Titolo dello studio	Real-world efficacy and safety of neoadjuvant dostarlimab in patients with dMMR/MSI-H locally advanced rectal cancer - RW-NEDOS
Promotore	Istituto Nazionale Tumori - IRCCS - Fondazione G. Pascale
Centro coordinatore	Istituto Nazionale Tumori di Napoli, IRCCS Fondazione G. Pascale
Sperimentatore Principale	Dott.ssa Maria Carmela Piccirillo SC Sperimentazioni Cliniche Istituto Nazionale Tumori di Napoli, IRCCS Fondazione G. Pascale Dr. Antonio Avallone SC Oncologia Medica Addominale Istituto Nazionale Tumori di Napoli, IRCCS Fondazione G. Pascale
Responsabile del Coordinamento	Dott.ssa Piera Gargiulo SC Sperimentazioni Cliniche Istituto Nazionale Tumori di Napoli, IRCCS Fondazione G. Pascale
Tipo di studio e fase	Osservazionale di coorte, retrospettivo/prospettico, multicentrico, farmacologico, no-profit
Parere del Comitato Etico	01/07/2025
Durata dello studio	La durata totale prevista dello studio è di circa un anno dalla chiusura del registro AIFA di Dostarlimab per l'indicazione nel cancro del retto (corrispondente ad un follow-up di 12 mesi dell'ultimo paziente inserito nel registro che ha acconsentito a partecipare allo studio)
DPO/RPD	Ing. Alessandro Manzoni

	Nome e Cognome	Ruolo	Firma	Data
Redazione	Piera Gargiulo	Responsabile del Coordinamento	Firmato digitalmente da: Piera Gargiulo Ruolo: DIRIGENTE MEDICO Organizzazione: IRCCS FONDAZIONE G. PASCALE/00911350635 Data: 06/10/2025 08:11:13	
Revisione	Gianfranco De Feo	Quality Assurance Manager	Firmato digitalmente da: Gianfranco De Feo Ruolo: DIRIGENTE SANITARIO Organizzazione: IRCCS FONDAZIONE G. PASCALE/00911350635 Data: 06/10/2025 08:26:46	
	Roberta Fusco	Ingegnere Biomedico	Firmato digitalmente da: Roberta Fusco Ruolo: DIRIGENTE INGEGNERE Organizzazione: IRCCS FONDAZIONE G. PASCALE/00911350635 Data: 02/10/2025 15:56:10	
Approvazione	Gianfranco De Feo	Quality Assurance Manager	Firmato digitalmente da: Gianfranco De Feo Ruolo: DIRIGENTE SANITARIO Organizzazione: IRCCS FONDAZIONE G. PASCALE/00911350635 Data: 06/10/2025 08:26:46	
	Alessandro Manzoni	DPO	Firmato digitalmente da: Alessandro Manzoni Ruolo: DIRIGENTE INGEGNERE Organizzazione: IRCCS FONDAZIONE G. PASCALE/00911350635 Data: 03/10/2025 14:22:10	
	Maria Carmela Piccirillo	Sperimentatore principale	Firmato digitalmente da: Maria Carmela Piccirillo Ruolo: DIRIGENTE MEDICO Organizzazione: IRCCS FONDAZIONE G. PASCALE/00911350635 Luogo: Napoli Data: 02/10/2025 16:32:13	
	Antonio Avallone	Sperimentatore principale	Firmato digitalmente da: Antonio Avallone Ruolo: DIRIGENTE MEDICO Organizzazione: IRCCS FONDAZIONE G. PASCALE/00911350635 Data: 03/10/2025 10:45:55	
	Maurizio Di Mauro	Titolare del trattamento dati	Firmato digitalmente da: Maurizio Di Mauro Ruolo: DIRETTORE GENERALE Organizzazione: IRCCS FONDAZIONE G.PASCALE/00911350635 Data: 07/10/2025 13:26:39	

Tracking delle modifiche

N° Rev.	Data	Motivo della modifica	Paragrafi	Pagine
1.0	15/09/2025	Prima emissione	Tutti	Tutte

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- GDPR, 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.	SI
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.	SI

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 GDPR;
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 dati personali effettuati presso il Centro Promotore è il Legale Rappresentante, Direttore Generale, dr. Maurizio Di Mauro
Responsabile della Protezione dei dati è il DOP del Centro Promotore, dr. Alessandro Manzoni

3.2 Soggetti interessati

L'attività interessa il trattamento di dati riguardanti:

- pazienti già in precedenza assistiti presso
- pazienti che hanno fornito in precedenza i propri campioni biologici presso
- pazienti arruolati in studi clinici o progetti di ricerca condotti presso

Istituto Nazionale Tumori di Napoli, IRCCS Fondazione G. Pascale

- Altro

Non applicabile

3.3 Descrizione del trattamento

3.3.1 Quale è il trattamento in considerazione?

Raccolta, analisi e pubblicazione di dati clinici e di outcome di pazienti con carcinoma rettale localmente avanzato dMMR/MSI-H trattati con dostarlimab neoadiuvante al fine di valutarne efficacia e sicurezza in un contesto real-world.

Raccolta dei Dati
Tipologia di dati raccolti:

- Dati anagrafici pseudonimizzati
- Dati relativi allo stato di salute
- Dati genetici (stato dMMR/MSI-H, mutazioni RAS/BRAF, Sindrome di Lynch). Tali dati rientrano nelle categorie particolari di dati personali, in quanto dati genetici ai sensi dell'art. 4.13) del GDPR, e saranno trattati senza eseguire test genetici aggiuntivi, nel rispetto del principio di minimizzazione. Il trattamento è giustificato in base all'art. 9.2.j) del GDPR, in quanto necessario per finalità di ricerca scientifica
- Dati sull'identità di genere e/o orientamento sessuale, raccolti esclusivamente su base volontaria (Patient–Reported Data), nella parte prospettica dello studio attraverso la somministrazione di un questionario (Sexual Orientation Gender Identity-SOGI) e hanno come finalità la promozione e il monitoraggio dell'equità di genere nella partecipazione alla ricerca in linea con i principi etici e inclusivi della stessa. Inoltre, tali dati potranno essere utilizzati per analisi di sottogruppo volte a promuovere una medicina di precisione sempre più inclusiva e sensibile all'identità di genere, nel rispetto del principio di equità. I dati non condizionano in alcun modo l'inclusione, l'arruolamento o la valutazione clinica dei partecipanti. Il conferimento è facoltativo e l'eventuale mancata compilazione del questionario non comporta alcuna conseguenza.

