

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 1 di 39

Titolo dello studio	Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS
Promotore	Istituto Nazionale Tumori IRCCS "Fondazione G. Pascale" (Promotore e Titolare del trattamento).
Centro Sperimentale	IRCCS Istituto Nazionale Tumori "Fondazione G. Pascale" di Napoli (unico centro, promotore e titolare del trattamento)
Principal Investigator (PI)	Dr. Rizio Esposito Abate S.C. Biologia Cellulare e Bioterapie - IRCCS Istituto Nazionale Tumori "Fondazione G. Pascale"
Tipo di studio e fase	Osservazionale, retrospettivo-prospettico, monocentrico, no-profit (Progetto di Ricerca Finalizzata Ministero della Salute, GR-2024-12377633)
Parere del Comitato Etico	Parere favorevole del Comitato Etico Territoriale Campania 1 (CET Campania 1), Protocollo n. 38/26 OSS, rilasciato in data 15/06/2026.
Durata dello studio	36 mesi
DPO/RPD	Ing. Alessandro Manzoni

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 2 di 39

	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: 03/09/2026 15:24:57	
	Elisa Pintauro	Ricercatore Sanitario	Firmato digitalmente da: Elisa Pintauro Ruolo: RICERCATORE SANITARIO DS Organizzazione: IRCCS FONDAZIONE G. PASCALE/00911350635 Data: 03/09/2026 15:00:22	
Revisione	Gianfranco De Feo	Quality Assurance	Firmato digitalmente da: Gianfranco De Feo Ruolo: DIRIGENTE SANITARIO Organizzazione: IRCCS FONDAZIONE G. PASCALE/00911350635 Data: 22/09/2026 08:25:11	
Approvazione	Maurizio Di Mauro	Titolare del trattamento dati	Firmato digitalmente da: Maurizio Di Mauro Ruolo: DIRETTORE GENERALE Organizzazione: IRCCS FONDAZIONE G. PASCALE/00911350635 Data: 30/08/2026 12:46:40	
	Alessandro Manzoni	DPO	Firmato digitalmente da: Alessandro Manzoni Ruolo: DIRIGENTE INGEGNERE Organizzazione: IRCCS FONDAZIONE G. PASCALE/00911350635 Data: 22/09/2026 12:12:55	
	Riziero Esposito Abate	Sperimentatore principale	Firmato digitalmente da: Riziero Esposito Abate Data: 08/09/2026 16:07:12	
	Gianfranco De Feo	Quality Assurance	Firmato digitalmente da: Gianfranco De Feo Ruolo: DIRIGENTE SANITARIO Organizzazione: IRCCS FONDAZIONE G. PASCALE/00911350635 Data: 22/09/2026 08:25:12	

Tracking delle modifiche

N° Rev.	Data	Motivo della modifica	Paragrafi	Pagine
0	01.07.2026	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

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 3 di 39

	Data prevista	Data effettiva	Firma
Rivalutazione a cura del QA			

Tabella dei Contenuti

Tracking delle modifiche	2
Storico della rivalutazione	2
1. Stima del rischio e pre-assessment.....	6
1.1 Stima del rischio.....	8
2. Quadro normativo	8
3. Contesto	9
3.1 Titolare e Responsabile della Protezione dei Dati	9
3.2 Soggetti interessati	9
3.3 Descrizione del trattamento	10
3.3.1 Quale è il trattamento in considerazione?	10
3.3.2 Quali sono le responsabilità connesse al trattamento?	11
3.3.3 Ci sono standard applicabili al trattamento?	13
3.4 Dati, processi e risorse di supporto	15
3.4.1 Quali sono i dati trattati?	15
3.4.2 Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?	16
3.4.3 Quali sono le risorse di supporto ai dati?	17
4. Valutazione di necessità e proporzionalità del trattamento.....	17
4.1 Proporzionalità e necessità.....	17
4.1.1 Gli scopi del trattamento sono specifici, espliciti e legittimi?	17
4.1.2 Quali sono le basi legali che rendono lecito il trattamento?	18
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)?	19
4.1.4 I dati sono esatti e aggiornati?	19
4.1.5 Qual è il periodo di conservazione dei dati?	20
4.2 Misure a tutela dei diritti degli interessati.....	20
4.2.1 Come sono informati del trattamento gli interessati?	20

