

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Versione 1.0 del 12.12.2025
		Pagina 1 di 34

Titolo dello studio	Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici
Promotore	Istituto Nazionale Tumori di Napoli, IRCCS G. Pascale
Centro di Sperimentazione	Istituto Nazionale Tumori di Napoli, IRCCS G. Pascale
Principal Investigator	Riziero Esposito Abate
Tipo di studio e fase	Studio Osservazionale Retrospektivo Multicentrico
Parere del Comitato Etico	Parere CET Campania 1 del 05.11.2025
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 DEL PROTOCOLLO Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Versione 1.0 del 12.12.2025
	Pagina 2 di 34	

	Nome e Cognome	Ruolo	Firma	Data
	Roberta Fusco	Ingegnere Biomedico		
	Elisa Pintauro	Ricercatore Sanitario		
Revisione	Gianfranco De Feo	Quality Assurance		
Approvazione	Maurizio Di Mauro	Titolare del trattamento dati		
	Alessandro Manzoni	DPO		
	Riziero Esposito Abate	Principal Investigator	<i>Riziero Esposito Abate</i>	18/12/2025
	Gianfranco De Feo	Quality Assurance		

Tracking delle modifiche

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

Storico della rivalutazione

Revisione annuale della DPIA o a seguito di verifiche/minacce

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

	Data prevista	Data effettiva	Firma
Rivalutazione a cura del QA			

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO	Versione 1.0 del 12.12.2025
	Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Pagina 3 di 34

Tabella dei Contenuti

Tracking delle modifiche.....	2
Storico della rivalutazione	2
1. Stima del rischio e pre-assessment	6
1.1 Stima del rischio	7
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?.....	10
3.3.3 Ci sono standard applicabili al trattamento?	12
3.4 Dati, processi e risorse di supporto	14
3.4.1 Quali sono i dati trattati?	14
3.4.2 Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?	14
3.4.3 Quali sono le risorse di supporto ai dati?.....	15
4. Valutazione di necessità e proporzionalità del trattamento	16
4.1 Proporzionalità e necessità	16
4.1.1 Gli scopi del trattamento sono specifici, espliciti e legittimi?	16
4.1.2 Quali sono le basi legali che rendono lecito il trattamento?	16
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)?	17
4.1.4 I dati sono esatti e aggiornati?.....	17
4.1.5 Qual è il periodo di conservazione dei dati?	17
4.2 Misure a tutela dei diritti degli interessati.....	17
4.2.1 Come sono informati del trattamento gli interessati?	17
4.2.2 Ove applicabile: come si ottiene il consenso degli interessati?	18
4.2.3 Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?.....	19
4.2.4 Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?.....	20
4.2.5 Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?	21
4.2.6 Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?	21

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO	Versione 1.0 del 12.12.2025
	Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Pagina 4 di 34

4.2.7 In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?	21
5. Motivi della valutazione d'impatto	21
6. Valutazione dei Rischi.....	22
6.1 Accesso illegittimo ai dati	22
6.1.1 Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?	22
6.1.2 Quali sono le principali minacce che potrebbero concretizzare il rischio?	22
6.1.3 Quali sono le fonti di rischio?	23
6.1.4 Quali misure fra quelle individuate contribuiscono a mitigare il rischio?	23
6.1.5 Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?	23
6.1.6 Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?.....	23
6.2 Modifiche indesiderate dei dati	23
6.2.1 Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?	23
6.2.2 Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?	23
6.2.3 Quali sono le fonti di rischio?	24
6.2.4 Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?	24
6.2.5 Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?	24
6.2.6 Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?.....	24
6.3 Perdita di dati	24
6.3.1 Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?	24
6.3.2 Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?	24
6.3.3 Quali sono le fonti di rischio?	25
6.3.4 Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?	25
6.3.5 Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?	25
6.3.6 Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?.....	25
7. Piano d'azione	25
7.1 Mitigazione dei rischi con Misure esistenti o pianificate	25

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Versione 1.0 del 12.12.2025
		Pagina 5 di 34

7.1.1 Pseudonimizzazione	25
7.1.2 Formazione e Sensibilizzazione	26
7.1.3 Tracciabilità.....	26
7.1.4 Politica di tutela della privacy.....	26
7.1.5 Gestione delle politiche di tutela della privacy	26
7.1.6 Minimizzazione dei dati.....	26
7.1.7 Controllo degli accessi logici.....	26
7.1.8 Limitazione dell'Accesso ai Dati.....	27
7.1.9 Audit e monitoraggi periodici.....	27
7.1.10 Sicurezza dei canali informatici.....	27
7.1.11 Procedure di sicurezza dei sistemi elettronici	27
7.1.12 Accesso controllato ai locali.....	27
7.1.13 Conservazione e archiviazione dei dati	27
7.2 Panoramica dei rischi	28
8. Risultato della DPIA	34

