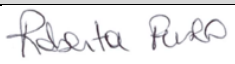
Titolo dello studio	KEAPness: un framework trascrizionale per la diagnosi molecolare della risposta all'immunoterapia nel tumore del polmone con potenziale agnostico
Promotore	IFO-IRE, Istituto Nazionale Tumori Regina Elena
Centro di Sperimentazione	Istituto Nazionale Tumori di Napoli, IRCCS G. Pascale
Principal Investigator	Dott. Alfonso De Stefano S.C. Oncologia Sperimentale Addome Istituto Nazionale Tumori IRCCS Fondazione G. Pascale
Tipo di studio e fase	Studio osservazionale retrospettivo-prospettico, non-farmacologico, di natura biologica, multicentrico
Parere del Comitato Etico	Parere favorevole del 26/07/2024
Durata dello studio	24 mesi
DPO/RPD	Ing. Alessandro Manzoni

	Nome e Cognome	Ruolo	Firma	Data
	Roberta Fusco	Ingegnere Biomedico		28/07/2025
Revisione	Gianfranco De Feo	Quality Assurance		29/07/2025
Approvazione	Maurizio Di Mauro	Titolare del trattamento dati	Firmato digitalmente da: Maurizio Di Mauro Ruolo: IL COMMISSARIO Organizzazione: IRCCS FONDAZIONE G. PASCALE/00911350635 Data: 31/07/2025 12:18:31	
	Alessandro Manzoni	DPO	Firmato digitalmente da: Alessandro Manzoni Ruolo: DIRIGENTE INGEGNERE Organizzazione: IRCCS FONDAZIONE G. PASCALE/00911350635 Data: 30/07/2025 11:28:35	
	Alfonso De Stefano	Principal Investigator Centro Satellite		30/07/2025
	Gianfranco De Feo	Quality Assurance		30/07/2025

Tracking delle modifiche

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

Storico della rivalutazione

Revisione annuale della DPIA o a seguito di verifiche/minacce

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

	Data prevista	Data effettiva	Firma
Rivalutazione a cura del QA			

Tabella dei Contenuti

1. Stima del rischio e pre-assessment

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

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

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

3.2 Soggetti interessati

L'attività interessa il trattamento di dati riguardanti:

- pazienti già in precedenza assistiti presso

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

- pazienti che hanno fornito in precedenza propri campioni biologici presso

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

Non applicabile

RICHIESTA DEL PARERE DEGLI INTERESSATI RELATIVAMENTE ALLA DPIA

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

MOTIVAZIONE DELLA MANCATA RICHIESTA DEL PARERE ALLA DPIA DEGLI INTERESSATI

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

- Tutti i dati clinici dei pazienti sono stati pseudonimizzati. Non vi è alcun utilizzo di dati biometrici, sensibili o correlati a individui identificabili.
- Non vi sono attività di profilazione o decisioni automatizzate che possano influire sugli interessati.
- Valutazione di Rischio: Determinazione che il rischio per i diritti e le libertà degli interessati è basso grazie a misure di protezione implementate e riportano nella DPIA.

- Autorizzazione generale del Garante n. 9/2016 → I trattamenti di dati sanitari per finalità di ricerca scientifica non richiedono necessariamente il coinvolgimento degli interessati nella valutazione d'impatto, se sono adottate misure di sicurezza adeguate.

3.3 Descrizione del trattamento

3.3.1 Quale è il trattamento in considerazione?

La presente DPIA riguarda il trattamento di dati personali effettuato nell'ambito dello studio clinico osservazionale (non interventistico) intitolato "KEAPness: un framework trascrizionale per la diagnosi molecolare della risposta all'immunoterapia nel tumore del polmone con potenziale agnostico", finanziato dal PNRR (codice PNRR-MCNT2-2023-12377963). Il trattamento prevede la raccolta, pseudonimizzazione, conservazione e analisi dei dati personali dei pazienti partecipanti allo studio, mediante sistemi informatici protetti. Le categorie di dati trattati comprendono dati anagrafici (es. informazioni demografiche di base dei soggetti), dati clinici (es. informazioni sanitarie relative ai pazienti affetti da tumore gastrico e pazienti con tumore metastatico differente dal NSCLC e che hanno ricevuto un ICI, alle terapie oncologiche somministrate e alla risposta clinica all'immunoterapia) e dati genetici/molecolari (es. profili di espressione genica e altri marcatori biomolecolari correlati alla patologia e alla risposta ai trattamenti). Tali dati vengono utilizzati esclusivamente per finalità di ricerca scientifica, in conformità al Regolamento (UE) 2016/679 (GDPR) e al Codice in materia di protezione dei dati personali (D.lgs. 196/2003 e s.m.i.). Tutti i dati dei partecipanti sono trattati in forma pseudonimizzata e custoditi su sistemi informatici sicuri, con l'adozione di misure tecniche e organizzative adeguate a garantire la riservatezza e la protezione delle informazioni trattate.