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 4 di 39

4.2.2 Ove applicabile: come si ottiene il consenso degli interessati?	21
4.2.3 Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?	21
4.2.4 Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?	23
4.2.5 Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?	24
4.2.6 Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?	25
4.2.7 In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?	26
5. Motivi della valutazione d'impatto.....	26
6. Valutazione dei Rischi.....	27
6.1 Accesso illegittimo ai dati	27
6.1.1 Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?	27
6.1.2 Quali sono le principali minacce che potrebbero concretizzare il rischio?	27
6.1.3 Quali sono le fonti di rischio?	27
6.1.4 Quali misure fra quelle individuate contribuiscono a mitigare il rischio?	28
6.1.5 Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?	28
6.1.6 Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?	28
6.2 Modifiche indesiderate dei dati	28
6.2.1 Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?	28
6.2.2 Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?	28
6.2.3 Quali sono le fonti di rischio?	28
6.2.4 Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?	29
6.2.5 Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?	29
6.2.6 Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?	29
6.3 Perdita di dati.....	29
6.3.1 Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?	29

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 5 di 39

6.3.2 Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?	29
6.3.3 Quali sono le fonti di rischio?	29
6.3.4 Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?	30
6.3.5 Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?	30
6.3.6 Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?	30
7. Piano d’azione	30
7.1 Mitigazione dei rischi con Misure esistenti o pianificate	30
7.1.1 Pseudonimizzazione	30
7.1.2 Minimizzazione dei dati	31
7.1.3 Limitazione dell'Accesso ai Dati	31
7.1.4 Backup	31
7.1.5 Formazione e Sensibilizzazione	31
7.1.6 Audit e Controlli Regolari	31
7.1.7 Sicurezza dei canali informatici	31
7.1.8 Gestione delle politiche di tutela della privacy	31
7.1.9 Procedure di sicurezza dei sistemi elettronici	31
7.1.10 Controllo degli accessi logici	32
7.1.11 Accesso controllato ai locali	32
7.1.12 Tracciabilità	32
7.1.13 Conservazione e archiviazione dei dati	32
7.1.14 Architettura e privacy by design	33
7.1.15 Gestione dei rapporti tra titolari e responsabili	33
7.2 Panoramica dei rischi	33
8. Risultato della DPIA	39

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 6 di 39

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

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 7 di 39

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

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 8 di 39

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	SI
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.

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 9 di 39

3. Contesto

3.1 Titolare e Responsabile della Protezione dei Dati

Titolare del trattamento dei Suoi dati personali è il Legale Rappresentante dell’ Istituto Nazionale Tumori IRCCS “Fondazione G. Pascale”. Responsabile scientifico (PI) dello studio: Dr. Riziero Esposito Abate

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

NA

- Altro

NA

RICHIESTA DEL PARERE DEGLI INTERESSATI RELATIVAMENTE ALLA DPIA

- ☐ È stato richiesto il parere degli interessati
☒ 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 presente Valutazione d’Impatto sulla Protezione dei Dati, ai sensi dell’art. 35, par. 9, del Regolamento (UE) 2016/679, sono di seguito esposte.

Lo studio heRAco tratta dati relativi alla salute e dati genetici (somatici), riconducibili alle categorie particolari di dati personali di cui all’art. 9 del GDPR. Tali dati sono trattati esclusivamente in forma pseudonimizzata: a ciascun partecipante viene assegnato un codice identificativo univoco; le informazioni direttamente identificative (nome, cognome,

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 10 di 39

codice fiscale, data di nascita completa) non sono associate ai dati dello studio nei sistemi di analisi. La lista di decodifica che consente il collegamento tra il codice pseudonimo e l'identità del paziente è custodita esclusivamente presso l'IRCCS Fondazione G. Pascale, su risorse distinte dai database di analisi e ad accesso strettamente controllato, riducendo significativamente il rischio di re-identificazione. Lo studio heRAco prevede la raccolta di dati genomici somatici (profilo mutazionale tumorale mediante Comprehensive Genomic Profiling, OncoPrint Comprehensive Plus; analisi del DNA tumorale circolante mediante Avida OncoLB) e dati trascrittomici (RNA-seq mediante AmpliSeq Transcriptome), nonché dati radiomici estratti da immagini TC. Non è prevista l'analisi di varianti germinali né il trattamento di dati biometrici.

Non vi sono, inoltre, attività di profilazione né processi decisionali automatizzati che producano effetti giuridici o incidano in modo analogo significativamente sugli interessati: i dati sono utilizzati esclusivamente in forma aggregata per finalità di ricerca scientifica svolte nell'interesse pubblico, ai sensi dell'art. 9(2)(j) del GDPR, dell'art. 110 del D.Lgs. 196/2003 e successive modifiche, e in conformità ai Provvedimenti del Garante n. 146/2019 e del 9 maggio 2024 (Regole deontologiche per il trattamento a fini statistici o di ricerca scientifica). A esito della presente valutazione, il rischio residuo per i diritti e le libertà degli interessati è stimato basso, grazie alle misure tecniche e organizzative implementate e descritte nella sezione 7 della presente DPIA.