1. Stima del rischio e pre-assessment

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

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

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Versione 1.0 del 12.12.2025
		Pagina 7 di 34

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).	
Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).	NO
Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).	SI
Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogni qualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 (criteri WP 29).	NO
Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).	NO
Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.	NO
Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.	NO
Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.	NO

1.1 Stima del rischio

Criteri utilizzati per la stima del rischio	Risposta
Il trattamento comporta la valutazione o assegnazione di un punteggio inclusiva di profilazione e previsione	NO
Il trattamento prevede un processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente	NO

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Versione 1.0 del 12.12.2025
		Pagina 8 di 34

Il trattamento consiste in un'attività di monitoraggio sistematico	NO
Il trattamento coinvolge dati sensibili o dati aventi carattere altamente personale	SI
Il trattamento di dati avviene su larga scala	NO
Il trattamento comporta la creazione di corrispondenze o combinazione di insiemi di dati	NO
Il trattamento coinvolge categorie di interessati vulnerabili	SI
Il trattamento coinvolge l'uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative	NO
Il trattamento impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto	NO
Medio/Elevato	

2. Quadro normativo

Regolamento (UE) 679/2016 (GDPR);

D.lgs. 196/2003 e s.m.i. per effetto del D.lgs. 101/2018;

Articolo 29 Working Party (2017), Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" in base alle disposizioni contenute nel Regolamento (UE) 679/2016;

Provvedimento 146/2019 del Garante per la protezione dei dati personali.

Provvedimento 298/2024 del Garante per la protezione dei dati personali.

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO	Versione 1.0 del 12.12.2025
	Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Pagina 9 di 34

3. Contesto

3.1 Titolare e Responsabile della Protezione dei Dati

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

3.2 Soggetti interessati

L'attività interessa il trattamento di dati riguardanti:

- pazienti già in precedenza assistiti presso

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

- pazienti che hanno fornito in precedenza propri campioni biologici presso

Non applicabile

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

Non applicabile

- Altro

Non applicabile

RICHIESTA DEL PARERE DEGLI INTERESSATI RELATIVAMENTE ALLA DPIA

- ☐ È stato richiesto il parere degli interessati
☒ Non è stato richiesto il parere degli interessati

MOTIVAZIONE DELLA MANCATA RICHIESTA DEL PARERE ALLA DPIA DEGLI INTERESSATI

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

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

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO	Versione 1.0 del 12.12.2025
	Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Pagina 10 di 34

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

3.3 Descrizione del trattamento

3.3.1 Quale è il trattamento in considerazione?

Il trattamento dei dati personali nell'ambito dello studio "Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici" consiste nella raccolta, registrazione, organizzazione, conservazione, consultazione, analisi e successiva anonimizzazione di dati personali e dati particolari relativi alla salute di pazienti affetti da carcinoma del colon-retto avanzato/metastatico. I dati trattati comprendono informazioni anagrafiche limitate (iniziali, sesso, data di nascita), dati clinici e clinico-patologici, dati molecolari derivanti da analisi di Real Time PCR e Next Generation Sequencing (NGS) su campioni biologici tumorali residui dell'attività diagnostica, nonché informazioni relative ai trattamenti oncologici effettuati e agli esiti clinici (PFS, OS). Il trattamento è effettuato per finalità di ricerca scientifica in ambito medico-oncologico, con disegno retrospettivo e osservazionale, senza alcun impatto sulle decisioni terapeutiche dei pazienti. I dati sono trattati in forma pseudonimizzata mediante attribuzione di un codice identificativo univoco; la chiave di collegamento è custodita separatamente presso il centro promotore. Al termine delle attività di accoppiamento con i dati clinici, i dati sono resi definitivamente anonimizzati.

3.3.2 Quali sono le responsabilità connesse al trattamento?

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

1. Titolare del Trattamento (Data Controller)

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

Responsabilità:

- Determinare le Finalità e i Mezzi del Trattamento: Decidere come e perché i dati personali devono essere trattati.
- Garantire la Conformità al GDPR: Assicurarsi che tutte le attività di trattamento siano conformi alle disposizioni del Regolamento Generale sulla Protezione dei Dati (GDPR).

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Versione 1.0 del 12.12.2025
		Pagina 11 di 34

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

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

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

Responsabilità:

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

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

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

3. Preposto autorizzato al trattamento

Per codesto progetto, questo ruolo è stato delegato al dr. Rizio Esposito Abate.

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.

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Versione 1.0 del 12.12.2025
		Pagina 12 di 34

Conformità alle Politiche Aziendali: Seguire le politiche e le procedure aziendali relative alla protezione dei dati.

