Titolo dello studio	SVILUPPO DI UNA PIATTAFORMA PER LA IMPLEMENTAZIONE CLINICA DELLA ONCOLOGIA DI PRECISIONE NELLE REGIONI DEL CENTRO SUD ITALIA (COESIT)
Promotore	Istituto Nazionale Tumori - IRCCS - Fondazione Pascale
Centro coordinatore	Istituto Nazionale Tumori di Napoli, IRCCS G. Pascale
Sperimentatore Principale	Dott.ssa Antonella De Luca SC Biologia Cellulare e Bioterapie Istituto Nazionale Tumori di Napoli, IRCCS G. Pascale
Responsabile Scientifico	Dott. Nicola Normanno Direzione Scientifica IRCCS Istituto Romagnolo per lo Studio dei Tumori (IRST)
Tipo di studio e fase	Osservazionale, multicentrico, retrospettivo e prospettico
Parere del Comitato Etico	Parere Emendamento Prot. v.3 del 21.03.2026
Durata dello studio	4 anni
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: 13/10/2025 12:36:56	
Revisione	Gianfranco De Feo	Quality Assurance	Firmato digitalmente da: Gianfranco De Feo Ruolo: DIRIGENTE SANITARIO Organizzazione: IRCCS FONDAZIONE G. PASCALE/00911350635 Data: 16/10/2025 16:29:32	
Approvazione	Maurizio Di Mauro	Titolare del trattamento dati	Firmato digitalmente da: Maurizio Di Mauro Ruolo: DIRETTORE GENERALE Organizzazione: IRCCS FONDAZIONE G.PASCALE/00911350635 Data: 21/10/2025 14:54:40	
	Alessandro Manzoni	DPO	Firmato digitalmente da: Alessandro Manzoni Ruolo: DIRIGENTE INGEGNERE Organizzazione: IRCCS FONDAZIONE G. PASCALE/00911350635 Data: 17/10/2025 14:55:13	
	Antonella De Luca	Sperimentatore principale	Firmato digitalmente da: Antonella De Luca Ruolo: DIRIGENTE MEDICO Organizzazione: IRCCS FONDAZIONE G. PASCALE/00911350635 Antonella De Luca	
	Gianfranco De Feo	Quality Assurance	Firmato digitalmente da: Gianfranco De Feo Ruolo: DIRIGENTE SANITARIO Organizzazione: IRCCS FONDAZIONE G. PASCALE/00911350635 Data: 16/10/2025 16:29:33	

Tracking delle modifiche

N° Rev.	Data	Motivo della modifica	Paragrafi	Pagine
0	16.09.2025	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, 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 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 Promotore è il Legale Rappresentante e la dr.ssa Antonella De Luca in qualità di Sperimentatore Principale

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

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

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

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

- Altro

NA

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:

- I dati vengono trattati in forma pseudonimizzata riducendo i rischi di re-identificazione. 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.

3.3 Descrizione del trattamento

3.3.1 Quale è il trattamento in considerazione?

Il trattamento dei dati personali previsto nell'ambito dello studio "COESIT" è finalizzato alla realizzazione di una piattaforma per la ricerca scientifica nel campo dell'oncologia di precisione. Il trattamento è multicentrico e osservazionale, con una natura dei dati sia retrospettiva che prospettica.
Dati Oggetto del Trattamento: Il trattamento riguarda diverse categorie di dati personali dei pazienti partecipanti, tra cui:

- ✓ **Dati Comuni:** dati anagrafici (età, sesso) in forma pseudoanonimizzata o anonima.
- ✓ **Dati Particolari (Sensibili):** Informazioni sanitarie, anamnesi clinica, stili di vita, dati genomici**.**

Modalità e Finalità del Trattamento: La base giuridica per il trattamento di queste categorie di dati è il consenso esplicito dell'interessato, come richiesto dall'art. 9 del GDPR. I dati raccolti verranno utilizzati per le seguenti finalità.