3.3.2 Quali sono le responsabilità connesse al trattamento?

Il trattamento dei dati personali riferiti ai partecipanti arruolati presso l'IRCCS "Fondazione Pascale" avviene sotto la responsabilità del medesimo Istituto, che agisce in qualità di Titolare autonomo del trattamento, ai sensi dell'art. 4, par. 7 del Regolamento (UE) 2016/679 (GDPR). Lo studio è promosso scientificamente dall'IFO-IRCCS (Istituto Nazionale Tumori Regina Elena), che tuttavia non riveste il ruolo di titolare per i dati raccolti localmente dal Pascale, né accede ai dati in forma identificabile.
I dati sono trattati esclusivamente da personale autorizzato e istruito, nel rispetto dell'art. 29 GDPR e dell'art. 2-quaterdecies del Codice Privacy. L'IRCCS Pascale ha designato i propri soggetti responsabili del trattamento ove necessario (es. laboratori, fornitori tecnici), mediante specifici contratti ex art. 28 GDPR.
Eventuali trasferimenti di dati pseudonimizzati o campioni biologici a soggetti terzi, incluso il promotore scientifico, avvengono solo se previsti nel protocollo e regolati da Material Transfer Agreement (MTA) e altri accordi conformi al GDPR. Il DPO dell'IRCCS "Fondazione Pascale" svolge attività di vigilanza e supporto rispetto alla protezione dei dati personali.

Eventuali accessi da parte di organismi di controllo (Comitato Etico, Autorità Garante, autorità sanitarie) avvengono esclusivamente per le finalità previste dalla normativa vigente, nel rispetto della riservatezza dei partecipanti.

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 dai partecipanti, assicurando che siano a conoscenza di come saranno utilizzati i loro dati.
- Valutazione dell'Impatto sulla Protezione dei Dati (DPIA): Condurre una DPIA 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 per 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 per il Centro di Sperimentazione il dott. Alfonso De Stefano.
Responsabilità:
Sicurezza dei Dati: Adottare misure tecniche e organizzative adeguate a garantire la sicurezza dei dati personali.

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.

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

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

3.3.3 Ci sono standard applicabili al trattamento?

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

1. Regolamento Generale sulla Protezione dei Dati (GDPR)
Il GDPR è il principale standard legale per la protezione dei dati personali nell'Unione Europea. Ecco alcuni dei requisiti chiave:
Principi del Trattamento dei Dati: I dati personali devono essere trattati in modo lecito, corretto e trasparente; raccolti per finalità determinate, esplicite e legittime; adeguati, pertinenti e limitati a quanto necessario; esatti e, se necessario, aggiornati; conservati in una forma che consenta l'identificazione degli interessati per un periodo non superiore al necessario; trattati in modo da garantire la sicurezza adeguata dei dati.
Diritti degli Interessati: Gli interessati hanno il diritto di accesso, rettifica, cancellazione, limitazione del trattamento, portabilità dei dati e opposizione al trattamento.
Valutazione d'Impatto sulla Protezione dei Dati (DPIA): Necessaria quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
Sicurezza dei Dati: Obbligo di implementare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Notifica di Violazione dei Dati: Obbligo di notificare le violazioni dei dati personali all'autorità di controllo entro 72 ore e, in certi casi, agli interessati.

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

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

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

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

6. Standard di sicurezza e qualità applicati
- Good Clinical Practice (ICH-GCP E6 R2).
- Good Pharmacoepidemiology Practices (GPP).
- ISO/IEC 27001 per la gestione della sicurezza delle informazioni.
- ISO/IEC 27002, 27017, 27018, ove applicabili, per la protezione dei dati in ambienti cloud e sanitari.
- 21 CFR Part 11 (FDA, per sistemi elettronici conformi).
- OSSTMM e OWASP per la sicurezza delle applicazioni web (es. piattaforma eCRF).
- NIST SP 800-115 per il penetration testing e la gestione dei rischi IT.
- Standard di pseudonimizzazione e crittografia riconosciuti a livello europeo.