Segnalazione di Incidenti: Segnalare tempestivamente eventuali incidenti di sicurezza o violazioni dei dati.

5. Partecipanti allo Studio

I partecipanti allo studio devono essere adeguatamente informati.

Responsabilità:

Seguire le procedure operative standard (SOP): Raccogliere, conservare e trasferire i dati clinici secondo le linee guida stabilite nel protocollo dello studio.

Garantire la riservatezza: Trattare i dati in modo anonimo e rispettare il principio di minimizzazione, limitando il trattamento ai dati strettamente necessari per gli scopi dello studio.

Rispettare i diritti degli interessati: Garantire che gli interessati possano esercitare i loro diritti, come l'accesso ai dati, la rettifica e il ritiro del consenso.

6. Sponsor

Lo Sponsor dello studio è responsabile del trattamento dei dati pseudonimizzati ricevuti dai centri ai fini di ricerca scientifica e statistica. Lo Sponsor assicura che i dati siano trattati mediante sistemi informatici sicuri, che includono misure quali controllo degli accessi, protocolli di cifratura, gestione delle credenziali e monitoraggio delle attività, e che ogni operazione sia eseguita nel rispetto dei principi di minimizzazione, limitazione delle finalità e protezione dei dati.

Una società specializzata esterna supporta lo Sponsor nella conduzione operativa dello studio e nella gestione degli strumenti elettronici utilizzati, operando quale responsabile del trattamento sulla base di istruzioni documentate e con specifiche misure di sicurezza. Tutti i soggetti coinvolti nel trattamento accedono ai dati solo nei limiti necessari allo svolgimento delle attività di loro competenza.

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.

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO	Versione 1.0 del 12.12.2025
	Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Pagina 13 di 34

Sicurezza dei Dati: Obbligo di implementare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

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

2. Norme di sicurezza della infrastruttura e dei sistemi elettronici

Presso l'IRCCS INT Napoli sono previste delle specifiche procedura di sicurezza per i sistemi elettronici (penetration test; firewall; back-up; disaster recovery; antivirus; verifica integrità dati back-up) nonché procedure di archiviazione dati storici (abilitazione accesso, consultazione, decommissioning, migrazione del dato, ecc...).

Con cadenza semestrale viene effettuato un risk assesment da parte di un ente terzo relativamente alla sicurezza dei suddetti sistemi.

3. Linee Guida del Comitato Europeo per la Protezione dei Dati (EDPB)

Il Comitato Europeo per la Protezione dei Dati (EDPB) pubblica linee guida, raccomandazioni e best practice per l'applicazione del GDPR.

Linee guida sulla DPIA: Forniscono dettagli su quando e come condurre una DPIA.

Linee guida sulla Trasparenza: Dettagli su come fornire informazioni agli interessati in modo trasparente e comprensibile.

Linee guida sulla Sicurezza dei Dati: Raccomandazioni sulle misure di sicurezza tecniche e organizzative da adottare.

4. Direttive Nazionali e Linee Guida Specifiche per la Ricerca Clinica

A seconda del paese, possono esserci direttive nazionali aggiuntive e linee guida specifiche per la ricerca clinica che devono essere seguite.

Linee guida di AIFA (Agenzia Italiana del Farmaco): In Italia, AIFA fornisce linee guida per la conduzione di sperimentazioni cliniche, inclusi gli aspetti di protezione dei dati.

Leggi Nazionali sulla Protezione dei Dati: Ogni paese può avere leggi specifiche che integrano o dettagliano ulteriormente i requisiti del GDPR.

5. Linee Guida etiche

Dichiarazione di Helsinki: Principi etici per la ricerca medica che coinvolge soggetti umani, sviluppata dall'Associazione Medica Mondiale (WMA).

Linee Guida ICH-GCP (Good Clinical Practice): Standard internazionale per la progettazione, conduzione, registrazione e reporting di studi clinici che coinvolgono soggetti umani.

6. Standard di sicurezza e qualità applicati

- Good Clinical Practice (ICH-GCP E6 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.

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Versione 1.0 del 12.12.2025
		Pagina 14 di 34

3.4 Dati, processi e risorse di supporto

3.4.1 Quali sono i dati trattati?

Nell'ambito dello studio vengono trattate le seguenti categorie di dati personali, prevalentemente in forma pseudonimizzata e successivamente anonimizzata:

- Dati personali comuni: dati identificativi indiretti quali iniziali del paziente, sesso, età e/o data di nascita, codice identificativo univoco assegnato allo studio; non sono utilizzati nominativi completi all'interno del database di ricerca.
- Dati particolari relativi alla salute (art. 9 GDPR): informazioni cliniche e clinico-patologiche relative alla diagnosi di carcinoma del colon-retto avanzato/metastatico, stadio di malattia, caratteristiche istologiche, andamento clinico e sopravvivenza.
- Dati molecolari di natura somatica: risultati di analisi di biologia molecolare effettuate su campioni tumorali (mutazione di BRAF, co-mutazioni in altri geni, stato di instabilità dei microsatelliti – MSI, Tumor Mutational Burden – TMB), ottenuti mediante tecniche di Real Time PCR, sequenziamento Sanger e Next Generation Sequencing (NGS). Non vengono analizzate né trattate varianti genetiche della linea germinale.
- Dati relativi ai trattamenti oncologici: informazioni sui farmaci somministrati, linee di trattamento, risposta terapeutica, progression free survival (PFS) e overall survival (OS).
- Dati amministrativi e di studio: informazioni necessarie alla gestione scientifica dello studio (codici di studio, centro di arruolamento, periodo di osservazione).

I dati sono raccolti a partire da campioni biologici e informazioni cliniche residui dell'attività diagnostico-assistenziale, nel contesto di uno studio retrospettivo e osservazionale, senza impatto sulle decisioni terapeutiche. Tutti i dati sono trattati nel rispetto dei principi di minimizzazione, limitazione delle finalità e riservatezza, secondo quanto previsto dal GDPR e dalla normativa nazionale vigente.

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

Il ciclo di vita del trattamento dei dati personali nell'ambito dello studio si articola nelle seguenti fasi:

1. Origine e raccolta dei dati

I dati personali e i dati particolari relativi alla salute e al profilo molecolare dei pazienti derivano da campioni biologici e informazioni clinico-patologiche già raccolti nel corso della normale attività diagnostico-assistenziale. Lo studio ha natura retrospettiva e osservazionale e non prevede la raccolta prospettica né ulteriori procedure cliniche o diagnostiche rispetto alla pratica clinica ordinaria. Il trattamento dei dati avviene previo consenso informato, ove applicabile, oppure secondo le deroghe previste dalla normativa per i dati retrospettivi di soggetti deceduti o non più contattabili, con pubblicazione della DPIA.

2. Pseudonimizzazione e registrazione

Al momento dell'inclusione nello studio, a ciascun soggetto viene attribuito un codice identificativo univoco. I dati clinici, patologici e molecolari sono registrati in un

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO	Versione 1.0 del 12.12.2025
	Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Pagina 15 di 34

database elettronico dedicato utilizzando esclusivamente tale codice. L'elenco di collegamento tra codice e identità del paziente è conservato separatamente e in modo sicuro presso il centro promotore, con accesso limitato ai soli soggetti autorizzati.

3. **Utilizzo e analisi dei dati**

I dati pseudonimizzati sono utilizzati per finalità di ricerca scientifica, in particolare per la validazione delle metodiche molecolari (Real Time PCR, NGS) e per le analisi statistiche e clinico-patologiche previste dal protocollo. Le elaborazioni possono includere strumenti informatici e processi parzialmente automatizzati, senza che siano effettuate decisioni automatizzate aventi effetti giuridici o clinici sui pazienti.

4. **Conservazione**

I dati sono conservati per tutta la durata dello studio e per il periodo successivo previsto dalle normative vigenti in materia di ricerca scientifica e documentazione clinica. Durante tale periodo, i dati restano pseudonimizzati e protetti mediante misure tecniche e organizzative adeguate a garantirne riservatezza, integrità e disponibilità.

5. **Anonimizzazione finale**

Al termine delle attività di accoppiamento tra dati molecolari e clinici, i dati vengono resi definitivamente anonimi, mediante eliminazione della chiave di re-identificazione. Una volta anonimizzati, i dati non sono più riconducibili agli interessati e possono essere utilizzati esclusivamente in forma aggregata per finalità scientifiche, statistiche e di pubblicazione.

3.4.3 Quali sono le risorse di supporto ai dati?

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

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

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

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

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO	Versione 1.0 del 12.12.2025
	Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Pagina 16 di 34

4. Valutazione di necessità e proporzionalità del trattamento

4.1 Proporzionalità e necessità

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

Gli scopi del trattamento dei dati personali nell'ambito dello studio sono chiaramente determinati, esplicitamente dichiarati e giuridicamente legittimi. In particolare, il trattamento è effettuato esclusivamente per finalità di ricerca scientifica in ambito medico-oncologico, come dettagliato nel protocollo di studio, nella sinossi e nei documenti di informativa e consenso.

Gli scopi sono specifici in quanto limitati alla validazione di metodiche di analisi molecolare (Real Time PCR e Next Generation Sequencing) per l'identificazione delle mutazioni di BRAF e di altri biomarcatori molecolari, nonché allo studio delle correlazioni tra profilo genomico e parametri clinico-patologici nei pazienti affetti da carcinoma del colon-retto metastatico.