1. **Creazione di un Database Comune:** I dati clinici e molecolari di circa 4000 pazienti all'anno, raccolti da diverse istituzioni partecipanti, confluiranno in un database centralizzato gestito dall'Istituto Nazionale Tumori "Fondazione Giovanni Pascale".
2. **Ricerca Scientifica:** I dati aggregati saranno analizzati per incrementare le conoscenze sui tumori, identificare nuovi biomarcatori prognostici e predittivi, e implementare strategie di oncologia di precisione. Ciò include studi sull'eterogeneità tumorale, sulla resistenza a terapie e sulla correlazione tra profilo genetico e fattori ambientali.
3. **Anonimizzazione e Pseudonimizzazione:** Per proteggere la privacy, ai pazienti viene assegnato un codice identificativo univoco. I dati vengono trattati in forma "pseudoanonimizzata", permettendo solo al medico dello studio e a soggetti autorizzati di risalire al nominativo. Al termine del periodo di conservazione, i dati verranno cancellati o resi completamente anonimi.
4. **Condivisione e Accesso:** L'accesso ai dati personali identificabili è strettamente limitato al medico sperimentatore, ai suoi collaboratori, al Comitato Etico e alle autorità regolatorie. I dati anonimizzati o aggregati potranno essere condivisi con ricercatori esterni e pubblicati su riviste scientifiche, senza mai rivelare l'identità del paziente.

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. Antonella De Luca.

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.

Nel contesto di codesto studio osservazionale, le responsabilità connesse al trattamento dei dati personali presso l'Istituto Nazionale dei Tumori IRCCS "Fondazione G. Pascale" di Napoli sono così ripartite:

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.

- 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".

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 R3).
- 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?

Il trattamento dei dati previsto dallo studio COESIT comprende una vasta gamma di informazioni personali, necessarie per raggiungere gli obiettivi di ricerca nell'ambito dell'oncologia di precisione. Vengono raccolti dati anagrafici comuni, quali età, sesso e località di residenza, quest'ultimo utile anche per analisi di geo-localizzazione. Accanto a questi, il cuore dello studio risiede nel trattamento di dati particolari e altamente sensibili. Questi includono informazioni sul tipo istologico della neoplasia, i trattamenti oncologici ricevuti e i farmaci assunti. Un elemento centrale è la raccolta di datimolecolari , ottenuti dall'analisi di campioni biologici (tessuto tumorale e sangue) tramite tecnologie di sequenziamento avanzato, che rivelano il profilo molecolare del tumore e la presenza di eventuali mutazioni. Infine, il quadro informativo è arricchito da dati relativi allo stile di vita,

come l'abitudine al fumo o il consumo di alcol, al fine di correlare il profilo genetico-molecolare con fattori di rischio ambientali e personali.

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

Il ciclo di vita del trattamento dei dati nello studio COESIT si articola in diverse fasi, che variano a seconda della tipologia di dati raccolti, ovvero se prospettici o retrospettivi.

1. Raccolta dei Dati e Base Giuridica Il ciclo ha due punti di partenza distinti:

- **Dati Prospettici:** Per i pazienti potenzialmente eleggibili e attivamente coinvolti, il processo inizia con la presentazione di un'informativa completa e la richiesta di **consenso informato documentato**. Questo consenso esplicito rappresenta la base giuridica per il trattamento dei loro dati personali e per l'utilizzo a fini scientifici. La partecipazione è volontaria e il paziente può rifiutare o revocare il consenso in qualsiasi momento.
- **Dati Retrospettivi:** Lo studio prevede anche l'inclusione di dati clinico-patologici e di CGP (Comprehensive Genomic Profiling) di **pazienti eleggibili deceduti o non raggiungibili**. Per questi casi, il trattamento si basa sull'**articolo 110 bis, comma 4 del Codice della Privacy**. Come richiesto da tale norma, prima dell'inizio della raccolta, il Promotore si impegna a produrre e pubblicare sul proprio sito web una Valutazione d'Impatto sulla Protezione dei Dati (DPIA).

2. Ingresso e Pseudonimizzazione dei Dati

Una volta autorizzata la raccolta (tramite consenso o nel rispetto dell'art. 110 bis), i dati vengono inseriti nella piattaforma dello studio. A ogni paziente viene assegnato un **codice numerico identificativo univoco**. Questo codice sostituisce il nominativo del paziente in tutte le successive comunicazioni e schede di raccolta dati. Una lista di decodifica, che permette di ricollegare il codice all'identità del paziente, viene conservata in modo sicuro ed esclusivo presso i singoli centri partecipanti e il centro coordinatore.

3. Centralizzazione e Gestione del Database

I dati pseudonimizzati, raccolti dai diversi centri, vengono centralizzati in una piattaforma di raccolta dati clinico-patologici e genetico-molecolari. Questa piattaforma è protetta da password e accessibile unicamente al personale autorizzato presso le istituzioni coinvolte nel progetto. Il centro coordinatore (Istituto Nazionale Tumori di Napoli) ha la responsabilità delle procedure di raccolta e gestione dei dati.