In considerazione della pseudonimizzazione applicata, dell'assenza di processi decisionali automatizzati e del livello di rischio residuo stimato, la consultazione preventiva degli interessati ai sensi dell'art. 35, par. 9, del GDPR è stata ritenuta non necessaria. Resta ferma la piena attuazione degli obblighi informativi previsti dagli artt. 13 e 14 del GDPR nei confronti dei pazienti viventi e contattabili (mediante foglio informativo e modulo di consenso informato sottoscritto prima dell'inclusione nello studio) e, per i pazienti deceduti o non rintracciabili dopo ragionevoli tentativi documentati (verifica dei registri clinici, consultazione della documentazione sanitaria, utilizzo dei recapiti telefonici eventualmente disponibili in cartella, accesso a dati di contatto pubblicamente accessibili), il trattamento è effettuato senza consenso ai sensi dell'art. 110-bis, comma 4, del Codice Privacy, applicando le garanzie dei Provvedimenti del Garante n. 146/2019 e del 9 maggio 2024 e sulla base di parere favorevole motivato del Comitato Etico, con adempimento degli obblighi di trasparenza tramite pubblicazione della presente DPIA sul sito istituzionale del Centro (IRCCS Fondazione G. Pascale).

3.3 Descrizione del trattamento

3.3.1 Quale è il trattamento in considerazione?

Lo studio heRAco ha natura osservazionale, retrospettivo-prospettica, monocentrica e no-profit. Promotore, unico centro di arruolamento e Titolare del trattamento è l'Istituto Nazionale Tumori IRCCS “Fondazione G. Pascale”, sotto la responsabilità del Dr. Riziero Esposito Abate (Principal Investigator, S.C. Biologia Cellulare e Bioterapie) e con la co-responsabilità della Dott.ssa Alessandra Sacco (Co-PI).

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 11 di 39

Il protocollo prevede: (a) per la parte retrospettiva, l’analisi di 150 campioni FFPE e dati clinici già disponibili presso la Biobanca e la cartella clinica dell’IRCCS Pascale, relativi a pazienti con CRC BRAFV600E trattati con terapie target; (b) per la parte prospettica, l’arruolamento di 20 nuovi pazienti con raccolta di campioni biologici freschi (sangue periferico per ctDNA, tessuto biotico) e dati clinici. I dati molecolari (CGP, RNA-seq, ctDNA) e radiomici vengono generati e analizzati internamente all’IRCCS Fondazione G. Pascale. Lo studio non prevede trasferimento di dati verso centri esterni o infrastrutture esterne all’Istituto. La durata complessiva è di 36 mesi. La numerosità campionaria totale è di 170 pazienti (150 retrospettivi + 20 prospettici).

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)

Trattandosi di uno studio monocentrico, l’unico Titolare del Trattamento è l’Istituto Nazionale Tumori IRCCS “Fondazione G. Pascale”, che riveste contestualmente il ruolo di Promotore dello studio. Il trattamento dei dati è interamente svolto all’interno dell’Istituto, sotto la responsabilità del Dr. Rizio Esposito Abate (PI, S.C. Biologia Cellulare e Bioterapie). Non è previsto alcun trasferimento di dati verso centri o soggetti esterni. Eventuali fornitori di servizi tecnici/IT (es. manutenzione di sistemi informativi istituzionali) operano come responsabili del trattamento ai sensi dell’art. 28 GDPR, attraverso specifici Data Processing Agreement.

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.).

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 12 di 39

- 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 lo studio heRAco, questo ruolo è svolto dal Dr. Rizio Esposito Abate, in qualità di Principal Investigator (PI) presso la S.C. Biologia Cellulare e Bioterapie dell'IRCCS Fondazione G. Pascale.

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. Ricercatori e personale clinico dello studio

I ricercatori e il personale clinico coinvolti nello studio devono essere adeguatamente formati sul trattamento dei dati e tenuti al rispetto della normativa vigente in materia di protezione dei dati personali.

Responsabilità:

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 13 di 39

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.