Tali finalità sono esplicite poiché comunicate in modo chiaro agli interessati attraverso l'informativa e il modulo di consenso, e sono descritte in modo dettagliato nella documentazione sottoposta e approvata dal Comitato Etico competente.

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

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

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

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Versione 1.0 del 12.12.2025
		Pagina 17 di 34

- Per i soggetti raggiungibili, il trattamento è effettuato anche sulla base del consenso informato scritto, ai sensi dell'art. 7 del GDPR, nel quale è illustrata la finalità scientifica e il trattamento dei dati.

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

L'asset di dati raccolti è stato definito, all'interno del relativo Protocollo, in stretta correlazione con gli obiettivi dello studio. Non sono quindi raccolti dati eccedenti rispetto alle finalità del trattamento.

4.1.4 I dati sono esatti e aggiornati?

I dati trattati nell'ambito dello studio sono esatti, pertinenti e, per quanto rilevante rispetto alle finalità di ricerca, aggiornati.

In particolare, i dati clinici, clinico-patologici e molecolari utilizzati derivano da documentazione sanitaria ufficiale e da referti diagnostici e di laboratorio prodotti nel corso della normale pratica clinico-assistenziale, garantendo un elevato livello di accuratezza e affidabilità delle informazioni.

Considerata la natura retrospettiva e osservazionale dello studio, l'aggiornamento dei dati è limitato al periodo di osservazione clinica disponibile nei sistemi informativi sanitari; ciò è coerente con le finalità scientifiche del trattamento, che non richiedono un aggiornamento continuo o prospettico delle informazioni. Eventuali incongruenze o dati incompleti vengono verificati e, ove possibile, corretti prima dell'inclusione nel database di ricerca.

Sono adottate procedure di controllo di qualità dei dati (data cleaning e verifica di coerenza) durante la fase di raccolta e analisi, al fine di ridurre il rischio di errori. Inoltre, gli interessati conservano il diritto di richiedere la rettifica dei dati inesatti nei limiti di quanto compatibile con l'integrità scientifica dello studio e con la normativa vigente.

Pertanto, il principio di esattezza dei dati è rispettato in modo proporzionato alle finalità di ricerca scientifica perseguite, in conformità all'art. 5 del GDPR e alle Linee Guida applicabili.

4.1.5 Qual è il periodo di conservazione dei dati?

Il periodo di conservazione dei dati corrisponde al periodo necessario per completare le attività di arruolamento, raccolta, analisi dei dati e interpretazione dei risultati necessarie a conseguire la redazione dell'elaborato finale e la relativa revisione, tenendo conto della necessità di mantenere a disposizione delle autorità competenti documenti e dati necessari per eventuali attività di verifica.

4.2 Misure a tutela dei diritti degli interessati

4.2.1 Come sono informati del trattamento gli interessati?

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO	Versione 1.0 del 12.12.2025
	Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Pagina 18 di 34

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

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

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

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

Modalità di acquisizione del consenso

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

Revoca del consenso

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

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Versione 1.0 del 12.12.2025
		Pagina 19 di 34

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

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

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

Diritto di Accesso

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

Procedura per Esercitare il Diritto di Accesso

1. Richiesta di Accesso:

- I pazienti possono presentare una richiesta di accesso ai loro dati personali. La richiesta può essere effettuata al DPO.
- Informazioni di contatto per le richieste di accesso sono generalmente fornite nel documento di informativa al trattamento dei dati e includono l'indirizzo e-mail del DPO.

2. Verifica dell'Identità:

- Prima di fornire l'accesso ai dati, l'Istituto verificherà l'identità del richiedente per garantire che i dati personali siano rilasciati alla persona corretta. Questo può includere la richiesta di una copia di un documento d'identità.

3. Fornitura delle Informazioni:

- Una volta verificata l'identità, l'Istituto fornirà una copia dei dati personali richiesti. Questo include le informazioni sui dati specifici raccolti, le finalità del trattamento, le categorie di dati trattati e qualsiasi altra informazione richiesta dal GDPR.
- Le informazioni saranno fornite in un formato chiaro e comprensibile.

Diritto di Portabilità dei Dati

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

Procedura per Esercitare il Diritto di Portabilità dei Dati

1. Richiesta di Portabilità:

- I pazienti possono presentare una richiesta per ottenere i loro dati personali in un formato portabile. La richiesta può essere effettuata al DPO.
- Informazioni di contatto per le richieste di accesso sono generalmente fornite nel documento di informativa al trattamento dei dati e includono l'indirizzo e-mail del DPO.

2. Verifica dell'Identità:

- Come per il diritto di accesso, l'Istituto verificherà l'identità del richiedente per garantire che i dati personali siano rilasciati alla persona corretta.

