

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Versione 1.0 del 16.01.2026
		Pagina 1 di 34

Titolo dello studio	Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata
Promotore	Fondazione Policlinico Universitario Campus Bio-Medico
Centro di Sperimentazione	Istituto Nazionale Tumori di Napoli, IRCCS G. Pascale
Principal Investigator	Dr. Roberta Caputo
Tipo di studio e fase	Studio Osservazionale Retrospektivo Multicentrico
Parere del Comitato Etico	Parere Unico CET Lazio del 07.11.2024
Durata dello studio	2 anni
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 Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Versione 1.0 del 16.01.2026
		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		
	Roberta Caputo	Principal Investigator		
	Gianfranco De Feo	Quality Assurance		

Tracking delle modifiche

N° Rev.	Data	Motivo della modifica	Paragrafi
1.0	16.01.2026	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 16.01.2026
		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	13
3.4.1 Quali sono i dati trattati?	13
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	15
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

	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 16.01.2026
		Pagina 4 di 34

4.2.6 Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?	21
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?	23
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?	24
6.2.2 Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?	24
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	25
6.3.1 Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?	25
6.3.2 Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?	25
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

	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 16.01.2026
	Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Pagina 5 di 34

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	26
7.1.1 Pseudonimizzazione	26
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.....	27
7.1.7 Controllo degli accessi logici.....	27
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	28
7.2 Panoramica dei rischi	28
8. Risultato della DPIA	34

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Versione 1.0 del 16.01.2026
		Pagina 6 di 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

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Versione 1.0 del 16.01.2026
		Pagina 7 di 34

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.	NO

1.1 Stima del rischio

Criteri utilizzati per la stima del rischio	Risposta
---	----------

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Versione 1.0 del 16.01.2026
		Pagina 8 di 34

Il trattamento comporta la valutazione o assegnazione di un punteggio inclusiva di profilazione e previsione	NO
Il trattamento prevede un processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente	NO
Il trattamento consiste in un'attività di monitoraggio sistematico	NO
Il trattamento coinvolge dati sensibili o dati aventi carattere altamente personale	SI
Il trattamento di dati avviene su larga scala	NO
Il trattamento comporta la creazione di corrispondenze o combinazione di insiemi di dati	NO
Il trattamento coinvolge categorie di interessati vulnerabili	SI
Il trattamento coinvolge l'uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative	NO
Il trattamento impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto	NO
Medio/Elevato	

2. Quadro normativo

Regolamento (UE) 679/2016 (GDPR);

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

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

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

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

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Versione 1.0 del 16.01.2026
		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 la dr. Rossella Di Franco 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.

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecán con o senza tossicità polmonare farmaco-relata	Versione 1.0 del 16.01.2026
		Pagina 10 di 34

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

3.3 Descrizione del trattamento

3.3.1 Quale è il trattamento in considerazione?

Il trattamento oggetto dello studio OMERO – “Uno studio italiano di pazienti con diagnosi di carcinoma uroteliale trattati con radioterapia stereotassica sulle sedi metastatiche” consiste nella radioterapia stereotassica (SBRT – Stereotactic Body Radiation Therapy) somministrata sulle sedi oligometastatiche in pazienti affetti da carcinoma uroteliale.

Lo studio è osservazionale multicentrico e retrospettivo: non prevede alcuna somministrazione di trattamenti sperimentali o interventi aggiuntivi rispetto alla normale pratica clinica.

L'attività di ricerca è limitata alla raccolta e analisi dei dati clinici relativi a pazienti che sono già stati trattati con SBRT nel periodo 2010–2024 presso i centri partecipanti.

L'obiettivo è documentare, a livello nazionale, la pratica clinica corrente nell'utilizzo della radioterapia stereotassica nel carcinoma uroteliale oligometastatico e valutarne gli esiti in termini di sopravvivenza, controllo locale della malattia, tossicità e sicurezza del trattamento.

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 Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Versione 1.0 del 16.01.2026
		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 alla dott. Rossella Di Franco.

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.