- 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.
- FAQ del Garante della Privacy (<https://www.garanteprivacy.it/temi/sanita-e-ricerca-scientifica/irccs>): Nel caso in cui gli IRCCS fondino il trattamento dei dati raccolti per finalità di cura per ulteriori finalità di ricerca sull’art. 110-bis, comma 4 del Codice,

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 14 di 39

essi devono obbligatoriamente svolgere e pubblicare la Valutazione d'impatto, sui propri siti web, in quanto tale articolo costituisce una di quelle disposizioni di legge alle quali fa riferimento l'art. 110 del Codice, prescrivendo tali ulteriori adempimenti"; "Qualora la pubblicazione per intero della VIP possa ledere diritti di proprietà intellettuale, segreti commerciali o altro, il titolare del trattamento può pubblicarla per estratto. Il mancato adempimento di tali obblighi comporta l'applicazione di una sanzione amministrativa, ai sensi dell'art. 166, comma 1 del Codice e dell'art. 83, par. 4 del Regolamento

- 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'INT IRCCS 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).

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 15 di 39

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?

Nell'ambito del trattamento oggetto della presente DPIA sono trattate le seguenti categorie di dati personali:

Dati personali comuni (pseudonimizzati):

- Nome, cognome e/o iniziali del paziente (utilizzati esclusivamente per la compilazione della lista di decodifica conservata presso ciascun centro, non trasmessa al promotore)
- Data di nascita
- Sesso

Dati particolari ai sensi dell'art. 9 GDPR (dati relativi alla salute):

- Diagnosi di carcinoma del colon-retto (CRC) con mutazione BRAFV600E confermata, data della diagnosi, sede del tumore primitivo (colon destro/sinistro/retto), stadio alla diagnosi (staging TNM), sedi di malattia metastatica, status di consensus molecolare (MSS/MSI-H), stato mutazionale di RAS (KRAS/NRAS wild-type)
- Stadio della malattia al momento della diagnosi
- Caratteristiche istopatologiche (tipo istologico adenocarcinoma, grado di differenziazione), report di patologia con documentazione della mutazione BRAFV600E (NGS o PCR), codice ICD-O/3 (C18-C20)
- Dati clinici al basale: performance status (ECOG PS), , imaging TC basale (con misurazioni lesioni target e non-target secondo RECIST 1.1), terapie target anti-BRAF/MEK ricevute (encorafenib + binimetinib, vemurafenib + cobimetinib,

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 16 di 39

dabrafenib + trametinib), linea di trattamento, durata del trattamento, risposta al trattamento (ORR, DCR, PFS, OS), tossicità (CTCAE v5.0), campioni biologici raccolti (FFPE, sangue periferico per ctDNA); dati di imaging TC per analisi radiomica; dati genomici somatici da CGP (Oncomine Comprehensive Plus, >500 geni); dati trascrittomici (RNA-seq, AmpliSeq Transcriptome); dati di biopsia liquida (ctDNA, Avida OncoLB).

Tutti i dati vengono trattati esclusivamente in forma pseudonimizzata, mediante attribuzione di un codice numerico progressivo a ciascun paziente arruolato. La lista di decodifica è custodita in forma riservata esclusivamente presso l'IRCCS Fondazione G. Pascale di Napoli e non viene trasmessa ad altri soggetti terzi.

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

Il ciclo di vita del trattamento dei dati personali oggetto della presente Valutazione d'Impatto sulla Protezione dei Dati si articola nelle seguenti fasi funzionali:

1. Raccolta dei dati

I dati personali e i dati relativi alla salute sono raccolti in modo retrospettivo presso i centri partecipanti allo studio, mediante estrazione dalle cartelle cliniche e dai sistemi informativi sanitari, nell'ambito dell'assistenza sanitaria ordinaria. La raccolta avviene esclusivamente per i pazienti eleggibili secondo i criteri definiti dal protocollo di studio.

2. Pseudonimizzazione e registrazione

I dati raccolti sono sottoposti a pseudonimizzazione mediante attribuzione di un codice identificativo univoco dello studio, che sostituisce ogni riferimento direttamente identificativo dell'interessato. I dati pseudonimizzati sono successivamente registrati in strumenti strutturati (es. CRF elettroniche o file di lavoro dedicati), accessibili esclusivamente al personale autorizzato.

3. Conservazione e gestione

I dati pseudonimizzati sono conservati su sistemi informatici protetti, secondo misure tecniche e organizzative adeguate ai sensi dell'art. 32 del Regolamento (UE) 2016/679, per un periodo di tempo limitato e proporzionato alle finalità di ricerca scientifica previste dal protocollo.

4. Analisi e utilizzo

I dati sono utilizzati per finalità di analisi statistica e scientifica, esclusivamente in forma pseudonimizzata e aggregata, al fine di valutare esiti clinici, efficacia e sicurezza delle strategie terapeutiche oggetto dello studio. Il trattamento non comporta processi decisionali automatizzati né attività di profilazione degli interessati.