4. Analisi e Utilizzo per la Ricerca

In questa fase, i dati vengono utilizzati per le finalità scientifiche dello studio. Le analisi sono condotte sui dati aggregati per identificare alterazioni genomiche, biomarcatori e correlazioni utili per l'avanzamento della medicina di precisione. I risultati delle ricerche

possono essere pubblicati e presentati in contesti scientifici, ma sempre in forma aggregata e anonima, in modo da non permettere l'identificazione dei singoli individui.

5. Conservazione dei Dati

I dati raccolti, sia prospettici che retrospettivi, vengono registrati, analizzati e conservati per tutta la durata del progetto (attualmente prevista in 4 anni) e per il periodo richiesto dalle normative vigenti, unitamente al codice che identifica il paziente.

6. Fine del Ciclo di Vita: Cancellazione o Anonimizzazione

Al termine del periodo di conservazione obbligatorio, il ciclo di vita del dato personale si conclude. Come specificato nel documento, i dati verranno **cancellati oppure resi anonimi** in modo che non sia più possibile risalire, in modo diretto o indiretto, all'identità dell'interessato. Questo passaggio finale assicura che, una volta esaurite le finalità dello studio e gli obblighi di legge, i dati personali non vengano conservati a tempo indeterminato.

3.4.3 Quali sono le risorse di supporto ai dati?

Nel contesto dello studio in oggetto, le risorse di supporto ai dati comprendono una varietà di strumenti, tecnologie e strutture per garantire una gestione efficiente, sicura e conforme alle normative dei dati raccolti. Ecco un elenco delle principali risorse di supporto ai dati utilizzate nello studio:

1. Piattaforma Tecnologica e Software

La risorsa tecnologica principale è la **piattaforma di raccolta dei dati clinico-patologici e genetico-molecolari**. Questa non è solo un semplice database, ma un'infrastruttura complessa che include:

- **Database Comune Centralizzato:** Un sistema per archiviare in modo strutturato tutti i dati raccolti dai vari centri, protetto da **password** e accessibile solo a personale autorizzato.
- **Pipeline Bioinformatiche:** Strumenti software specifici per analizzare e interpretare i dati grezzi di sequenziamento genomico (NGS). Il progetto mira a creare un **network bioinformatico** per condividere e standardizzare queste pipeline tra le istituzioni.

2. Risorse Umane e Competenze Professionali

Il trattamento dei dati è supportato da un team multidisciplinare di professionisti con ruoli ben definiti:

- **Personale Medico e Sperimentatori:** Medici e ricercatori dei centri partecipanti che raccolgono il consenso, inseriscono i dati clinici e sono responsabili della gestione dei pazienti. Sono gli unici, insieme ad altro personale autorizzato della struttura, a poter accedere alla lista di decodifica per collegare il codice all'identità del paziente.

3. Entità Organizzative e Istituzionali

Diverse istituzioni collaborano, fornendo risorse e supporto:

- **Istituto Nazionale Tumori "Fondazione Giovanni Pascale":** Agisce come **Promotore no profit** e **Centro Coordinatore**. Ha la responsabilità principale delle procedure di raccolta e gestione dei dati e della proprietà intellettuale dei risultati.
- **Istituzioni Partecipanti:** Una rete di ospedali e centri di ricerca (Policlinico Gemelli, ISMETT, IRST, ecc.) che fungono da centri di raccolta dati, contribuendo ad alimentare la piattaforma con le informazioni dei loro pazienti.
- **Azienda Partner (Kelyon):** Una **Digital Health Company** esterna che collabora al progetto. Kelyon apporta competenze specifiche nello sviluppo di software per dispositivi medici e applicazioni di sanità digitale supportando lo sviluppo industriale delle pipeline bioinformatiche.

4. Risorse Fisiche

- **Biobanche:** I centri COESIT dispongono di biobanche dove sono conservati i **campioni biologici** (tessuto tumorale, sangue, ecc.) da cui vengono estratti i dati genetici. Queste rappresentano una risorsa fondamentale per le analisi retrospettive e per la ricerca di nuovi biomarcatori.

Queste risorse combinano tecnologia, infrastruttura, personale e procedure per supportare efficacemente la gestione dei dati nello studio, assicurando la qualità, la sicurezza e la conformità dei dati trattati.

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?