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO	Versione 1.0 del 12.12.2025
	Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Pagina 20 di 34

3. Fornitura dei Dati:

- I dati personali saranno forniti in un formato strutturato, di uso comune e leggibile da dispositivo automatico (ad esempio, formato CSV o XML).
- Se richiesto, i dati possono essere trasmessi direttamente a un altro titolare del trattamento indicato dal paziente, a condizione che ciò sia tecnicamente fattibile.

Contatti per Esercitare i Diritti

- **DPO:** Ing. Alessandro Manzoni
 - **E-mail:** a.manzoni@istitutotumori.na.it
- **Principal Investigator:** Rizio Esposito Abate
 - **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)?

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

Al Titolare locale (Centro sperimentale – Istituto Pascale)

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

Limiti applicabili al diritto all'oblio

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

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

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

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO	Versione 1.0 del 12.12.2025
	Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Pagina 21 di 34

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

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

Contatto con il Centro sperimentale (Istituto Pascale)

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

Eccezioni e limiti

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

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

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

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

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

5. Motivi della valutazione d'impatto

La redazione della presente Valutazione d'Impatto sulla Protezione dei Dati (DPIA) è ritenuta necessaria ai sensi dell'art. 35 del Regolamento (UE) 2016/679, in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento dei dati personali previsti dallo studio.

In particolare, lo studio comporta il trattamento su di dati particolari relativi alla salute e di dati di natura somatica, ottenuti mediante analisi molecolari avanzate (Real Time PCR, Next

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Versione 1.0 del 12.12.2025
		Pagina 22 di 34

Generation Sequencing, Comprehensive Genomic Profiling), che rientrano tra le categorie di dati ad elevato rischio per i diritti e le libertà degli interessati.

Inoltre, lo studio ha carattere retrospettivo e osservazionale e include anche dati riferibili a pazienti deceduti o non più contattabili; in tali casi il trattamento avviene in assenza di consenso diretto, sulla base delle specifiche deroghe previste dalla normativa nazionale e nel rispetto dell'art. 110-bis del Codice Privacy. Tale circostanza rende necessario valutare preventivamente e documentare le misure adottate per ridurre il rischio di re-identificazione e garantire un adeguato livello di tutela dei diritti degli interessati.

Ulteriori elementi che giustificano la DPIA sono rappresentati dall'utilizzo di strumenti informatici e database elettronici, dalla complessità delle analisi effettuate su dati molecolari ad elevato contenuto informativo e dalla durata pluriennale del trattamento.

La DPIA consente pertanto di identificare, valutare e mitigare in modo sistematico i rischi potenziali per i diritti e le libertà fondamentali degli interessati, di dimostrare la conformità del trattamento ai principi del GDPR (liceità, correttezza, trasparenza, minimizzazione, limitazione della conservazione, integrità e riservatezza) e di garantire che il trattamento dei dati avvenga nel rispetto delle finalità di ricerca scientifica e delle norme etiche applicabili.

6. Valutazione dei Rischi

Per ogni trattamento vengono individuati gli asset direttamente o indirettamente ad esso collegati. Per ognuno di essi, il processo di analisi dei rischi esamina le vulnerabilità, le relative minacce, e le contromisure, dirette o indirette, attuate, fornendo il livello di rischio. Tale livello tiene anche conto della probabilità e dell'impatto che l'attuazione della minaccia avrebbe sui dati personali trattati, per mezzo degli specifici asset.

In tal senso si procede ad individuare una scala di indice dei rischi da un livello di rischio molto basso sino ad un livello molto alto.

6.1 Accesso illegittimo ai dati

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

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

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

Vulnerabilità informatiche, attacco basato su chiave compromessa, attacco denial of service di rete, spoofing d'identità, attacco man in the middle, attacco di riproduzione RTP, virus, worm, phishing, malware.

Locale lasciato aperto o non custodito.

Trasmissione informatica o comunicazione verbale di dati personali a soggetti non autorizzati.

Accesso e/o trattamento dei dati personali per finalità diverse da quelle autorizzate.

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO	Versione 1.0 del 12.12.2025
	Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Pagina 23 di 34

Allontanarsi dalla propria postazione lasciando il PC connesso.
 Copiare i dati su dispositivi removibili e trasportabili all'esterno senza autorizzazione.
 Modifica accidentale dei dati.
 Cancellazione accidentale dei dati.
 Inoltro di dati a soggetti non autorizzati a conoscerli.
 Emergenza non sanitaria con impatto sul sistema informatico (incendio, alluvione, terremoto).

6.1.3 Quali sono le fonti di rischio?

Umano, Strumenti vulnerabili.