Modalità di raccolta dei Dati:
I dati saranno raccolti dai centri partecipanti, inseriti in una piattaforma web-based dedicata e trasferiti in forma pseudonimizzata al promotore per l'analisi scientifica. Potranno essere inclusi anche dati di partecipanti deceduti o non contattabili, in conformità all'art. 110-bis del Codice Privacy, previo controllo di eventuali opposizioni espresse in vita.

3.3.2 Quali sono le responsabilità connesse al trattamento?

Nello studio, le responsabilità connesse al trattamento dei dati personali riguardano vari attori e possono essere indicate come segue:
Titolare del trattamento
Il Titolare del trattamento è l'Istituto Nazionale Tumori – IRCCS "Fondazione G. Pascale", Napoli con sede legale in Via Mariano Semmola, Napoli (NA), C.F. e P.I. 00911350635, in persona del Direttore Generale, Dott. Maurizio Di Mauro.
Responsabilità:

- Determina le finalità e i mezzi del trattamento: decide come e perché i dati personali devono essere trattati
- Garantisce la conformità del trattamento al GDPR e al Codice Privacy
- Definisce le misure tecniche e organizzative per la sicurezza dei dati (art. 32 GDPR)
- Coordina e pubblica 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
- Gestisce i Diritti degli interessati: si assicura che gli interessati possano esercitare i loro diritti (accesso, rettifica, cancellazione)
- Fornisce informazioni chiare e trasparenti agli interessati riguardo al trattamento dei loro dati (Informativa sulla Privacy)
- Implementa misure tecniche e organizzative adeguate per proteggere i dati personali (sicurezza dei 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.

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 sorvegliare che IRCCS "Fondazione G. Pascale", Napoli rispetti le normative sulla protezione dei dati. Il DPO del Titolare del Trattamento è l'Ing. Alessandro Manzoni raggiungibile al seguente indirizzo: Responsabile della protezione dei dati personali - Istituto Nazionale Tumori IRCCS "Fondazione G. Pascale", via Mariano Semmola n.52, 80131 Napoli-
E-mail: protocollo@pec.istitutotumori.na.it; dpo@istitutotumori.na.it; rpd@pec.principaletumori.na.it; a.manzoni@istitutotumori.na.it

Responsabilità:

- Sorvegliare la conformità del trattamento alle normative vigenti
- Fornire consulenza al Responsabile del Trattamento e ai dipendenti riguardo agli obblighi del GDPR e delle altre normative
- Fungere da punto di contatto con il Garante Privacy.

Responsabile Interno del Trattamento dei Dati
Il Responsabile Interno del Trattamento dei dati è una persona che tratta i dati personali sotto l'autorità del Titolare del Trattamento. Per lo studio questo ruolo è stato delegato al Dr. Francesco Perrone che

può essere contattato presso la SC di Sperimentazioni Cliniche, dell'IRCCS "Fondazione G. Pascale", via Mariano Semmola n.52, 80131 Napoli (e-mail: f.perrone@istitutotumori.na.it).
Resposabilità:

- Agire secondo istruzioni del Titolare, evitando qualsiasi utilizzo non autorizzato o incompatibile dei dati personali
- Implementare misure tecniche e organizzative adeguate per garantire la sicurezza dei dati, tra cui pseudonimizzazione, crittografia, controllo degli accessi e tracciabilità delle operazioni
- Garantire la raccolta dei dati da parte dei centri partecipanti attraverso una piattaforma web-based conforme alle policy privacy e al principio di minimizzazione
- Assicurare la formazione e la riservatezza del personale autorizzato al trattamento dei dati sotto la sua supervisione
- 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)
- Garantire la conservazione dei dati per un periodo non superiore a quello necessario agli scopi per i quali sono stati raccolti e trattati
- Assicurare una compiuta informativa ai soggetti interessati.

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 e alle Procedure Privacy dell'IRCCS "Fondazione G. Pascale".

Centri Partecipanti
L'IRCCS "Fondazione G. Pascale", quale Titolare del Trattamento e Promotore, prima dell'avvio dello studio, ha predisposto il protocollo e individuato i Centri partecipanti.
I Centri partecipanti, nel rispetto del Protocollo e delle procedure operative del Promotore:

- non sono assoggettati a vincoli di subordinazione nei confronti del Promotore
- dispongono di propria autonomia organizzativa
- gestiscono e custodiscono sotto la propria responsabilità la documentazione di pertinenza.

Pertanto, i singoli Centri e il Promotore, cui sono imputabili responsabilità distinte nell'ambito dello studio, si configurano, quali titolari autonomi del trattamento.

3.3.3 Ci sono standard applicabili al trattamento?

Normativa europea e nazionale

- Regolamento (UE) 2016/679 (GDPR)
- D.Lgs. 196/2003 – Codice Privacy, come modificato dal D.Lgs. 101/2018.

- Art. 110 e 110-bis del Codice Privacy – Trattamento dati sanitari per ricerca scientifica senza consenso (retrospettivi e pazienti deceduti o irraggiungibili).
- Provvedimento Garante Privacy 19 dicembre 2018 – Regole deontologiche per trattamenti a fini di ricerca scientifica.
- Linee guida del Garante Privacy del 5 giugno 2019 (Provvedimento n. 146) – Trattamenti di dati a fini di ricerca scientifica.
- Deliberazione del Garante Privacy 9 maggio 2024 (n. 298, GU n. 130 del 5 giugno 2024) – Regole deontologiche aggiornate per trattamenti a fini statistici o di ricerca, in attuazione alla modifica dell'art. 110.
- Linee Guida WP 248 "in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato ai fini del regolamento UE 2016/679".
- Provvedimento del Garante per la protezione dei dati personali n. 467 dell'11/10/2018, "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, Reg. UE n. 2016/679".