3.4 Dati, processi e risorse di supporto

3.4.1 Quali sono i dati trattati?

Dati anagrafici e demografici (pseudonimizzati):

- Età
- Sesso
- Eventualmente centro clinico di arruolamento

Dati clinici e sanitari:

- Diagnosi istologica (es. NSCLC, tumore gastrico, tumore metastatico differente dal NSCLC e che hanno ricevuto un ICI)
- Stadio della malattia
- ECOG Performance Status (PS)
- Numero e sedi di metastasi
- Eventuali recidive
- Tipologia e data di trattamenti ricevuti (chemioterapia, immunoterapia, radioterapia, ecc.)
- Risposta ai trattamenti (es. risposta obiettiva, PFS, OS)
- Follow-up clinico (inclusi eventi di progressione e sopravvivenza)
- Dati genetici e molecolari (ottenuti da tessuti tumorali):
- Mutazioni somatiche (es. KEAP1, NRF2 e altre)
- CNAs (Copy Number Alterations)
- Riarrangiamenti genici
- Espressione genica (RNA-seq)
- Firma molecolare KEAPness
- TMB (Tumor Mutational Burden)
- Firma immunitaria/microambientale (es. classificazione immunofenotipica)
- Presenza di neo-antigeni (HLA typing, predizione epitopica)

Dati derivati da analisi di laboratorio sperimentali:

- Risultati funzionali da linee cellulari (saggi di vitalità, risposta a farmaci)
- Eventuali risultati di manipolazione genetica in vitro (CRISPRi, overespressione genica)
- Dati identificativi indiretti (solo a livello locale):
- Codice univoco assegnato allo studio (pseudonimo)
- Collegamento tra codice e identità personale custodito esclusivamente presso il centro

Tutti i dati sono trattati in forma pseudonimizzata, e non vengono trasferiti con elementi identificativi diretti. L'identificabilità del soggetto è possibile solo a livello locale per esigenze cliniche o diritti dell'interessato, sotto il controllo del Titolare del trattamento (es. IRCCS Pascale).

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

Nell'ambito dello studio "KEAPness", il ciclo di vita del trattamento dei dati presso il centro si sviluppa come segue:

1. Raccolta dati
    - Viene effettuata retrospettivamente, accedendo alle cartelle cliniche o archivi pre-esistenti relativi a pazienti che soddisfano i criteri di inclusione.
    - Viene effettuata prospetticamente, mediante raccolta di dati clinici (diagnosi, terapia, follow-up) e prelievo di campioni biologici (tessuto tumorale) durante il percorso clinico dei pazienti arruolati.
2. Pseudonimizzazione
    - Ad ogni paziente viene assegnato un codice identificativo univoco utilizzato nelle registrazioni di progetto.
    - Le informazioni identificative (nome, cognome, codice fiscale, ecc.) restano locali al centro e non sono trasferite né accessibili al promotore.
3. Registrazione e archiviazione
    - I dati — in forma pseudonimizzata — sono registrati su registri cartacei o sistemi informatici locali, protetti da misure di sicurezza (accesso autorizzato, ambienti controllati).
    - I campioni biologici sono conservati in biobanche o depositi dedicati, etichettati con il medesimo codice.
4. Elaborazione e analisi
    - I dataset vengono utilizzati per analisi statistico-bioinformatiche volte a identificare la firma trascrizionale KEAPness, biomarcatori molecolari e correlazioni con la risposta all'immunoterapia.
    - Le analisi includono tecniche come WES (Whole Exome Sequencing), RNA-seq (Whole Transcriptome Sequencing), analisi clonale, e metodologie funzionali in vitro.
5. Condivisione dei dati e dei campioni
    - I dati pseudonimizzati e i campioni biologici possono essere condivisi con il promotore o laboratori terzi solo se previsto dal protocollo, e previa formalizzazione mediante accordi specifici (es. Material Transfer Agreement, nomina a responsabile art. 28 GDPR).
    - In nessun caso vengono condivisi dati identificativi diretti.
6. Monitoraggio e controllo
    - Vengono effettuate attività di controllo qualità sui dati raccolti (accuratezza, completezza) e tracciamento degli accessi o modifiche (audit trail), nel rispetto di eventuali verifiche effettuate dal Comitato Etico o altre autorità.
7. Conservazione secondaria e riuso
    - Al termine dello studio, i dati e i campioni possono essere conservati per un ulteriore periodo, in forma pseudonimizzata o anonimizzata, per futuri studi compatibili con le finalità della ricerca, con approvazione del Comitato Etico e in rispetto dell'art. 89 GDPR.
8. Cancellazione o anonimizzazione

- Al termine dei periodi autorizzati, i dati personali sono cancellati o resi irreversibilmente anonimi, garantendo l'impossibilità di re-identificare i soggetti.