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Versione 1.0 del 16.01.2026
		Pagina 12 di 34

Responsabilità:

Riservatezza: Mantenere la riservatezza delle informazioni personali trattate.

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

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

5. Partecipanti allo Studio

I partecipanti allo studio devono essere adeguatamente informati.

Responsabilità:

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

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

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

3.3.3 Ci sono standard applicabili al trattamento?

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

1. Regolamento Generale sulla Protezione dei Dati (GDPR)

Il GDPR è il principale standard legale per la protezione dei dati personali nell'Unione Europea. Ecco alcuni dei requisiti chiave:

Principi del Trattamento dei Dati: I dati personali devono essere trattati in modo lecito, corretto e trasparente; raccolti per finalità determinate, esplicite e legittime; adeguati, pertinenti e limitati a quanto necessario; esatti e, se necessario, aggiornati; conservati in una forma che consenta l'identificazione degli interessati per un periodo non superiore al necessario; trattati in modo da garantire la sicurezza adeguata dei dati.

Diritti degli Interessati: Gli interessati hanno il diritto di accesso, rettifica, cancellazione, limitazione del trattamento, portabilità dei dati e opposizione al trattamento.

Valutazione d'Impatto sulla Protezione dei Dati (DPIA): Necessaria quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

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

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

2. Norme di sicurezza della infrastruttura e dei sistemi elettronici

Presso l'IRCCS INT Napoli sono previste delle specifiche procedura di sicurezza per i sistemi elettronici (penetration test; firewall; back-up; disaster recovery; antivirus; verifica

	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 16.01.2026
	Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Pagina 13 di 34

integrità dati back-up) nonché procedure di archiviazione dati storici (abilitazione accesso, consultazione, decommissioning, migrazione del dato, ecc...).

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

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

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

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

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

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

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

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

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

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

5. Linee Guida etiche

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

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

6. Standard di sicurezza e qualità applicati

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

3.4 Dati, processi e risorse di supporto

3.4.1 Quali sono i dati trattati?

	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 16.01.2026
	Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Pagina 14 di 34

Nell'ambito dello studio osservazionale multicentrico retrospettivo "OMERO – Uno studio italiano di pazienti con diagnosi di carcinoma uroteliale trattati con radioterapia stereotassica sulle sedi metastatiche", vengono trattati dati personali appartenenti a categorie particolari, in quanto relativi alla salute dei pazienti oncologici.

I dati sono raccolti unicamente da documentazione clinica esistente (cartelle cliniche, referti radioterapici e oncologici, registri di trattamento) presso i centri partecipanti, senza che siano previste nuove procedure diagnostiche o terapeutiche per i soggetti coinvolti.

In particolare, i dati trattati includono:

- Dati demografici essenziali, necessari per la caratterizzazione clinica dei pazienti (età, sesso, stato di performance secondo ECOG, anno del trattamento);
- Dati clinici e patologici: diagnosi istologica di carcinoma uroteliale, sede e numero delle metastasi (massimo 5 lesioni), data della diagnosi metastatica, caratteristiche del trattamento ricevuto;
- Dati terapeutici: parametri della radioterapia stereotassica (dose totale, frazionamento, sede trattata, periodo di esecuzione);
- Dati di outcome: sopravvivenza globale, sopravvivenza libera da malattia, controllo locale delle lesioni trattate, tempo alla successiva linea terapeutica, eventuale tossicità acuta e tardiva associata al trattamento;
- Dati relativi alla pratica clinica dei diversi centri (criteri di selezione dei pazienti, impostazione del trattamento e follow-up clinico).

I dati non contengono elementi identificativi diretti dei pazienti: ciascun centro assegna un codice numerico univoco al momento della raccolta, mantenendo separatamente la chiave di collegamento tra il codice e l'identità del soggetto. Il promotore e i centri partecipanti trattano esclusivamente i dati pseudonimizzati, in conformità al principio di minimizzazione e al Regolamento (UE) 2016/679.

Non sono previsti trattamenti automatizzati, profilazione o trasferimenti dei dati verso Paesi terzi.