Linee guida e standard internazionali

- ICH-GCP (International Council for Harmonisation – Good Clinical Practice) – Principi di buona pratica clinica applicabili anche agli studi osservazionali.
- Dichiarazione di Helsinki – Principi etici per la ricerca medica su soggetti umani.
- Linee guida AIFA per studi osservazionali e registri di farmacovigilanza.

Policy interne e misure di sicurezza

- Procedure interne del Titolare (IRCCS "Fondazione G. Pascale") per la gestione e protezione dei dati personali.
- Politiche di pseudonimizzazione, crittografia e controllo accessi implementate nella piattaforma eCRF.
- Documentazione tecnica sulla sicurezza informatica.

3.4 Dati, processi e risorse di supporto

3.4.1 Quali sono i dati trattati?

- Dati anagrafici pseudonimizzati
- Dati relativi allo stato di salute (altezza e peso alla diagnosi, ECOG PS, patologie e terapie concomitanti)

-Dati relativi alla patologia tumorale (data diagnosi, stadio TNM, grado, istologia, localizzazione del tumore) e relativo trattamento (dostarlimab, chemioterapia neoadiuvante, radioterapia neoadiuvante o chemioradioterapia)
- Dati genetici (stato dMMR/MSI-H, mutazioni RAS/BRAF, Sindrome di Lynch). L'esecuzione di tali analisi genetiche rientra nella pratica clinica
-Dati sull'identità di genere e/o orientamento sessuale, raccolti esclusivamente su base volontaria (Patient–Reported Data), nella parte prospettica dello studio attraverso la somministrazione di un questionario (SOGI), hanno come finalità la promozione e il monitoraggio dell'equità di genere nella partecipazione alla ricerca, in linea con i principi etici e inclusivi della ricerca. Tali dati potranno essere utilizzati per analisi di sottogruppo volte a promuovere una medicina di precisione sempre più inclusiva e sensibile all'identità di genere. I dati non condizionano in alcun modo l'inclusione, l'arruolamento o la valutazione clinica dei partecipanti. Il conferimento è facoltativo e l'eventuale mancata compilazione del questionario non comporta alcuna conseguenza.

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

Gli obiettivi dello studio richiedono la raccolta di dati clinici ottenibili dalle cartelle cliniche dei pazienti.
L'attività sarà svolta presso il Centro partecipante, direttamente dallo Sperimentatore Principale e dallo staff da lui delegato e consisterà nell'estrazione dei dati inerenti ai partecipanti inclusi nello studio dalle rispettive cartelle cliniche.
I dati saranno raccolti soltanto dai soggetti autorizzati ed ai soli fini definiti nello studio.
Tutti i dati raccolti saranno pseudonimizzati e inseriti nella piattaforma web-based dello Promotore accessibile esclusivamente mediante credenziali personalizzate di autenticazione del personale autorizzato (https://usc.istitutotumori.na.it).
A tutti i partecipanti sarà assegnato un codice numerico personale univoco e progressivo. Il documento contenente le informazioni che permettono la decifratura dei codici sarà conservato dal centro partecipante come documento riservato essenziale alla conduzione dello studio, in accordo alle GCP e accessibile solo ai soggetti preposti al trattamento dei dati, in qualità di incaricati o responsabili (Sperimentatore Principale e staff da lui delegato, Clinical Monitor).
Ulteriori misure di sicurezza previste dalla piattaforma web-based dello Promotore sono: trasferimento dei dati cifrato (protocollo HTTPS, certificato SSL) e archiviazione sicura, tracciamento di accessi e modifiche (audit trail).
I dati identificativi dei partecipanti saranno quindi trattati esclusivamente presso il Centro da parte dello Sperimentatore Principale e dello staff da lui delegato, nella fase iniziale di arruolamento e di raccolta dei dati, e durante le attività di monitoraggio da parte dei Clinical Monitor incaricati dallo Promotore.
I dati saranno conservati per un periodo di almeno 7 anni, come previsto dalla normativa vigente.

3.4.3 Quali sono le risorse di supporto ai Dati?

- Piattaforma per il Remote Data Entry dello Promotore

- Cartelle dei partecipanti presso il Centro e presenti su dispositivi informatici e supporti cartacei

- Server mail per la comunicazione criptata delle informazioni

- Backup e misure di sicurezza IT predisposte dall'IRCCS Pascale per garantire integrità, disponibilità e riservatezza dei dati.

- Infrastrutture IT

Sistemi di prevenzione e resilienza informatica, che includono:

- Controllo degli accessi con credenziali
- Log di accesso
- Sistemi di backup remoto
- Disaster recovery e Business Continuity Plan

Rete; Protezione tramite:

- Firewall
- VPN (Virtual Private Network)
- Test di penetrazione
- Monitoraggio della rete
- Sistemi di sorveglianza del perimetro digitale

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 dei dati personali nel contesto dello studio sono considerati specifici, espliciti e legittimi per le seguenti ragioni:
Finalità chiaramente definite nel protocollo di studio
Lo studio ha come obiettivo la valutazione dell'attività e della sicurezza del trattamento neoadiuvante con dostarlimab in pazienti con carcinoma rettale localmente avanzato dMMR/MSI-H, in contesto real-world. Tali finalità sono dettagliate nel protocollo di studio.
Finalità esplicite e trasparenti:
I partecipanti ricevono un'informativa chiara e completa circa l'uso dei loro dati. Per la parte retrospettiva, potranno essere inclusi anche i partecipanti 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
Legittimità e interesse pubblico:
Lo studio condotto risponde a un interesse pubblico contribuendo a migliorare la conoscenza e la pratica clinica in oncologia. Il trattamento dei dati è legittimo poiché rispetta il GDPR e la normativa

vigente. I dati raccolti sono adeguati, pertinenti e limitati a quanto necessario per il raggiungimento delle finalità scientifiche.

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

Le basi giuridiche del trattamento si rinvengono nei seguenti riferimenti normativi:
Parte prospettica:

- Art. 6, par. 1, lett. e) GDPR – Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico (ricerca scientifica in ambito sanitario).
- Art. 9, par. 2, lett. j) GDPR – Il trattamento di categorie particolari di dati (dati sanitari e genetici) è consentito per finalità di ricerca scientifica, con garanzie adeguate e nel rispetto del principio di minimizzazione.
- Consenso informato dei partecipanti, come misura aggiuntiva di trasparenza e tutela.