Sì, gli scopi del trattamento dei dati per lo studio COESIT sono specifici, espliciti e legittimi:

- Specifici: Le finalità non sono generiche, ma dettagliatamente circoscritte alla "realizzazione di una piattaforma per l'oncologia di precisione nel centro-sud Italia" e ai suoi sotto-obiettivi, come la mappatura di alterazioni genomiche, l'identificazione di biomarcatori e la standardizzazione di procedure bioinformatiche, come analiticamente descritto nel protocollo di studio.
- Espliciti: Gli scopi sono comunicati in modo chiaro e trasparente ai partecipanti attraverso l'informativa fornita prima della raccolta del consenso, garantendo che gli interessati siano pienamente consapevoli delle modalità e delle finalità di utilizzo dei loro dati.
- Legittimi: La legittimità del trattamento si fonda su una duplice e solida base giuridica: il consenso esplicito dell'interessato (art. 9.2.a GDPR) per i dati raccolti prospetticamente, e le garanzie previste dall'art. 110 bis del Codice della Privacy per il trattamento di dati retrospettivi a fini di ricerca scientifica. La finalità stessa di ricerca medica riveste inoltre un rilevante interesse pubblico, rafforzando la legittimità del trattamento.

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

Il trattamento dei dati personali effettuato nell'ambito dello studio presso l'Istituto Nazionale dei Tumori IRCCS "Fondazione G. Pascale" di Napoli è lecito ai sensi del Regolamento (UE) 2016/679 (GDPR) e della normativa nazionale (D.lgs. 196/2003 e successive modificazioni), sulla base delle seguenti disposizioni:

Per soggetti viventi:

- Art. 6(1)(a) GDPR – Il paziente firma un modulo di consenso informato, dopo essere stato adeguatamente informato sul trattamento dei dati, sulle finalità dello studio e sui propri diritti.
  Art. 6(1)(e) GDPR – Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico (ricerca scientifica in ambito sanitario).
- Art. 9(2)(a) GDPR – *Consenso esplicito per categorie particolari di dati*: Il trattamento riguarda dati sanitari e genetici, e pertanto è ammesso solo previa acquisizione del consenso esplicito da parte del soggetto.
- Art. 9(2)(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.

Per soggetti deceduti o non rintracciabili:

- 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.

- Art. 9(2)(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.

Queste basi legali, in combinazione con le misure di sicurezza adottate, rendono il trattamento conforme ai principi di liceità, correttezza e trasparenza (art. 5 GDPR).

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, il trattamento rispetta il principio di minimizzazione dei dati sancito dall'art. 5.1.c del GDPR. I dati raccolti sono adeguati, pertinenti e limitati a quanto strettamente necessario per le finalità di ricerca.

- Adeguati: L'insieme dei dati clinici, genomici, anamnestici e relativi allo stile di vita è considerato il set informativo minimo sufficiente per condurre analisi scientifiche significative nell'ambito dell'oncologia di precisione e per correlare i profili molecolari con gli esiti clinici e i fattori di rischio.
- Pertinenti: Ciascuna categoria di dati ha una chiara e diretta rilevanza per gli obiettivi specifici dello studio, come la mappatura delle mutazioni, la valutazione della risposta alle terapie o l'analisi epidemiologica su base geografica. Non vengono raccolte informazioni che esulano da tali scopi.
- Limitati: La raccolta è circoscritta alle sole informazioni indispensabili per rispondere alle domande del protocollo di ricerca. Inoltre, l'adozione sistematica della pseudonimizzazione fin dalla fase di raccolta agisce come misura tecnica di minimizzazione, limitando la circolazione dei dati identificativi diretti.

4.1.4 I dati sono esatti e aggiornati?

Sì, il trattamento è strutturato per rispettare il principio di accuratezza (art. 5.1.d GDPR), prevedendo misure per garantire che i dati siano esatti e, dove necessario, aggiornati.

- Esattezza: L'accuratezza dei dati è garantita alla fonte, poiché le informazioni cliniche sono inserite da personale medico qualificato basandosi sulla documentazione sanitaria, mentre i dati genomici sono prodotti da laboratori specializzati che seguono protocolli standardizzati e sono soggetti a controlli di qualità incrociati, come previsto dal protocollo di studio.
- Aggiornamento: Lo studio implementa meccanismi di aggiornamento differenziati. I dati clinici relativi al percorso del paziente vengono aggiornati prospetticamente. Gli interessati possono esercitare il diritto di rettifica per correggere inesattezze. Aspetto fondamentale, il protocollo prevede una rivalutazione scientifica periodica (annuale) delle varianti genetiche a significato incerto (VUS), assicurando che non solo il dato grezzo, ma anche la sua interpretazione clinica, sia mantenuta aggiornata secondo le più recenti evidenze scientifiche.