Le informazioni sono utilizzate esclusivamente per le finalità scientifiche previste dal protocollo e saranno successivamente conservate per il periodo indicato nella sezione dedicata alla conservazione e archiviazione dei dati.

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

- **Raccolta**

I dati clinici e patologici dei pazienti affetti da carcinoma uroteliale oligometastatico già trattati con radioterapia stereotassica (SBRT) vengono estratti dalle cartelle cliniche, dai referti radioterapici/oncologici e da registri di trattamento presenti presso i centri partecipanti. Lo studio è di natura osservazionale retrospettiva e multicentrica.

- **Pseudonimizzazione e codifica**

Al momento della raccolta, ciascun centro assegna un codice identificativo univoco al paziente. I dati personali identificativi diretti sono separati dal file dei dati clinici e conservarsi localmente presso il centro stesso. I dati trasmessi al promotore o condivisi tra centri sono esclusivamente pseudonimizzati.

- **Trasmissione e archiviazione**

	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 16.01.2026
	Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Pagina 15 di 34

I dati pseudonimizzati vengono trasmessi dai singoli centri partecipanti al promotore e archiviati in modo sicuro per consentire le analisi statistiche previste dallo studio. I documenti originali e le fonti dati restano conservati presso i centri di origine, ai fini di tracciabilità e verifica.

- **Elaborazione e analisi**

I dati raccolti sono trattati ai fini delle finalità dello studio: descrizione della pratica clinica italiana, valutazione degli outcome in pazienti trattati con SBRT, confronto tra centri partecipanti. Le analisi statistiche e i report sono eseguiti utilizzando i dati pseudonimizzati.

- **Conservazione**

I dati pseudonimizzati e la documentazione associata sono conservati per un periodo conforme alla normativa applicabile e alle indicazioni del protocollo. Le fonti originali restano disponibili per l'accesso in caso di verifica o audit.

- **Cancellazione o anonimizzazione**

Alla scadenza del periodo di conservazione previsto, o al termine della ragione per la quale sono trattati, i dati identificativi o le chiavi di collegamento vengono cancellati o i dati vengono resi anonimi in modo irreversibile, in conformità al principio di limitazione della conservazione.

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)

4. Valutazione di necessità e proporzionalità del trattamento

	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 16.01.2026
	Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Pagina 16 di 34

4.1 Proporzionalità e necessità

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

Gli scopi del trattamento dei dati personali nello studio osservazionale multicentrico retrospettivo "OMERO – Uno studio italiano di pazienti con diagnosi di carcinoma uroteliale trattati con radioterapia stereotassica sulle sedi metastatiche" sono specifici, espliciti e legittimi, come chiaramente descritti nella Sinossi e nel Protocollo di studio.

L'obiettivo dello studio è quello di raccogliere e analizzare i dati clinici di pazienti affetti da carcinoma uroteliale oligometastatico che hanno ricevuto radioterapia stereotassica (SBRT) sulle sedi metastatiche, al fine di descrivere la pratica clinica adottata nei diversi centri italiani e di valutare gli esiti in termini di controllo locale della malattia, sopravvivenza e sicurezza del trattamento.

Le finalità sono dunque scientifiche, in quanto orientate alla conoscenza e al miglioramento della pratica clinica oncologica; esplicite, poiché chiaramente definite nel protocollo approvato dal Comitato Etico competente; e legittime, in quanto conformi all'art. 9, par. 2, lett. j) del Regolamento (UE) 2016/679 e all'art. 110-bis del D.Lgs. 196/2003, che consentono il trattamento di dati relativi alla salute per fini di ricerca scientifica nel rispetto delle misure di garanzia e delle disposizioni etiche e regolatorie applicabili.

I dati raccolti saranno utilizzati esclusivamente per le finalità scientifiche previste dallo studio e non saranno oggetto di ulteriori trattamenti incompatibili con tali scopi.

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	Versione 1.0 del 16.01.2026
	Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	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 in questione sono estrapolati dalle cartelle cliniche. Detta circostanza determina una garanzia di controllo ed esattezza degli stessi derivante dall'applicazione dei rigorosi standard tradotti nelle procedure di gestione dei singoli Centri coinvolti. Il Promotore e gli altri soggetti coinvolti nello Studio provvedono inoltre a formare il proprio personale al fine di presidiare adeguatamente in rischio di errore umano.