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

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

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

Importante/Grave

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

Poco Probabile

6.2 Modifiche indesiderate dei dati

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

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

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

Vulnerabilità informatiche, attacco basato su chiave compromessa, attacco denial of service di rete, spoofing d'identità, attacco man in the middle, attacco di riproduzione RTP, virus, worm, phishing, malware.

Locale lasciato aperto o non custodito.

Trasmissione informatica o comunicazione verbale di dati personali a soggetti non autorizzati.

Accesso e/o trattamento dei dati personali per finalità diverse da quelle autorizzate.

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO	Versione 1.0 del 12.12.2025
	Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Pagina 24 di 34

Allontanarsi dalla propria postazione lasciando il PC connesso.

Copiare i dati su dispositivi removibili e trasportabili all'esterno senza autorizzazione.

Modifica accidentale dei dati.

Cancellazione accidentale dei dati.

Inoltro di dati a soggetti non autorizzati a conoscerli.

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

6.2.3 Quali sono le fonti di rischio?

Strumenti vulnerabili, Umano

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

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

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

Importante/Grave

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

Poco probabile

6.3 Perdita di dati

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

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

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

Cancellazione accidentale dei dati.

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

Modifica accidentale dei dati, vulnerabilità informatiche, attacco basato su chiave compromessa, attacco denial of service di rete, spoofing d'identità, attacco man in the middle, attacco di riproduzione RTP, virus, worm, phishing, malware.

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO	Versione 1.0 del 12.12.2025
	Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Pagina 25 di 34

Locale lasciato aperto o non custodito.
Allontanarsi dalla propria postazione lasciando il PC connesso.

6.3.3 Quali sono le fonti di rischio?

Strumenti vulnerabili, Umano.

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

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

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

Grave/Importante

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

Poco Probabile

7. Piano d'azione

7.1 Mitigazione dei rischi con Misure esistenti o pianificate

7.1.1 Pseudonimizzazione

A ciascun soggetto incluso nello studio viene assegnato un codice identificativo univoco, utilizzato per la registrazione e l'analisi dei dati clinici, clinico-patologici e molecolari all'interno del database di ricerca. Il nominativo e gli altri dati identificativi diretti non sono inseriti nel database di studio.

La chiave di re-identificazione, che consente di associare il codice all'identità del paziente, è conservata separatamente dal database di ricerca, presso il centro promotore, con accesso limitato esclusivamente al personale autorizzato e designato dal Titolare del trattamento. Sono adottate misure tecniche e organizzative idonee a prevenire accessi non autorizzati, usi impropri o divulgazioni indebite.

La pseudonimizzazione è mantenuta per tutta la durata delle attività di raccolta e analisi dei dati; al termine delle operazioni di accoppiamento tra dati clinici e molecolari, i dati sono sottoposti a anonimizzazione definitiva mediante eliminazione della chiave di re-identificazione. Tale misura garantisce che i dati utilizzati per finalità scientifiche e di pubblicazione non siano più riconducibili agli interessati, in conformità ai principi di minimizzazione, integrità e riservatezza previsti dal GDPR.

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO	Versione 1.0 del 12.12.2025
	Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Pagina 26 di 34

7.1.2 Formazione e Sensibilizzazione

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

7.1.3 Tracciabilità

La tracciabilità del trattamento dei dati è garantita attraverso l'assegnazione a ciascun paziente di un codice numerico identificativo univoco, che viene utilizzato per tutte le attività di registrazione, analisi e gestione dei dati clinici e molecolari. Tale codice è riportato nelle schede di raccolta dati e nel database elettronico utilizzato per lo studio. L'elenco che consente l'associazione tra il codice identificativo e l'identità del paziente è conservato separatamente ed è disponibile esclusivamente presso il centro promotore dello studio. I dati sono raccolti e registrati in un database elettronico accessibile presso la Struttura Complessa di Biologia Cellulare e Bioterapie dell'Istituto Nazionale Tumori "Fondazione G. Pascale", e l'accesso è riservato al personale coinvolto nello studio.

La gestione centralizzata della registrazione, raccolta e conservazione dei dati consente di ricostruire le fasi del trattamento e di garantire la corretta attribuzione dei dati ai soggetti inclusi nello studio, nel rispetto delle procedure approvate dal Comitato Etico e delle norme di buona pratica clinica.

7.1.4 Politica di tutela della privacy

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

7.1.5 Gestione delle politiche di tutela della privacy

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

Il titolare garantisce Trasparenza e Comunicazione:

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

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

Tutti i Centri coinvolti nel trattamento si avvalgono di un DPO che vigila sulla compliance data protection. Il Centro Promotore è dotato di un Modello Organizzativo Data Protection che prevede la *review* periodica delle policy data protection e del registro dei trattamenti.