5. Comunicazione e condivisione

I dati possono essere comunicati o condivisi con soggetti terzi coinvolti nello studio, esclusivamente in forma pseudonimizzata e nel rispetto delle finalità scientifiche previste, nonché delle garanzie adeguate in caso di trasferimenti verso Paesi terzi.

6. Conservazione finale e cancellazione

Al termine dello studio e decorsi i termini di conservazione previsti dalla normativa vigente e dal protocollo di ricerca, i dati personali sono cancellati o resi definitivamente anonimi, in modo da impedire l'identificazione degli interessati.

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 17 di 39

3.4.3 Quali sono le risorse di supporto ai dati?

Le risorse di supporto ai dati utilizzate presso l'IRCCS "Fondazione G. Pascale", in qualità di unico centro promotore dello studio heRAco, comprendono:

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

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

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

4. Valutazione di necessità e proporzionalità del trattamento

4.1 Proporzionalità e necessità

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

Le finalità del trattamento dei dati personali nell'ambito dello studio heRAco sono definite in modo specifico, esplicito e legittimo, in conformità all'art. 5, par. 1, lett. b) del GDPR.

Obiettivo primario dello studio heRAco: valutare il ruolo dell'eterogeneità tumorale spaziale e temporale del carcinoma del colon-retto con mutazione BRAFV600E nella risposta alle terapie target mediante un approccio multi-omico integrato (genomica, trascrittomica, radiomica, analisi della biopsia liquida).

Endpoints primari: correlazione tra profilo genomico tumorale (CGP) e risposta al trattamento target; identificazione di biomarcatori predittivi di risposta/resistenza. Obiettivi secondari: (a) caratterizzazione dell'evoluzione clonale mediante ctDNA (biopsia liquida); (b) integrazione dei dati radiomici (TC) con il profilo molecolare per la stratificazione prognostica; (c) analisi trascrittomica dell'eterogeneità intratumorale. Le informazioni raccolte sono finalizzate a generare evidenze scientifiche sul meccanismo di resistenza alle terapie target nel CRC BRAFV600E, identificare nuovi biomarcatori prognostici e predittivi,

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 18 di 39

e contribuire allo sviluppo di approcci terapeutici personalizzati per questa patologia a prognosi severa.

La popolazione di studio comprende pazienti adulti (età ≥ 18 anni) con diagnosi confermata di carcinoma del colon-retto (CRC) con mutazione BRAFV600E, trattati con terapie target anti-BRAF/MEK presso l'IRCCS Fondazione G. Pascale di Napoli: (a) 150 pazienti retrospettivi, con campioni FFPE già disponibili presso la Biobanca istituzionale; (b) 20 pazienti prospettici, arruolati durante il periodo dello studio. La numerosità campionaria totale attesa è di 170 pazienti. La durata complessiva dello studio è di 36 mesi.

Il trattamento dei dati è strettamente funzionale al perseguimento di tali finalità di ricerca scientifica, svolte nell'interesse pubblico, senza scopo di lucro e nel rispetto dei principi etici internazionali (Dichiarazione di Helsinki, ICH-GCP).

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

Il trattamento dei dati personali effettuato nell'ambito dello studio heRAco presso l'IRCCS “Fondazione G. Pascale” di Napoli, in qualità di unico centro promotore e titolare del trattamento, 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.

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 19 di 39

Base giuridica per le finalità di studio e di ricerca scientifica: Art. 110 bis c.4, Codice Privacy (D.Lgs. 196/2003 e ss.mm.), secondo il quale: "Non costituisce trattamento ulteriore da parte di terzi il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell'osservanza di quanto previsto dall'articolo 89 del Regolamento". Si informa l'Interessato che la Valutazione d'impatto svolta sarà pubblicata e consultabile sul sito Istituzionale dell'IRCCS Fondazione G.Pascale (<https://newportal.istitutotumori.na.it/privacy/vip/>). 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)?

I dati personali oggetto del trattamento sono stati selezionati sulla base del principio di minimizzazione (art. 5, par. 1, lett. c) GDPR): vengono raccolte esclusivamente le variabili cliniche, anagrafiche, istologiche, molecolari e radiomiche strettamente indispensabili per il raggiungimento degli obiettivi dello studio heRAco. Il set di variabili è quello definito nell'Elenco Variabili allegato al protocollo heRAco, organizzato in domini secondo le fasi dello studio (dati anagrafici, clinici e istologici alla diagnosi; dati molecolari da CGP Oncomine Comprehensive Plus, ctDNA Avida OncoLB e RNA-seq AmpliSeq Transcriptome; features radiomiche; follow-up oncologico).