Tutti i Centri provvedono a registrare lo storico delle modifiche apportate alle cartelle e l'identificativo degli utenti che le apportano.

Con riferimento specifico al *data entry* dello studio in oggetto, i PI dei singoli Centri di arruolamento si occupano, personalmente o attraverso il proprio staff (debitamente formato e istruito), dell'estrazione dei dati dalle cartelle e operano una verifica di coerenza dei dati al fine di circoscrivere possibili errori umani. In nessun caso sarà ammessa la raccolta di dati incompleti o imprecisi.

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?

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

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Versione 1.0 del 16.01.2026
		Pagina 18 di 34

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 Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Versione 1.0 del 16.01.2026
		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:

	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 16.01.2026
	Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Pagina 20 di 34

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

3. Fornitura dei Dati:

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

Contatti per Esercitare i Diritti

- **DPO:** Ing. Alessandro Manzoni
 - **E-mail:** a.manzoni@istitutotumori.na.it
- **Principal Investigator:** Dott. Roberta Caputo
 - **E-mail:** r.caputo@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.

	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 16.01.2026
	Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Pagina 21 di 34

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

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

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

Contatto con il Centro sperimentale (Istituto Pascale)

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

Eccezioni e limiti

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

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

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

	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 16.01.2026
	Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Pagina 22 di 34

La valutazione d'impatto sulla protezione dei dati (DPIA) è stata condotta in quanto il trattamento dei dati personali previsto dallo studio presenta caratteristiche che, in base al Regolamento (UE) 2016/679 e alle Linee guida del Gruppo di lavoro Articolo 29 (WP 248 rev.01), possono comportare un rischio elevato per i diritti e le libertà degli interessati.

In particolare, il trattamento soddisfa più di due dei criteri individuati dall'European Data Protection Board per cui la DPIA risulta necessaria, e precisamente:

- trattamento di categorie particolari di dati, in quanto vengono utilizzati dati relativi alla salute dei pazienti oncologici, talvolta associati a informazioni genetiche o cliniche sensibili;
- presenza di soggetti vulnerabili, trattandosi di pazienti oncologici in condizioni cliniche delicate;
- uso di sistemi informatici dedicati per la raccolta, pseudonimizzazione e gestione dei dati di ricerca.

Inoltre, la DPIA si rende opportuna in ragione della natura retrospettiva dello studio, che comporta il riutilizzo di dati clinici originariamente raccolti per finalità di cura e successivamente trattati per scopi di ricerca scientifica. Tale modalità richiede una valutazione puntuale delle misure tecniche e organizzative adottate per garantire la riservatezza, la sicurezza e la minimizzazione del rischio di reidentificazione.

La DPIA è pertanto finalizzata a:

- analizzare i rischi connessi al trattamento di dati sanitari e genetici su larga scala;
- valutare la correttezza e adeguatezza delle misure tecniche e organizzative adottate dai centri partecipanti e dal promotore;
- garantire la piena conformità dello studio al Regolamento (UE) 2016/679, al D.lgs. 196/2003 s.m.i. e alle Linee guida del Garante per la protezione dei dati personali in materia di ricerca scientifica.

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?

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Versione 1.0 del 16.01.2026
		Pagina 23 di 34

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

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

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

Locale lasciato aperto o non custodito.

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

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

Allontanarsi dalla propria postazione lasciando il PC connesso.

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

Modifica accidentale dei dati.

Cancellazione accidentale dei dati.

Inoltro di dati a soggetti non autorizzati a conoscerli.

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

6.1.3 Quali sono le fonti di rischio?

Umano, Strumenti vulnerabili.

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

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

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

Importante/Grave

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

Poco Probabile

6.2 Modifiche indesiderate dei dati

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Versione 1.0 del 16.01.2026
		Pagina 24 di 34

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

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

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

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

Locale lasciato aperto o non custodito.