4.1.5 Qual è il periodo di conservazione dei dati?

Il periodo di conservazione dei dati è definito in conformità al principio di limitazione della conservazione (art. 5.1.e GDPR) ed è strettamente legato alle finalità di ricerca scientifica e agli obblighi normativi del settore. Come esplicitato nel protocollo di studio, i dati personali dei partecipanti, in forma pseudoanonima, saranno conservati per tutta la durata del progetto (attualmente prevista in 4 anni) e, successivamente, per l'ulteriore periodo richiesto dalle normative vigenti in materia di sperimentazione clinica e buona pratica clinica.

4.2 Misure a tutela dei diritti degli interessati

4.2.1 Come sono informati del trattamento gli interessati?

Gli interessati vengono informati del trattamento dei propri dati personali secondo quanto previsto dagli articoli 13 e 14 del GDPR, con modalità distinte in base alla loro reperibilità e condizione:

Pazienti viventi e contattabili

- Ricevono foglio informativo e modulo di consenso informato (ICF) prima dell'inclusione nello studio.
- L'informativa descrive in modo chiaro e trasparente:
  - Le finalità del trattamento,
  - Le categorie di dati trattati,
  - Le modalità di pseudonimizzazione,
  - I soggetti coinvolti,
  - I diritti dell'interessato,
  - Le modalità di esercizio dei diritti e i dati di contatto del DPO.
- Il trattamento ha inizio solo dopo la firma del consenso informato.

Pazienti deceduti o non rintracciabili

- Ai sensi dell'art. 14 GDPR e dell'art. 110 del Codice Privacy, viene pubblicata la valutazione di impatto.
- Le modalità previste includono:
  - Pubblicazione sul sito web dello sponsor (Istituto Pascale).
  - Pubblicazione sul sito web del centro sperimentale (Istituto Pascale).
- Se un paziente si ripresenta in reparto (es. per follow-up), il ricercatore ha l'obbligo di:
  - Informarlo tempestivamente,
  - Acquisire il consenso esplicito per il proseguimento del trattamento.

Questa procedura garantisce il rispetto del principio di trasparenza e il diritto degli interessati a essere informati in modo chiaro e completo, anche nei casi in cui il consenso non sia materialmente ottenibile.

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

Per i pazienti viventi e 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 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**: Dr.ssa Antonella De Luca
  - **E-mail**: a.deluca@istitutotumori.na.it
  - **Telefono**: 08117770603

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)?

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

Diritto di Rettifica

Il diritto di rettifica consente ai pazienti di correggere i propri dati personali in caso di inesattezze o completare i dati incompleti.

Procedura per Esercitare il Diritto di Rettifica

1. **Richiesta di Rettifica**:
   - I pazienti possono presentare una richiesta di rettifica dei 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 effettuare qualsiasi rettifica, l'Istituto verificherà l'identità del richiedente per garantire che le modifiche siano apportate ai dati della persona corretta. Questo può includere la richiesta di una copia di un documento d'identità.
3. **Rettifica dei Dati**:
   - Una volta verificata l'identità, l'Istituto procederà alla rettifica dei dati personali come richiesto. Il paziente riceverà conferma che le modifiche sono state effettuate.

Diritto di Cancellazione (Diritto all'Oblio)

Il diritto di cancellazione consente ai pazienti di richiedere la cancellazione dei propri dati personali quando non sono più necessari per gli scopi per cui sono stati raccolti o trattati, o se il trattamento è illegale, tra le altre ragioni.

Procedura per Esercitare il Diritto di Cancellazione

1. **Richiesta di Cancellazione**:
   - I pazienti possono presentare una richiesta di cancellazione dei 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 effettuare qualsiasi cancellazione, l'Istituto verificherà l'identità del richiedente per garantire che i dati siano cancellati per la persona corretta. Questo può includere la richiesta di una copia di un documento d'identità.
3. **Valutazione della Richiesta**:
   - L'Istituto valuterà la richiesta per garantire che ci siano motivi legittimi per la cancellazione secondo il GDPR. Ad esempio, i dati personali devono essere cancellati se non sono più necessari per le finalità per cui sono stati raccolti,

se il paziente ritira il consenso e non ci sono altre basi legali per il trattamento, o se il trattamento è illegale.