Parte retrospettiva:

- Art. 110 e 110-bis del Codice Privacy – Il trattamento di dati sanitari già disponibili nelle cartelle cliniche può essere effettuato senza consenso, previo parere del Comitato Etico e pubblicazione della DPIA, quando non sia possibile informare i soggetti senza sforzi sproporzionati. Inclusione di dati di pazienti deceduti o non contattabili, nel rispetto di eventuali opposizioni espresse in vita, con pubblicazione preventiva della DPIA.

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)?

Sì. I dati trattati nello studio sono selezionati in modo da rispettare il principio di minimizzazione (art. 5, par. 1, lett. c) GDPR).

- Vengono raccolti solo dati anagrafici pseudonimizzati, dati clinici, genetici e sugli outcome terapeutici necessari agli obiettivi di ricerca
- I dati SOGI sono acquisiti solo su base volontaria e utilizzati per analisi di equità
- Non vengono trattati dati eccedenti o non pertinenti rispetto alle finalità dello studio.

4.1.4 I dati sono esatti e aggiornati?

Sì. I dati trattati nello studio sono considerati esatti e aggiornati in quanto:

- provengono da documentazione clinica ufficiale (cartelle cliniche, referti diagnostici e registri ospedalieri) redatta da professionisti sanitari
- per la parte prospettica, i dati vengono raccolti direttamente dal centro partecipante durante le visite cliniche e inseriti sulla piattaforma web-based dello Promotore
- sono previste procedure di data cleaning e validazione per garantire correttezza, coerenza e aggiornamento continuo dei dati inseriti

- eventuali errori o incongruenze rilevate in fase di monitoraggio vengono corretti dal centro secondo le indicazioni del Responsabile interno del trattamento.

4.1.5 Qual è il periodo di conservazione dei Dati?

I Dati saranno conservati per tutta la durata dello studio, necessario per la raccolta, analisi e monitoraggio dei risultati clinici. Dopo la conclusione dello studio, i dati saranno conservati per ulteriori 7 anni, come previsto dalla normativa in materia di studi osservazionali.

4.2 Misure a tutela dei diritti degli interessati

4.2.1 Come sono informati del trattamento gli interessati?

Verrà raccolto il consenso informato degli Interessati alla partecipazione allo studio e al trattamento dei dati personali in tutti i casi in cui sarà possibile fornire loro un'adeguata informativa e acquisirne il relativo consenso. Il centro partecipante effettuerà ogni ragionevole sforzo per contattare tutti i partecipanti idonei all'arruolamento.
Tuttavia, all'esito della ricerca, alcuni dei partecipanti potranno risultare deceduti o non rintracciabili. In questi casi, lo Sperimentatore Principale (o lo staff medico delegato) provvederà a documentare l'assenza del consenso.

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

Il consenso degli interessati viene ottenuto attraverso un processo rigoroso e ben documentato, conforme alle normative etiche e legali.
Prima della raccolta dei dati, lo Sperimentatore Principale (o lo staff medico delegato) incontra il partecipante per spiegare lo studio, rispondere a eventuali domande e assicurarsi che il partecipante comprenda tutte le informazioni, e consegna le Informative e Consenso per lo studio e per il Trattamento dati. Al partecipante viene dato il tempo necessario per riflettere sulle informazioni ricevute, discutere con familiari o amici se lo desidera, e fare ulteriori domande. Successivamente, il partecipante firma il documento di informativa al trattamento dei dati e il documento di consenso informato. La firma indica che il partecipante acconsente volontariamente alla partecipazione e al trattamento dei suoi dati personali secondo quanto descritto. I documenti vengono archiviati in modo sicuro presso il centro partecipante, insieme alla documentazione dello studio.
Questo processo è progettato per assicurare che i partecipanti comprendano pienamente il trattamento dei loro dati e partecipino volontariamente. Questo processo rispetta le normative etiche e legali e garantisce che i diritti dei partecipanti siano protetti durante tutto lo svolgimento dello studio.
Per i partecipanti deceduti o irrintracciabili, lo Sperimentatore Principale dovrà documentare in cartella clinica che l'arruolamento del partecipante è avvenuto senza la raccolta del consenso con la relativa motivazione dell'impossibilità della raccolta e l'esecuzione e descrizione dei tentativi fatti per contattarlo/rintracciarlo.
Il centro partecipante effettuerà tutti i ragionevoli sforzi per contattare i partecipanti idonei allo studio, verificando anche lo stato in vita e consultando documentazione clinica, recapiti telefonici e anagrafi. Tuttavia, alcuni partecipanti potranno risultare deceduti o irreperibili.
L'impossibilità di ottenere il consenso sarà attestata solo dopo tre tentativi di contatto telefonico, effettuati in giorni e orari differenti, e registrati nella cartella clinica.

Un numero maggiore di tentativi sarebbe sproporzionato rispetto alle risorse disponibili, data la natura osservazione no-profit dello studio.
L'inclusione dei dati dei soggetti deceduti o non contattabili è necessaria al fine di garantire la completezza del campione e l'accuratezza dei risultati. Limitare la popolazione arruolata ai soli partecipanti che sottoscrivono il consenso comporterebbe una drastica riduzione della dimensione campionaria, pregiudicando gli obiettivi dello studio.

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

Il **diritto di accesso** consente ai partecipanti di ottenere conferma se i loro dati personali sono trattati e, in tal caso, di accedere a tali dati insieme ad alcune informazioni aggiuntive.
Il **diritto di portabilità** dei dati consente ai partecipanti 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
Nel foglio informativo e modello di consenso al trattamento predisposto dall'IRCCS "Fondazione G. Pascale" e fornito al centro partecipante è chiaramente indicato che gli Interessati hanno il diritto di esercitare i loro diritti (artt. 15 e ss del GDPR) inviando una richiesta scritta direttamente al Titolare del Trattamento dati, al DPO o alla Persona autorizzata al trattamento dei dati personali che opera sotto l'autorità diretta del Titolare. Prima di fornire l'accesso ai dati, l'IRCCS "Fondazione G. Pascale" 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.
Una volta verificata l'identità, l'IRCCS "Fondazione G. Pascale" 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. Il titolare del trattamento è tenuto a rispondere alla richiesta dell'interessato entro un mese e a motivare la sua eventuale intenzione di non accogliere tali richieste. Le informazioni saranno fornite in un formato chiaro e comprensibile.