3.4.3 Quali sono le risorse di supporto ai dati?

Le risorse di supporto ai dati utilizzate presso l'IRCCS "Fondazione Pascale" nell'ambito dello studio KEAPness comprendono:

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

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

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

4. Valutazione di necessità e proporzionalità del trattamento

4.1 Proporzionalità e necessità

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

1. Specifici:
   Il trattamento dei dati personali è finalizzato unicamente allo svolgimento dello studio di ricerca clinico-traslazionale "KEAPness", il cui obiettivo è sviluppare e validare strumenti molecolari per prevedere la risposta all'immunoterapia nei tumori solidi, in particolare NSCLC e tumore gastrico. Le finalità sono chiaramente descritte nel protocollo, suddivise in tre obiettivi scientifici distinti (identificazione della firma KEAPness, tracciamento evolutivo clonale, analisi funzionale preclinica).

2. Espliciti:
   Le finalità sono dichiarate in modo trasparente nel protocollo e nei documenti informativi rivolti ai pazienti (consenso informato), e risultano coerenti con le attività scientifiche previste. I dati raccolti sono trattati unicamente per queste finalità, senza usi incompatibili.
3. Legittimi:
   Il trattamento è giustificato dall'art. 9(2)(j) del GDPR ("trattamento necessario per finalità di ricerca scientifica") e dagli artt. 99–110-bis del Codice Privacy italiano. Il trattamento avviene inoltre nel rispetto dei principi di minimizzazione, proporzionalità e tutela dei diritti dell'interessato.

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

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

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

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

I dati raccolti nello studio "KEAPness" sono adeguati, pertinenti e limitati a quanto strettamente necessario per il raggiungimento delle specifiche finalità scientifiche previste dal protocollo. In particolare, sono trattate le seguenti categorie di dati:

- Dati anagrafici minimi (es. età, sesso), utili alla caratterizzazione dei soggetti;
- Dati clinici rilevanti ai fini dell'analisi di efficacia dell'immunoterapia (es. diagnosi, stadio di malattia, trattamenti ricevuti, risposta terapeutica);

- Dati molecolari/genetici essenziali per lo studio della firma trascrizionale KEAPness e l'identificazione di biomarcatori predittivi;
- Dati derivati da campioni biologici raccolti in modo mirato e specifico.

Durante la progettazione dello studio è stato applicato il principio di data minimization ai sensi dell'art. 5, par. 1, lett. c) del GDPR, evitando la raccolta di dati non pertinenti o non necessari rispetto alle finalità indicate. I dati identificativi diretti non sono oggetto di trasferimento e rimangono accessibili esclusivamente presso il centro di arruolamento, garantendo la massima protezione dei partecipanti.

4.1.4 I dati sono esatti e aggiornati?

I dati raccolti nell'ambito dello studio "KEAPness" sono acquisiti da fonti ufficiali e affidabili, quali le cartelle cliniche ospedaliere, i registri sanitari e la documentazione medica disponibile presso il centro, garantendone l'esattezza al momento della registrazione.
Nel caso di raccolta prospettica, i dati sono aggiornati direttamente dal personale clinico incaricato, in tempo reale o in prossimità dell'evento clinico, secondo quanto previsto nel protocollo.
Nel caso di dati retrospettivi, viene verificata la coerenza e completezza delle informazioni raccolte, con possibilità di aggiornamento in fase di revisione clinica. Il centro adotta procedure di controllo interno per garantire l'accuratezza e, ove necessario, l'aggiornamento dei dati.
Il principio di esattezza (art. 5, par. 1, lett. d) del GDPR) è rispettato mediante la verifica dei dati da parte di personale autorizzato, che ha accesso diretto alla documentazione sanitaria originale. Errori o discrepanze eventualmente rilevati vengono corretti nel rispetto della tracciabilità delle modifiche.