7.1.6 Minimizzazione dei dati

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

7.1.7 Controllo degli accessi logici

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO	Versione 1.0 del 12.12.2025
	Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Pagina 27 di 34

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

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

7.1.8 Limitazione dell'Accesso ai Dati

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

7.1.9 Audit e monitoraggi periodici

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

7.1.10 Sicurezza dei canali informatici

La rete ospedaliera prevede l'implementazione di sistemi di protezione adeguati: firewall, antivirus volti a garantire la sicurezza della rete.

Per maggiori dettagli vedi sezione 3.4.3

7.1.11 Procedure di sicurezza dei sistemi elettronici

I server (centrali o in cloud) sono collocati in ambienti protetti, con controlli ambientali (clima, accessi fisici) e ridondanza hardware.

Policy di physical access control impediscono l'accesso non autorizzato ai locali dove risiedono i sistemi.

I sistemi elettronici includono soluzioni di ridondanza per prevenire la perdita dei dati in caso di guasti.

I server sono protetti da firewall configurati per bloccare accessi non autorizzati.

Sistemi di rilevamento delle intrusioni (IDS) monitorano continuamente il traffico per individuare comportamenti anomali o potenziali attacchi.

I sistemi sono dotati di software antivirus aggiornati regolarmente per prevenire malware e attacchi informatici.

Tutti i software utilizzati (sistemi operativi, applicazioni) vengono aggiornati periodicamente per risolvere vulnerabilità note.

7.1.12 Accesso controllato ai locali

Accesso al reparto con badge.

7.1.13 Conservazione e archiviazione dei dati

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 i centri partecipanti e/o presso il promotore 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 DEL PROTOCOLLO Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Versione 1.0 del 12.12.2025
		Pagina 28 di 34

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.

7.2 Panoramica dei rischi

7.2.1 Analisi complessiva del dell'entità del rischio

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

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

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

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

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

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Versione 1.0 del 12.12.2025
		Pagina 29 di 34

1	Trascurabile	Possibilità di lesione grave (ad esempio, lesione permanente o lesione che richiede ospedalizzazione o trattamento riabilitativo specifico per un periodo di tempo significativo).
---	--------------	--

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

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

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Versione 1.0 del 12.12.2025
		Pagina 30 di 34

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. Modifica accidentale dei dati.	Pseudonimizzazione, Sicurezza dei canali informatici, Procedure di sicurezza dei sistemi elettronici, Controllo degli accessi logici, Formazione e Sensibilizzazione, Tracciabilità, Politica di tutela della privacy, Minimizzazione dei dati, Limitazione dell'Accesso ai Dati, Accesso controllato ai locali, Audit e monitoraggi periodici	Grave	Poco probabile	Medio	Limitata/Improbabile	Basso

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO	Versione 1.0 del 12.12.2025
	Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Pagina 31 di 34

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
		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. Allontanarsi dalla propria postazione	Pseudonimizzazione, Formazione e Sensibilizzazione, Minimizzazione dei dati, Limitazione dell'Accesso ai Dati, Sicurezza dei canali informatici, Procedure di sicurezza dei sistemi elettronici, Controllo degli accessi logici, Tracciabilità, Politica di tutela della privacy, Accesso controllato ai locali, Audit e monitoraggi periodici, Conservazione e archiviazione dei dati.	Grave	Poco probabile	Medio	Limitata/Improbabile	Basso

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO	Versione 1.0 del 12.12.2025
	Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Pagina 32 di 34

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
		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, attacco man in the middle, attacco di riproduzione RTP, virus, worm,	Formazione e Sensibilizzazione, Sicurezza dei canali informatici, Limitazione dell'Accesso ai Dati, Controllo degli accessi logici, Accesso controllato ai locali, Procedure di sicurezza dei sistemi elettronici, Conservazione e archiviazione dei dati.	Grave	Poco probabile	Medio	Limitata/Improbabile	Basso

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Le mutazioni di BRAF nel carcinoma del colon retto metastatico: metodiche di indagine e correlazioni con parametri clinico-patologici	Versione 1.0 del 12.12.2025
		Pagina 33 di 34

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
		phishing, malware. Locale lasciato aperto o non custodito. Allontanarsi dalla propria postazione lasciando il PC connesso.						

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

8. Risultato della DPIA

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

Tutto ciò valutato e considerato che:

Risultati della valutazione d'impatto	
☐ Rischio residuo elevato	☒ Rischio residuo non elevato
Le misure tecniche e organizzative individuate per mitigare l'impatto del trattamento non sono ritenute sufficienti. Il rischio residuale per i diritti e le libertà degli 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 nello studio in oggetto, il titolare del trattamento ha identificato i seguenti risultati chiave:

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