Contatti per Esercitare i Diritti

DPO: Ing. Alessandro Manzoni
E-mail: protocollo@pec.istitutotumori.na.it; dpo@istitutotumori.na.it; rpd@pec.istitutotumori.na.it; a.manzoni@istitutotumori.na.it

Autorizzato al Trattamento dati: Dr. Francesco Perrone
E-mail: f.perrone@istitutotumori.na.it

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

Il **diritto di rettifica** consente ai partecipanti di correggere i propri dati personali in caso di inesattezze o completare i dati incompleti.
Il **diritto di cancellazione** (diritto all'oblio) consente ai partecipanti di richiedere la cancellazione dei propri dati personali quando non sono più necessari per gli scopi per cui sono stati raccolti o trattati, se il trattamento è illegale o per le altre ragioni previste dal GDPR.

Nel foglio informativo e modello di consenso al trattamento predisposto dall' IRCCS "Fondazione G. Pascale" e fornito al centro partecipante è chiaramente indicato che gli Interessati hanno il diritto di esercitare i loro diritti (artt. 15 e ss del GDPR) inviando una richiesta scritta direttamente al Titolare del Trattamento dati, al DPO o alla Persona autorizzata al trattamento dei dati personali che opera sotto l'autorità diretta del Titolare. Prima di fornire l'accesso ai dati, l'IRCCS "Fondazione G. Pascale" verificherà l'identità del richiedente per garantire che i dati personali siano rilasciati alla persona corretta.
Per la rettifica, una volta verificata l'identità, l'IRCCS "Fondazione G. Pascale" procederà alla rettifica dei dati personali come richiesto. Il paziente riceverà conferma che le modifiche sono state effettuate.
Per la richiesta di cancellazione, se la richiesta di cancellazione è valida, l'IRCCS "Fondazione G. Pascale" procederà alla cancellazione dei dati personali. Il paziente riceverà conferma che i dati sono stati cancellati.
Il titolare del trattamento è tenuto a rispondere alla richiesta dell'interessato entro un mese e a motivare la sua eventuale intenzione di non accogliere tali richieste.

Contatti per Esercitare i Diritti

DPO: Ing. Alessandro Manzoni
E-mail: protocollo@pec.istitutotumori.na.it; dpo@istitutotumori.na.it; rpd@pec.istitutotumori.na.it; a.manzoni@istitutotumori.na.it

Autorizzato al Trattamento dati: Dr. Francesco Perrone
E-mail: f.perrone@istitutotumori.na.it
.

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 e di **opposizione** inviando una richiesta scritta al Titolare del Trattamento dati, al DPO o alla Persona autorizzata al trattamento dei dati personali che opera sotto l'autorità diretta del Titolare, utilizzando i contatti indicati nel modulo di consenso informato e nella informativa privacy.
Limitazione del trattamento: la richiesta deve contenere l'identificazione dell'interessato e le motivazioni (es. contestazione dell'accuratezza dei dati, trattamento illecito, difesa di un diritto in sede giudiziaria, opposizione in corso di verifica).
Opposizione al trattamento: la richiesta deve indicare le attività di trattamento contestate e le motivazioni (es. trattamento basato su interessi legittimi o finalità di marketing diretto).
Il titolare del trattamento è tenuto a rispondere alla richiesta dell'interessato entro un mese e a motivare la sua eventuale intenzione di non accogliere tali richieste.

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

Ai sensi dell'articolo 28 del GDPR, il Titolare del trattamento (IRCCS "Fondazione G. Pascale") si servirà esclusivamente di Responsabili del trattamento che presentano garanzie sufficienti in termini

di competenza, misure tecniche e organizzative adeguate per garantire la protezione dei dati personali dei partecipanti allo studio.
I rapporti con ciascun Responsabile del trattamento saranno regolati da specifici contratti o atti giuridici vincolanti che definiranno oggetto, durata, finalità e modalità del trattamento, nonché le categorie di dati trattati e gli obblighi reciproci. I Responsabili del trattamento saranno tenuti a trattare i dati esclusivamente su istruzioni documentate del Titolare, a garantire riservatezza, sicurezza e assistenza per l'esercizio dei diritti degli interessati e la gestione di eventuali data breach. Al termine delle attività, i dati saranno restituiti o cancellati, salvo obblighi legali di conservazione, e il Titolare potrà effettuare verifiche e audit per garantire la conformità alle norme.

Non è attualmente previsto il trattamento dei dati da parte di Responsabili esterni per lo studio.

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

Lo studio non comporta il trasferimento di dati fuori Unione Europea (UE) .
Tuttavia, in caso di eventuale trasferimento dei dati al di fuori dell'UE, verrebbe garantita una protezione equivalente: il trasferimento sarebbe legittimato da una decisione di adeguatezza ovvero regolato dall'utilizzo di clausole contrattuali standard, conformi alle decisioni dell'Unione Europea in materia di trasferimento di dati personali verso Paesi terzi. Ciò garantirebbe il rispetto dei diritti degli Interessati ed il trattamento dei dati personali in conformità alle normative vigenti sulla protezione dei dati.

5. Motivi della valutazione d'impatto

La DPIA è stata realizzata per valutare i potenziali rischi che possono derivare dall'attività di raccolta, gestione ed analisi dei dati nei confronti degli interessati, onde poter garantire un intervento preventivo attraverso opportune misure di sicurezza.
L'esecuzione della DPIA è stata ritenuta necessaria in ragione:

- lo studio prevede il trattamento di categorie particolari di dati (art. 9 GDPR, tra cui:
  - Dati genetici: Considerati dati personali ad alta sensibilità, poiché possono rivelare informazioni uniche e intime sui partecipanti.
  - Dati sanitari: Informazioni cliniche relative a diagnosi e trattamenti del carcinoma rettale dMMR/MSI-H localmente avanzato
  - Dati sull'identità di genere e/o orientamento sessuale, raccolti esclusivamente su base volontaria (Patient–Reported Outcome), nella parte prospettica dello studio
- lo studio, per la parte retrospettiva, prevede l'inclusione anche di partecipanti deceduti o non contattabili ai sensi dell'art. 110-bis, comma 4, del Codice Privacy
- Attraverso le analisi dello studio, vengono valutati in modo sistematico aspetti personali concernenti la salute dei partecipanti.