4.1.5 Qual è il periodo di conservazione dei dati?

Fase attiva dello studio
I dati personali e molecolari dei partecipanti sono conservati per l'intera durata dello studio, comprensiva delle analisi, validazioni e pubblicazioni previste nel protocollo.

Estensione post-studio (conservazione secondaria)
Dopo la chiusura dello studio, le informazioni pseudonimizzate possono essere conservate per un periodo aggiuntivo allo scopo di:

- garantire la conclusione delle attività scientifiche (es. richieste di accesso ai dati da parte del promotore o autorità);
- consentire un eventuale **riuso per studi affini**, purché approvati dal Comitato Etico e conformi all'art. 89 del GDPR e all'art. 110-bis del Codice Privacy.

Cancellazione o anonimizzazione
Al termine del periodo autorizzato, i dati personali verranno:

- **cancellati** o

- **irreversibilmente anonimizzati**, rendendo impossibile la re-identificazione dei soggetti, conformemente agli obblighi legali e regolamentari.

Questa politica garantisce che i dati vengano conservati solo per il tempo strettamente necessario alle finalità dello studio, assicurando la conformità al principio di limitazione della conservazione di cui all'art. 5 GDPR.

4.2 Misure a tutela dei diritti degli interessati

4.2.1 Come sono informati del trattamento gli interessati?

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

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

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

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

Procedura per Esercitare il Diritto di Accesso

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

trattamento, le categorie di dati trattati e qualsiasi altra informazione richiesta dal GDPR.
- Le informazioni saranno fornite in un formato chiaro e comprensibile.

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

Procedura per Esercitare il Diritto di Portabilità dei Dati
1. **Richiesta di Portabilità**:
   - I pazienti possono presentare una richiesta per ottenere i loro dati personali in un formato portabile. La richiesta può essere effettuata al DPO.
   - Informazioni di contatto per le richieste di accesso sono generalmente fornite nel documento di informativa al trattamento dei dati e includono l'indirizzo e-mail del DPO.
2. **Verifica dell'Identità**:
   - Come per il diritto di accesso, l'Istituto verificherà l'identità del richiedente per garantire che i dati personali siano rilasciati alla persona corretta.
3. **Fornitura dei Dati**:
   - I dati personali saranno forniti in un formato strutturato, di uso comune e leggibile da dispositivo automatico (ad esempio, formato CSV o XML).
   - Se richiesto, i dati possono essere trasmessi direttamente a un altro titolare del trattamento indicato dal paziente, a condizione che ciò sia tecnicamente fattibile.

Contatti per Esercitare i Diritti
- **DPO**: Ing. Alessandro Manzoni
  - **E-mail**: a.manzoni@istitutotumori.na.it
- **Principal Investigator**: Dott. Alfonso De Stefano
  - **E-mail**: a.destefano@istitutotumori.na.it
  - **Telefono**: 08117770359

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

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

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

Al Titolare locale (Centro sperimentale – Istituto Pascale)

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

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

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

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

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

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

Contatto con il Centro sperimentale (Istituto Pascale)

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

Eccezioni e limiti

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

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

L'Istituto agisce come titolare autonomo del trattamento, in relazione alla raccolta e pseudonimizzazione dei dati. Tuttavia, interagisce con i responsabili incaricati dal promotore sulla base di:

- Accordi contrattuali e documenti di adesione allo studio, che disciplinano ruoli e responsabilità.
- Procedure operative condivise (SOP).
- Designazione interna del personale autorizzato e formazione sul rispetto della normativa privacy.

Questi contratti e accordi garantiscono che tutti i soggetti coinvolti trattino i dati personali in modo conforme al principio di responsabilizzazione (accountability) e al quadro normativo del Regolamento (UE) 2016/679.

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

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

5. Motivi della valutazione d'impatto

La presente valutazione d'impatto sulla protezione dei dati (DPIA) è stata effettuata in conformità all'art. 35 del Regolamento (UE) 2016/679 (GDPR), in quanto il trattamento dei dati personali previsto dallo studio "KEAPness" presenta un rischio elevato per i diritti e le libertà fondamentali degli interessati, a causa di una o più delle seguenti condizioni:

1. Trattamento di categorie particolari di dati (art. 9 GDPR)

   Lo studio prevede il trattamento di dati personali sensibili, in particolare dati relativi alla salute, genetici, biologici e molecolari raccolti da soggetti con patologie oncologiche.