Non vengono raccolti dati ulteriori rispetto a quanto necessario: non sono richiesti dati biometrici, economici o dati di contatto dei pazienti oltre a quelli strettamente funzionali al follow-up clinico già presente in cartella. I dati identificativi diretti (nome, cognome, codice fiscale, recapiti) non vengono mai inseriti nei database di analisi dello studio, ma sono conservati esclusivamente nella lista di decodifica custodita presso l'IRCCS Fondazione G. Pascale, separata dai database e ad accesso strettamente controllato. Lo studio prevede l'utilizzo di campioni biologici (tessuto FFPE archiviato in biobanca per i pazienti retrospettivi; campioni di sangue periferico per l'analisi ctDNA nei pazienti prospettici) esclusivamente nell'ambito di procedure già effettuate o previste per scopi clinici o di ricerca approvati. I dati di imaging (TC, RM) sono acquisiti in forma pseudonimizzata per l'estrazione di features radiomiche, nell'ambito delle procedure diagnostiche già effettuate in pratica clinica.

Il database elettronico è strutturato per raccogliere solo le variabili previste dal CRF dello studio, impedendo l'inserimento di dati non pertinenti o eccedenti rispetto alle finalità dichiarate.

4.1.4 I dati sono esatti e aggiornati?

I dati personali trattati provengono da fonti primarie certificate (cartelle cliniche, referti diagnostici, registri informativi sanitari istituzionali dei centri partecipanti), che garantiscono un elevato grado di accuratezza e affidabilità. La raccolta retrospettiva avviene mediante consultazione diretta delle fonti originarie da parte del personale sanitario autorizzato e specificamente formato.

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 20 di 39

In fase di inserimento nel database, il personale di ricerca è tenuto a verificare la correttezza dei dati immessi e a segnalare eventuali incongruenze o lacune. Qualora, nel corso dello studio, emergessero inesattezze o aggiornamenti necessari (es. decesso del paziente, revisione dello stadio della malattia), il dato viene tempestivamente rettificato nel database nel rispetto dell'art. 5, par. 1, lett. d) del GDPR. I pazienti viventi contattabili possono inoltre esercitare il diritto di rettifica dei propri dati ai sensi dell'art. 16 GDPR.

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. I dati personali dei partecipanti saranno conservati per tutta la durata del progetto 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 e 110-bis del Codice Privacy, viene pubblicata la valutazione di impatto.
- Le modalità previste includono:
 - Pubblicazione sul sito web dell'Istituto Nazionale Tumori IRCCS "Fondazione G. Pascale" di Napoli (in qualità di Promotore e unico Titolare)

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 21 di 39

- 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

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 22 di 39

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

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 23 di 39

- **Principal Investigator:** Dr. Rizio Esposito Abate (PI, S.C. Biologia Cellulare e Bioterapie, IRCCS Pascale, e-mail: r.espositoabate@istitutotumori.na.it).

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

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

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.

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 24 di 39

- 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.

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 25 di 39

- 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?

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 26 di 39

Trattandosi di uno studio monocentrico, il trattamento dei dati è effettuato esclusivamente presso l'IRCCS Fondazione G. Pascale di Napoli, unico Titolare del trattamento. Il personale autorizzato (PI Dr. Rizio Esposito Abate e collaboratori delegati) opera nel pieno rispetto del protocollo di studio e della presente DPIA, che definiscono modalità, finalità e limiti del trattamento dei dati. Non sono previsti rapporti con centri coordinatori esterni né trasferimenti di dati verso soggetti terzi nell'ambito della gestione interna dello studio. Eventuali fornitori esterni di servizi tecnici/IT (es. manutenzione IT, sequenziamento in service) coinvolti dall'Istituto sono designati Responsabili del trattamento ai sensi dell'art. 28 GDPR mediante specifici Data Processing Agreement che definiscono ambito, durata, natura e finalità del trattamento, nonché le misure di sicurezza e riservatezza applicabili. Il personale autorizzato al trattamento opera esclusivamente su istruzione documentata del Titolare e del Principal Investigator, è soggetto a obbligo di riservatezza e riceve formazione adeguata sulle normative in materia di protezione dei dati.

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

Lo studio heRAco è uno studio monocentrico condotto interamente presso l'IRCCS Fondazione G. Pascale, unico Titolare del trattamento. Tutti i dati personali pseudonimizzati rimangono custoditi all'interno dell'Istituto. Non è previsto alcun trasferimento di dati pseudonimizzati verso centri terzi o verso sistemi esterni all'infrastruttura dell'IRCCS Pascale. Lo studio è interamente soggetto al Regolamento (UE) 2016/679 (GDPR) e alla normativa nazionale vigente.