La DPIA per lo studio è stata ritenuta necessaria in ragione delle linee guida e dei requisiti specificati nel Provvedimento del Garante n. 146/2019. La valutazione d'impatto assicura che tutti i rischi associati al trattamento dei dati personali siano identificati e mitigati adeguatamente, garantendo la protezione dei diritti e delle libertà degli interessati e assicurando la conformità con le normative sulla protezione dei dati.

6. Valutazione dei Rischi

Misure di sicurezza esistenti e pianificate
L' attività di raccolta dati sarà svolta presso il Centro partecipante dallo Sperimentatore Principale e dallo staff da lui delegato. Tali dati saranno inseriti all'interno di un database elettronico (eCRF), da parte dello Sperimentatore Principale e dello staff opportunamente autorizzato e addestrato.
Tale database è sviluppato e configurato appositamente per ridurre al minimo l'utilizzazione dei dati personali al di fuori delle finalità dello studio. I dati verranno inseriti all'interno della eCRF previa pseudonimizzazione e ogni partecipante sarà identificato solo attraverso un codice numerico progressivo. Il documento contenente le informazioni che permettono la decifratura dei codici sarà conservato dal centro partecipante come documento riservato essenziale alla conduzione dello studio, in accordo alle GCP e accessibile solo ai soggetti preposti al trattamento dei dati, in qualità di incaricati o responsabili (Sperimentatore Principale e staff da lui delegato, Clinical Monitor).
L'eCRF sarà accessibile, dai soggetti autorizzati, mediante credenziali di autenticazione personali e non cedibili. Il database elettronico verrà chiuso al termine dello studio, dopo che ne sarà stata verificata la completezza ed accuratezza. Attraverso i protocolli http e SSL con accesso tramite username e password sono garantiti elevati livelli di sicurezza e riservatezza delle informazioni, assicurando la trasmissione dei dati tramite un canale di connessione sicuro e cifrato.

I dati identificativi dei partecipanti saranno trattati esclusivamente presso il Centro partecipante da parte dello Sperimentatore Principale e dello staff da lui delegato, nella fase iniziale di arruolamento e di raccolta prospettica e retrospettiva dei dati e durante le attività di monitoraggio remoto e on-site da parte dei Clinical Monitor incaricati.
I dati raccolti ai fini dello studio saranno trattati con la massima riservatezza e saranno pseudonimizzati con un codice univoco attribuito ai singoli partecipanti; il codice univoco non includerà nessun dato personale direttamente riconducibile al paziente (nome, cognome o numero numero di telefono) e sarà utilizzato al posto del nome del partecipante e di altre informazioni che direttamente e facilmente lo identifichino.

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 dei risultati della ricerca.

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

Le principali minacce che potrebbero concretizzare il rischio di accesso illegittimo ai dati includono:

a) le potenziali vulnerabilità dei software utilizzati per il trattamento dei dati possono essere sfruttate da hacker per accedere ai dati personali

b) i malintenzionati potrebbero cercare di ottenere informazioni sensibili come password o dati personali, inviando comunicazioni fraudolente che sembrano provenire da fonti affidabili

c) persone interne all'organizzazione coinvolta nel trattamento dei dati come dipendenti disonesti o negligenti potrebbero abusare o divulgare dati sensibili

d) l'eventuale mancanza di adeguate procedure e misure di sicurezza potrebbe facilitare l'accesso illegittimo ai dati

e) l'eventuale mancanza di sicurezza fisica potrebbe consentire l'accesso illegittimo ai dati.

6.1.3 Quali sono le fonti di rischio?

Le fonti di rischio per l'accesso illegittimo ai dati possono derivare da diverse situazioni o fattori. Alcune delle principali fonti di rischio includono:

a) vulnerabilità informatiche (tecniche o di sicurezza)
b) attacchi informatici (phishing, malware, ransomware, virus o gli attacchi DDoS)
c) accesso da parte del personale non autorizzato
d) mancanza di adeguati controlli di accesso e di autenticazione
e) mancanza di consapevolezza da parte degli utenti sulle pratiche di sicurezza

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

Le misure di sicurezza che saranno adottate includono:

a) accesso limitato e controllato ai dati personali del solo personale autorizzato sia a livello fisico che informatico
b) pseudonimizzazione dei dati e comunicazione degli stessi tramite chiave crittografica
c) protezione fisica dell'infrastruttura informatica utilizzata nello studio
d) audit e monitoraggi periodici
e) formazione del personale coinvolto sui rischi associati all'accesso illegittimo ai dati personali
f) tracciabilità
g) minimizzazione

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

In ragione della sensibilità dei dati trattati e degli impatti potenziali, l'accesso illegittimo ai dati personali potrebbe causare importanti violazioni della privacy degli Interessati. Tuttavia, le misure pianificate per mitigare il rischio di accesso illegittimo ai dati e l'adozione di politiche e procedure di sicurezza contribuiscono a ridurre significativamente la gravità del rischio.
Grave

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

La probabilità di rischio residuo è valutata come 'Trascurabile', considerando le minacce potenziali (accessi non autorizzati, perdita o alterazione dei dati) e l'efficacia delle misure di mitigazione adottate, quali pseudonimizzazione, minimizzazione dei dati, controllo degli accessi con credenziali nominali, piattaforma web protetta da crittografia SSL/HTTPS e audit trail per monitorare ogni operazione
Poco probabile/Trascurabile

6.2 Modifiche indesiderate dei Dati

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

La concretizzazione del rischio di modifiche indesiderate dei dati potrebbe compromettere l'integrità e l'affidabilità dei dataset clinici, causando errori nelle analisi statistiche, valutazioni di efficacia/sicurezza e potenziali distorsioni dei risultati della ricerca. Un'alterazione dei dati sanitari potrebbe comportare una violazione della privacy degli interessati, con conseguenze psicologiche e sociali (ad esempio, stigma o discriminazioni), oltre a possibili costi economici per la correzione dei dati e la gestione di incidenti di sicurezza. Tali eventi inciderebbero negativamente sulla qualità scientifica e sulla credibilità dello studio, riducendo la validità dei risultati e il loro impatto nella comunità scientifica.