2. Volume e complessità dei dati trattati

   Sono oggetto di trattamento informazioni cliniche dettagliate e dati derivanti da tecniche avanzate di analisi (es. RNA-seq, WES), che richiedono elevati livelli di protezione e un'attenta gestione in termini di pseudonimizzazione, accesso e conservazione.

3. Mancanza di possibilità per l'interessato di esercitare pienamente alcuni diritti

   In applicazione dell'art. 89 GDPR e dell'art. 110-bis del Codice Privacy, alcuni diritti

dell'interessato (come il diritto alla cancellazione) possono essere limitati, rendendo necessaria una valutazione preventiva dell'impatto del trattamento.

4. Coinvolgimento di più soggetti esterni (multi-centro, laboratori, partner tecnici)

   La pluralità di soggetti coinvolti nel trattamento comporta un rischio aggiuntivo legato alla circolazione di dati pseudonimizzati, che richiede un'analisi dettagliata delle misure tecniche e organizzative adottate.

6. Valutazione dei Rischi

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

6.1 Accesso illegittimo ai dati

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

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

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

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

6.1.3 Quali sono le fonti di rischio?

Umano, Strumenti vulnerabili.

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

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

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

Importante/Grave

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

Poco Probabile

6.2 Modifiche indesiderate dei dati

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

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

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

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

Emergenza non sanitaria con impatto sul sistema informatico (incendio, alluvione, terremoto).

6.2.3 Quali sono le fonti di rischio?

Strumenti vulnerabili, Umano

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

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

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

Importante/Grave

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

Poco probabile

6.3 Perdita di dati

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

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

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

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

6.3.3 Quali sono le fonti di rischio?

Strumenti vulnerabili, Umano.

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

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

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

Grave/Importante

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

Poco Probabile

7. Piano d'azione

7.1 Mitigazione dei rischi con Misure esistenti o pianificate

7.1.1 Pseudonimizzazione

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

7.1.2 Formazione e Sensibilizzazione

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

7.1.3 Tracciabilità

- **Autenticazione degli utenti mediante password**:
  - Ogni utente autorizzato (ricercatori, personale medico) dispone di credenziali per accedere alla piattaforma.
- **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.

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

7.1.5 Gestione delle politiche di tutela della privacy
Il titolare del trattamento segue la procedura istituzionale che garantisce la tutela della privacy: Regolamento per la protezione dei dati personali in attuazione del D. Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali".
Il titolare garantisce Trasparenza e Comunicazione:
- Informazione chiara e trasparente sulle finalità del trattamento e sulle modalità di esercizio dei diritti degli interessati.
- Pubblicazione di informazioni relative allo studio e ai suoi scopi, quando possibile, per mantenere la trasparenza con il pubblico e con gli interessati.

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

7.1.6 Minimizzazione dei dati
La CRF raccoglie solo le variabili essenziali per le finalità dello studio, in conformità al principio di necessità e minimizzazione (art. 5.1.c GDPR).

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

7.1.8 Limitazione dell'Accesso ai Dati
Solo i ricercatori direttamente coinvolti nello studio e con un ruolo specifico hanno accesso ai dati pseudonimizzati. I dati condivisi con il promotore sono resi pseudonimizzati, includendo solo le informazioni strettamente necessarie per lo studio.

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

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

7.1.11 Procedure di sicurezza dei sistemi elettronici
I server 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.
I server sono protetti da firewall configurati per bloccare accessi non autorizzati.

Sistemi di rilevamento delle intrusioni (IDS) monitorano continuamente il traffico per individuare comportamenti anomali o potenziali attacchi.
I sistemi sono dotati di software antivirus aggiornati regolarmente per prevenire malware e attacchi informatici.
Tutti i software utilizzati (sistemi operativi, applicazioni) vengono aggiornati periodicamente per risolvere vulnerabilità note.

7.1.12 Accesso controllato ai locali
Accesso al reparto con badge.

7.1.13 Contrattualizzazione con Responsabili Esterni
Contrattualizzazione chiara con i Responsabili Esterni (promotore) e acquisizione di accordi scritti che definiscano obblighi, ruoli e misure di protezione (art. 28 GDPR).

7.2 Panoramica dei rischi

7.2.1 Analisi complessiva del dell'entità del rischio

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

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

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

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

Gravità (G)		**Descrizione**
5	Gravissima	Possibilità di lesione grave (ad esempio, lesione permanente o lesione che richiede ospedalizzazione o

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

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

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

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

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