Non è previsto alcun trasferimento di dati personali identificabili verso Paesi terzi al di fuori dell'Unione Europea/SEE. La pubblicazione dei risultati dello studio (riviste scientifiche, congressi, ClinicalTrials.gov) avverrà esclusivamente in forma aggregata e anonima, in conformità a quanto disposto dal protocollo. Eventuali condivisioni con soggetti extra-UE/SEE potranno avvenire solo previa anonimizzazione completa dei dati o, ove ciò non sia possibile, tramite gli strumenti di cui agli artt. 44-49 GDPR (decisioni di adeguatezza, clausole contrattuali standard, ecc.).

5. Motivi della valutazione d'impatto

La presente Valutazione d'Impatto sulla Protezione dei Dati (DPIA) è stata predisposta ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (GDPR) e dell'art. 110-bis, comma 4, del D.lgs. 196/2003 (Codice Privacy), sulla base delle seguenti motivazioni:

1. Trattamento su larga scala di dati sanitari (categorie particolari ai sensi dell'art. 9 GDPR)
Lo studio prevede il trattamento di dati relativi alla salute di pazienti oncologici, appartenenti alle categorie particolari di dati di cui all'art. 9 GDPR, per le quali è obbligatoria la DPIA ai sensi dell'art. 35, par. 3, lett. b) e del Provvedimento del Garante n. 467/2018.
2. Inclusione di soggetti deceduti o non rintracciabili (art. 110-bis Codice Privacy)
La natura retrospettiva dello studio comporta l'arruolamento di pazienti per i quali non è materialmente

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 27 di 39

possibile acquisire il consenso, in quanto deceduti o persi al follow-up. In tali casi, ai sensi dell'art. 110-bis, comma 4, del Codice Privacy e della Deliberazione del Garante n. 298/2024, il trattamento è subordinato alla pubblicazione preventiva della presente DPIA sul sito istituzionale del promotore.

3. Lo studio prevede il trattamento di dati genomici (CGP Oncomine Comprehensive Plus), di DNA tumorale circolante (ctDNA Avida OncoLB), di dati trascrittomici (AmpliSeq Transcriptome Human Gene Expression) e di dati radiomici di pazienti con carcinoma colorettale BRAFV600E. L'eventuale inclusione di pazienti retrospettivi con materiale in biobanca e l'impiego di dati genetici somatici (non sono previste analisi di varianti germinali) configurano un trattamento ad alto rischio che richiede un'analisi sistematica dei rischi per la riservatezza, integrità e disponibilità dei dati degli interessati.

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

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 28 di 39

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, Sicurezza dei canali informatici, Procedure di sicurezza dei sistemi elettronici, Controllo degli accessi logici, Formazione e Sensibilizzazione, Tracciabilità, Minimizzazione dei dati, Limitazione dell'Accesso ai Dati, Accesso controllato ai locali, Audit e monitoraggi periodici, Architettura e privacy by design; Gestione dei rapporti tra titolari e responsabili.

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

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 29 di 39

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?

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, Accesso controllato ai locali, Audit e monitoraggi periodici; Conservazione e archiviazione dei dati; Architettura e privacy by design; Gestione dei rapporti tra titolari e responsabili.

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?

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 30 di 39

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?

Formazione e Sensibilizzazione, Sicurezza dei canali informatici, Limitazione dell'Accesso ai Dati, Controllo degli accessi logici, Accesso controllato ai locali, Procedure di sicurezza dei sistemi elettronici; Conservazione e archiviazione dei dati; Architettura e privacy by design; Gestione dei rapporti tra titolari e responsabili.

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

Per lo studio heRAco, la procedura di pseudonimizzazione prevede l’assegnazione a ciascun partecipante di un codice identificativo univoco (ID studio). Nei database di analisi (genomica, trascrittomica, radiomica) non sono presenti identificativi personali diretti (nome, cognome, numero di identificazione nazionale, data di nascita completa). La lista di decodifica è custodita esclusivamente presso l’IRCCS Fondazione G. Pascale, separata dai database di analisi e con accesso riservato al solo medico sperimentatore e ai soggetti espressamente autorizzati. Non è previsto alcun trasferimento di dati pseudonimizzati a

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 31 di 39

soggetti terzi o a centri promotori esterni, essendo lo studio monocentrico. Tutti i trattamenti avvengono all'interno dell'infrastruttura informatica dell'IRCCS Pascale.

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.

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

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 32 di 39

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).