4. **Cancellazione dei Dati**:
    - Se la richiesta di cancellazione è valida, l'Istituto procederà alla cancellazione dei dati personali. Il paziente riceverà conferma che i dati sono stati cancellati.

Gli interessati possono esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio) 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 corretti e cancellati in modo sicuro e trasparente quando richiesto.

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

Per esercitare i loro diritti di limitazione e di opposizione nel contesto del progetto in oggetto, gli interessati possono seguire un processo strutturato basato sulle normative GDPR.

Esercizio dei Diritti di Limitazione del Trattamento

1. **Richiesta Scritta**
    - Gli interessati possono presentare una richiesta scritta DPO.
    - La richiesta deve includere sufficienti informazioni per identificare l'interessato e specificare chiaramente che si tratta di una richiesta di limitazione del trattamento dei dati personali.
2. **Motivazioni della Richiesta**
    - Gli interessati devono specificare le ragioni per cui richiedono la limitazione, come ad esempio:
        - Contestazione dell'accuratezza dei dati personali.
        - Il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati, preferendo invece la limitazione del loro uso.
        - Il responsabile del trattamento non necessita più dei dati personali ai fini del trattamento, ma gli interessati ne hanno bisogno per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
        - L'interessato si è opposto al trattamento e sta aspettando la verifica se i motivi legittimi del responsabile del trattamento prevalgono su quelli dell'interessato.
3. **Conferma della Ricezione**
    - Il DPO deve confermare la ricezione della richiesta e informare l'interessato delle azioni intraprese entro un mese dalla ricezione della richiesta.

Esercizio dei Diritti di Opposizione

1. **Richiesta Scritta**

- Gli interessati possono inviare una richiesta scritta al responsabile del trattamento o al DPO, indicando chiaramente che si tratta di una richiesta di opposizione al trattamento dei dati personali.
- La richiesta deve includere sufficienti informazioni per identificare l'interessato e specificare le attività di trattamento a cui si oppongono.

2. **Motivazioni della Richiesta**
   - Gli interessati devono spiegare le ragioni dell'opposizione, come ad esempio:
     - Il trattamento si basa su interessi legittimi perseguiti dal responsabile del trattamento o da terzi, e l'interessato desidera opporsi per motivi connessi alla sua situazione particolare.
     - Il trattamento dei dati personali è effettuato per finalità di marketing diretto.
3. **Risposta alla Richiesta**
   - Il responsabile del trattamento deve rispondere senza ingiustificato ritardo e comunque entro un mese dalla ricezione della richiesta. Se il responsabile del trattamento decide di non soddisfare la richiesta dell'interessato, deve fornire una spiegazione dettagliata dei motivi.

Modalità di Contatto

- **Dettagli di Contatto**: Gli interessati possono trovare i dettagli di contatto del responsabile del trattamento e del DPO nel modulo di consenso informato e nelle informative sulla privacy fornite all'inizio del progetto.
- **Canali di Comunicazione**: Le richieste possono essere inviate tramite email, posta o attraverso una piattaforma online dedicata, se disponibile.

Gli interessati nel progetto in oggetto possono esercitare i loro diritti di limitazione e di opposizione presentando richieste scritte al DPO, che devono rispondere entro i termini previsti dalle normative GDPR. Il processo è supportato da misure di sicurezza e trasparenza per garantire che i diritti degli interessati siano rispettati e protetti.

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

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

Diritto di Limitazione del Trattamento

Il diritto di limitazione del trattamento consente ai pazienti di richiedere la limitazione del trattamento dei loro dati personali in determinate circostanze.

Procedura per Esercitare il Diritto di Limitazione

1. **Richiesta di Limitazione**:
   - I pazienti possono presentare una richiesta per limitare il trattamento dei loro dati personali. La richiesta può essere effettuata per iscritto, via e-mail o tramite altri canali di comunicazione forniti dallo studio.

- Le informazioni di contatto per le richieste di limitazione sono fornite nel documento di consenso informato e includono l'indirizzo e-mail e il numero di telefono del Principal Investigator o del coordinatore dello studio.