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

Le principali minacce che potrebbero concretizzare il rischio di modifiche indesiderate dei dati includono:

a) errori commessi dagli operatori durante l'inserimento, la manipolazione o la gestione dei dati
b) accesso non autorizzato da parte di individui o entità esterne
c) modifiche indesiderate da parte di persone interne all'organizzazione coinvolta nel trattamento dei dati
d) attacchi informatici (malware, virus o ransomware) con compromissione della sicurezza dei sistemi informatici
e) trasferimento dei dati da un sistema all'altro su reti non sicure
f) mancanza di adeguate misure di sicurezza.

6.2.3 Quali sono le fonti di rischio?

Le fonti di rischio per le modifiche indesiderate ai dati possono derivare da diverse situazioni o fattori. Alcune delle principali fonti di rischio includono:

a) vulnerabilità informatiche (tecniche o di sicurezza)
b) attacchi informatici (phishing, malware, ransomware, virus o gli attacchi DDoS)

c) accesso da parte del personale non autorizzato
d) mancanza di adeguati controlli di accesso e di autenticazione
e) mancanza di consapevolezza da parte degli utenti sulle pratiche di sicurezza.

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

Per mitigare il rischio di modifiche indesiderate dei dati, all'interno dello studio saranno adottate una serie di misure di sicurezza:

a) implementare un sistema di gestione degli accessi che permetta solo alle persone autorizzate di accedere ai dati

b) utilizzare strumenti di monitoraggio e rilevamento delle attività anomale per identificare potenziali tentativi di modifiche indesiderate o accessi non autorizzati

c) verificare l'integrità dei dati tramite il monitoraggio

d) effettuare regolari backup dei dati che consentano il ripristino in caso di manomissione

e) pseudonimizzare i dati e comunicare gli stessi tramite chiave crittografica

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

In ragione della sensibilità dei dati trattati e degli impatti potenziali, le modifiche indesiderate e non autorizzate dei dati personali potrebbe causare importanti violazioni della privacy degli Interessati. Tuttavia, le misure pianificate e l'adozione di politiche di sicurezza per mitigare tale rischio contribuiscono a ridurre significativamente la gravità del rischio.
Grave

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

La probabilità di rischio residuo è valutata come 'Trascurabile', considerando le minacce potenziali e l'efficacia delle misure di mitigazione adottate, quali pseudonimizzazione, minimizzazione dei dati, controllo degli accessi con credenziali nominali, piattaforma web protetta da crittografia SSL/HTTPS e audit trail per monitorare ogni operazione.
Poco probabile/Trascurabile

6.3 Perdita di Dati

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

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

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

Le principali minacce che potrebbero concretizzare il rischio di perdita di dati sono:

a) eventi come incendi, allagamenti, danni fisici ai dispositivi di archiviazione o guasti tecnici

b) gli errori umani, come la cancellazione accidentale di dati, la sovrascrittura di file importanti o l'errata configurazione dei sistemi

c) attacco hacker

d) perdita o furto dei dispositivi di archiviazione

e) vulnerabilità dei sistemi, violazioni delle politiche di sicurezza o accesso non autorizzato ai dati da parte di personale interno.

6.3.3 Quali sono le fonti di rischio?

Le fonti di rischio per la perdita dei dati possono derivare da diverse situazioni o fattori. Alcune delle principali fonti di rischio includono:

a) infrastrutture tecnologiche (guasti hardware, errori di configurazione o vulnerabilità di sicurezza)
b) processi operativi interni (errori umani o procedure inadeguate)
c) minacce informatiche (attacchi o intrusioni)
d) azioni o negligenze umane (cancellazioni accidentali, comportamenti non conformi)
e) eventi naturali o fisici (incendi, allagamenti, furti o danni alle strutture)
f) fornitori esterni (malfunzionamenti, errori o violazioni presso i provider di servizi di archiviazione o trattamento).

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

Per mitigare il rischio di perdita dei dati, lo studio adotta misure tecniche e organizzative quali:

a) backup regolari e archiviazione sicura
b) crittografia dei dati in transito
c) controlli di accesso e autenticazione per il personale autorizzato
d) monitoraggio delle anomalie
e) formazione sulla sicurezza dei dati

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

In ragione della sensibilità dei dati trattati e degli impatti potenziali, la perdita dei dati personali potrebbe causare importanti violazioni della privacy degli Interessati. Tuttavia, le misure pianificate e l'adozione di politiche di sicurezza per mitigare tale rischio contribuiscono a ridurre significativamente la gravità del rischio.
Grave

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

La probabilità di rischio residuo è valutata come 'Trascurabile', considerando le minacce potenziali e l'efficacia delle misure di mitigazione adottate, quali pseudonimizzazione, minimizzazione dei dati, controllo degli accessi con credenziali nominali, piattaforma web protetta da crittografia SSL/HTTPS e audit trail per monitorare ogni operazione.
Poco probabile/Trascurabile

7. Piano d'azione

7.1 Mitigazione dei rischi con Misure esistenti o pianificate

7.1.1 Pseudonimizzazione

Tutti i dati raccolti sono pseudonimizzati: il codice del partecipante è noto solo al centro. I codici identificativi sono gestiti separatamente e conservati con accesso riservato solo allo Sperimentatore Principale e dallo staff da lui delegato.

7.1.2 Minimizzazione dei Dati
Lo studio raccoglie e utilizza solo i dati strettamente necessari per il raggiungimento delle sue finalità in conformità al principio di necessità e minimizzazione (art. 5.1.c GDPR).

7.1.3 Limitazione dell'Accesso ai Dati
Solo lo Sperimentatore Principale e lo staff da lui delegato, direttamente coinvolti nello studio e con un ruolo specifico, hanno accesso ai dati pseudonimizzati.

7.1.4 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.

