locali dove risiedono i sistemi.
I sistemi elettronici includono soluzioni di ridondanza per prevenire la perdita dei dati in caso di guasti.
I server sono protetti da firewall configurati per bloccare accessi non autorizzati.
Sistemi di rilevamento delle intrusioni (IDS) monitorano continuamente il traffico per individuare comportamenti anomali o potenziali attacchi.
I sistemi sono dotati di software antivirus aggiornati regolarmente per prevenire malware e attacchi informatici.
Tutti i software utilizzati (sistemi operativi, applicazioni) vengono aggiornati periodicamente per risolvere vulnerabilità note.

7.1.12 Accesso controllato ai locali
Accesso al reparto con badge.

7.1.13 Conservazione e archiviazione dei dati
Le informazioni personali emerse da questo studio possono essere conservate per 7 anni successivamente alla redazione dei risultati dello studio.
Le cartelle cliniche saranno esaminate solamente presso l'ospedale al fine di controllare le informazioni necessarie per lo svolgimento dello studio, senza violare la riservatezza dei pazienti. Tutte le informazioni raccolte a scopo di attività mediche, statistiche o regolatorie associate allo studio saranno identificate con un codice numerico o alfanumerico. Il nome completo dei pazienti o eventuali dettagli relativi all'indirizzo e al numero telefonico non saranno inclusi in queste analisi.
Il personale clinico e di ricerca, appositamente autorizzato, tratterà i dati identificando ciascun partecipante con un codice numerico o alfanumerico assegnato a ciascun soggetto; i dati saranno elaborati e conservati unitamente a tale codice in un database dedicato con accesso limitato e controllato nel Centro.

7.2 Panoramica dei rischi

7.2.1 Analisi complessiva del dell'entità del rischio

	Gravità (G)				
Probabilità (P)	*Trascurabile*	*Marginale*	*Limitata*	*Grave*	*Gravissima*
Improbabile	1x1	1x2	1x3	1x4	1x5
Poco probabile/Trascurabile	2x1	2x2	2x3	2x4	2x5
Probabile	3x1	3x2	3x3	3x4	3x5
Molto probabile	4x1	4x2	4x3	4x4	4x5
Quasi certo	5x1	5x2	5x3	5x4	5x5

La probabilità di occorrenza è definita in accordo alla tabella seguente:

Probabilità (P)		**Descrizione**
5	Quasi certo	Si prevede che si verifichi, anche se non sistematicamente, in modo intermittente (>10^{-3})
4	Molto probabile	Probabile che si verifichi, anche se a volte, in modo intermittente (<10^{-3} e >10^{-4})
3	Probabile/Limitata	Si verifica raramente e irregolarmente (<10^{-4} e >10^{-5})
2	Poco probabile	Improbabile che si verifichi, si prevede che si verifichi raramente (<10^{-5} e >10^{-6})
1	Improbabile/Trascurabile	Il verificarsi sarebbe veramente inaspettato (<10^{-6})

La severità dell'evento rischioso è definita in accordo alla tabella seguente:

Gravità (G)		**Descrizione**
5	Gravissima	Possibilità di lesione grave (ad esempio, lesione permanente o lesione che richiede ospedalizzazione o trattamento riabilitativo specifico per un periodo di tempo significativo).
4	Grave/Importante	Possibilità di lesioni moderate (ad esempio, che possono essere recuperate in breve tempo ma richiedono ospedalizzazione o trattamento specifico).
3	Limitata	Possibilità di lesioni lievi (ad esempio, che non richiedono ospedalizzazione e che guariscono spontaneamente in breve tempo).
2	Marginale	Nessuna lesione ma possibile disagio, dolore, piccoli problemi estetici.
1	Trascurabile	Possibilità di lesione grave (ad esempio, lesione permanente o lesione che richiede ospedalizzazione o trattamento riabilitativo specifico per un periodo di tempo significativo).

La matrice dei rischi utilizza le tre aree comuni in cui i rischi vengono classificati come:

Risk Area	Risk acceptability	Color
R1	Rischio basso (accettabile)	Verde
R2	Rischio medio (misure di controllo richieste)	Giallo
R3	Rischio alto (inaccettabile, misure di controllo richieste)	Rosso

Rischio	Impatti potenziali	Minacce	Misure di Mitigazione (MIT)	Gravità	Probabilità	ENTITA' COMPLESSIVA DEL RISCHIO	Gravità/Probabilità dopo implementazioni delle MIT	ENTITA' COMPLESSIVA DEL RISCHIO RESIDUO
Accesso illegittimo ai dati	Violazione della Privacy, Implicazioni Psicologiche e Sociali, Discriminazione, Costi, Diffusione risultati della ricerca	Vulnerabilità informatiche, attacco basato su chiave compromessa, attacco denial of service di rete, spoofing d'identità, attacco man in the middle, attacco di riproduzione RTP, virus, worm, phishing, malware. Locale lasciato aperto o non custodito. Trasmissione informatica o comunicazione verbale di dati personali a soggetti non autorizzati. Accesso e/o trattamento dei dati personali per finalità diverse da quelle autorizzate. Allontanarsi dalla propria postazione lasciando il PC connesso. Copiare i dati su dispositivi removibili e trasportabili all'esterno senza autorizzazione.	Pseudonimizzazione, Sicurezza dei canali informatici, Procedure di sicurezza dei sistemi elettronici, Controllo degli accessi logici, Formazione e Sensibilizzazione, Tracciabilità, Politica di tutela della privacy, Minimizzazione dei dati, Limitazione dell'Accesso ai Dati, Accesso controllato ai locali, Audit e monitoraggi periodici	Grave	Poco probabile	**Medio**	Limitata/Improbabile	**Basso**