I dati saranno conservati su server situati all'interno del Centro Elaborazione Dati (CED), che garantisce un ambiente sicuro e controllato.

7.1.11 Accesso controllato ai locali

Accesso al reparto con badge. Per lo studio heRAco, i locali del CED dell'IRCCS Fondazione G. Pascale che ospitano le infrastrutture informatiche istituzionali, i database di analisi (genomica, radiomica, trascrittomica) e la lista di decodifica sono ad accesso fisico controllato secondo le procedure di sicurezza istituzionali, con videosorveglianza, badge elettronico autorizzato e sistemi antintrusione.

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.

7.1.13 Conservazione e archiviazione dei dati

I dati personali e sanitari raccolti nell'ambito dello studio sono conservati in conformità al principio di limitazione della conservazione di cui all'art. 5, par. 1, lett. e) del Regolamento (UE) 2016/679. In particolare, la documentazione dello studio (cartelle cliniche, fonti originarie, registri interni) è archiviata presso il centro per il periodo necessario ad assolvere obblighi regolatori, etici, di audit e sorveglianza scientifica, come previsto dal protocollo. Al termine del periodo definito, i supporti contenenti dati identificabili vengono cancellati o i dati vengono resi anonimi, e rimangono solo le informazioni in forma aggregata o non riconducibili agli interessati.

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 33 di 39

Le cartelle cliniche saranno esaminate solamente presso l’ospedale al fine di controllare le informazioni necessarie per lo svolgimento dello studio, senza violare la riservatezza dei pazienti. Tutte le informazioni raccolte a scopo di attività mediche, statistiche o regolatorie associate allo studio saranno identificate con un codice numerico o alfanumerico. Il nome completo dei pazienti o eventuali dettagli relativi all’indirizzo e al numero telefonico non saranno inclusi in queste analisi.

Il personale clinico e di ricerca, appositamente autorizzato, tratterà i dati identificando ciascun partecipante con un codice numerico o alfanumerico assegnato a ciascun soggetto; i dati saranno elaborati e conservati unitamente a tale codice in un database dedicato con accesso limitato e controllato nel Centro.

7.1.14 Architettura e privacy by design

La gestione dei dati dello studio heRAco segue un modello monocentrico: tutti i dati pseudonimizzati sono gestiti interamente presso l’IRCCS Fondazione G. Pascale. La privacy by design ai sensi dell’art. 25 GDPR è perseguita mediante: pseudonimizzazione precoce dei dati a livello di arruolamento; minimizzazione delle variabili raccolte (limitate a quelle definite nel protocollo di studio); separazione tra la lista di decodifica e i database di analisi; accesso ai dati riservato al solo personale autorizzato mediante credenziali personali e role-based access control; analisi e pubblicazione dei risultati esclusivamente in forma aggregata e anonima. La gestione complessiva dei dati è integralmente ricompresa nella presente DPIA istituzionale dell’IRCCS Fondazione G. Pascale.

7.1.15 Gestione dei rapporti tra titolari e responsabili

Trattandosi di uno studio monocentrico, l’IRCCS Fondazione G. Pascale è il solo Titolare del trattamento.

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 ($>10^{-3}$)

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 34 di 39

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	Nessun impatto significativo per gli interessati. Eventuale disagio minimo, rapidamente superabile e senza conseguenze sulla vita quotidiana, sulla salute o sui diritti degli interessati.

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

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 35 di 39

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, Minimizzazione dei dati, Limitazione dell'Accesso ai Dati, Accesso controllato ai locali, Audit e monitoraggi periodici, Architettura e privacy by design; Gestione dei rapporti tra titolari e responsabili	Grave	Poco probabile	Medio	Limitata/Improbabile	Basso

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 36 di 39

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, Accesso controllato ai locali, Audit e monitoraggi periodici; Conservazione e archiviazione dei dati; Architettura e privacy by design; Gestione dei rapporti tra titolari e responsabili.	Grave	Poco probabile	Medio	Limitata/Improbabile	Basso

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 37 di 39

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

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO “Fondazione Giovanni Pascale” – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI: Assessment of the role of tumor heterogeneity of BRAF mutant colorectal carcinoma in the response to targeted therapies using multi-omics approaches (Acronimo: heRAco) – Protocollo n. 38/26 OSS	Versione 1.0 del 01.07.2026
		Pagina 38 di 39

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.						

8. Risultato della DPIA

Il 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 interessati 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, 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; Architettura e privacy by design; Gestione dei rapporti tra titolari e responsabili.
- **Coinvolgimento delle Parti Interessate:** è stato considerato il feedback degli esperti in materia di protezione dei dati.