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

7.1.6 Sicurezza dei canali informatici
La rete dell'IRCCS "Fondazione G. Pascale prevede l'implementazione di sistemi di protezione adeguati: firewall, antivirus volti a garantire la sicurezza della rete.

7.1.7 Gestione delle politiche di tutela della privacy

Il titolare del trattamento segue il Regolamento Privacy istituzionale che garantisce la tutela della privacy adottato dall' Istituto, ai sensi del GDPR.
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.

7.1.8 Politica di tutela della privacy

L'esercizio dei diritti di privacy da parte degli interessati sarà consentito conformemente al GDPR e alla normativa privacy applicabile.

7.1.9 Procedure di sicurezza dei sistemi elettronici

I server che ospitano i dati sono collocati in ambienti protetti, con accesso fisico limitato al personale autorizzato.
I sistemi elettronici includono soluzioni di ridondanza per prevenire la perdita dei dati in caso di guasti.
Backup regolari (giornalieri, settimanali) dei dati sono archiviati in sedi sicure.
I server sono protetti da firewall configurati per bloccare accessi non autorizzati.
I 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.

7.1.10 Controllo degli accessi logici

L'accesso ai dati è limitato al personale autorizzato attraverso:

- Credenziali individuali
- Criteri di password robusti (es. lunghezza minima, rotazione periodica)

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	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

Risk Area	Risk acceptability	Color
R3	Rischio alto (inaccettabile, misure di controllo richieste)	Rosso

Rischio	**Impatti potenziali**	**Minacce**	**Misure di Mitigazione (MIT)**	**Gravità**	**Probabilità**	**ENTITA' COMPLESSIVA DEL RISCHIO**	**Probabilità dopo implementazioni delle MIT**	**ENTITA' COMPLESSIVA DEL RISCHIO RESIDUO**
Accesso illegittimo ai dati	Violazione della privacy; Implicazioni psicologiche e sociali; Discriminazione; Costi economici; Diffusione di risultati della ricerca.	Le potenziali vulnerabilità dei software utilizzati per il trattamento dei dati possono essere sfruttate da hacker per accedere ai dati personali; i malintenzionati potrebbero cercare di ottenere informazioni sensibili come password o dati personali, inviando comunicazioni fraudolente che sembrano provenire da fonti affidabili; persone interne all'organizzazione coinvolta nel trattamento dei dati come dipendenti disonesti o negligenti potrebbero abusare o divulgare dati sensibili; l'eventuale mancanza di adeguate procedure e misure di sicurezza potrebbe facilitare l'accesso illegittimo ai dati; l'eventuale mancanza di sicurezza fisica potrebbe consentire l'accesso illegittimo ai dati.	Pseudonimizzazione, Sicurezza dei canali informatici, Procedure di sicurezza dei sistemi elettronici, Controllo degli accessi logici, Formazione e Sensibilizzazione, Minimizzazione dei dati, Limitazione dell'Accesso ai Dati, Accesso controllato ai locali, Audit e monitoraggi regolari	Grave	Poco probabile/Trascurabile	**Medio**	Improbabile	**Basso**
Modifiche indesiderate dei dati	La concretizzazione del rischio di modifiche indesiderate dei dati potrebbe compromettere l'integrità e l'affidabilità dei dataset clinici, causando errori nelle analisi statistiche, valutazioni di efficacia/sicurezza e potenziali distorsioni dei risultati della	Errori commessi dagli operatori durante l'inserimento, la manipolazione o la gestione dei dati; accesso non autorizzato da parte di individui o entità esterne; modifiche indesiderate da parte di persone interne all'organizzazione coinvolta nel trattamento dei	Pseudonimizzazione, Sicurezza dei canali informatici, Procedure di sicurezza dei sistemi elettronici, Controllo degli accessi logici, Formazione e Sensibilizzazione, Minimizzazione dei dati, Limitazione dell'Accesso ai Dati, Accesso controllato ai locali, Audit e monitoraggi regolari	Grave	Poco probabile/Trascurabile	**Medio**	Improbabile	**Basso**

	ricerca. Un'alterazione dei dati sanitari potrebbe comportare una violazione della privacy degli interessati, con conseguenze psicologiche e sociali (ad esempio, stigma o discriminazioni), oltre a possibili costi economici per la correzione dei dati e la gestione di incidenti di sicurezza. Tali eventi inciderebbero negativamente sulla qualità scientifica e sulla credibilità dello studio, riducendo la validità dei risultati e il loro impatto nella comunità scientifica.	dati; attacchi informatici (malware, virus o ransomware) con compromissione della sicurezza dei sistemi informatici; trasferimento dei dati da un sistema all'altro su reti non sicure; mancanza di adeguate misure di sicurezza.						
Perdita di dati	Violazione della privacy; Implicazioni psicologiche e sociali; Discriminazione; Costi; Diffusione risultati della ricerca.	Eventi come incendi, allagamenti, danni fisici ai dispositivi di archiviazione o guasti tecnici; gli errori umani, come la cancellazione accidentale di dati, la sovrascrittura di file importanti o l'errata configurazione dei sistemi; attacco hacker; perdita o furto dei dispositivi di archiviazione; vulnerabilità dei sistemi, violazioni delle politiche di sicurezza o accesso non autorizzato ai dati da parte di personale interno.	Sicurezza dei canali informatici, Procedure di sicurezza dei sistemi elettronici, Controllo degli accessi logici, Formazione e Sensibilizzazione, Limitazione dell'Accesso ai Dati, Accesso controllato ai locali	Grave	Poco probabile/Trascurabile	**Medio**	Improbabile	**Basso**

La verifica dell'implementazione delle MIT identificate saranno effettuate ogni 12 mesi dalla data di emissione del documento e 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 nel progetto "**RW-NEDOS**", 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. Queste includono la pseudonimizzazione dei dati; la minimizzazione dei dati; il controllo e la limitazione degli accessi; il backup; la formazione continua del personale; audit e controlli regolari; la sicurezza dei canali informatici e la Gestione delle politiche di tutela della privacy, Trasparenza e Comunicazione.
- **Coinvolgimento delle Parti Interessate**: è stato considerato il feedback degli esperti in materia di protezione dei dati.