2. **Verifica dell'Identità**:
   - Prima di procedere con la limitazione del trattamento, l'Istituto verificherà l'identità del richiedente per garantire che la richiesta sia legittima. Questo può includere la richiesta di una copia di un documento d'identità.
3. **Valutazione della Richiesta**:
   - L'Istituto valuterà la richiesta per verificare se rientra nelle condizioni previste dal GDPR per la limitazione del trattamento, che includono:
     - L'interessato contesta l'accuratezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'accuratezza di tali dati.
     - Il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo.
     - Il titolare non ha più bisogno dei dati personali ai fini del trattamento, ma essi sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
     - L'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.
4. **Limitazione del Trattamento**:
   - Se la richiesta di limitazione è valida, l'Istituto procederà a limitare il trattamento dei dati personali. Questo potrebbe comportare la marcatura dei dati personali memorizzati con l'obiettivo di limitare il loro trattamento in futuro. Il paziente riceverà conferma che la limitazione è stata applicata.

Diritto di Opposizione

Il diritto di opposizione consente ai pazienti di opporsi al trattamento dei loro dati personali in determinate circostanze, in particolare quando il trattamento è basato su un interesse pubblico o legittimo del titolare del trattamento.

Procedura per Esercitare il Diritto di Opposizione

1. **Richiesta di Opposizione**:
   - I pazienti possono presentare una richiesta di opposizione al trattamento dei loro dati personali. La richiesta può essere effettuata per iscritto, via e-mail o tramite altri canali di comunicazione forniti dallo studio.
   - Le informazioni di contatto per le richieste di opposizione sono fornite nel documento di consenso informato e includono l'indirizzo e-mail e il numero di telefono del Principal Investigator o del coordinatore dello studio.
2. **Verifica dell'Identità**:
   - Prima di procedere con l'opposizione al trattamento, l'Istituto verificherà l'identità del richiedente per garantire che la richiesta sia legittima. Questo può includere la richiesta di una copia di un documento d'identità.
3. **Valutazione della Richiesta**:

- L'Istituto valuterà la richiesta per verificare se rientra nelle condizioni previste dal GDPR per l'opposizione al trattamento. In particolare, l'interessato ha il diritto di opporsi al trattamento dei dati personali che lo riguardano quando:
  - Il trattamento si basa su un interesse pubblico o legittimo del titolare del trattamento, compresa la profilazione.
  - I dati personali sono trattati per finalità di marketing diretto.

4. **Sospensione del Trattamento**:
   - Se la richiesta di opposizione è valida, l'Istituto sospenderà il trattamento dei dati personali, a meno che non dimostri motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, i diritti e le libertà dell'interessato, oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Il paziente riceverà conferma che l'opposizione è stata applicata.

Gli interessati possono esercitare i loro diritti di limitazione e di opposizione 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 trattati in modo conforme ai diritti degli interessati.

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.
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 presente Valutazione d'Impatto sulla Protezione dei Dati (DPIA) è redatta in quanto il trattamento di dati personali previsto dallo studio COESIT presenta un medio/elevato rischio per i diritti e le libertà delle persone fisiche. Tale obbligo discende dalla presenza concomitante di molteplici criteri identificati dall'art. 35 del GDPR e dalle linee guida del Garante per la Protezione dei Dati Personali. I motivi principali sono:

1. Trattamento di Dati di Soggetti Vulnerabili: I partecipanti allo studio sono pazienti oncologici. In ragione della loro condizione di salute e della relazione di cura con le strutture sanitarie, sono considerati "soggetti vulnerabili". Il trattamento di dati relativi

a questa categoria di interessati richiede un'attenzione e una valutazione dei rischi particolarmente approfondita.

2. Trattamento in Assenza di Consenso (per Dati Retrospettivi): Come esplicitamente previsto dal protocollo, una parte del trattamento riguarda dati di pazienti deceduti o non raggiungibili e si basa sull'art. 110 bis del Codice della Privacy, quindi in assenza di un consenso diretto dell'interessato. Sebbene legittimo, questo scenario richiede una valutazione preventiva dei rischi e delle garanzie ancora più rigorosa, che trova nella DPIA il suo strumento naturale.

La DPIA per lo Studio "COESIT" 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

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 economici relativi alla gestione dei dati recuperati e successivamente persi.

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

Accessi Non Autorizzati, Vulnerabilità nei Sistemi Informatici, Errori Umani, Mancanza di Formazione, Attacchi Informatici, Comportamenti Malintenzionati, Vulnerabilità Software.

6.1.3 Quali sono le fonti di rischio?

Un dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole, ovvero un dipendente che si renda responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione, un utente o il suo entourage, negligente o malintenzionato, che ha accesso illegittimo ai dati archiviati nei database dello studio.