Rischio	Impatti potenziali	Minacce	Misure di Mitigazione (MIT)	Gravità	Probabilità	ENTITA' COMPLESSIVA DEL RISCHIO	Gravità/Probabilità dopo implementazioni delle MIT	ENTITA' COMPLESSIVA DEL RISCHIO RESIDUO
		Modifica accidentale dei dati. Cancellazione accidentale dei dati. Inoltro di dati a soggetti non autorizzati a conoscerli.						
Modifiche indesiderate dei dati	Violazione della Privacy, Implicazioni Psicologiche e Sociali, Discriminazione, Costi, Diffusione risultati della ricerca	Vulnerabilità informatiche, attacco basato su chiave compromessa, attacco denial of service di rete, spoofing d'identità, attacco man in the middle, attacco di riproduzione RTP, virus, worm, phishing, malware. Locale lasciato aperto o non custodito. Trasmissione informatica o comunicazione verbale di dati personali a soggetti non autorizzati. Accesso e/o trattamento dei dati personali per finalità diverse da quelle autorizzate.	Pseudonimizzazione, Formazione e Sensibilizzazione, Minimizzazione dei dati, Limitazione dell'Accesso ai Dati, Sicurezza dei canali informatici, Procedure di sicurezza dei sistemi elettronici, Controllo degli accessi logici, Tracciabilità, Politica di tutela della privacy, Accesso controllato ai locali, Audit e monitoraggi periodici, Conservazione e archiviazione dei dati.	Grave	Poco probabile	**Medio**	Limitata/Improbabile	**Basso**

Rischio	Impatti potenziali	Minacce	Misure di Mitigazione (MIT)	Gravità	Probabilità	ENTITA' COMPLESSIVA DEL RISCHIO	Gravità/Probabilità dopo implementazioni delle MIT	ENTITA' COMPLESSIVA DEL RISCHIO RESIDUO
		Allontanarsi dalla propria postazione lasciando il PC connesso. Copiare i dati su dispositivi removibili e trasportabili all'esterno senza autorizzazione. Modifica accidentale dei dati. Cancellazione accidentale dei dati. Inoltro di dati a soggetti non autorizzati a conoscerli.						
Perdita di dati	Violazione della Privacy, Implicazioni Psicologiche e Sociali, Costi, Diffusione risultati della ricerca	Cancellazione accidentale dei dati. Emergenza non sanitaria con impatto sul sistema informatico (incendio, alluvione, terremoto). Modifica accidentale dei dati, vulnerabilità informatiche, attacco basato su chiave compromessa, attacco denial of service di rete, spoofing d'identità,	Formazione e Sensibilizzazione, Sicurezza dei canali informatici, Limitazione dell'Accesso ai Dati, Controllo degli accessi logici, Accesso controllato ai locali, Procedure di sicurezza dei sistemi elettronici, Conservazione e archiviazione dei dati.	Grave	Poco probabile	**Medio**	Limitata/Improbabile	**Basso**

Rischio	Impatti potenziali	Minacce	Misure di Mitigazione (MIT)	Gravità	Probabilità	ENTITA' COMPLESSIVA DEL RISCHIO	Gravità/Probabilità dopo implementazioni delle MIT	ENTITA' COMPLESSIVA DEL RISCHIO RESIDUO
		attacco man in the middle, attacco di riproduzione RTP, virus, worm, phishing, malware. Locale lasciato aperto o non custodito. Allontanarsi dalla propria postazione lasciando il PC connesso.						

La verifica dell'implementazione delle MIT identificate sarà effettuata comunque prima dell'eventuale chiusura dello studio. Conseguentemente sarà aggiornata la tabella di analisi dei rischi ed il documento corrente.

8. Risultato della DPIA

Il Promotore (in qualità di titolare del trattamento) adotta tutte le misure tecniche ed organizzative necessarie a garantire l'utilizzo dei dati personali nell'ambito degli studi clinici nel rispetto dei diritti e delle libertà degli interessati.
Tutto ciò valutato e considerato che:

Risultati della valutazione d'impatto	
☐ **Rischio residuo elevato**	■ **Rischio residuo non elevato**
Le misure tecniche e organizzative individuate per mitigare l'impatto del trattamento non sono ritenute sufficienti. Il rischio residuale per i diritti e le libertà degli interessanti resta elevato.	Le misure tecniche e organizzative individuate per mitigare l'impatto del trattamento sono ritenute sufficienti.

Il Titolare del trattamento – a seguito dei risultati della DPIA - pertanto dichiara che le misure riducono significativamente la probabilità e l'impatto dei rischi.

A seguito dell'analisi dettagliata e sistematica dei trattamenti dei dati personali nello studio in oggetto, il titolare del trattamento ha identificato i seguenti risultati chiave:

- Valutazione dei Rischi: I principali rischi per i diritti e le libertà degli interessati sono stati valutati, con particolare attenzione ai rischi di violazione della riservatezza, integrità e disponibilità dei dati personali.
- Misure di Mitigazione: Sono state identificate e implementate adeguate misure tecniche e organizzative per mitigare i rischi identificati.
- La funzione privacy è stata coinvolta durante tutto il processo di mappatura del trattamento e valutazione del rischio. Il DPO ha partecipato alla fase finale di verifica, durante la quale è emersa la corretta valutazione iniziale del rischio, nonché l'adeguatezza delle misure tecniche e organizzative adottate per la mitigazione del rischio e del danno.