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

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

Allontanarsi dalla propria postazione lasciando il PC connesso.

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

Modifica accidentale dei dati.

Cancellazione accidentale dei dati.

Inoltro di dati a soggetti non autorizzati a conoscerli.

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

6.2.3 Quali sono le fonti di rischio?

Strumenti vulnerabili, Umano

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

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

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Versione 1.0 del 16.01.2026
		Pagina 25 di 34

6.3 Perdita di dati

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

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

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

Cancellazione accidentale dei dati.

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

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

Locale lasciato aperto o non custodito.

Allontanarsi dalla propria postazione lasciando il PC connesso.

6.3.3 Quali sono le fonti di rischio?

Strumenti vulnerabili, Umano.

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

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

	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 16.01.2026
	Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Pagina 26 di 34

7.1 Mitigazione dei rischi con Misure esistenti o pianificate

7.1.1 Pseudonimizzazione

In ogni centro aderente verrà assegnato a d ogni paziente un codice alfanumerico specifico ideato dal centro aderente stesso, diverso da quello della cartella clinica, la cui chiave di decifrazione rimarrà nelle mani del centro aderente. Al centro coordinatore verranno inviati i dati solo con il codice alfanumerico.

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

Nel corso dello studio osservazionale retrospettivo, la tracciabilità dei dati è garantita mediante procedure standardizzate che assicurano la corretta gestione, verifica e rintracciabilità di tutte le operazioni effettuate sui dati personali trattati.

Ogni soggetto incluso nello studio è identificato attraverso un codice numerico o alfanumerico univoco, attribuito al momento della pseudonimizzazione. Tale codice consente di collegare in modo controllato i dati pseudonimizzati alla documentazione clinica originale, garantendo la possibilità di verifica e validazione delle informazioni, ma senza compromettere l'anonimato del paziente.

La chiave di collegamento tra il codice e l'identità del soggetto è conservata in un archivio elettronico sicuro, protetto da credenziali e accessibile esclusivamente al personale clinico e di ricerca autorizzato del centro partecipante.

I flussi informativi tra i centri partecipanti e il promotore avvengono in modo controllato e documentato.

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.

	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 16.01.2026
	Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Pagina 27 di 34

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

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

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecán con o senza tossicità polmonare farmaco-relata	Versione 1.0 del 16.01.2026
		Pagina 28 di 34

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.

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.

7.2 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 $>10^{-5}$)

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Versione 1.0 del 16.01.2026
		Pagina 29 di 34

2	Poco probabile	Improbabile che si verifichi, si prevede che si verifichi raramente ($<10^{-5}$ e $>10^{-6}$)
1	Improbabile/Trascurabile	Il verificarsi sarebbe veramente inaspettato ($<10^{-6}$)

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

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

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

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

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Versione 1.0 del 16.01.2026
		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	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 Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Versione 1.0 del 16.01.2026
		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
		senza autorizzazione. 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	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 Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Versione 1.0 del 16.01.2026
		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
		diverse da quelle autorizzate. Allontanarsi dalla propria postazione lasciando il PC connesso. Copiare i dati su dispositivi removibili e trasportabili all'esterno senza autorizzazione. Modifica accidentale dei dati. Cancellazione accidentale dei dati. Inoltro di dati a soggetti non autorizzati a conoscerli.						
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,	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 Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecán con o senza tossicità polmonare farmaco-relata	Versione 1.0 del 16.01.2026
		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
		attacco denial of service di rete, spoofing d'identità, attacco man in the middle, attacco di riproduzione RTP, virus, worm, phishing, malware. Locale lasciato aperto o non custodito. Allontanarsi dalla propria postazione lasciando il PC connesso.						

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.

	ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI	
	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEL PROTOCOLLO Raccolta di informazioni clinico-radiologiche in pazienti in trattamento con Trastuzumab-Deruxtecan con o senza tossicità polmonare farmaco-relata	Versione 1.0 del 16.01.2026
		Pagina 34 di 34

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'adequatezza delle misure tecniche e organizzative adottate per la mitigazione del rischio e del danno.