Accessi esterni malevoli e malintenzionati: tentativi non autorizzati da parte di attori esterni (come hacker, criminali informatici o software dannosi) di penetrare il sistema informatico ospedaliero/la rete ospedaliera.

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

Pseudonimizzazione, Minimizzazione dei dati, Limitazione degli accessi, Formazione e Sensibilizzazione, Audit e Controlli Regolari, Sicurezza dei canali informatici, Gestione delle politiche di tutela della privacy, procedure di sicurezza dei sistemi elettronici, valutazione di impatto specifica per gli studi clinici di cui alla delibera 677/2024.

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

Limitata

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, Diffusione risultati della ricerca

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

Accessi Non Autorizzati, Comportamenti Malintenzionati (interni/esterni), Errori Umani

6.2.3 Quali sono le fonti di rischio?

Un dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole, ovvero un

dipendente che si renda responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione, un utente o il suo entourage, negligente o malintenzionato, che ha accesso illegittimo ai dati archiviati nei database dello studio.

Accessi esterni malevoli e maleintenzionati: tentativi non autorizzati da parte di attori esterni (come hacker, criminali informatici o software dannosi) di penetrare il sistema informatico ospedaliero/la rete ospedaliera.

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

Controllo degli accessi logici, Formazione e Sensibilizzazione, Backup, Gestione delle politiche di tutela della privacy, procedure di sicurezza dei sistemi elettronici, valutazione di impatto specifica per gli studi clinici di cui alla delibera 677/2024.

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

Trascurabile

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?

Impossibilità di concludere la ricerca, costi economici relativi alla gestione dei dati recuperati e successivamente persi

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

Errori Umani, Mancanza di Formazione, Errori di Backup, Guasti Hardware, Vulnerabilità Software, Attacchi Informatici, Comportamenti Malintenzionati, Disastri Naturali

6.3.3 Quali sono le fonti di rischio?

Un dipendente che si renda responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione, un utente o il suo entourage, negligente o malintenzionato, che ha accesso illegittimo ai dati archiviati nei database dello studio.

Accessi esterni malevoli e maleintenzionati: tentativi non autorizzati da parte di attori esterni (come hacker, criminali informatici o software dannosi) di penetrare il sistema informatico ospedaliero/la rete ospedaliera.

Sistemi elettronici compromessi.

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

Controllo degli accessi logici, Backup, Sicurezza dei canali informatici, procedure di sicurezza dei sistemi elettronici.

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

Limitata

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

Tutti i dati raccolti sono pseudonimizzati: il codice del paziente è noto solo al centro.
I codici identificativi sono gestiti separatamente e conservati con accesso riservato solo al personale autorizzato.

7.1.2 Minimizzazione dei dati

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

7.1.3 Limitazione dell'Accesso ai Dati

Solo i ricercatori direttamente coinvolti nello studio e con un ruolo specifico hanno accesso ai dati pseudonimizzati. I dati condivisi con altri centri o ricercatori sono resi pseudonimizzati, includendo solo le informazioni strettamente necessarie per le analisi.

7.1.4 Backup

Vengono effettuati backup regolari dei dati per prevenire la perdita di informazioni in caso di guasti tecnici o incidenti su supporto elettronico esterno protetto da password conservato dal PI dello studio.
In ogni caso viene effettuato, come da procedura aziendale, un backup periodico di tutte le cartelle condivise in intranet.

7.1.5 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.

7.1.6 Audit e Controlli Regolari

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

7.1.7 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

7.1.8 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.

7.1.9 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.

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).

7.1.11 Accesso controllato ai locali

Accesso al reparto con badge.

7.1.12 Tracciabilità

- **Autenticazione degli utenti mediante password**:
  - Ogni utente autorizzato (ricercatori, personale medico) dispone di credenziali per accedere ai pc istituzionali.
- **Tracciabilità dei record pseudonimizzati**:
  - I dati dei pazienti sono identificati da un codice pseudonimo, rendendo possibile tracciare l'intero ciclo di vita di ogni record senza esporre dati personali identificativi.

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
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	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.	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 a 12 mesi dalla data di emissione del documento e 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 nel progetto "**COESIT**", 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; 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, procedure di sicurezza dei sistemi elettronici; controllo degli accessi logici; Accesso controllato ai locali; Tracciabilità.
- **Coinvolgimento delle Parti Interessate**: è stato considerato il feedback degli esperti in materia di protezione dei dati.